KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed University Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2017 onwards)
DEPARTMENT OF COMMERCE (CA)

SYLLABUS

Semester VI

		L	T	P	C
17CCU604 B	**CYBER CRIMES AND LAWS**	**6**	**2**	**-**	**6**

SCOPE :
Cyber Crimes and Laws represents the basic principles and concepts of cyber crimes and laws. It gives the in-depth knowledge to the regarding the computer networks.

OBJECTIVE
- This paper intends to create an understanding towards the cyber crimes and to familiarize the students with the application of cyber laws in general.

UNIT- I

Cyber Crimes: Introduction- Computer crime and cyber crimes; Distinction between cyber crime and conventional crimes; cyber forensic; Kinds of cyber crimes- cyber stalking, cyber terrorism, forgery and fraud, crimes related to IPRs, computer vandalism; Privacy of online data; Cyber Jurisdiction; Copyright issues; and Domain name dispute etc.

UNIT-II

Definition and Terminology (Information Technology Act, 2000): Concept of Internet, Internet Governance, E-Contract, E-Forms, Encryption, Data Security. Access, Addressee, Adjudicating Officer, Affixing Digital Signatures, Appropriate Government, Certifying Authority, Certification Practice Statement,

UNIT-III

Computer: Computer Network, Computer Resource, Computer System, Cyber Appellate Tribunal, Data, Digital Signature, Electronic Form, Electronic Record, Information, Intermediary, Key Pair,

Originator, Public Key, Secure System, Verify, and Subscriber as defined in the Information Technology Act, 2000.

UNIT-IV

Electronic Records : Authentication of Electronic Records; Legal Recognition of Electronic Records; Legal Recognition of Digital Signatures; Use of Electronic Records and Digital Signatures in Government and its Agencies; Retention of Electronic Records; Attribution, Acknowledgement and Dispatch of Electronic Records; Secure Electronic Records and Digital Signatures.

UNIT-V

Regulatory Framework: Regulation of Certifying Authorities; Appointment and Functions of Controller; License to issue Digital Signatures Certificate; Renewal of License; Controller's Powers; Procedure to be Followed by Certifying Authority; Issue, Suspension and Revocation of Digital Signatures Certificate, Duties of Subscribers; Penalties and Adjudication; Appellate Tribunal; Offences

Suggested Readings:

Text Book :

1. Chaffey, Dave (2009). *E-business and E-commerce Management* [4th Edition]. New Delhi, Pearson Education.

Reference Books:

1. Efraim Turban, Jae Lee, King, David, and HM Chung. (2001). *Electronic Commerce-A managerial Perspective*. New Delhi, Pearson Education.
2. Joseph, P.T *E-Commerce-An Indian Perspective* [5th Edition]. New Delhi, Prentice Hall of India.
3. Painttal. D (2002). *Law of Information Technology*. New Delhi, Taxmann Publications Pvt. Ltd.
4. Dietel, Harvey M., Dietel, Paul J., and Kate Steinbuhler (2009). *E-business and E-commerce for managers*. New Delhi, Pearson Education.

5. Brian, Craig *Cyber Law: The Law of the Internet and Information Technology*. New Delhi, Pearson Education.
6. Sharma J. P, Sunaina Kanojia. (2012). *Cyber Laws* [1st Edition] New Delhi, Ane Books Pvt Ltd.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University)
(Established under section 3 of UGC Act 1956)
Coimbatore-641021
DEPARTMENT OF COMMERCE (UG)

Name: **S.Boopathi Raja & R.Lydia Priyadharsini**
Department: **Commerce(CA)**
Subject Code: **17CCU604 B** Semester: **VI**
Subject: **CYBER CRIMES AND LAWS- Lesson Plan** Year: **2017-20 Batch**

UNIT – 1			
S. No	**Lecture Hours**	**Contents**	**References**
1.	1	Introduction	W2
2.	1	Computer crime and cyber crimes	W2
3.	1	Distinction between cyber crime and conventional crimes	W1
4.	1	Tutorial I	-
5.	1	cyber forensic	W1
6.	1	Kinds of cyber crimes	W3
7.	1	cyber stalking, cyber terrorism	W4
8.	1	Tutorial II	-
9.	1	forgery and fraud, crimes related to IPRs	W6
10.	1	computer vandalism	W5
11.	1	Privacy of online data	W5
12.	1	Tutorial III	-
13.	1	Cyber Jurisdiction, Copyright issues	W6
14.	1	Domain name dispute	T1: Pg.No.: 38-141
15.	1	Tutorial IV	-
16.	1	Recapitulation and Discussion of Important Questions	-
Total no. of Hours planned for Unit 1			**16**
UNIT – 2			
1.	1	Concept of Internet	T1: Pg.No.: 136-138
2.	1	E-Contract, E-Forms	T1: Pg.No.: 238-241
3.	1	Tutorial V	-
4.	1	Encryption	R2: Pg.No.: 263-269
5.	1	Affixing Digital Signatures	R3: Pg. No: 67-69
6.	1	Data Security	R3: Pg. No: 139-140
7.	1	Tutorial VI	-
8.	1	Access	R3: Pg. No: 141-142
9.	1	Addressee	R3: Pg. No: 133-135
10.	1	Adjudicating Officer	R2: Pg.No.: 10-15
11.	1	Tutorial VII	-
12	1	Appropriate Government	R3: Pg. No: 150-152

13.	1	Certifying Authority	R3: Pg. No: 53-55
14.	1	Certification Practice Statement	R3: Pg. No: 61-64
15.	1	Tutorial VIII	-
16.	1	Recapitulation and Discussion of Important Questions	-
Total no. of Hours planned for Unit 2			**16**
UNIT – 3			
1.	1	Computer Network	W8
2.	1	Computer Resource	W8
3.	1	Computer System	W8
4.	1	Tutorial IX	-
5.	1	Cyber Appellate Tribunal	W7
6.	1	Data, Digital Signature	R2: Pg. No.: 273-278
7.	1	Electronic Form	R3: Pg. No: 88-90
8.	1	Tutorial X	-
9.	1	Electronic Record	R3: Pg. No: 55, 149
10.	1	Information, Intermediary	R3: Pg. No: 145,144
11.	1	Key Pair, Originator	R3: Pg. No: 68-70,134
12.	1	Tutorial XI	-
13.	1	Public Key, Secure System	R3: Pg. No: 65-67
14.	1	Verify, and Subscriber as defined in the Information Technology Act, 2000.	W7
15.	1	Verify, and Subscriber as defined in the Information Technology Act, 2000.	W7
16.	1	Tutorial XII	-
17.	1	Recapitulation and Discussion of Important Questions	-
Total number of hours planned for Unit 3			**17**
UNIT – 4			
1.	1	Authentication of Electronic Records	R3: Pg. No: 138-139
2.	1	Legal Recognition of Electronic Records	W9
3.	1	Tutorial XIII	-
4.	1	Legal Recognition of Digital Signatures	R2: Pg. No.: 271
5.	1	Use of Electronic Records and Digital Signatures in Government and its Agencies	J1
6.	1	Tutorial XIV	-
7.	1	Retention of Electronic Records, Attribution	W10
8.	1	Acknowledgement and Dispatch of Electronic Records	R3: Pg. No: 63-64
9.	1	Tutorial XV	-
10.	1	Secure Electronic Records, Digital Signatures	W11
11.	1	Tutorial XVI	-
12	1	Recapitulation and Discussion of Important Questions	-
Total no. of Hours planned for Unit 4			**12**
UNIT – 5			
1.	1	Regulation of Certifying Authorities	R3: Pg. No: 52-53
2.	1	Appointment and Functions of Controller	R3: Pg. No: 59-60

3.	1	License to issue Digital Signatures Certificate	R3: Pg. No: 60-61
4.	1	Tutorial XVII	-
5.	1	Renewal of License	R3: Pg. No: 61-62
6.	1	Controller's Powers	R3: Pg. No: 158-159
7.	1	Procedure to be Followed by Certifying Authority	R3: Pg. No: 94-95
8.	1	Tutorial XVIII	-
9.	1	Issue, Suspension and Revocation of Digital Signatures Certificate	R3: Pg. No: 110-115
10	1	Issue, Suspension and Revocation of Digital Signatures Certificate	R3: Pg. No: 115-120
11.	1	Duties of Subscribers	R3: Pg. No: 125-127
12.	1	Tutorial XIX	-
13.	1	Penalties and Adjudication	W11
14.	1	Appellate Tribunal; Offences	W11
15.	1	Tutorial XX	-
16.	1	Recapitulation and Discussion of Important Questions	-
17.	1	Discussion of previous ESE question papers	-
18.	1	Discussion of previous ESE question papers	-
19.	1	Discussion of previous ESE question papers	-
Total no. of Hours planned for Unit 5			**19**

Suggested Readings:

Text Book:

1. Chaffey, Dave (2009). *E-business and E-commerce Management* [4th Edition]. New Delhi, Pearson Education.

Reference Books:

1. Efraim Turban, Jae Lee, King, David, and HM Chung. (2001). *Electronic Commerce-A managerial Perspective*. New Delhi, Pearson Education.
2. Joseph, P.T, *E-Commerce-An Indian Perspective* [5th Edition]. New Delhi, Prentice Hall of India.
3. Painttal. D (2002). *Law of Information Technology*. New Delhi, Taxmann Publications Pvt. Ltd.
4. Dietel, Harvey M., Dietel, Paul J., and Kate Steinbuhler (2009). *E-business and E-commerce for managers*. New Delhi, Pearson Education.
5. Brian, Craig *Cyber Law: The Law of the Internet and Information Technology*. New Delhi, Pearson Educatio.
6. Sharma J. P, Sunaina Kanojia. (2012). *Cyber Laws* [1st Edition] New Delhi, Ane Books Pvt Ltd.

Website:

W1: www.computerhope.com

W2: www.searchsecurity.techtarget.com

W3: www.digit.in/technology-guides/fasttrack-to-cyber-crime

W4: www.techopedia.com

W5: www.web24.com.au/tutorials

W6: www.legalserviceindia.com/articles

W7: www.vakilno1.com/legalviews

W8: www.tutorialspoint.com

W9: www. lawgic.info

W10: www.itlaw.in

W11: www.meity.gov.in

Journals:

J1. Journal of the International Academy for Case Studies

UNIT-I

SYLLABUS

Cyber Crimes: Introduction- Computer crime and cyber crimes; Distinction between cyber crime and conventional crimes; cyber forensic; Kinds of cyber crimes- cyber stalking, cyber terrorism, forgery and fraud, crimes related to IPRs, computer vandalism; Privacy of online data; Cyber Jurisdiction; Copyright issues; and Domain name dispute etc.

Introduction:

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.

Common types:

Cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. More serious crimes like cyber terrorism are also of significant concern. Cybercrime encompasses a wide range of activities, but these can generally be broken into two categories:

- Crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DoS) attacks.
- Crimes that use computer networks to advance other criminal activities. These types of crimes include cyber stalking, phishing and fraud or identity theft.

The FBI identifies cybercrime fugitives who have allegedly committed bank fraud and trafficked counterfeit devices that access personal electronic information. The FBI also provides information on how to report cybercrimes, as well as useful intelligence information about the latest cybercriminals.

Computer Crime and cyber crimes

Alternatively referred to as cyber crime, e-crime, electronic crime, or hi-tech crime. Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Examples of Computer Crimes

Computer crime laws in many states prohibit a person from performing certain acts without authorization, including:

- Improperly accessing a computer, system, or network;
- Modifying, damaging, using, disclosing, copying, or taking programs or data;
- Introducing a virus or other contaminant into a computer system;
- Using a computer in a scheme to defraud;
- Interfering with someone else's computer access or use;
- Using encryption in aid of a crime;
- Falsifying email source information; and
- Stealing an information service from a provider.

Examples of Cyber Crime

Copyright violation - Stealing or using another person's copyrighted material without permission.

Cracking - Breaking or deciphering codes that are being used to protect data.

Cyber terrorism - Hacking, threats, and blackmailing towards a business or person.

Cyberbully or Cyberstalking - Harassing or stalking others online.

Cybersquatting - Setting up a domain of another person or company with the sole intentions of selling it to them later at a premium price.

Creating Malware - Writing, creating, or distributing malware (e.g., viruses and spyware.)

Denial of Service attack - Overloading a system with so many requests it cannot serve normal requests.

Espionage - Spying on a person or business.

Fraud - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.

Harvesting - Collect account or other account related information on other people.

Human trafficking - Participating in the illegal act of buying or selling other humans.

Identity theft - Pretending to be someone you are not.

Illegal sales - Buying or selling illicit goods online including drugs, guns, and psychotropic substances.

Intellectual property theft - Stealing practical or conceptual information developed by another person or company.

IPR violation - An intellectual property rights violation is any infringement of another's copyright, patent, or trademark.

Phishing - Deceiving individuals to gain private or personal information about that person.

Salami slicing - Stealing tiny amounts of money from each transaction.

Scam - Tricking people into believing something that is not true.

Slander - Posting libel or slander against another person or company.

Software piracy - Copying, distributing, or using software that is copyrighted that you did not purchase.

Spamming - Distributed unsolicited e-mail to dozens or hundreds of different addresses.

Spoofing - Deceiving a system into thinking you are someone you really are not.

Typosquatting - Setting up a domain that is a misspelling of another domain.

Unauthorized access - Gaining access to systems you have no permission to access.

Wiretapping - Connecting a device to a phone line to listen to conversations.

Distinction between cyber crime and conventional crimes

The term ‘cyber crime’ is a misnomer. The concept of cyber-crime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state.

Before evaluating the concept of cyber-crime it is obvious that the concept of conventional crime be discussed and the points of similarity and deviance between both these forms may be discussed.

Conventional crime

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment."

(1). The hallmark of criminality is that, it is breach of the criminal law.

(2). A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

Cyber crime

Cyber-crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to be those crime, where either the computer is an object or subject of the conduct constituting crime. "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime."

A generalized definition of cyber crime may be " unlawful acts wherein the computer is either a tool or target or both. The computer may be used as a tool in the following kinds of activity-financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

Distinction between conventional and cyber crime

There is apparently no distinction between cyber and conventional crime. However on a deep introspection we may say that there exist a fine line of demarcation between the conventional and cyber crime. The demarcation lies in the involvement of the medium in cases of cyber crime. The prerequisite for cyber crime is that there should be an involvement of the virtual cyber medium at any stage.

Cyber forensic (computer forensics)

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Forensic investigators typically follow a standard set of procedures: After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation. Computer forensics has become its own area of scientific expertise, with accompanying coursework and certification.

Kinds of cyber crimes

The 12 types of Cyber CrimeIn order to protect yourself you need to know about the different ways in which your computer can be compromised and your privacy infringed. In this section, we discuss a few common tools and techniques employed by the cyber criminals. This isn't an exhaustive list by any means, but will give you a comprehensive idea of the loopholes in networks and security systems, which can be exploited by attackers, and also their possible motives for doing so.

The 12 types of cyber crime

There are literally a dozen ways in which a cybercrime can be perpetrated, and you need to know what they are In order to protect yourself you need to know about the different ways in which your computer can be compromised and your privacy infringed. In this section, we discuss a few common tools and techniques employed by the cyber criminals. This isn't an exhaustive list by any means, but will give you a comprehensive idea of the loopholes inner works and security systems, which can be exploited by attackers, and also their possible motives for doing so.

1. Hacking: In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the 'hacking') are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons.

They're usually technology buffs who have expert-level skills in one particular software program or language. As for motives, there could be several, but the most common are pretty simple and can be explained by a human tendency such as greed, fame, power, etc. Some people do it purely to show-off their expertise – ranging from relatively harmless activities such as modifying software (and even hardware) to carry out tasks that are outside the creator's intent, others just want to cause destruction. Greed and sometimes voyeuristic tendencies may cause a hacker to break into systems to steal personal banking information, a corporation's financial data, etc. They also try and modify systems so hat they can execute tasks at their whims. Hackers displaying such destructive conduct are also called "Crackers" at times.

They are also called "Black Hat" hackers On the other hand, there are those who develop an interest in computer hacking just out of intellectual curiosity. Some companies hire these computer enthusiasts to find flaws in their security systems and help fix them. Referred to as "White Hat" hackers, these guys are against the abuse of computer systems. They attempt to break into network systems purely to alert the owners of flaws. It's not always altruistic, though, because many do this for fame as well, in order to land jobs with top companies, or just to be termed as security experts. "Grey Hat" is another term used to refer to hacking activities that are a cross between black and white hacking. Some of the most famous computer geniuses were once hackers who went on to use their skills for constructive technological development. Dennis Ritchie and Ken Thompson, the creators of the UNIX operating system (Linux's predecessor), were two of them. Shawn Fanning, the developer of Napster, Mark Zuckerberg of Facebook fame, and many more are also examples. The first step towards preventing hackers from gaining access to your systems is to learn how hacking is done. Of course it is beyond the scope of this Fast Track to go into great details, but we will cover the various techniques used by hackers to get to you via the internet.

a. SQL Injections: An SQL injection is a technique that allows hackers to play upon the security vulnerabilities of the software that runs a web site. It can be used to attack any type of unprotected or improperly protected SQL database. This process involves entering portions of SQL code into a web form entry field – most commonly usernames and passwords – to give the hacker further access to the site backend, or to a particular user's account. When you enter logon information into sign-in fields, this information is typically converted to an SQL command. This command checks the data you've entered against the relevant table in the database. If your input data matches the data in the table, you're granted access, if not, you get the kind of error you would have seen when you put in a wrong password. An SQL injection is usually an additional command that when inserted into the web form, tries to change the content of the database to reflect a successful login. It can also be used to retrieve information such as credit card numbers or passwords from unprotected sites.

b. Theft of FTP Passwords: This is another very common way to tamper with web sites. FTP password hacking takes advantage of the fact that many webmasters store their website login information on their poorly protected PCs.

The thief searches the victim's system for FTP login details, and then relays them to his own remote computer. He then logs into the web site via the remote computer and modifies the web pages as he or she pleases.

c. Cross-site scripting: Also known as XSS (formerly CSS, but renamed due to confusion with cascading style sheets), is a very easy way of circumventing a security system. Cross-site scripting is a hard-to-find loophole in a web site, making it vulnerable to attack. In a typical XSS attack, the hacker infects a web page with a malicious client-side script or program. When you visit this web page, the script is automatically downloaded to your browser and executed.

Typically, attackers inject HTML, JavaScript, VBScript, ActiveX or Flash into a vulnerable application to deceive you and gather confidential information. If you want to protect your PC from malicious hackers, investing in a good firewall should be first and foremost. Hacking is done through a network, so it's very important to stay safe while using the internet. You'll read more about safety tips in the last chapter of this book.

2. Virus dissemination: Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. "Worms" unlike viruses don't need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term "worm" is sometimes used to mean selfreplicating "malware" (MALicious softWARE). These terms are often used interchangeably in the context of the hybrid viruses/worms that dominate although mankind's best invention, the net is still a minefield of threats the current virus scenario. "Trojan horses" are different from viruses in their manner of propagation. They masquerade as a legitimate file, such as an email attachment from a supposed friend with a very believable name, and don't disseminate themselves. The user can also unknowingly install a Trojan-infected program via drive-by downloads when visiting a website, playing online games or using internet-driven applications. A Trojan horse can cause damage similar to other viruses, such as steal information or hamper/disrupt the functioning of computer systems. A simple diagram to show how malware can propagate How does this happen? Well, the malicious code or virus is inserted into the chain of command so that when the infected program is run, the viral code is also executed (or in some cases, runs instead of the legitimate program).

Viruses are usually seen as extraneous code attached to a host program, but this isn't always the case. Sometimes, the environment is manipulated so that calling a legitimate uninfected program calls the viral program. The viral program may also be executed before any other program is run. This can virtually infect every executable file on the computer, even though none of those files' code was actually tampered with. Viruses that follow this modus operandi include "cluster" or "FAT" (File Allocation Table) viruses, which redirect system pointers to infected files, associate viruses and viruses that modify the Windows Registry directory entries so that their own code is executed before any other legitimate program. Computer viruses usually spread via removable media or the internet.

A flash disk, CD-ROM, magnetic tape or other storage device that has been in an infected computer infects all future computers in which it's used. Your computer can also contract viruses from sinister email attachments, rogue web sites or infected software. And these disseminate to every other computer on your network. All computer viruses cause direct or indirect economic damages. Based on this, there are two categories of viruses:1) Those that only disseminate and don't cause intentional damage2) Those which are programmed to cause damage. However, even by disseminating, they take up plenty of memory space, and time and resources that are spent on the clean-up job. Direct economic damages are caused when viruses alter the information during digital transmission. Considerable expenses are incurred by individuals, firms and authorities for developing and implementing the anti-virus tools to protect computer systems.

3. Logic bombs: A logic bomb, also known as "slag code", is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as "time-bombs". For example, the infamous "Friday the 13th" virus which attacked the host systems only on specific dates; it "exploded" (duplicated itself) every Friday that happened to be the thirteenth of a month, thus causing system slowdowns. Logic bombs are usually employed by disgruntled employees working in the IT sector.

You may have heard of "disgruntled employee syndrome" wherein angry employees who've been fired use logic bombs to delete the databases of their employers, stultify the network for a while or even do insider trading. Triggers associated with the execution of logic bombs can be a specific date and time, a missing entry from a database or not putting in a command at the usual time, meaning the person doesn't work there anymore. Most logic bombs stay only in the network they were employed in. So in most cases, they're an insider job. This makes them easier to design and execute than a virus. It doesn't need to replicate; which is a more complex job. To keep your network protected from the logic bombs, you need constant monitoring of the data and efficient anti-virus software on each of the computers in the network. There's another use for the type of action carried out in a logic bomb "explosion" – to make restricted software trials. The embedded piece of code destroys the software after a defined period of time or renders it unusable until the user pays for its further use. Although this piece of code uses the same technique as a logic bomb, it has a non-destructive, non-malicious and user-transparent use, and is not typically referred to as one.

4. Denial-of-Service attack: A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it. Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. DoS attacks violate the acceptable use policies of virtually all internet service providers. Another variation to a denial-of-service attack is known as a "Distributed Denial of Service" (DDoS) attack wherein a number of geographically widespread perpetrators flood the network traffic. Denial-of-Service attacks typically target high profile web site servers belonging to banks and credit card payment gateways. Websites of companies such as Amazon, CNN, Yahoo, Twitter and eBay are not spared either.

5. Phishing: This technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing. You've probably received email containing links to legitimate appearing websites. You probably found it suspicious and didn't click the link. Smart move. How phishing can net some really interesting catches. The malware would have installed itself on your computer and stolen private information. Cyber-criminals use social engineering to trick you into downloading malware off the internet or make you fill in your personal information under false pretenses. A phishing scam in an email message can be evaded by keeping certain things in mind.

Look for spelling mistakes in the text. Cyber-criminals are not known for their grammar and spelling.

Hover your cursor over the hyperlinked URL but don't click. Check if the address matches with the one written in the message.

Watch out for fake threats. Did you receive a message saying "Your email account will be closed if you don't reply to this email"? They might trick you by threatening that your security has been compromised.

Attackers use the names and logos of well-known web sites to deceive you. The graphics and the web addresses used in the email are strikingly similar to the legitimate ones, but they lead you to phony sites.

Not all phishing is done via email or web sites. Vishing (voice phishing) involves calls to victims using fake identity fooling you into considering the call to be from a trusted organisation. They may claim to be from a bank asking you to dial a number (provided by VoIP service and owned by attacker) and enter your account details. Once you do that, your account security is compromised. Treat all unsolicited phone calls with skepticism and never provide any personal information.

Many banks have issued preemptive warnings informing their users of phishing scams and the do's and don'ts regarding your account information.

6. Email bombing and spamming: Email bombing is characterized by an abuser sending huge volumes of email to a target address resulting in victim's email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters. Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker's control) as a DDoS attack. This type of attack is more difficult to control due to multiple source addresses and the bots which are programmed to send different messages to defeat spam filters.

"Spamming" is a variant of email bombing. Here unsolicited bulk messages are sent to a large number of users, indiscriminately. Opening links given in spam mails may lead you to phishing web sites hosting malware. Spam mail may also have infected files as attachments. Email spamming worsens when the recipient replies to the email causing all the original addressees to receive the reply. Spammers collect email addresses from customer lists, newsgroups, chat-rooms, web sites and viruses which harvest users' address books, and sell them to other spammers as well. A large amount of spam is sent to invalid email addresses. Email filters cleaning out spam mail Sending spam violates the acceptable use policy (AUP) of almost all internet service providers. If your system suddenly becomes sluggish (email loads slowly or doesn't appear to be sent or received), the reason may be that your mailer is processing a large number of messages. Unfortunately, at this time, there's no way to completely prevent email bombing and spam mails as it's impossible to predict the origin of the next attack. However, what you can do is identify the source of the spam mails and have your router configured to block any incoming packets from that address.

7. Web jacking: Web jacking derives its name from "hijacking". Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests. Cases have been reported where the attacker has asked for ransom, and even posted obscene material on the site. The web jacking method attack may be used to create a clone of the web site, and present the victim with the new link saying that the site has moved. Unlike usual phishing methods, when you hover your cursor over the link provided, the URL presented will be the original one, and not the attacker's site. But when you click on the new link, it opens and is quickly replaced with the malicious web server. The name on the address bar will be slightly different from the original website that can trick the user into thinking it's a legitimate site.

For example, "gmail" may direct you to "gmai1". Notice the one in place of 'L'. It can be easily overlooked. Obviously not gmail.com, but still enough people click Web jacking can also be done by sending a counterfeit message to the registrar controlling the domain name registration, under a false identity asking him to connect a domain name to the webjacker's IP address, thus sending unsuspecting consumers who enter that particular domain name to a website controlled by the webjacker. The purpose of this attack is to try to harvest the credentials, usernames, passwords and account numbers of users by using a fake web page with a valid link which opens when the user is redirected to it after opening the legitimate site.

8. Cyber stalking: Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn't physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It's an invasion of one's online privacy. Cyber stalking uses the internet or any other electronic means and is different from offline stalking, but is usually accompanied by it. Most victims of this crime are women who are stalked by men and children who are stalked by adult predators and pedophiles.

Cyber stalkers thrive on inexperienced web users who are not well aware of netiquette and the rules of internet safety. A cyber stalker may be a stranger, but could just as easily be someone you know. Cyber stalkers harass their victims via email, chat rooms, web sites, discussion forums and open publishing web sites (e.g. blogs). The availability of free email / web site space and the anonymity provided by chat rooms and forums has contributed to the increase of cyber stalking incidents. Everyone has an online presence nowadays, and it's really easy to do a Google search and get one's name, alias, contact number and address, contributing to the menace that is cyber stalking. As the internet is increasingly becoming an integral part of our personal and professional lives, stalkers can take advantage of the ease of communications and the availability of personal information only a few mouse clicks away. In addition, the anonymous and non-confrontational nature of internet communications further tosses away any disincentives in the way of cyber stalking. Cyber stalking is done in two primary ways:

Internet Stalking: Here the stalker harasses the victim via the internet. Unsolicited email is the most common way of threatening someone, and the stalker may even send obscene content and viruses by email. However, viruses and unsolicited telemarketing email alone do not constitute cyber stalking. But if email is sent repeatedly in an attempt to intimidate the recipient, they may be considered as stalking. Internet stalking is not limited to email; stalkers can more comprehensively use the internet to harass the victims. Any other cyber-crime that we've already read about, if done with an intention to threaten, harass, or slander the victim may amount to cyber stalking.

Computer Stalking: The more technologically advanced stalkers apply their computer skills to assist them with the crime. They gain unauthorized control of the victim's computer by exploiting the working of the internet and the Windows operating system. Though this is usually done by proficient and computer savvy stalkers, instructions on how to accomplish this are easily available on the internet.

Cyber stalking has now spread its wings to social networking. With the increased use of social media such as Facebook, Twitter, Flickr and YouTube, your profile, photos, and status updates are up for the world to see. Your online presence provides enough information for you to become a potential victim of stalking without even being aware of the risk. With the "check-ins", the "life-events", apps which access your personal information and the need to put up just about everything that you're doing and where you're doing it, one doesn't really leave anything for the stalkers to figure out for themselves. Social networking technology provides a social and collaborative platform for internet users to interact, express their thoughts and share almost everything about their lives. Though it promotes socialisation amongst people, along the way it contributes to the rise of internet violations.

9. Data diddling: Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that's programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data. This is one of the simplest methods of committing a computer-related crime, because even a computer amateur can do it. Despite this being an effortless task, it can have detrimental effects. For example, a person responsible for accounting may change data about themselves or a friend or relative showing that they're paid in full. By altering or failing to enter the information, they're able to steal from the enterprise. Other examples include forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements. Electricity boards in India have been victims of data diddling by computer criminals when private parties were computerizing their systems.

10. Identity Theft and Credit Card Fraud: Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name. The imposter may also use your identity to commit other crimes. "Credit card fraud" is a wide ranging term for crimes involving identity theft where the criminal uses your credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is your pre-approved card falling into someone else's hands. Credit card fraud is the most common way for hackers to steal your money. He can use it to buy anything until you report to the authorities and get your card blocked. The only security measure on credit card purchases is the signature on the receipt but that can very easily be forged.

However, in some countries the merchant may even ask you for an ID or a PIN. Some credit card companies have software to estimate the probability of fraud. If an unusually large transaction is made, the issuer may even call you to verify. Often people forget to collect their copy of the credit card receipt after eating at restaurants or elsewhere when they pay by credit card. These receipts have your credit card number and your signature for anyone to see and use. With only this information, someone can make purchases online or by phone. You won't notice it until you get your monthly statement, which is why you should carefully study your statements. Make sure the website is trustworthy and secure when shopping online. Some hackers may get a hold of your credit card number by employing phishing techniques. Sometimes a tiny padlock icon appears on the left screen corner of the address bar on your browser which provides a higher level of security for data transmission. If you click on it, it will also tell you the encryption software it uses. A more serious concern is the use of your personal information with the help of stolen or fake documents to open accounts (or even worse, using your existing account) to take a loan in your name. These unscrupulous people can collect your personal details from your mailbox or trash can (remember to shred all sensitive documents). Think of all the important details printed on those receipts, pay stubs and other documents.

You won't know a thing until the credit card people track you down and tail you until you clear all your dues. Then for months and months you'll be fighting to get your credit restored and your name cleared. With rising cases of credit card fraud, many financial institutions have stepped in with software solutions to monitor your credit and guard your identity. ID theft insurance can be taken to recover lost wages and restore your credit. But before you spend a fortune on these services, apply the no-cost, common sense measures to avert such a crime.

11. Salami slicing attack: A "salami slicing attack" or "salami fraud" is a technique by which cyber-criminals steal money or resources a bit at a time so that there's no noticeable difference in overall size. The perpetrator gets away with these little pieces from a large number of resources and thus accumulates a considerable amount over a period of time. The essence of this method is the failure to detect the misappropriation. The most classic approach is "collect-the-roundoff" technique. Most calculations are carried out in a particular currency are rounded off up to the nearest number about half the time and down the rest of the time. If a programmer decides to collect these excess fractions of rupees to a separate account, no net loss to the system seems apparent. This is done by carefully transferring the funds into the perpetrator's account. Attackers insert a program into the system to automatically carry out the task. Logic bombs may also be employed by unsatisfied greedy employees who exploit their know-how of the network and/or privileged access to the system. In this technique, the criminal programs the arithmetic calculators to automatically modify data, such as in interest calculations. Stealing money electronically is the most common use of the salami slicing technique, but it's not restricted to money laundering.

The salami technique can also be applied to gather little bits of information over a period of time to deduce an overall picture of an organisation. This act of distributed information gathering may be against an individual or an organisation. Data can be collected from web sites, advertisements, documents collected from trash cans, and the like, gradually building up a whole database of factual intelligence about the target. Since the amount of misappropriation is just below the threshold of perception, we need to be more vigilant. Careful examination of our assets, transactions and every other dealing including sharing of confidential information with others might help reduce the chances of an attack by this method.

12. Software Piracy: Thanks to the internet and torrents, you can find almost any movie, software or song from any origin for free. Internet piracy is an integral part of our lives which knowingly or unknowingly we all contribute to. This way, the profits of the resource developers are being cut down. It's not just about using someone else's intellectual property illegally but also passing it on to your friends further reducing the revenue they deserve. Piracy is rampant in India, but you knew that Software piracy is the unauthorized use and distribution of computer software. Software developers work hard to develop these programs and piracy curbs their ability to generate enough revenue to sustain application development. This affects the whole global economy as funds are relayed from other sectors which results in less investment in marketing and research. The following constitute software piracy:

Loading unlicensed software on your PC

Using single-licensed software on multiple computers

Using a key generator to circumvent copy protection

Distributing a licensed or unlicensed ("cracked") version of software over the internet and offline

"Cloning" is another threat. It happens when someone copies the idea behind your software and writes his own code. Since ideas are not copy protected across borders all the time, this isn't strictly illegal. A software "crack" is an illegally obtained version of the software which works its way around the encoded copy prevention. Users of pirated software may use a key generator to generate a "serial" number which unlocks an evaluation version of the software, thus defeating the copy protection. Software cracking and using unauthorized keys are illegal acts of copyright infringement. Using pirated material comes with its own risks. The pirated software may contain Trojans, viruses, worms and other malware, since pirates will often infect software with malicious code. Users of pirated software may be punished by the law for illegal use of copyrighted material. Plus you won't get the software support that is provided by the developers. To protect your software from piracy if you're a developer, you should apply strong safeguards. Some websites sell software with a "digital fingerprint" that helps in tracing back the pirated copies to the source. Another common method is hardware locking. Using this, the software license is locked to specific computer hardware, such that it runs only on that computer. Unfortunately, hackers continue to find their way around these measures.

13. Others: So far we've discussed the dedicated methods of committing cyber crimes. In a nutshell, any offence committed using electronic means such as net extortion, cyber bullying, child pornography and internet fraud is termed as cyber crime. The internet is a huge breeding ground for pornography, which has often been subject to censorship on grounds of obscenity. But what may be considered obscene in India might not be considered so in other countries. Since every country has a different legal stand on this subject matter, pornography is rampant online. However, according to the Indian Constitution, largely, pornography falls under the category of obscenity and is punishable by law. Child pornography is a serious offence, and can attract the harshest punishments provided for by law. Pedophiles lurk in chat rooms to lure children. The internet allows long-term victimization of such children, because the pictures once put up, spread like wild-fire, and may never get taken down completely. Internet crimes against children are a matter of grave concern, and are being addressed by the authorities, but this problem has no easy solution.

Cyber Stalking

Definition

Cyberstalking is a criminal practice where an individual uses the Internet to systematically harass or threaten someone. This crime can be perpetrated through email, social media, chat rooms, instant messaging clients and any other online medium. Cyberstalking can also occur in conjunction with the more traditional form of stalking, where the offender harasses the victim offline.

There is no unified legal approach to cyberstalking, but many governments have moved toward making these practices punishable by law. Cyberstalking is sometimes referred to as Internet stalking, e-stalking or online stalking.

Cyberstalking is one of several cybercrimes that have been enabled by the Internet. It overlaps with cyberbullying and cyberluring in that many of the same techniques are used. Social media, blogs, photo sharing sites and many other commonly used online sharing activities provide cyberstalkers with a wealth of information that helps them plan their harassment. By collecting personal data (profile pages) and making notes of frequented locations (photo tags, blog posts), the cyberstalker can begin to keeping tabs on an individual's daily life.

The National Center for Victims of Crime (NCVC) suggests that victims of cyberstalking take the following steps:

- For minors, inform parents or a trusted adult
- File a complaint with the cyberstalker's Internet service provider
- Collect evidence, document instances and create a log of attempts to stop the harassment

- Present documentation to local law enforcement and explore legal avenues
- Get a new email address and increase privacy settings on public sites
- Purchase privacy protection software
- Request removal from online directories

The NCVC also emphasizes that a victim of cyberstalking should never agree to meet the stalker in person.

Cyber terrorism

Cyberterrorism is defined by U.S. Federal Bureau of Investigation as a premeditated attack against a computer system, computer data, programs and other information with the sole aim of violence against clandestine agents and subnational groups. The main aim behind cyberterrorism is to cause harm and destruction.

Cyberterrorism can be explained as internet terrorism. With the advent of the internet, individuals and groups are misusing the anonymity to threaten individuals, certain groups, religions, ethnicities or beliefs. Cyberterrorism can be broadly categorized under three major categories:

- Simple: This consists of basic attacks including the hacking of an individual system.
- Advanced: These are more sophisticated attacks and can involve hacking multiple systems and/or networks.
- Complex: These are coordinated attacks that can have a large-scale impact and make use of sophisticated tools.

Methods of cyberterrorism

Cyberterror operations can use many different attack methods, including:

- Advanced persistent threat (APT) actors may use sophisticated and concentrated network attacks in which they gain access to a network and stay there undetected for a long period of time with the intention of stealing data, rather than cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense, manufacturing and the financial industry.
- Viruses, computer worms and malware targeting control systems can affect water supplies, transportation systems, power grids, critical infrastructure and military systems and may be used to further cyberterrorist goals.

- DoS attacks, cybersecurity events that occur when attackers take action to prevent legitimate users from accessing targeted computer systems, devices or other network resources.
- Hacking and theft of critical data from institutions, governments and businesses.
- Ransomware that holds computer systems hostage until the victims pay ransom.
- Phishing attacks, attempts by cybercriminals to collect information from victims through email, which they can then use to access systems or steal the victims' identities.

Cyber terrorist attackers can use virtually any attack method used by cybercriminals to further their political or social goals. Cyber attacks across cultural, social, economic and political motivations.

Forgery and fraud

Forgery (also known as "uttering a false instrument") is a serious offense, punishable as a felony in all fifty states and by the federal government. Forgery involves the making, altering, use, or possession of a false writing in order to commit a fraud. It can occur in many forms, from signing another person's name on a check to falsifying one's own academic transcript. When the subject of forgery is currency, it is also called counterfeiting.

Making, altering, using, or possessing

The first element of forgery is that a person must make, alter, use, or possess a false writing. When they think of forgery, many people think only of making false writings, such as forging letters or certificates, but altering an existing writing may also be forgery if the alteration is "material," or affects a legal right. For example, forging another person's signature on a document is a material alteration because it misrepresents the identity of the person who signed the document, which has serious legal consequences. Deleting, adding, or changing significant portions of documents may also be "material" alterations, if these changes affect the legal rights or obligations represented in the documents. Additionally, as discussed above, using or possessing false writings also constitutes forgery, although in some jurisdictions this is known as "uttering a forged instrument."

A false writing

Not all writings meet the definition of forgery. To serve as the basis for forgery charges, the writing in question must have both legal significance and be false, as discussed below.

The writing must have apparent legal significance. In order to be punishable as forgery, the writing in question must have apparent legal significance. This includes government-issued documents such as drivers' licenses and passports; transactional documents such as deeds, conveyances, and receipts; financial instruments such as currencies, checks, or stock certificates; and other documents such as wills, patents, medical prescriptions, and works of art.

To have legal significance, a document need not necessarily be a legal or government-issued document--it must simply affect legal rights and obligations. For this reason, documents such as letters of recommendation or notes from physicians may also be the subjects of forgery. In contrast, signing another person's name to a letter to a friend would probably not constitute forgery, because in most cases it would not have legal significance.

The writing must be false. To be considered false, the writing itself must be fabricated or materially altered so that it purports to be or represent something that it is actually not. Generally, simply inserting false statements into a writing is not enough to meet this requirement, if those misrepresentations do not change the fundamental meaning of the writing itself. For example, if you insert a false statement into a letter you wrote, you have not committed forgery. However, it is forgery if you write a letter of legal significance, but present it as a letter written by someone else.

With the intent to defraud

In order to be guilty of forgery, the defendant must have intended to defraud someone or some entity, such as a government agency (though the fraud need not have been completed). This element prevents people who possess or sign fraudulent documents, without knowing that the documents are false, from being subject to criminal liability. For instance, if you purchase a used car, but later find out that the title to the car was forged by the seller, you would not be subject to forgery charges for the possession of the forged title because you had no intent to defraud.

Crimes related to IPRs

Intellectual property (**IP**) is a category of property that includes intangible creations of the human intellect, and primarily encompasses copyrights, patents, and trademarks. It also includes other types of rights, such as trade secrets, publicity rights, moral rights, and rights against unfair competition.

Intellectual property rights include patents, copyright, industrial design rights, trademarks, plant variety rights, trade dress, geographical indications, and in some jurisdictions trade secrets. There are also more specialized or derived varieties of *sui generis* exclusive rights, such as circuit design rights (called mask work rights in the US) and supplementary protection certificates for pharmaceutical products (after expiry of a patent protecting them) and database rights (in European law).

The term "industrial property" is sometimes used to refer to a large subset of intellectual property rights including patents, trademarks, industrial designs, utility models, service marks, trade names, and geographical indications.

Patents

A patent is a form of right granted by the government to an inventor or their successor-in-title, giving the owner the right to exclude others from making, using, selling, offering to sell, and importing an invention for a limited period of time, in exchange for the public disclosure of the invention. An invention is a solution to a specific technological problem, which may be a product or a process and generally has to fulfill three main requirements: it has to be new, not obvious and there needs to be an industrial applicability. To enrich the body of knowledge and stimulate innovation, it is an obligation for patent owners to disclose valuable information about their inventions to the public.

Copyright

A copyright gives the creator of an original work exclusive rights to it, usually for a limited time. Copyright may apply to a wide range of creative, intellectual, or artistic forms, or "works". Copyright does not cover ideas and information themselves, only the form or manner in which they are expressed.

Industrial design rights

An industrial design right (sometimes called "design right" or *design patent*) protects the visual design of objects that are not purely utilitarian. An industrial design consists of the creation of a shape, configuration or composition of pattern or color, or combination of pattern and color in three-dimensional form containing aesthetic value. An industrial design can be a two- or three-dimensional pattern used to produce a product, industrial commodity or handicraft. Generally speaking, it is what makes a product look appealing, and as such, it increases the commercial value of goods.

Plant varieties

Plant breeders' rights or plant variety rights are the rights to commercially use a new variety of a plant. The variety must amongst others be novel and distinct and for registration the evaluation of propagating material of the variety is considered.

Trademarks

A trademark is a recognizable sign, design or expression which distinguishes products or services of a particular trader from the similar products or services of other traders.

Trade dress

Trade dress is a legal term of art that generally refers to characteristics of the visual and aesthetic appearance of a product or its packaging (or even the design of a building) that signify the source of the product to consumers.

Trade secrets

A trade secret is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known or reasonably ascertainable, by which a business can obtain an economic advantage over competitors and customers. There is no formal government protection granted; each business must take measures to guard its own trade secrets (e.g., Formula of its soft drinks is a trade secret for Coca-Cola.)

Computer Vandalism

Vandalism is an "action involving deliberate destruction of or damage to public or private property"

Vandals often use hacking techniques to deface a website or destroy data and files, but there are also those who just want to steal resources (make use of other people's servers without their knowledge or permission) or to cover their tracks by stealthily making use of hardware owned by legitimate businesses to carry out processing for illegal operations or to relay spam and viruses to others.

The best defence against the majority of these types of attacks comes through installing and maintaining the latest versions of anti-virus and firewall software. As new threats are identified, updates are issued which can identify and neutralise most harmful operations before they have a chance to do any damage. Having a server fully managed by a reputable hosting company ensures that these defences are always in place.

Perhaps a more sinister threat is that of "black hat" hackers, or "crackers". As a general definition, "white hat" hackers are enthusiasts who enjoy learning the intricacies (including weaknesses) of computer systems with no malicious intent, whereas "black hat" hackers are those whose sole purpose is to break into systems and gain access to information and functions to which they are not entitled. The word "hacker" was originally used to refer to the "white hat" variety, whereas "cracker" was used to identify "black hats". The media have since latched onto the word "hacker" almost exclusively in connection with "black hat" hacking, and this is usually what is understood by the term "hacking" today.

SQL Injection

One popular and potentially devastating method of attack is SQL injection. Any web application that makes use of a database usually communicates with the database for necessary functions using a special language known as Structured Query Language, or SQL. By issuing an SQL command to a database server, the web application can control virtually any aspect of the database – adding, editing, or deleting records or tables of data. Although a powerful tool in the hands of a software developer, SQL can become a lethal weapon in the hands of a hacker.

Of course, the web server would need to be configured in such a way that prevents third parties from issuing SQL commands to the database, whilst allowing legitimate requests from the web application to be processed. The problem arises though where a programmer incorporates user input directly into an SQL command quite a common practise.

For example, a program might want to issue an SQL command such as this:

SELECT * FROM users WHERE first_name = 'John'

This SQL command would request all of the records from the user table in the database where the first name matches the value supplied (in this case John). In many instances, the value to be matched against will need to come from the text that is entered into a form on the website, so instead of the program explicitly using the value John, it would need to insert the text that was entered by the user perhaps like this (using PHP as the programming language):

SELECT * FROM users WHERE first_name = ' . $_POST['first_name'] .

In this case, the value from the form (the $_POST['first_name'] bit) is inserted directly into the command. This would work fine for normal use, but if a hacker realised how this SQL command was constructed, he could inject his own SQL command and perform any operation he likes on the database.

For example, instead of entering a value like John in the website's form, he could type something like this:

'; DROP users;

The single quote mark and semi-colon will cause the original SQL command to end, and then the hacker can type any SQL command he likes to be run afterwards in this case, the command DROP users; would delete the users table from the database completely.

All user input must therefore be carefully validated by the programmer, especially before use in an SQL command, and in particular single quote marks should be either removed or 'escaped' – which means they are tagged with a special symbol (or 'escape character' – usually a forward slash '/') that lets the database server know that the quote mark is part of the data and not part of the SQL command.

Cross Site Scripting (XSS)

Cross Site Scripting is a hacking technique whereby malicious scripting code (usually javascript) is injected into user input forms (in a similar way to SQL injection attacks) or incorporated in a URL query string. The threat is greatest when the user input is then output in a dynamically generated web page, and especially if the data is displayed as HTML code.

A malicious entry could include a piece of javascript which performs virtually any action on an innocent end-user's browser (typically a hacker would try to get users to visit the infected page, often by posting links in forums etc), including cookie theft (enabling the hacker to then log in as the other user and access their account), or logging the user's activity for example recording keystrokes so as to intercept passwords etc.

The methods of counteracting cross site scripting are similar to those of SQL injection all data entry (whether posted in a form or passed in a URL) must be carefully validated to ensure that it does not contain special characters (such as greater than or less than symbols) which could allow scripting code to be embedded in the data. These special characters can be represented in hexadecimal notation as well as plain text, so both need to be checked for by the script. Where special characters are to be legitimately allowed, they must be converted to HTML character codes before being displayed in a web page this prevents them from being interpreted as script by the browser.

Directory Traversal

A website is stored within a file system on a server. Some of the server's file system is therefore exposed to the outside world and can be accessed by an end-user's web browser. The part of the file system (or directory structure) that is visible to the outside world is limited to a specific root folder and its contents. Any folders higher up the hierarchy (ie. before you get to the root folder) are theoretically unreachable by the world at large – only authorised users who are logged in on the web server itself can access such folders.

For example, on the actual web server, you might have a directory structure similar to this:

home
username
public_html
images
downloads
private
documents
passwords

In the above example, the public_html folder is the root folder for the website. Anything underneath that folder in the hierarchy can be accessed by a web browser. All of the other folders are not accessible to the world at large because they are not located under the public_html folder.

In a directory traversal attack though, a poorly written script can allow a hacker to access those other folders and read their contents – just using a web browser. This is because a server-side scripting language, such as PHP, runs on the server as though it were a logged-in user – the scripting language has access to all of the folders and files, not just those underneath the root. If a script reads (or outputs the contents of) files on the server as part of its legitimate processing, it must be written in such a way that the files that are used cannot be specified arbitrarily by the end user.

Taking the above directory structure as an example, suppose there was a script on the server that reads the contents of a text file in the public_html folder and outputs it to the screen. If the end user were able to specify the name of the text file to be displayed, the script would need to make sure that the name they entered was still within the public_html folder. If they entered a file name like '..privatepasswordspasswordlist.txt', the two dots at the start would tell the script to move up in the directory structure – effectively breaking out of the website's root folder – and then the hacker can specify any file path he likes whether within the website's root or not.

Therefore, where user input is used as the basis of files that are to be read (or more importantly, output) by a dynamic web page, the script must include a validation routine that ensures that the value entered by the user is legitimate and does not allow the directory structure to be traversed.

Denial of Service Attacks (DOS, DDOS)

A denial of service attack takes place when a hacker overloads a system with large or repeated requests for a service. For example, where a script requires some intensive processing on the server, if lots of requests are received at the same time, this can cause the server to slow down to such an extent that legitimate requests from others cannot be processed. In some instances, a denial of service attack can cause the server to crash completely.

In an effort to prevent denial of service attacks, many scripts which require intensive processing will only allow a single request from any one user (for example, by checking the IP address of the source of the request, and only allowing one request from that IP address within a certain time period). However, distributed denial of service attacks (DDOS) involve a hacker impersonating hundreds or even thousands of different users in such a way that the script cannot tell whether the requests are legitimate or not.

DDOS attacks are very difficult to prevent, but they can also be very difficult to carry out – the effort involved in executing such an attack without being traced means that in most cases it is not a worthwhile excercise from the hackers point of view; they would prefer to use easier methods of attack. If a server has strong defences in other areas though, and an attacker has a strong grudge against a company, a DDOS attack becomes more likely. For this reason, it is usually large corporations and financial institutions who suffer from these attacks.

HTTP Sniffing

HTTP stands for Hyper Text Transfer Protocol, and it is the mechanism used to transfer data from one computer to another across the internet. You can use HTTP to request information from a server, or to send information to a client by wrapping the request or data in a packet.

An HTTP packet consists of a header section which identifies the purpose of the packet (eg. to request a file), the destination (eg. the address of the website the file is being requested from), the format of the request (eg. what type of encoding is used in the main text of the packet), and whether the packet is in one part or has been split up and sent as separate parts (so the server can collect all of the parts it needs before dealing with the request), among other things.

Usually, HTTP packets wing their way across the internet from one machine to another without any human intervention, and without anyone seeing what the packets contain. However, the data in an HTTP packet is usually just plain text – it is not encrypted in any way and can easily be intercepted, read, and even changed en-route by anybody with the appropriate software and technical skill.

The programs used to intercept HTTP requests are known as HTTP sniffers and they are often used to sniff out important information that can be used maliciously (there are also legitimate uses for HTTP sniffers for example, they can be useful in debugging applications that rely on the transfer of HTTP packets). Any data sent over plain HTTP is therefore susceptible to interception, and must be presumed insecure.

For this reason, any sensitive data that must be transferred from one machine to another on the internet should not be sent as a plain HTTP packet. This includes login screens, and forms that collect sensitive personal information such as credit card details. In these instances it is usually best to use HTTPS.

HTTPS is very similar to HTTP; it's just that the data in the packet is encrypted. So even if someone uses as HTTP sniffer, they will not be able to read any of the data without a special key and that key is held securely on the receiving computer. If a hacker tries to change the data, this will be detected by the receiving machine, because it will no longer be able to decrypt the package.

Other Tactics

There are numerous other tactics that can be used to break into a computer system, and these usually involve discovering weaknesses or loopholes in the server software's defences. When a programmer writes software that runs on a web server, he tries to make sure that the software cannot be abused but it can be very difficult to foresee every eventuality; vandals and hackers are always pushing software to the limit and trying out operations which the software was not designed to handle, in an attempt to discover a way in.

Usually, hackers practise using a copy of the software on their own server so that they can try out different tactics without getting caught when they find something that works, they can then use it on other people's servers. For this reason, it is often well-established server software that is the focus of the attack, rather than proprietary scripts written for a specific site.

Manufacturers and vendors of software packages for web servers often advise on configuration recommendations which will negate common attack tactics, but sometimes even the manufacturers are unaware of, or don't bother warning about a loophole which can easily be exploited.

For example, sometimes the default configuration options are geared towards making the software easy to use and powerful rather than secure.

Installation log files, release notes, welcome screens, and various other files which are generally just ignored by server administrators can be the source of valuable information for a hacker.

For example, just knowing which version of operating system your server runs can allow a hacker to exploit a known weakness in that particular version. If he cannot find out what version you are using, he risks being caught if he just tries out an exploit on the off-chance that it will be successful. It is therefore important to make the hacker's job as difficult as possible by obscuring any information that could be used to identify what software and versions the server is using.

Privacy of online data

Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences.

Internet privacy and anonymity are paramount to users, especially as e-commerce continues to gain traction. Privacy violations and threat risks are standard considerations for any website under development.

Internet privacy is also known as online privacy.

Internet privacy is cause for concern for any user planning to make an online purchase, visit a social networking site, participate in online games or attend forums. If a password is compromised and revealed, a victim's identity may be fraudulently used or stolen.

Internet privacy risks include:

- Phishing: An Internet hacking activity used to steal secure user data, including username, password, bank account number, security PIN or credit card number.
- Pharming: An Internet hacking activity used to redirect a legitimate website visitor to a different IP address.
- Spyware: An offline application that obtains data without a user's consent. When the computer is online, previously acquired data is sent to the spyware source.
- Malware: An application used to illegally damage online and offline computer users through Trojans, viruses and spyware.

Internet privacy violation risks may be minimized, as follows:

- Always use preventative software applications, such as anti-virus, anti-malware, anti-spam and firewalls
- Avoid shopping on unreliable websites
- Avoid exposing personal data on websites with lower security levels

- Clear the browser's cache and browsing history on a consistent basis
- Always use very strong passwords consisting of letters, numerals and special characters

Cyber jurisdiction

Jurisdiction is the territorial area of authority to hear and judge cases. The internet, however, has no territorial boundaries: it is a virtual world of interconnected computer networks, known as cyberspace.

Example:

Company A purchases online payment software delivered as a download. The software corrupts A's server. The seller, company B does not have a physical store in any particular country. B sells its software exclusively as a web service. Questions immediately arise about jurisdiction. Is it:

- Where the software download was receipted?
- Where the software was downloaded?
- The location of B's Internet Protocol (IP) address?

Similarly, what about hacking cases. Is jurisdiction where the hacking occurs or the location of the server that is attacked?

US approach

The United States' (US) focus is on the characteristics of the internet presence. Jurisdiction is determined by a 'sliding scale' analysis of the interactivity of the website concerned. Three categories have emerged:

- **Passive websites**: present information but do not accept information, sell products or offer services. Generally, the US courts do not find jurisdiction with these websites.
- **Intermediate websites**: the courts assess the level of interactivity and commercial nature of the exchange of information. The question, in some cases, is whether the nature of the commercial activity is substantial enough to be a substitute for a physical store. In one case, jurisdiction was found over a party who, through its website, had signed up subscribers to its business. However, where a website provided information and a link about tour packages, this did not constitute the kind of interactivity required to establish jurisdiction.

- **Active websites**: jurisdiction is found over providers of websites that actively conduct their business over the internet by displaying products or services and allowing the user to enter into contracts and purchase products.

Returning to our example, in the US a court where A is situated will have jurisdiction as B's website is 'active'. The website permits the software to be downloaded to A's IP address in its location. If, however, B's website merely provided information about the software, and a physical address from which it could be physically ordered, then it is unlikely that a US court would find jurisdiction.

European Union rules

The basic rule under Regulation 1215/2012 (Brussels Regulation recast) is that jurisdiction is based on the domicile of the defendant.

In our scenario, B can be sued in the European Union Member State in which it is domiciled (i.e. has its principal place of business). Note: the location of B's IP address is not determinative of domicile; it tells us no more than the location of a computer and its user.

There are exceptions to the basic rule:

- A person may be sued in the place of the performance of the contract unless otherwise agreed. A software company's terms might specify the place of performance of the contract.
- In tort, a person may be sued in another Member State where the harmful event occurred. In our scenario this would be where A's server that has suffered corruption is located.
- A 'consumer' may also sue in the Member State of their domicile.

Copy right issues and domain name dispute etc.

Copy right Issues

Copyright is one of those thorny issues that are always causing pain to creative types. After all, if you write something, make music, take a photograph, or in some other way create, in theory you should receive full credit (and payment). In the US this falls under title 17, which deals with "original works of authorship", including literary, dramatic, musical, artistic, architectural, and some other intellectual works.

Unfortunately, particularly with the vast free market that is the internet, it's increasingly common for people to feel they should get everything for nothing.

There are a number of issues that can arise, and below we'll take a look at seven of these along with the best way to resolve them.

1. Plagiarism

This is the ultimate nightmare: when someone steals your ideas, writing, music or other intellectual property and pretends that it's theirs. People are allowed to quote a limited amount of your work, but are supposed to give full credit to you.

Where you are losing out substantially, you can take the offender to court under the provisions of section 1498 of title 28. This grants temporary and final injunctions to prevent copyright infringement. Copyright is automatic, and exists from the moment of creation.

A US court can also impound material (such as copies of molds or master tapes), and can order them to be destroyed. More information is available here.

You may also recover damages, if your case is proved, plus any additional profits the other party has made from your work. There's a presumption that an infringement was deliberate, but if someone who has breached copyright proves that it was unintentional, it could reduce your damages, or destroy your case.

You could also be able to recover your legal fees, but this is at the court's discretion. Note that you have to take action within five years of the breach of copyright in a criminal case, and within three years in a civil case.

2. Ownership

Under US law, the owner, manufacturer, or creator (which may not be the same person) can copy a work, create derivatives, sell, rent, lease or lend copies, and publicly perform works or musical recordings.

Who owns the copyright? If you were employed by a company when you created your work, your employer usually owns the copyright. If you were working on commission or freelance, you retain copyright unless you assign it to the purchaser under a legal agreement. Always check contracts for clauses assigning copyright.

Just because someone buys your work doesn't mean they can alter, copy, or publicly display it. They should ask your permission first.

The moral here is to ensure your contract terms are very clear on who owns copyright, if you would like to keep it or prevent particular uses (such as alteration). You may be happy to assign copyright to a purchaser, but be aware that this is forever. You can't then sell the same thing to someone else; the second product would have to be substantively different.

If you're simply selling goods, such as jewellery or pottery, you automatically retain copyright.

3. Website Copyright

The basic design of a website is copyright, as are its contents, including text, graphics, any audio or video, HTML and other markup code, lists of websites and links, as well as any other original material.

Some websites expressly forbid 'deep' links – links that bypass their home page – so it is best to check before doing this. Stanford has more information.

4. Creative Commons, Freeware, and Shareware

If you want to share your work, are not worried about payment, but want to remain within the boundaries of copyright law and get credit for your work, you may want to investigate Creative Commons licenses.

These are valid globally and are based on copyright law. The Creative Commons website asks a few simple questions, such as whether you want to allow commercial use or derivative works, to determine the sort of license you need. A credit to the creator is a fundamental part of this format.

Freeware and shareware are software offered free of charge, though shareware often either restricts the software's functions or includes a free trial time limit. Removing the restrictions or time limit would breach copyright.

Even freeware (like Skype) will usually have restrictions on modification and reverse engineering. If you're creating shareware or freeware, you can create a pre-download agreement.

5. Length of Copyright

Many people presume copyright is a brief thing, and that copying a work created ten years ago is okay. In 1998, President Clinton signed the Sonny Bono Copyright Extension Act, which extends existing copyrights by 20 years, and brought the US into line with Europe. The basic term of protection is now the life of the creator, plus 70 years, for works created after January 1978 in the US. Work for hire has a 95-year copyright.

There are different lengths of copyright for some media – 25 years for photographs and 50 years for films. This means that if you find an older piece of your work has been reproduced without your permission, you can still sue for breach of copyright.

6. Breach of Copyright Abroad

US copyright laws don't apply to other countries, though often relevant foreign laws are similar to those in the US, as you can see from this UK website.

Many countries have signed up to the Universal Copyright Convention, or the World Intellectual Property Organization Copyright Treaty, which protects computer software.

Most countries have signed the earlier Berne Convention, and Wikipedia has a useful list of which countries have signed up to which agreements. For work published online, there is ongoing debate about how the "country of origin" should be defined.

This legal website provides an interesting primer on how to undertake actions in other countries.

7. Exceptions

Very short items are not covered by US copyright, including names, titles, brief phrases, or lists. However, you can cover some such items by use of trademarks or patents (think McDonalds' "I'm Lovin It").

The Berne Convention allows for "fair use" of copyright works (in a 'transformative' way; for example, in parody, research, or news reporting).

To sum up, there are various issues and solutions when it comes to copyright:

Plagiarism, which can be resolved in court.

Ownership, details of which should be set out in your contract.

Website content stealing, which falls under copyright law and can go to court.

Creative Commons, freeware and shareware, for which you can gain protection through licenses and legal agreements.

Copyright provides lifetime protection and beyond, so you can sue for breach of copyright on older pieces of work.

Many other countries have strong copyright protection in place – check online for further details.

There are exceptions to copyright law, but very short pieces of work can be covered by trademark or patent law.

Domain Name System

The Domain Name System (DNS) serves the central function of facilitating usersability to navigate the Internet. It does so with the aid of two components: the domain name and its corresponding Internet Protocol (IP) number. A domain name is the human-friendly address of a computer that is usually in a form that is easy to remember or to identify, such as www.wipo.int. An IP number is the unique underlying numeric address, such as 192.91.247.53. Distributed databases contain the list of domain names and their corresponding address and perform the function of mapping the domain names to their IP numeric addresses for the purpose of directing requests to connect computers on the Internet. The DNS is structured in a hierarchical manner which allows for the decentralized administration of name-to-address mapping.

DOMAIN NAME ISSUES: With the advancement of e-commerce, the domain names have come to acquire the same value as a trademark or the business name of a company. The value attached to domain names makes it lucrative for cyber criminals to indulge in domain name infringements and the global nature and easier and inexpensive procedure for registering domain names further facilitates domain name infringements. When a person gets a domain name registered in bad faith, i.e. in order to make huge profits by registering a domain name corresponding to a trademark of another person, with an intent to sell the domain name to the trademark owner at a higher price, such activities are known as cybersquatting. The IT Act does not deal with the domain name issues. In India the domain name infringement cases are dealt with according to the trademark law. With most of the countries providing for specific legislations for combating and curbing cyber squatting, India also needs to address the issue and formulate legal provisions against cyber squatting.

For settlement of Disputes, WIPO has introduced a new mechanism called ICANN (Internet Corporation for Assigned Names and Numbers) for settlement of disputes relating to domain names.

As the parties are given the right to file the case against the decision of ICANN in their respective jurisdictions, the decisions of ICANN is having only persuasive value for the domain users.

Cyber squatting

Cyber squatting is the act of registering a domain name that is same as, or confusingly similar to, the trademark of another with the intention of selling (at a profit) the domain name to the trademark owner.

As long as a cyber squatter owns the domain name, the trademark owner cannot register his own trademark as a domain name. Thereby, a cyber squatter breaches the right of the trademark owner to utilize his own trademark. It is relevant to note that there is nothing wrong with the practice of reserving a domain name. Often, cyber squatters register words or phrases they hope will someday be sought after by new companies or new businesses. Such speculative domain name registration, (read, speculative cyber squatting) is very much legitimate.

ICANN and UDRP

In 1993, pursuant to a grant from the National Science Foundation, a central registry for domain names was created in United States. Initially, Network Solutions Inc.(NSI) acted as the sole administrator over the domain name registry with dominion over Second-Level Domains with respect to Top-Level Domains (TLDs), i.e. .com, .net and .org. This monopoly of NSI pertaining to domain name registration was ended pursuant to a White Paper written by the National Tele Communications and Information Agency, US Department of Commerce in June, 1998 which called for the formation of a new non-profit corporation by private sector Internet stakeholders to administer the policy of domain names system, Consequently ICANN was born.

Uniform Domain Name Dispute Resolution policy (UDRP) was adopted on 24th October, 1999 by ICANN realizing the potential threat presented by Cybersquatting. The policy offers an expedited administrative proceeding for trademark holders to contest abusive registrations of domain names, which may result in the cancellation, suspension or transfer of a domain name by the registrar.

India and Domain Name Dispute Resolution

The ccTLDs category is specific and distinct from the gTLDs and correlate to the names of specific countries and territories. Various corporations today not only register their trade name and their core brands as gTLDs, but also as ccTLDs in select countries where they see future business potential. Functionally, there is no dissimilarity between the gTLD and the ccTLD. A domain name registered in a ccTLD provides exactly the same connectivity as a domain name registered in a gTLD.

There are at present more than 200 ccTLDs. Each of these domains bears a two letter country code derived from Standard 3166 of the International Standardization Organization.

An example would be: Yahoo.com is a gTLD. However, Yahoo.co.in would be a ccTLD registered in India. Similarly, Yahoo.co.au would be a ccTLD registered in Australia.

Part A (ONE Mark)
Multiple Choice Questions
Online Examination

Part B (2 Marks)

1. Define cyber crime and its types.
2. Give five examples for computer and cyber crimes.
3. Distinction between Conventional and cyber crime.
4. Discuss the cyber forensics.
5. Explain the cyber stalking.
6. Discuss cyber terrorism and its categories.
7. How can minimize the Internet privacy violation risks?
8. Define Cyber jurisdiction.
9. What is cyber squatting?

Part C (8 Marks)

1. Write in brief about kinds of cyber crimes.
2. Describe the cyber terrorism and its methods.
3. What is a crime related IPRs and explain the types.
4. What is computer vandalism and discuss its most popular attacking methods.
5. List out the types of copy right issues.
6. Discuss about Domain name issues and ICANN.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed University Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2017 onwards)
DEPARTMENT OF COMMERCE (CA)

SUBJECT: : Cyber Crime and Laws
SEMESTER : VI
SUBJECT CODE: 17CCU604B CLASS : III B.COM CA
UNIT : 1

S.NO	QUESTIONS	OPTION 1	OPTION 2	OPTION 3	OPTION 4	ANSWER
1	Cybercrime is defines as a crime in which a_____is the object of the crime	phone	television	computer	magazine	computer
2	Criminals who perform illegal activities using computer are called	hackers	stealers	corrupters	destroyers	hackers
3	Collecting personal or financial information is called _____	cracking	harvesting	scamming	spamming	harvesting
4	_____is the act of disguising a communication from an unknown source as being from a known, trusted source.	Spamming	Phising	Spoofing	scamming	Spoofing
5	Connecting to a device to a phone line to listen to conversations is called_____	Wiretapping	Salami slicing	Typosquatting	spamming	Wiretapping
6	_____is tricking people to believe into something that's not true	scam	slander	spam	piracy	Scam
7	Computer_____is the application of investigation and analysis techniques to gather and preserve evidence from a computer device	criminalistics	Pattern analysitics	Federal investigations	forensics	Forensics
8	_____hackers are those who develop an interest in computer hacking just out of intellectual curiosity	Black hat	Grey hat	White hat	Brown hat	Black hat
9	The hackers who are against the abuse of computer systems is called _____	Grey hat	White hat	Brown hat	Black hat	White hat
10	Cross site scripting is also known as _____	css	xss	lss	mss	Xss
11	Computer virus is a_____that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.	A piece of code	A piece of memory	A piece of data	A piece of file	A piece of code
12	_____almost always cause at least some harm to the network, even if only by consuming bandwidth	virus	bacteria	worms	Trojan horse	Worms
13	_____is a set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects.	Dynamic bomb	constant bomb	static bomb	Logic bomb	Logic bomb
14	DOS is abbreviated as _____	Denial of Service	Directory of Service	Denial of Source	Directory of Source	Denial of Service
15	_____is the telephone equivalent of phishing	Vishing	thrashing	cracking	surfing	Vishing
16	Abuser send huge volumes of data to target email address is called_____	Email bombing	Logic bombing	Net bombing	Dynamic bombing	Email bombing
17	A_____is a collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware.	surfnet	potnet	botnet	Mailnet	botnet
18	Hackers takes the control of website fraudulently is called _____	hijacking	webjacking	sitejacking	netjacking	Webjacking
19	The victim is pursued or followed in online is called _____	Cyber stalking	Cyber spoofing	Cyber scamming	Cyber surfing	Cyber stalking
20	_____occurs when someone with access to information doing some sort changes to information before it is entered into a computer.	Data corrupting	Data stealing	Data diddling	Data destroying	Data diddling
21	Criminals steal only small amount of money in online is called _____	Slandering	Salami slicing	Spoofing	Scamming	Salami slicing
22	NCVC stands for _____	National Center for Victims of Crime	National Conference for Victims of Crime	National Center for Victims of Cost	Notable Center for Victims of Crime	National Center for Victims of Crime
23	_____is the politically motivated use of computers and information technology to cause severe disruption or widespread fear	Cyber slandering	Cyber threatening	Cyber violence	Cyber terrorism	Cyber terrorism

24	a type of malicious software designed to block access to a computer system until a sum of money is paid is called _____	Dataware	spyware	ransomware	malware	Ransomware
25	Counterfeiting is the forgery in _____	copyright	currency	document	software	Currency
26	IPR in Cyberspace stands for _____	Intellectual Property	Impulse Response	In Progress Review	Impulse Response	Intellectual Property
27	_____is action of involving deliberate destruction of or damage to public or private property.	Sql injection	vandalism	Copyright violence	piracy	vandalism
28	Directory traversal is a type of_____exploit that is used by attackers to gain unauthorized access to restricted directories and files	CSS	XSS	HTTP	HTML	HTTP
29	A_____is a form of right granted by the government to an inventor or successor in title.	patent	copyright	trademark	tradedress	patent
30	The websites which only present information but does not accept information is called_____website.	Passive	Inter	Dorminant	Active	Passive
31	The_____is stealing ideas, writing, music or other intellectual property	Plugiarism	ownership	Copyright	Patent	Plugiarism
32	_____is software that is available for use at no monetary cost.	Freeware	default	implicit	copy	Freeware
33	Which of the below which falls under copyright law?	Plugiarism	Website Content stealing	Ownership stealing	Trademark stealing	Website Content stealing
34	The_____is a distributed directory that resolves human-readable hostnames, such as www.dyn.com, into machine-readable IP addresses	DNS	DCS	DMS	DFS	DNS
35	_____is registering, trafficking in, or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else.	cybersquatting	Cyberphising	cyberstalking	cyberpharming	cybersquatting
36	Criminal liability is the liability that arises out of _____or committing a criminal act	breaking a rule	breaking a protocol	breaking a law	breaking a guideline	breaking a law
37	Recognizing the rights of breeders is called_____in cyber law	plant variety protection	Seed variety protection	Soil variety protection	tree variety protection	plant variety protection
38	Which is used by end user to access resources from outside?	browser	server	hub	host	browser
39	The websites they conduct their business over internet are called _____	Active	Passive	Inter	Super	Active
40	Hacking an individual system comes under which cyber attack?	complex	advanced	simple	Severe	simple
41	_____attackers can use vitually any attack method as cybercriminals and cause only destruction	Cyber hacker	Cyber terrorist	Cyber attacker	Cyber stalker	Cyber terrorist
42	The legal term for protecting the way of packaging a product is called _____	Trade secret	Trade dress	Plant variety	Copyright	Trade dress
43	Originally cracker was used to refer_____hackers	Black Hat	White Hat	Pink Hat	Red Hat	Black Hat
44	Programmer incorporates user input directly into an SQL command into the website is called _____	SQL Injection	SQL Destruction	SQL Corruption	SQL Construction	SQL Injection
45	Which makes the hacker to login as other user and access their account?	Connection theft	ID theft	Cookie theft	Session theft	Cookie theft
46	Antivirus_____is a type of utility used for scanning and removing viruses from your computer.	Ransom ware	Free ware	Malware	Software	Software
47	An_____address (IP address) is a numerical label assigned to each device connected to a computer network	Internet Protocol	Internet Suite	Internet device	Internet System	Internet Protocol
48	WIPO introduced a new mechanism called_____for settlement of disputes.	IWANN	ICANN	IMANN	ISANN	ICANN
49	A_____is a top-level domain name that is used to define the domain for a particular country or a geographical area.	ccTLD	gcTLD	mcTLD	scTLD	ccTLD
50	Which gives rights to the creator of the original work only for a limited time?	Patent	Copyright	Intellectual Property	Traderight	Copyright
51	Spying on a person or business is known as _____	Espionage	Harvesting	Cracking	Cyberstalking	Espionage
52	Someone copies the idea behind your software and writes his own code is called_____	Cloning	Pharming	Phishing	Spamming	Cloning
53	software that is available free of charge and often distributed informally for evaluation, after which a fee may be requested for continued use is known as_____	shareware	commonware	freeware	ransomware	shareware
54	_____is the form of right granted by the government to an inventor	copyright	trademarks	patent	Industrial design rights	patent
55	_____is an internet hacking activity used to redirect a legitimate website visitor to s different IP address	Sniffing	Phishing	Pharming	vandaling	Pharming
56	Jurisdiction is the_____area of authority to hear and judge cases	Provincial	territorial	topical	sectional	territorial
57	The purpose of_____ attack is to overload the system	Harvesti	Pharmin	Denial of	Phising	Denial

		ng	g	service		service attack
58	What is the most important activity in system cracking?	Information gathering	Cracking passwords	Escalating privileges	Covering attacks	Cracking passwords
59	Services running on a system are determined by _____	Sytem's IP address	IP directory	System's network name	Port assigned	Port assigned
60	An online application that illegally damage online and offline users is known as_____	common ware	ransom ware	malware	spyware	malware

UNIT-II

SYLLABUS

Definition and Terminology (Information Technology Act, 2000): Concept of Internet, Internet Governance, E-Contract, E-Forms, Encryption, Data Security. Access, Addressee, Adjudicating Officer, Affixing Digital Signatures, Appropriate Government, Certifying Authority, Certification Practice Statement.

Definition and Terminology (Information Technology Act, 2000)

The original Act contained 94 sections, divided in 13 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India.

The Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The formations of Controller of Certifying Authorities was directed by the Act, to regulate issuing of digital signatures. It also defines cyber crimes and prescribed penalties for them. It also established a Cyber Appellate Tribunal to resolve disputes rising from this new law. The Act also amended various sections of Indian Penal Code, 1860, Indian Evidence Act, 1872, Banker's Book Evidence Act, 1891, and Reserve Bank of India Act, 1934 to make them compliant with new technologies.

Offences

List of offences and the corresponding penalties:

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme,	Imprisonment up to three years, or/and with fine up to □200,000

		computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to □500,000
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to □100,000
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to □100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to □100,000
66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to □200,000
66F	Acts of cyberterrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of	Imprisonment up to life.

		threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to □1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to □1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to □1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to □1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediately (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure	Imprisonment up to three years, or/and with fine up to □200,000

		compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.	
69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.

71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to □100,000

Concept of Internet

What is the Internet?

The Internet is a global network of networks connecting millions of users worldwide via many computer networks using a **simple standard common addressing system** and **basic communications protocol** called TCP/IP (Transmission Control Protocol/Internet Protocol). This allows messages sent over the Internet to be broken into small pieces, called packets, which travel over many different routes between source and destination computers.

Clients and Servers

Internet resources -- information and services -- are provided through host computers, known as servers. The **server** is the computer system that contains information such as electronic mail, database information, or text files. As a customer, or **client**, you access those resources via client programs (applications) which use TCP/IP to deliver the information to your screen in the appropriate format for your computer.

One important kind of client program is called a **browser**, which is used to search through information provided by a specific type of server. A browser helps you view and navigate through information on the Internet. Today's most popular browsers, including Mosaic(R), Netscape(TM) Navigator, and the Microsoft Internet Explorer offer a graphical interface to the World Wide Web.

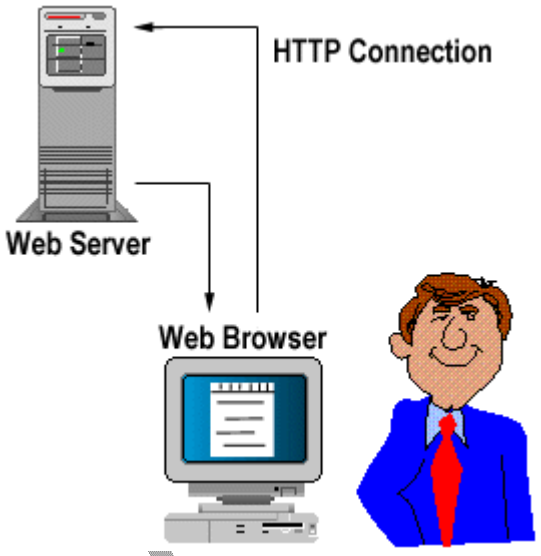
Client/Server Operation

A client/server system works something like this:

- A big hunk of computer (called a server) sits in some office somewhere with a bunch of files that people might want access to. This computer runs a software package (uh...also called a server unfortunately) that listens all day long to requests over the wires.
- Typically, these requests will be in some language and some format that the computer understands, but in English sound something like, "hello software package running on a big

hunk of computer, please give me the file called "mydocument.txt" that is located in the directory "/usr/people/myname".

- The "server software" will then access the server hardware, find the requested file, send it back over the wires to the "client" who requested it, and then wait for another request from the same or another client.
- Usually, the "client" is actually a software program, like Netscape Navigator, that is being operated by a person who is the one who really wants to see the file. The client software however, deals with all the underlying client/server protocol stuff and then displays the document (that usually means interpreting HTML, but we'll get there in just a bit) to the human user.
- The whole process looks something like the figure below:



Hypertext Documents

The WWW makes extensive use of **hypertext documents** which contain

- Multimedia data such as text, images, sounds, video clips etc.
- Links to other documents (situated anywhere on the web).

HTTP

- The client/server protocol used to exchange hypertext documents is called HTTP (HyperText Transport Protocol). The main thing you need to know is that HTTP is a language spoken between your web browser (client software) and a web server (server software) so that they can communicate with each other and exchange files.

- HTTP is a "request-response" type protocol that specifies that a client will open a connection to a server then send a request using a very specific format. The server will then respond and close the connection.

HTML

Hypertext documents are represented using a specialized markup language called HTML (Hyper Text Markup Language).

Basic WWW Concepts

1. **BROWSER** -- A WWW browser is software on your computer that allows you to access the World Wide Web. Examples include *Netscape Navigator* and *Microsoft Internet Explorer*. Please know that a browser can't work its magic unless you are somehow connected to the Internet. At home, that is normally accomplished by using a modem that is attached to your computer and your phone line and allows you to connect to, or dial-up, an Internet Service Provider (ISP). At work, it may be accomplished by connecting your workplace's local area network to the Internet by using a router and a high speed data line.
2. **HYPERTEXT AND HYPERMEDIA** -- Hypertext is text that contains electronic links to other text. In other words, if you click on hypertext it will take you to other related material. In addition, most WWW documents contain more than just text. They may include pictures, sounds, animations, and movies. Documents with links that contain more than just text are called hypermedia.
3. **HTML (HYPERTEXT MARKUP LANGUAGE)** -- HTML is a set of commands used to create world wide web documents. The commands allow the document creator to define the parts of the document. For example, you may have text marked as headings, paragraphs, bulleted text, footers, etc. There are also commands that let you import images, sounds, animations, and movies as well as commands that let you specify links to other documents. If you wanted to create your own web page, you would need to know HTML or be able to use a tool that can generate HTML such as Claris *HomePage* or Adobe *PageMill*.
4. **URL (UNIFORM RESOURCE LOCATOR)** -- Links between documents are achieved by using an addressing scheme. That is, in order to link to another document or item (sound, picture, movie), it must have an address. That address is called its URL. The URL identifies the host computer name, directory path, and file name of the item. It also identifies the protocol used to locate the item such as hypertext, gopher, ftp, telnet or news. For example, the URL for the main page of the OPEN (Oregon Public Education Network) website is http://www.open.k12.or.us

5. **HTTP (HYPERTEXT TRANSPORT PROTOCOL)** -- HTTP is the protocol used to transfer hypertext or hypermedia documents.
6. **HOME PAGE** -- A home page is usually the starting point for locating information at a WWW site. Currently, the home page for Roseburg High School's web site is located at http://schools.rosenet.net/roseburg/rhs/
7. **CLIENTS AND SERVERS** -- If a computer has a web browser installed, it is known as a client. A host computer that is capable of providing information to others is called a server. A server requires special software in order to provide web documents to others.

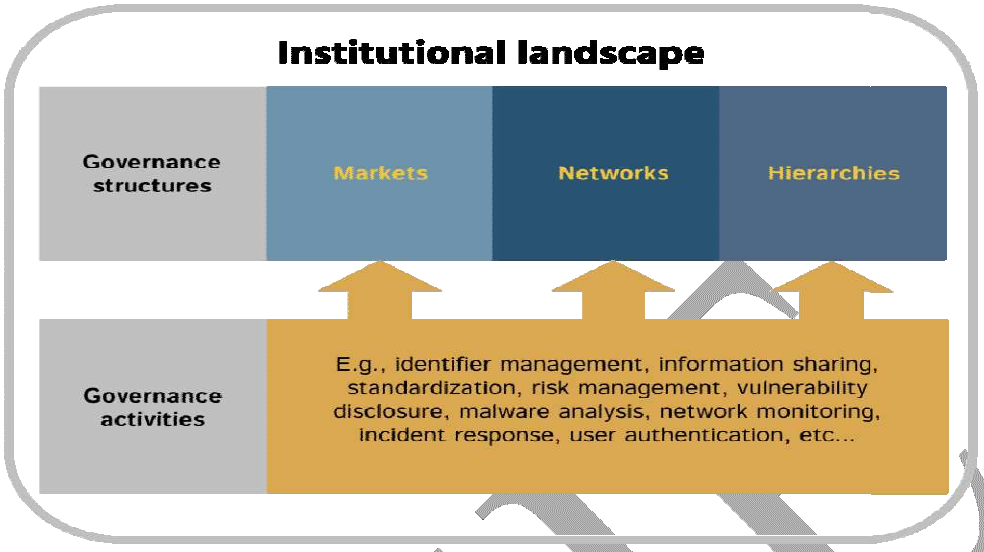
Internet Governance

Internet governance refers to the rules, policies, standards and practices that coordinate and shape global cyberspace. The Internet is a vast network of independently-managed networks, woven together by globally standardized data communication protocols (primarily, Internet Protocol, TCP, UDP, DNS and BGP). The common adoption and use of these protocols unified the world of information and communications like never before. Millions of digital devices and massive amounts of data, software applications, and electronic services became compatible and interoperable. The Internet created a new environment, a complex and dynamic "cyberspace."

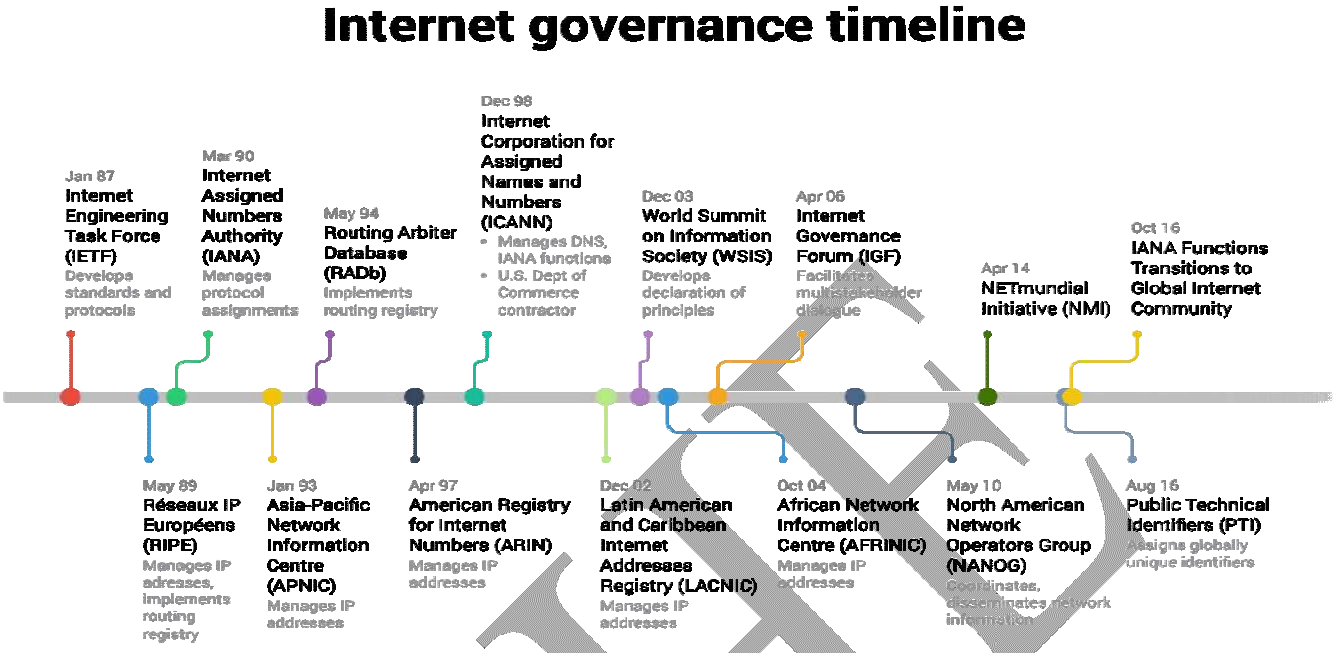
While Internet connectivity generated innovative new services, capabilities and unprecedented forms of sharing and cooperation, it also created new forms of crime, abuse, surveillance and social conflict. Internet governance is the process whereby cyberspace participants resolve conflicts over these problems and develop a workable order.

The Forms of Internet Governance

Internet *governance* and not *government* because many issues in cyberspace are not and probably cannot be handled by the traditional territorial national institutions. *Governance* implies a polycentric, less hierarchical order; it requires transnational cooperation amongst standards developers, network operators, online service providers, users, governments and international organizations if it is to solve problems while retaining the openness and interoperability of cyberspace. For better or worse, national policy plays an important role in shaping the Internet, but the rise of cyberspace has produced, and will continue to produce, new institutions and governance arrangements that respond to its unique characteristics.



IGP's analysis of the Internet governance space is informed by institutional economics, which identifies three broad categories of governance: markets, hierarchies and networks. *Markets* are driven by private transactions and the price mechanism. *Hierarchies* govern interactions through orders or compulsion by an authority, such as law enforcement by a state, a binding treaty, or the organizational control of a firm *Networks* are semi-permanent, voluntary negotiation systems that allow interdependent actors to opt for collaboration or unilateral action in the absence of an overarching authority. Internet governance involves a complex mixture of all three governance structures, including various forms of self-governance by market actors.



E-Contract

DEFINITION OF E-CONTRACT

E-contract is any kind of contract formed in the course of e-commerce by the interaction of two or more individuals using electronic means, such as e- mail, the interaction of an individual with an electronic agent, such as a computer program, or the interaction of at least two electronic agents that are programmed to recognize the existence of a contract. E-contract is a contract modeled, specified, executed and deployed by a software system.

Essentials of an electronic contract:

As in every other contract, an electronic contract also requires the following necessary requirements:

1. An offer requirements to be made

In many contacts (whether online or conventional) the offer is not made directly one-on-one. The consumer 'browses' the available goods and services showed on the seller's website and then chooses what he would like to purchase. The offer is not made by website showing the items for sale at a particular price.

This is essentially an invitation to offer and hence is revocable at any time up to the time of acceptance. The offer is made by the customer on introduction the products in the virtual 'basket' or 'shopping cart' for payment.

2. The offer needs to be acknowledged

As stated earlier, the acceptance is usually assumed by the business after the offer has been made by the consumer in relation with the invitation to offer. An offer is revocable at any time until the acceptance is made.

Processes available for forming electronic contracts include:

I. E-mail: Offers and acceptances can be exchanged entirely by e-mail, or can be collective with paper documents, faxes, telephonic discussions etc.

II. Web Site Forms: The seller can offer goods or services (e.g. air tickets, software etc.) through his website. The customer places an order by completing and communicating the order form provided on the website. The goods may be actually delivered later (e.g. in case of clothes, music CDs etc.) or be directly delivered electronically (e.g. e-tickets, software, mp3 etc.).

III. Online Agreements: Users may need to take an online agreement in order to be able to avail of the services e.g. clicking on "I accept" while connecting software or clicking on "I agree" while signing up for an email account.

3. There has to be legal consideration

Any contract to be enforceable by law must have legal consideration, i.e., when both parties give and receive something in return. Therefore, if an auction site eases a contract between two parties where one Ecommerce – Legal Issues such as a person provides a pornographic movie as consideration for purchasing an mp3 player, then such a contract is void.

4. There has to be an intention to create lawful relations

If there is no intention on the part of the parties to create lawful relationships, then no contract is possible between them. Usually, agreements of a domestic or social nature are not contracts and therefore are not enforceable, e.g., a website providing general health related data and instructions.

5. The parties must be able to contract.

Contracts by minors, lunatics etc. are void. All the parties to the contract must be lawfully competent to enter into the contract.

6. There must be free and unaffected consent

Consent is said to be free when there is absence of coercion, misrepresentation, undue influence or fraud. In other words, there must not be any agitation of the will of any party to the contract to enter such contract. Usually, in online contracts, especially when there is no active real-time communication between the contracting parties, e.g., between a website and the customer who buys through such a site, the click through process ensures free and genuine consent.

7. The object of the contract needs to be lawful

A valid contract presumes a lawful object. Thus a contract for selling narcotic drugs or pornography online is void.

8. There must be conviction and possibility of performance

A contract, to be enforceable, must not be ambiguous or unclear and there must be possibility of performance. A contract, which is impossible to perform, cannot be enforced, e.g., where a website promises to sell land on the moon.

TYPES OF ELECTRONIC CONTRACTS

Employment Contracts

The Information Technology is determined by manpower in Indian context and thus employment contracts are vital. With high erosion rate as well as the confidentiality involved in the work employment contracts become crucial. Apart from that Indian Labour practices are based on tough labour laws and not the hire and fire processes of the first world. In this background copyright issue of software development assumes vital importance. Apart from that contracts for on-site development and sending the workforce abroad and security clauses will play a crucial role in employment contracts. Firms hiring personnel abroad apart from their personnel need to include the relevant employment contract of the place of action.

Consultant Agreements

The normal requirements of Indian Contracts Act of 1872 will apply on any consultant agreement. But particularly in Information Technology industry where the infrastructure to function is low and connectivity is very high consultancy with experience marketing and business development and technology development is a very dominant mode of contract. Here proper care to be taken in Consultant agreements where issues of Intellectual Property Rights, privacy will play an important role. If care is not taken it may lead to cost of business and loss of clients.

Contractor Agreements

As manufacturing companies subcontract their business, Information Technology also subcontract their work due to changing orders and would like to cut on the cost of regular workforce and attendant legal and financial problems. At the same time in manufacturing business, tough labour laws like the Contract Labour (Abolition and Regulation) Act of 1970 in force could lead to a different type of legal twist. However if care is taken to subcontract keeping the requirements of the contract Act and the Contract Labour abolition act the anticipated objectives could be met. Here again privacy, consumer liability and copy right issues assume great importance and care to be taken in representation such contracts.

Sales, Re-Seller and Distributor Agreements

In software and Internet dealings though the order of middle men are done away with, it still requires a circulation network and hence prescribed issues come into play in that feature of business. In first place one needs to see whether software is a good in the Sale of Goods Act.

Software is a programme of instructions, which operate the system or hardware to function in a planned manner. Hence there arises an effort to classify and define in legal terms of the vague nature of software in comparison with other products. The code and its source can be understood as information planned in a way to operate the system leading to the conclusion it is not a property and not a good in the legal intellect. In *Aerodynamics Systems Product* v. *General Automation limited*, the argument upraised by the defendants that though software can be a subject matter of sale, software them self is pure information, and the transmission of software is a service and not sale of goods. There is another explanation of Software to be considered as Goods where it is likened to that of a book containing information, which is considered as goods under the Sale of Goods Act. As the value of the book is not the mere value of the inlet jacket, paper and materials used in its creation, but one that of the value of the information limited in it, software is also a product –a floppy, or a CD-ROM or simply stored in hard disc but the value is much higher than the simple storage device.

Hence software due its high value in terms of application is measured as goods for the purpose of legal classification. Having recognized it as good the distribution, reseller agreement should take care of the aspect of Monopoly Restrictive Trade Practices (in future the competition law) provincial authority and other tax instruments.

Non-Disclosure Agreements

Non-Disclosure Agreements are part of IT contracts, which identify binding agreements with employees apart from the standard confidentiality agreements. The Indian Contract Act 1872 has provisions for the same and it undertakes importance in an industry which is purely knowledge based and one which can be easily repeated ruining the business.

Software Development and Licensing Agreements

A license is an authorisation given to do a specific manufacture/sales/marketing/distribution, which is legitimate. License plays a prevailing form of contract in mass marketing activity of any kind including Information Technology. Software licensing has a historical background where originally it was pushed with the hardware and was given free and its use and application was limited to that of operating the system and few other features. Later in late 60's and early 70's hardware makers in Europe marketed software distinctly. Later software makers resorted to license their products distinctly from that of the hardware. In normal ownership, the product sold becomes the exclusive property of the buyer who can do whatsoever he wants. In case of software, the product can be copied easily and will adversely affect the manufacturer of his sale and thus the entire investment-return processes and future spur to invest in making software. Thus software business became a business of license command. These licenses are issued in persistence or for a limited period. Licensing agreement normally forbids reverse-engineering, de-compiling or any other manipulation of the software, which can be marketed easily with some alterations. Licenses are issued for a single machine practise at a specified location with a provision for backup in the same machine in case of a crash or unreliable functioning. Multiple machine licenses are also given. The license agreement also protects the user from any copyright or other intellectual property violation of the manufacturer. The licensing agreements become vital in Cyber Contracts. Similarly software development is another agreement between joint ventures of companies or for awarding development of software to multiple parties, which assume vital importance in contracts of cyber world.

Shrink Wrap Contracts

A Shrink Wrap contract is the former license agreement required upon the buyer when he buys software. Before he or she tears the pack to use it, he or she is made mindful by tearing the cover or the wrap that they are sure by the license agreement of the manufacture. This is done as previous deliberated to protect the interests of the manufacturer where the consumer cannot replicate the package, copy it or sell it or donate it to others moving the sale of the software. The license, which is contracted and enfolded in the product, which becomes enforceable and taken as consent before the buyer tears the package. The usual sections that are part of the shrink-wrap license are that of

a) prohibiting illegal creation of copies

b) prohibiting payments of the software

c) prohibition of contrary engineering, de-compilation or adjustment

d) prohibition of usage in more than one computer definite for that purpose

e) disclaimer of contracts in respect of the product sold

f) limitations of responsibility

The reason and business sense is that to guard the manufacturer of the package, as it is easy to copy, operates and duplicate under other brand name. Critiques contend that shrink-wrap license agreement is in contradiction of the basic principle of contract of offer, consideration and acceptance as the licensee is unsettled. Several cases to this effect have been dispensed in US courts.

Click Wrap Contracts

An online buyer or user clicks on the I AGREE button on a webpage to purchase or download a program. The term is derived from the fact that such agreements most times require clicking an on-screen icon to signal acceptance. Types of Click Wrap Contract. A Type and Click is also a kind of Click wrap contract where the user must type I ACCEPT or other specified words in an on-screen box and then click submit or similar button. It denotes acceptance of the terms before download can commence. Icon Clicking is where the user must have to click on OK or I AGREE button on a dialogue box or pop up window. The user rejects by clicking CANCEL or CLOSING THE WINDOW.

DIFFERENCE BETWEEN SHRINK WRAP AND CLICK WRAP E- CONTRACTS

Shrink Wrap

1. Consumer does not know the key terms of the contract.

2. People agree to the terms by using the software which they have already purchased. 3. They have questionable enforceability.

4. Conclusion of contract is by breaking the seal used to bind.

Click Wrap

1. Consumer can go through the terms of the contract.

2. Allows users to read the terms of the agreement before accepting them.

3. They have gained universal acceptance.

4. Through the simple act of clicking the "accept" button Shrink wrap Click Wrap

Source Code Escrow Agreements

In software development many principal firms who participate in development are keen to guard the source code of the software, which is the most appreciated and cautious part of the computer programme. Copyright owners of such source code may have to disclose this to countless developers who will be developing definite software based on the source code. In these conditions, the copyright owner will credit the source code to specified source code escrow agents who will release the code on the development of the product upon agreed terms. In cyber contracts, such agreements and also the terms and conditions to contract with the escrow agents become vital.

E-Forms

Electronic forms (eforms) provide a series of fields where data is collected, often using a Web browser. They take the place of paper forms and are designed to capture, validate, and submit data to a recipient for forms processing in a more efficient manner. E-forms allow data to be captured electronically which can speed back-end processing of form-based information. Data can also be exchanged with back-end systems.

Benefits of Using e Forms

Form Submitter

eForms provide simplicity for the person submitting the eform. It enables them to complete the form electronically which means no mailing of forms, and saving them time, money, and hassle. The process is self-serve, they don't have to directly speak with anyone to start or complete the process; and they can fill out the form whenever they like. Plus, form submitters can get real-time feedback via email confirmation that lets them know the form was submitted and it has been received.

Form Processor

eForms also benefit the forms creator and people processing the form. For example, the form can be a "smart" form in that it does things like require certain fields be completed, force users' answers to match certain values by controlling the type of data that is entered and captured, and they provide immediate feedback should an answer conflict or not meet requirements. This ensures only valid forms reach processing, saving even more time. Form data can also be captured into other systems, eliminating the need to re-enter form information.

Where can Electronic Forms be used?

When thinking about how your organization collects data, there are likely opportunities everywhere to embrace eForm technology.

Here are just a few examples of how you can benefit from using eforms and some of the types of forms that could be used.

- Accounting: Use for Purchase Orders, Expense Reports, Capital Expenditure Requests, Mileage Reimbursement.
- Human Resources: Use for Position Changes, I-9, Vacation Requests, Time Sheets, Employee Reviews.
- Engineering: Use for Defect Tracking, Engineering Change Orders, Product Enhancement Requests.
- Manufacturing: Use for Employee Training Certification, Safety Inspections, Document Change Requests, Quality Assurance Variances.
- Customer Service: Use for Survey forms, Customer Warranty Requests, Requests for customer service, incident reports.

The types of forms are endless. Virtually any circumstance where collecting and acting upon information or interacting with customers or employees are all great potentials for electronic forms technology.

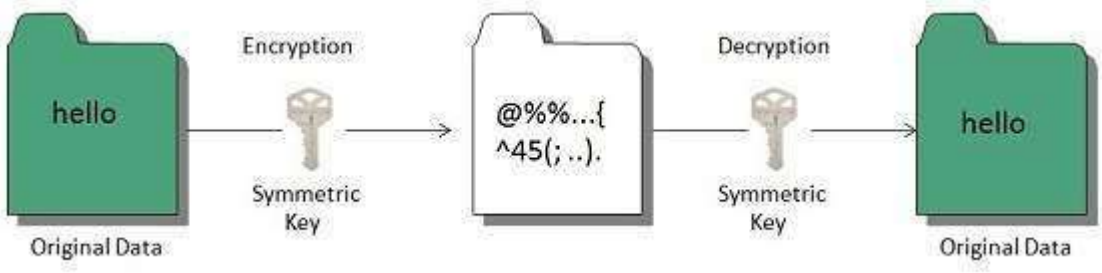
Encryption

The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text ;* encrypted data is referred to as *cipher text*.

There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.

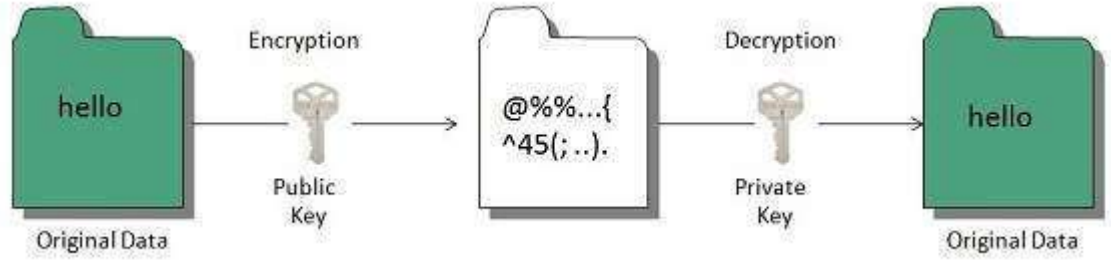
SYMMETRIC KEY ENCRYPTION

Symmetric key encryption algorithm uses same cryptographic keys for both encryption and decryption of cipher text.



PUBLIC KEY ENCRYPTION

Public key encryption algorithm uses pair of keys, one of which is a secret key and one of which is public. These two keys are mathematically linked with each other.



Data Security

Data security refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. Data security includes data encryption, tokenization, and key management practices that protect data across all applications and platforms.

Why Data Security?

Organizations around the globe are investing heavily in information technology (IT) cyber defense capabilities to protect their critical assets. Whether an enterprise needs to protect a brand, intellectual capital, and customer information or provide controls for critical infrastructure, the means for incident detection and response to protecting organizational interests have three common elements: people, processes, and technology.

Data Security Techniques

The following are broach techniques used in the field of Data Security to improve security.

Stop Collecting Unneeded Data

The last decade of IT management has seen a shift in how data is considered. Previously it was an asset: having more data was almost always better than less as you could never be sure ahead of time what you might want to do with it.

Today, data is a liability. The threat of a reputation-destroying data breach, loss in the millions or stiff regulatory fines all reinforce the thought that collecting anything beyond the minimum amount of sensitive data is extremely dangerous.

To that end: review all data collection procedures. Document why each data point is needed from a business stand point.

Purge Stale Data

Data that is not on your network is data that can't be compromised. Put in place systems that track file access and automatically archive files that haven't been accessed for years. In the modern age of near yearly acquisitions, reorganizations and "synergistic relocations" it's quite likely that networks of any significant size have multiple forgotten servers that are kept around for reasons no one is quite sure of.

Quarantine Sensitive Files

Earlier, we described a common scenario where a file containing sensitive data was placed on a share open to the entire company. Systems that continually classify data and take preemptive action to move those files to a secure location are worth their weight in gold as they dramatically shorten the length of time that data is not under the proper control.

Track User Behavior against Data Groups

The general term plaguing rights management within an organization is "overpermissioning'. That one-off, temporary projects or rights grants on the network rapidly become a baroque and convoluted web of interdependencies that result in users collectively having access to far more data on the network than they need for their role.

Systems that profile user behavior and automatically put in place permissions to match that behavior limits the potential damage that any one user (or malicious attacker who compromises their account) can do.

Respect Data Privacy

Data Privacy is a distinct aspect of cybersecurity dealing with the rights of individuals and the proper handling of data under your control. For more, read our Guide to Data Privacy

Data Security Regulations: GDPR, HIPAA and SOX

Regulations such as HIPAA (healthcare), SOX (public companies) and GDPR (anyone who knows that the EU exists) are best considered from a data security perspective. While there are other aspects of them, at their core they require that organizations:

- Track what kinds of sensitive data they possess
- Be able to produce that data on demand
- Prove to auditors that they are taking appropriate steps to safeguard the data

All of which fit not just comfortably within a data security mindset, but all but require it.

Practical Data Security

For companies that have a hold on data and have security obligations due to GDPR or other regulatory requirements, understanding what data security means at Varonis will help you manage and meet data protection and privacy regulations requirements.

The mission at Varonis is simple: your data is our primary focus, and our data security platform protects your file and email systems from cyber attacks and insider threats. We're fighting a different battle – so your data is protected first. Not last.

We continuously collect and analyze activity on your enterprise data, both on-premises and in the cloud. We then leverage five metadata streams to ensure that your organization's data has confidentiality, integrity, and availability.

Users and Groups – Varonis collects user and group information and maps their relationships for a complete picture of how user accounts are organized.

Permissions – We add the file system structure and permissions from the platforms that we monitor, and combine everything into a single framework for analysis, automation, and access visualization.

Access Activity – Varonis continually audits all access activity, and records & analyzes every touch by every user. Varonis automatically identifies administrators, service accounts and executives and creates a baseline of all activity. Now you can detect suspicious behavior, whether it's an insider accessing sensitive content, an administrator abusing their privileges, or ransomware like CryptoLocker.

Perimeter Telemetry – Varonis Edge analyzes data from perimeter devices such as VPN proxy servers, and DNS and combines this information with data access activity to detect and stop malware apt intrusions and data exfiltration.

Content Classification – We then scan for sensitive and critical data, and can absorb classification from other tools like DLP or e-Discovery. Now we know where sensitive data lives and where it's overexposed.

Access

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

Types of access control

The main types of access control are:

- **Mandatory access control (MAC)**: A security model in which access rights are regulated by a central authority based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system or security kernel, grants or denies access to those resource objects based on the information security clearance of the user or device. For example, Security Enhanced Linux is an implementation of MAC on the Linux operating system.
- **Discretionary access control (DAC):** An access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.
- **Role-based access control (RBAC):** A widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions -- executive level, engineer level 1 -- rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC frameworks.
- **Rule-based access control:** A security model in which the system administrator defines the rules that to govern access to resource objects. Often these rules are based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and role-based access control to enforce access policies and procedures.
- **Attribute-based access control (ABAC):** A methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.

Addressee

i. Addressee: The term is defined under Sec 2(b) of the Information Technology Act, "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary.

ii. Intermediary: The term is defined under Sec 2(w) of the IT Act, "intermediary" with respect to any particular electronic records means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.

iii. Originator: The term is defined under Sec 2(za) of the IT Act, "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.

Further, Sec 11 of the IT Act refers to the attribution of the electronic records, it states that any electronic communication can be attributed to the Originator if communication has been sent by originator or by the person authorized by the Originator or through an automatically operated information system.

Its an important element in electronic contract, as it helps to decide the obligation on the Parties. If an information was communicated either through a person authorized on behalf of Originator of through the automatic system, then it is deemed that communication has taken place.

Adjudicating Officer

The Information Technology Act, which has been passed by both the Houses of Parliament, has finally come into effect from Aug15, 2000. The draft Rules have also been framed and are presently being hosted on the official website of the Ministry of Information Technology for the purpose of inviting comments and suggestions from the general public.

Rule 3 of the draft Information Technology (Procedure for holding inquiry and imposing penalties by adjudicating officer) Rules, 2000, provides for the Central Government to appoint an adjudicating officer. However, such officer can be appointed only when the Central Government is of the opinion that there are grounds for adjudicating under Chapter IX of the Act. Neither the Act nor the Rules specify as to who is entitled to file a complaint/claim/petition under Chapter IX of the Act.

Further, neither the Act nor the Rules prescribe for an authority before which a claim/complaint/petition can be filed under Chapter IX of the Act. Therefore, the right to have one's grievance redressed under Chapter IX of the Act is still not a statutory right. It remains the subjective discretion of the Central Government to decide whether a contravention under Chapter IX has been committed and only when it is satisfied in this regard, it would appoint an adjudicating officer to inquire into the alleged contravention. It is still not clear as to who is to take the decision that a contravention deserves to be inquired into by the adjudicating officer. It is also not clear whether an adjudicating officer can be appointed suo motu by the government or only on a representation made.

Rule 5 of the same draft Rules prescribes that while adjudging the quantum of penalty under Section 43, 44 or 45, the adjudicating officer shall have due regard to the following factors namely :-

a. the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
b. the amount of loss caused to any person as a result of the default;
c. the repetitive nature of the default.

A contravention of Section 43 can result only in "damages by way of compensation payable to the person so affected" . No penalty can be imposed under this Section. When the Act itself does not provide for the payment of penalty under Section 43, there can be no question of the Rules empowering the AO to adjudge the quantum of penalty for a contravention under of Section 43 of the Act.

Another issue of concern is the enforceability of an order passed under Section 43 by the Adjudicating Officer. Neither the Act nor the Rules specifically provide for the execution of the AO's order, in the event of any compensation by way of damages being awarded by him. Since the order of the AO cannot be treated as a "decree", it is not capable of being executed by the Civil Courts. Therefore, any order passed by the AO under Section 43 would be a "toothless" order, incapable of being enforced. Assuming that the order of the AO becomes final, the only way of recovering dues under such an order would be to institute a Civil Suit (based on the AO's order), obtain a decree and execute the same. The very purpose of barring the jurisdiction of the Civil Court under Section 61 of the IT Act is therefore defeated.

The need of the hour is therefore to specify as to who is entitled to invoke chapter IX of the Act, prescribe the manner in which a complaint is to be filed under Chapter IX and also to specify the authority which is to decide whether an adjudicating officer is to be appointed or not.

It is also necessary for the lawmakers to immediately amend Section 43 of the Act and clearly spell out that a contravention of that provision could result not only in damages but in penalty as well. The Act also needs to be appropriately amended to specify the manner in which an order for payment of compensation by way of damages is to be enforced.

Affixing Digital Signatures

Affixing digital signature, with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature. [Information Technology Act, 2000 (21 of 2000), s. 2 (1) (d)].

Digital Signature Vs. Electronic Signature

The Information Technology Amendment Bill 2006, replaces the word "Digital" with the word "Electronic" at several places in the principal act, which creates a slight difference between the two, electronic signature is wide in nature, while the digital signature is one of the many kinds of electronic signature.

Section 2(ta) "electronic signature" means authentication of any electronic record by a subscriber by means of an electronic technique specified in the second schedule and includes digital signature and section 2(p) defined "Digital Signature Certificate" means a Digital Signature Certificate issued Under sub-section (4) of section 35.

Appropriate Government

In relation to public authority which is established, constituted, owned, controlled or substantially financed by funds provided directly or indirectly—

(i) by the Central Government or the Union Territory administration, the Central Government,

(ii) by the State Government, the State Government [Right to Information Act, 2005 (22 of 2005), s. 2(a)] The Appropriate Government means, in relation to fees or stamp relating to documents presented or to be presented before any officer serving under the Central Government, that Government, and in relation to any other fees or stamps, the State Government.

Certifying Authority

A certificate authority (CA) is a trusted entity that issues digital certificates, which are data files used to cryptographically link an entity with a public key. Certificate authorities are a critical part of the internet's public key infrastructure (PKI) because they issue the Secure Sockets Layer (SSL) certificates that web browsers use to authenticate content sent from web servers.

Uses of a certificate authority

The best-known use of certificate authorities is for issuing SSL certificates to entities that publish content on the web. Certificate authorities issue three levels of SSL certificate, corresponding to different levels of trust in those certificates. Certificates with higher levels of trust usually cost more because they require more work on the part of the certificate authority.

The three different levels of trusted certificates include:

1. **Extended Validation (EV)** certificates provide the highest level of assurance that the certificate authority has validated the entity requesting the certificate. The Certification Authority Browser Forum (CA/Browser Forum) spells out detailed requirements for the process that certificate authorities must apply when verifying information provided by the applicant for an EV certificate. For example, an individual requesting an EV certificate must be validated through face-to-face interaction with the applicant as well as review of a personal statement, one primary form of identification such as passport, driver's license or military ID, as well as two secondary forms of identification.
2. **Organization Validated (OV)** certificates provide the next highest level of assurance. Certificate authorities generally perform some level of vetting of the applicants, which may include telephone verification as well as use of external or third parties to confirm information submitted by the applicant.

   OV certificates can be issued if the applicant can demonstrate that it holds administrative control of the domain name for which the certificate is requested and that the organization can be shown to exist as a legal entity.
3. **Domain Validated (DV)** certificates require only that the applicant demonstrate ownership of the domain for which the certificate is being requested. DV certificates can be acquired almost instantly and at a low -- or no -- cost. For example, Let's Encrypt is a free service that can be used to get SSL certificates at no cost.

Certification Practice Statement

A Certification Practice Statement (CPS) is a notification from a certificate authority that shows how they handle elements of security processes. Certificate authorities are responsible for providing digital certificates for websites that provide security encryption.

Some elements of a CPS include documenting practices of:

- issuance
- publication
- archiving
- revocation
- renewal

By detailing the practice of issuance, revocation and renewal, a CPS aids entities in judging the relative reliability of a given certificate authority.

Certificate Authority

In a certificate authority, the CPS should derive from the organization's certificate policy and may be referenced in issued certificates

Web of trust

Because individuals act as certifiers in a web of trust, individual CPS documents are sometimes used. For example, in a PGP WoT, the CPS might state that the certifying entity checked two forms of legal government ID before signing the person's public key.

Digital signatures

When verifying digital signatures, it's necessary to review the CPS so as to determine the meaning of the issuance of the certificate by the certifying entity.

Part A (ONE Mark)
Multiple Choice Questions
Online Examination

Part B (2 Marks)

1. Define information technology act, 2000.
2. What is internet?
3. Discuss the Internet governance.
4. Define E- Contract.
5. Difference between shrink wrap and click wrap e- contracts.
6. What are the benefits of using e Forms.
7. Where can Electronic Forms be used?
8. Why Data Security?
9. Give note on i) Addressee ii) Adjudicating Officer
10. What is CPS?

Part C (8 Marks)

1. List out any eight offences and the corresponding penalties.
2. How the client/server system works explain with diagram.
3. Describe the basic www concepts.
4. Explain the Forms of Internet Governance with diagram.
5. Discuss the essentials of an electronic contract.
6. List out the types of electronic contract.
7. What is encryption and explain its type with diagram?
8. Describe the Data Security Techniques.
9. Explain the types of access control.
10. Explain the three different levels of trusted certificates.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed University Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2017 onwards)
DEPARTMENT OF COMMERCE (CA)

SUBJECT: : Cyber Crime and Laws
SEMESTER : VI
SUBJECT CODE: 17CCU604B CLASS : III B.COM CA
UNIT : II

S.NO	QUESTIONS	OPTION 1	OPTION 2	OPTION 3	OPTION 4	ANSWER
1	How much fine to be paid for tampering with computer source documents?	₹400,000	₹300,000	₹200,000	₹500,000	₹200,000
2	Which protocol will send the data in packets all over the internet?	HTTP	TCP/IP	SMTP	UDP	TCP/IP
3	Internet resources, information and services,are provided through	Servers	Clients	Customers	Browsers	Servers
4	The connection which is used between client and server is _____	HTTP	TCP/IP	SMTP	UDP	HTTP
5	Browser is_____on your computer that allows you to access the World Wide Web.	hardware	firmware	software	sharewar e	software
6	Documents with links that contain more than just text are called _____	netmedia	hyperme dia	textmedia	multime dia	hypermedi a
7	Which language is used to develop world wide web documents?	CSS	XML	SGML	HTML	HTML
8	_____ protocol used to transfer hypertext or hypermedia documents.	HTTP	SMTP	FTP	TCP	HTTP
9	Cheating another person using computer resources come under _____ section	66C	66D	66B	66A	66D
10	Which of the following which is not a browser?	Mozilla FireFox	Main frame	Apple Safari	Netscape Navigato r	Main frame
11	HTML stands for _____	Hypertex t markup language	Hypertra nsfer markup language	Hypertext medium language	Hypertra nsfer mid language	Hypertext markup language
12	Modem is a device attached to computer and_____to access internet	Pager	printer	telephone	Radio	telephone
13	The address of world wide web page is _____	FRL	URL	MRL	CRL	URL
14	_____is a vast network of independently-managed networks	Intranet	supernet	globalnet	internet	internet
15	E-Contract does not include _____	e-mail	Web forms	Phone conversati on	Online agreeme nts	Phone conversati on
16	A_____contract is the former license agreement required upon the buyer when he buys software	Click wrap	Shrink Wrap	Non disclosure	Consulta nt agreeme nt	Shrink Wrap
17	_____contract is typically requested by a party licensing software, to ensure maintenance of the software instead of abandonment or orphaning	Shrink Wrap	Software Develop ment and Licensin g	Source Code Escrow	Click wrap	Source Code Escrow
18	E-Forms provide a series of fields where data is collected, often using a _____.	browser	hub	server	host	browser
19	The translation of data into a secret code is called_____	Decrypti on	encryptio n	descriptio n	subscript ion	encryption
20	cipher text refers to_____file	Encrypte d	Decrypte d	Binarycod ed	Decimal coded	Encrypted
21	asymmetric encryption is also called_____encryption	Referenc e key	Source key	Public key	Private key	Public key
22	cryptography is the process of converting ordinary plain text into _____text and vice-versa.	decimal	Machine readable	cipher	decipher	cipher
23	Which of the following is not a data security?	Encrypti on	Token manage ment	tokenizati on	Packet transfer	Packet transfer
24	_____ access control limits connections to computer networks, system files and data.	Logical	Physical	conceptual	network	Logical
25	A security model in which access rights are regulated by a central authority based on multiple levels of security is called_____access control	Rule	Role	Discretion ary	Mandato ry	Mandatory
26	Lack of centralized control is disadvantage in_____access system	Attribute	Rule	Role	Discretio nary	Discretion ary

27	RBAC systems can be used to enforce_____and DAC frameworks.	MAC	AOC	ROC	TAC	MAC
28	_____ means a person who is intended by the originator to receive the electronic record but does not include any intermediary.	Addressee	Receiver	Orginator	Reciptor	Addressee
29	a dcode which is attached to an electronically transmitted document to verify its contents and the sender's identity is called _____	Internet signature	Digital signature	Web signature	Electronic signature	Digital signature
30	symbols or other data in digital form attached to an electronically transmitted document as verification of the sender's intent to sign the document is called _____	Internet signature	Digital signature	Web signature	Electronic signature	Electronic signature
31	A certificate authority (CA) is a trusted entity that issues digital certificates, which are data files used to cryptographically link an entity with a _____	primary key	public key	private key	partial key	public key
32	certificate authority (CA) issues_____certificates that web browsers use to authenticate content sent from web servers.	SSL	STL	SGL	SML	SSL
33	_____certificates provide the highest level of assurance	Extended Validation (EV)	Domain Validated	Technolgy Validated	Organization Validated	Extended Validation (EV)
34	Who is responsible for providing digital certificates for websites?	Domain authority	Digital authority	Certificate authority	Web authority	Certificate authority
35	CPS stands for_____.	Certification Practical Statement	Certification Planning Statement	Certification Practice Statement	Certification Projecting Statement	Certification Practice Statement
36	In_____protocol packets travel over many different between source and destination computers.	TCP/IP	UDP	FTP	SMTP	TCP/IP
37	Hypertext documents are represented using a specialised markup language called _____	HTML	XML	SGML	CML	HTML
38	ISP stands for_____	Internal service provider	Internet server provider	Internet service provider	Internal server provider	Internet service provider
39	_____is the process whereby cyberspace participants resolve conflicts	Internet governance	Internet Cyber	Internet resolver	Internet provider	Internet governance
40	Indian Contracts Act of_____will apply on any consultant agreement.	1874	1872	1873	1871	1872
41	Which of the following is a service and not sale of goods?	transmission of CD	transmission of book	transmission of software	transmission of hardware	transmission of software
42	prohibiting illegal creation of copies is come under which contract?	Non disclosure	Shrink wrap	Clip wrap	Consultant	Shrink wrap
43	To read a_____file, you must have access to a secret key or password	subscripted	ciberscripted	encrypted	decrypted	encrypted
44	The general term plaguing rights management within an organization is _____.	overthinking	overpermissioning	Overwriting	overwhelming	overpermissioning
45	Varonis is a_____platform that protects your file and email servers from cyberattacks and insider threats.	Data security	Data transmitting	Data analyzing	Data streaming	Data security
46	_____control is a security technique that regulates who or what can view or use resources in a computing environment	Access	Configure	Transmit	Security	Access
47	In Electronic forms data is collected using web _____	server	host	browser	storage	browser
48	_____encryption algorithm uses same cryptographic keys for both encryption and decryption of cipher text.	Asymmetric key	Public key	Primary key	Symmetric key	Symmetric key
49	Which algorithm uses public key for encryption and private key for decryption?	symmetric key	Private key	Primary key	ASymmetric key	ASymmetric key
50	"Digital Signature Certificate" means a Digital Signature Certificate issued Under sub-section (4) of section _____	35	25	55	45	35
51	Which certificates are needed to publish contents on the web	WSL	SSL	RSL	MSL	SSL
52	Which certification includes confirmation of the information submitted by using telephone or external or third parties	Enterprise Validated	Organization Validated	Extended Validated	Domain Validated	Organization Validated
53	Which of the following certificates acquired almost low or free cost	Extended Validated	Enterprise Validated	Domain Validated	Organization Validated	Domain Validated
54	When verifying_____, it's necessary to review the CPS	Internet	digital	Web	Electroni	digital

		signatures	signatures	signatures	c signatures	signatures
55	Which_____spells out detailed requirements for the process that certificate authorities must use to verify information	CA/Browser Forum	CA/Host Forum	CA/Server Forum	CA/Database Forum	CA/Browser Forum
56	How many levels of SSL certificates issued by Certificate Authority?	five	three	four	two	three
57	Cryptolocker is a_____threat that gained notoriety over the last years.	Firmware	Malware	Software	Hardware	Malware
58	URL stands for_____	unary resource locator	uniform resource locator	uniform reign locator	unary reign locator	uniform resource locator
59	How many years of imprisonment for receiving stolen computer or communication device?	five	three	two	four	three
60	Imprisonment for life is the punishment for which offense?	cyberterrorism	cybersniffing	cyberstalking	cybersquatting	cyberterrorism

UNIT-III

SYLLABUS

Computer: Computer Network, Computer Resource, Computer System, Cyber Appellate Tribunal, Data, Digital Signature, Electronic Form, Electronic Record, Information, Intermediary, Key Pair, Originator, Public Key, Secure System, Verify, and Subscriber as defined in the Information Technology Act, 2000.

Computer: Computer Network

Computer is an advanced electronic device that takes raw data as an input from the user and processes it under the control of a set of instructions (called program), produces a result (output), and saves it for future use.

A **computer network** is a system in which multiple computers are connected to each other to share information and resources.

Characteristics of a Computer Network

- Share resources from one computer to another.
- Create files and store them in one computer, access those files from the other computer(s) connected over the network.
- Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over the network.

Following is the list of hardware's required to set up a computer network.

- Network Cables
- Distributors
- Routers
- Internal Network Cards
- External Network Cards

Network Cables

Network cables are used to connect computers. The most commonly used cable is Category 5 cable RJ-45.

Distributors

A computer can be connected to another one via a serial port but if we need to connect many computers to produce a network, this serial connection will not work.

The solution is to use a central body to which other computers, printers, scanners, etc. can be connected and then this body will manage or distribute network traffic.

Router

A router is a type of device which acts as the central point among computers and other devices that are a part of the network. It is equipped with holes called ports. Computers and other devices are connected to a router using network cables. Now-a-days router comes in wireless modes using which computers can be connected without any physical cable.

Network Card

Network card is a necessary component of a computer without which a computer cannot be connected over a network. It is also known as the network adapter or Network Interface Card (NIC). Most branded computers have network card pre-installed. Network cards are of two types: Internal and External Network Cards.

Internal Network Cards

Motherboard has a slot for internal network card where it is to be inserted. Internal network cards are of two types in which the first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA). Network cables are required to provide network access.

External Network Cards

External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network.

Universal Serial Bus (USB)

USB card is easy to use and connects via USB port. Computers automatically detect USB card and can install the drivers required to support the USB network card automatically.

Computer Resource

A system resource is any usable part of a computer that can be controlled and assigned by the operating system so all of the hardware and software on the computer can work together as designed.

System resources can be used by users, like you, when you open programs and apps, as well as by services which are usually started automatically your operating system.

You can run low on system resources or even run completely out of a system resource since they're limited. Limited access to any particular system resource reduces performance and usually results in an error of some kind.

Examples of System Resources

System resources are often talked about in relation to system memory (your computer's RAM) but resources might also come from the CPU, the motherboard, or even other hardware.

While there are many individual segments of a complete computer system that could be considered *system resources*, there are generally four major resource types, all viewable and configurable from within Device Manager:

- Interrupt Requests (IRQ) Lines
- Direct Memory Access (DMA) Channels
- Input/Output (I/O) Port Addresses
- Memory Address Ranges

An example of system resources at work can be seen when you open any program on your computer. As the application is loading, the operating system is reserving a particular amount of memory and CPU time that the program needs to function. It does this by using system resources that are available at the present time.

System resources aren't unlimited. If you have 4 GB of RAM installed on your computer, but the operating system and various programs are using a total of 2 GB, you really only have 2 GB of system resources (in the form of system memory, in this case) that are readily available for other things.

If not enough memory is available, Windows will attempt to store some things in a *swap file* (or paging file), a virtual memory file stored on the hard drive, to free up memory for the program.

If even this pseudo-resource fills up, which happens when the swap file reaches its maximum possible size, Windows will start alerting you that "virtual memory is full" and that you should close down programs to free up some memory.

Computer System

A computer system is a basic, complete and functional computer, including all the hardware and software required to make it functional for a user.

It should have the ability to receive user input, process data, and with the processed data, create information for storage and/or output.

It s a system of hardware devices organized according to the following system functions:

Input

The input devices of a computer system include computer keyboards, touch screens, pens, electronic mice, and optical scanners. They convert data into electronic form for direct entry or through a telecommunications network into a computer system.

Processing

The central processing unit (CPU) is the main processing component of a computer system. (In microcomputers, it is the main microprocessor. Conceptually, the circuitry of a CPU can be subdivided into two major subunits: the arithmetic-logic unit and the control unit. The electronic circuits (known as registers) of the arithmetic-logic unit perform the arithmetic and logic functions required to execute software instructions.

Output

The output devices of a computer system include video display units, printers, and audio response units. They convert electronic information produced by the computer system into human-intelligible form for presentation to end users.

Storage

The storage function of a computer system takes place in the storge circuits of the computer's primary storage unit, or memory, supported by secondary storage devices such as magnetic disk and optical disk drives. These devices store data and software instructions needed for processing. Computer processors may also include storage circuitry called cache memory for high-speed, temporary storage of instruction and data elements.

Control

The control unit of a CPU is the control component of a computer system. Its registers and other circuits interpret software instructions and transmit directions that control the activities of the other components of the computer system.

Cyber Appellate Tribunal

Cyber Appellate Tribunal was established under the Information Technology Act, 2000. The first Cyber Appellate Tribunal in India was formed by the Central Government in accordance with the provisions described under Section 48(1) of the Information Technology Act, 2000.

The Cyber Appellate Tribunal is not guided or governed by the Code of Civil Laws but is guided by the principle of Natural Justice. It has the same power as a Civil Court.

The Cyber Appellate Tribunal has powers to regulate its own procedure including the place at which it has its sittings. Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228 and for the purposes of section 196 of the Indian Penal Code and the Cyber .Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

Procedure and powers of the Cyber Appellate Tribunal. –

(a) Calling and binding the attendance of any person and examining him on oath;
(b) Demanding the discovery and production of documents or other electronic records;
(c) Receiving evidence on affidavits;
(d) Issuing commissions for the examination of witnesses or documents;
(e) Reviewing its decisions;
(f) Dismissing an application for default or deciding it ex parte;
(g) Any other matter which may be prescribed.

Data

Data is distinct pieces of information, usually formatted in a special way. All software is divided into two general categories: data and programs. Programs are collections of instructions for manipulating data.

Data can exist in a variety of forms — as numbers or text on pieces of paper, as bits and bytes stored in electronic memory, or as facts stored in a person's mind. Since the mid-1900s, people have used the word data to mean computer information that is transmitted or stored.

Data are the values of subjects with respect to qualitative or quantitative variables.

Data and information are often used interchangeably; however, the extent to which a set of data is informative to someone depends on the extent to which it is unexpected by that person.

Data is measured, collected and reported, and analyzed, whereupon it can be visualized using graphs, images or other analysis tools. Data as a general concept refers to the fact that some existing information or knowledge is *represented* or *coded* in some form suitable for better usage or processing. *Raw data* ("unprocessed data") is a collection of numbers or characters before it has been "cleaned" and corrected by researchers.

Raw data needs to be corrected to remove outliers or obvious instrument or data entry errors (e.g., a thermometer reading from an outdoor Arctic location recording a tropical temperature). Data processing commonly occurs by stages, and the "processed data" from one stage may be considered the "raw data" of the next stage. Field data is raw data that is collected in an uncontrolled "in situ" environment. Experimental data is data that is generated within the context of a scientific investigation by observation and recording. Data has been described as the new oil of the digital economy.

Digital Signature

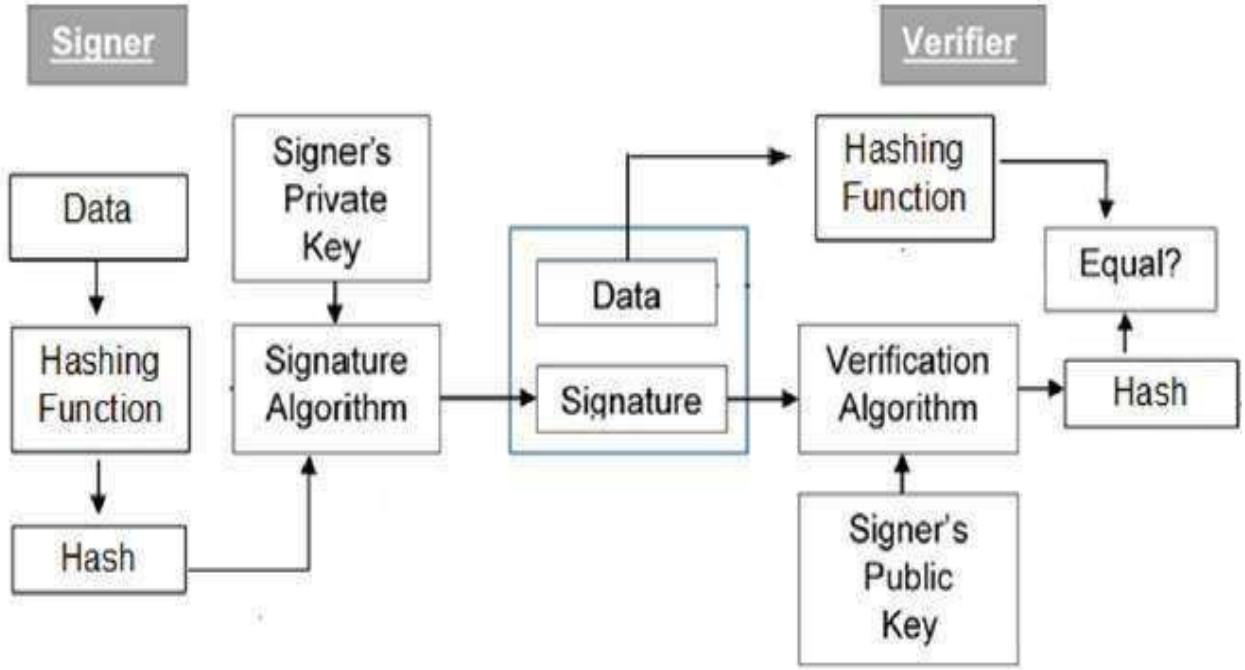
Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration −



The following points explain the entire process in detail −

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created.

Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence **signing a hash is more efficient than signing the entire data**.

Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

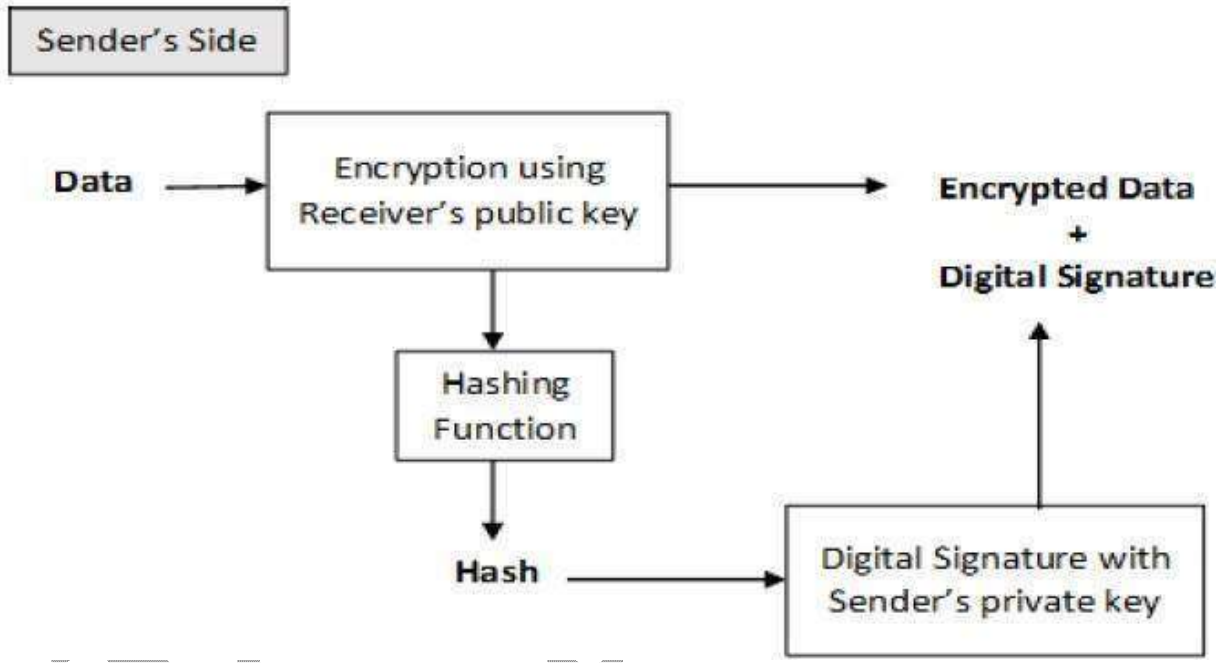
Encryption with Digital Signature

In many digital communications, it is desirable to exchange an encrypted messages than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing PKC for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

This can archived by combining digital signatures with encryption scheme. Let us briefly discuss how to achieve this requirement. There are **two possibilities, sign-then-encrypt** and **encrypt-then-sign**.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration −



The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.

Electronic Form

A webform, web form or HTML form on a web page allows a user to enter data that is sent to a server for processing. Forms can resemble paper or database forms because web users fill out the forms using checkboxes, radio buttons, or text fields.

6 types of electronic forms

We propose that this spectrum in electronic forms can be divided up into 6 levels:

Level	Name	Content
1	"Static"	Electronic distribution
2	"Editable"	Level 1 plus typing
3	"Fillable"	Level 2 plus form widgets
4	"Validating"	Level 3 plus feedback based on internal rules
5	"Smart"	Level 4 plus form changes based on internal rules
6	"Connected"	Level 5 plus connectivity

These levels will make more sense after reading the descriptions and examples below.

Level 1: Static

This is the previously described lowest level of the electronic forms spectrum. The form is essentially a paper form distributed electronically. It could just as easily be posted or faxed, for all the interactivity and intelligence it has (i.e. none). Also, getting data from the form to a database or system is usually manual (e.g. data entry from printouts).

Level 2: Editable

At this level, the form-filler can type into the form but it does not respond intelligently. The form must be printed or saved and attached to an email to be submitted. In most cases, manual processes are still required to get data from the form into a database or system.

An example of a Level 2 form is a Microsoft Word document that has been prepared *without*using any specific forms functionality. In such a form, the places where data should be entered are often indicated by rows of underscores, dotted lines or tables.

Level 3: Fillable

Level 3 is where electronic forms begin to offer real value. The use of form widgets — such as drop down boxes — reduces both errors and workload, as there are now limitations on the type of data that can be entered.

This is the first level at which data may be able to be programmatically extracted from the form and placed into a database. Whether this can be done, however, depends on how the form has been developed.

Examples of Level 3 forms include:

- Fillable PDFs
- Word forms
- Web forms (i.e. forms that are filled out using a Web browser like Internet Explorer or Firefox).

Level 4: Validating

The change between Level 3 and Level 4 is the introduction of interactivity. At Level 4, the form *provides feedback* in response to entries from the form-filler. This feedback is triggered by rules that are 'internal', i.e. contained entirely within the form.

Validation is the typical Level 4 interactivity. Validation is the checking of answers provided against definitions of what is acceptable. For example, a Level 4 form will report back if mandatory fields have been left unanswered.

Level 5: Smart

Level 5 forms now have two ways that they can respond to form-filler answers:

- present feedback; *and*
- modify the form itself.

When we talk about modifying the form itself in response to answers provided, we are most often referring to as 'conditional branching'. For example, it doesn't make sense (usually!) to ask a male respondent if they are pregnant. The question on pregnancy is *conditional* upon the answer to the question about the respondent's sex. In Level 5 forms, this branching is managed for the respondent and the form adapts to ensure that the respondent is not burdened with irrelevant questions.

Level 6: Connected

Level 6 is the highest level in the electronic forms spectrum. Forms at this level have full interactivity and intelligence thanks to connections with either a network or the Internet (or both). These connections allow the form to:

- apply rules that rely on external data (e.g. check that a requested business name isn't already registered); and
- submit data directly to a database.

Therefore, level 6 forms can leverage all that the electronic medium provides.

Most Level 6 forms are interactive applications (e.g. on the desktop) or web forms. This is because these platforms provide the connectivity and programming capability that enable Level 6 forms.

8 Reasons Why E-Forms Can Transform Your Business

1 -- Eliminate the Paper from the Beginning.

E-forms are more than just an electronic version of a paper form. They promptly capture, verify, approve and integrate data with the critical business systems used to run organizations. When information is automatically captured and distributed without a paper form to begin with, business processes are streamlined, efficiency is improved, costs are cut and your organization becomes a little greener.

2 -- Release the Information Needed to Run Your Business.

Most of the information needed to run your business is trapped on paper and paper equivalents such as Word® documents, PDF files and pre-printed forms. By capturing and moving crucial information—previously trapped —into core business systems faster and more affordably, e-forms enable organizations to improve customer service, shorten cycle times and lower operating costs.

3 -- Integrate Data with Core Business Systems Automatically.

Once submitted, data entered on an e-form can be saved to one or more business system databases automatically and seamlessly. With two-way integration, an existing database can pre-fill a form, allowing for confirmation of information and elimination of user error. Integration is secure and works within an organization's IT architectural structure and standards. Data captured on e-forms are typically sent to HR, finance, customer support and custom applications. The e-forms themselves reside within an electronic content management system for secure storage, retrieval, distribution and management.

4 -- Improve Data Accuracy.

Auto drop down lists and completion guides with field-specific instructions ensure data is captured accurately and completely. E-forms can auto-populate fields based on prior data entered and validate field-level data and form-level completeness before submission. Without the need for someone to manually enter data from a paper form into another system, data entry errors are eliminated and no data is lost in transcription.

5 -- Kick off Automated Workflow.

Once submitted, e-forms can implement an automated workflow based on an organization's business rules. Employee applications can be distributed to the appropriate individual in HR for review, sales orders can be sent to a manager for approval and then on to distribution for delivery, credit applications can be sent to the appropriate manager in the finance department for immediate review and approval. Automated workflow is seamless, quick and ensures accountability.

6 -- Digitally Signed E-Forms are legally binding.

Digital signature technology allows users to sign an e-form without the need for distributed digital certificates or third party certificate authorities. Existing login ID/Passwords can be used for signing e-forms and built-in encryption tools allow for secure transmission of data.

7 -- Easy to Design & Set Up.

E-forms are easy to design, create and publish with no programming skills required. Features such as drag and drop, pre-built field validation controls and group controls ensure sophisticated layouts with trouble-free design and implementation. Existing paper forms and PDFs can be easily copied or customized so screens can have a familiar user interface to speed adoption.

8 -- Realize a Quick ROI.

E-forms can deliver an ROI in as little as a few months, depending upon the number of forms processed monthly. Form completion costs, processing costs and correction costs are radically reduced. Paper related expenses, such as supplies, storage and transportation, are eliminated altogether.

Electronic Record

Electronic records are those which require a machine to be read. This refers to computer-generated records, and also those stored on visual and aural media such as voicemail systems, DVDs, videotapes, cinematographic film, cassette tapes, compact discs, mini-discs and microforms such as microfiche and microfilm etc. Examples of **electronic records** include: e-mail messages, word-processed documents, **electronic** spreadsheets, digital images and databases.

Benefits of electronic records

- Technologies such as e-mail, facsimile and conference calling facilitate rapid transmission of documents and information and enable quicker transaction of business.
- Electronic records are easily amended and updated.
- Electronic record formats such as geographic information systems, film and sound recordings, add vivid and interesting visual dimensions to written records.
- Electronic records use space much more efficiently than paper records. For example, a huge database may be stored on a single compact disc but if its contents were printed off or created in a paper format, it would be much more costly in terms of required storage.
- Paper formats cannot adequately capture some records, for example, a written description will not have the same impact as a film recording.
- Electronically stored records, specifically those stored on computer, are more easily accessible than those stored on paper.
- Electronic devices are modern, efficient, streamlined and attractive to users.
- Computer-generated records, for example, those stored in a database format may generally be retrieved very rapidly.

Challenges advanced by electronic records

1: **Obsolescence**

Obsolescence is a concern with both electronic hardware and software. For instance, the prevalence of videotapes is currently being threatened by the emergence of DVDs; floppy disks have changed radically in terms of physical size and capacity in the past decade and have now been outstripped by zip disks and the various types of compact discs that are on the market; the functionality of computer software changes rapidly as new versions come on-stream.

2: **Security**

Measures should be implemented to ensure that records stored electronically are secure. Records should be inviolate or tamperproof; secure from unauthorised access and accidental or deliberate removal and alteration. This is particularly important if records are tendered as evidence in a legal case. (Incidentally, an observation that merits mention is that many databases do not fulfil the definition of records, and instead are mere information. Criteria of records are that they must be fixed and linked to a specific business function. Many databases are generic banks of changing information, for example, containing names and other details of contacts or biographical and academic information relating to the student body.

3: **Technical expertise**

In order that the benefits of technology and electronic records are fully exploited, and effectively managed, expertise should be readily available.

4: **Ownership and custody**

This section deals with the custody of electronic records. This involves and complicates several other issues. In common with other records, electronic records must be retained for as long as they are required. While this is not problematic where records are only required for a short and defined period of time, some electronic records possess continuing value and will be retained on a permanent basis as archives. In the last few hundred years, archives services, have for the most part, centralised archives, that is, taken custody of them. This tradition has begun to change with reference to electronic records and because of a lack of availability of three resources: money, expertise and time.

5: **System compatibility**

A frequently encountered problem arises where a hybrid record-keeping system is in operation, that is, one reliant on both paper and electronic mechanisms. A common example would be where incoming correspondence is retained on paper files and outgoing correspondence created electronically is retained in an electronic medium. In order for the record-keeping system to be complete and accurate, there must be links between the paper and electronic systems. If not, information and evidence will be retrieved inaccurately and in an incomplete manner.

6: **Authenticity**

Because electronic records may be amended at the touch of a button, for example, overwritten, deleted or altered, it is difficult to prove what the original or authentic record comprised. Alteration of records may have serious legal consequences.

Information

It means, "information" includes data, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;

Information is any entity or form that provides the answer to a question of some kind or resolves uncertainty. It is thus related to data and knowledge, as data represents values attributed to parameters, and knowledge signifies understanding of real things or abstract concepts. As it regards data, the information's existence is not necessarily coupled to an observer (it exists beyond an event horizon, for example), while in the case of knowledge, the information requires a cognitive observer.

Information is conveyed either as the content of a message or through direct or indirect observation. That which is perceived can be construed as a message in its own right, and in that sense, information is always conveyed as the content of a message.

Information can be encoded into various forms for transmission and interpretation (for example, information may be encoded into a sequence of signs, or transmitted via a signal). It can also be encrypted for safe storage and communication.

Information reduces uncertainty. The uncertainty of an event is measured by its probability of occurrence and is inversely proportional to that. The more uncertain an event, the more information is required to resolve uncertainty of that event. The bit is a typical unit of information, but other units such as the nat may be used. For example, the information encoded in one "fair" coin flip is $\log_2(2/1) = 1$ bit, and in two fair coin flips is $\log_2(4/1) = 2$ bits.

The concept that *information is the message* has different meanings in different contexts. Thus the concept of information becomes closely related to notions of constraint, communication, control, data, form, education, knowledge, meaning, understanding, m ental stimuli, pattern, perception, representation, and entropy.

Intermediary

It means "intermediary" with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

Section 79 of the Information Technology Act, 2000 (I.T. Act, 2000) deals with the liability of the Network Service Providers. The explanation to this section provides that 'Network Service Providers' means an 'Intermediary'. According to Section 2 (w) 'Intermediary', with respect to any particular electronic message "means any person who on behalf of another receives, stores or transmits that message or provides any service with respect to that message."

Role of Intermediaries

Various types of intermediaries are involved in delivering content online to the end-users, since making a work available over the Internet involves a chain of intermediate service providers. For e.g., a person who is interested in launching a website will first obtain an account with a hosting service provider and then will upload web pages onto his web site which is physically located on the host's 'server' and which can be very well described as a very large hard disc which is directly accessible on the Internet. When the information is stored on the server, the uploaded documents become instantly available to all those with a connection to the Internet.

An access provider in turn provides access to the Internet. On the way from host to access provider to end user, the transported document passes through the infrastructure of a network provider, who apart from providing the physical facilities to transport a signal, also transmits and routes it to the designated recipient. It is quiet common for a single legal entity to provide the complete range of these services.

Hence, ISPs play an instrumental role in transmitting or disseminating third party content, but neither initiates nor takes any part in a decision to disseminate any particular material.

ISPs perform the following tasks:

- Provides access to the network.
- Website building and hosting.
- Hosting mailing list, e-mail services.
- Act as an intermediary with respect to any particular electronic message between an originator and an addressee but is himself none of them.
- Offer electronic news, storage space, games and other entertainment; or
- Simply receive data, convert that data into a form consistent with the IP protocol and forward the results to independent computers that in turn provide richer services and interactions.

They control the point at which information residing on a privately owned computer network first comes in contact with the public network. They control the gateway through which every legal and illegal act and information enters and re-enters the public network. It can be said that ISP may act as an 'information carrier' or as 'information publisher' depending upon the nature of its functions.

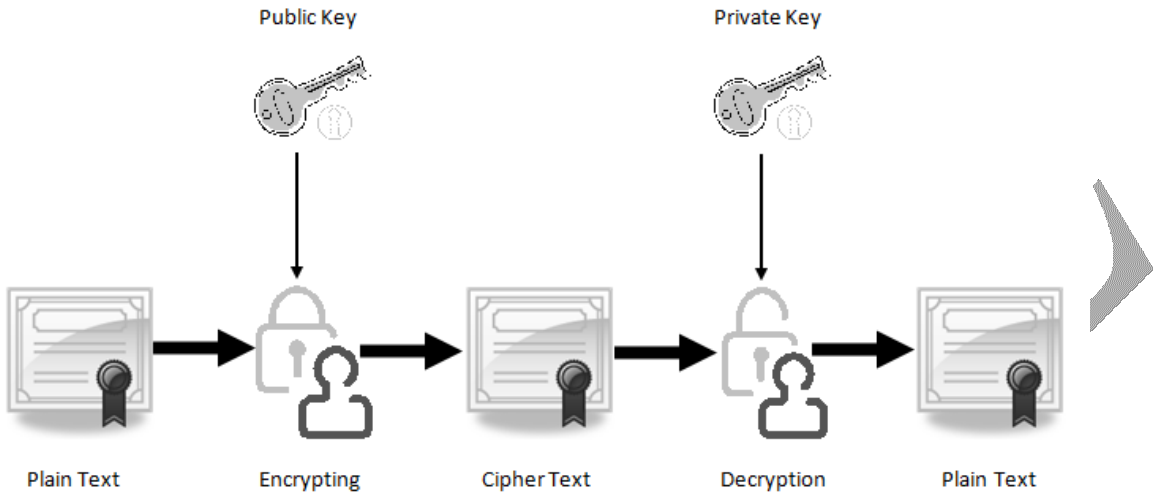
Key Pair

"key pair", in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key.

Private Key and public key are a part of encryption that encodes the information. Both keys work in two encryption systems called symmetric and asymmetric. Symmetric encryption (private-key encryption or secret-key encryption) utilize the same key for encryption and decryption.

Asymmetric encryption utilizes a pair of keys like public and private key for better security where a message sender encrypts the message with the public key and the receiver decrypts it with his/her private key.

Public and Private key pair helps to encrypt information that ensures data is protected during transmission.



Public Key:

Public key uses asymmetric algorithms that convert messages into an unreadable format. A person who has a public key can encrypt the message intended for a specific receiver. The receiver with the private key can only decode the message, which is encrypted by the public key. The key is available via the public accessible directory.

Private Key:

The private key is a secret key that is used to decrypt the message and the party knows it that exchange message. In the traditional method, a secret key is shared within communicators to enable encryption and decryption the message, but if the key is lost, the system becomes void. To avoid this weakness, PKI (public key infrastructure) came into force where a public key is used along with the private key. PKI enables internet users to exchange information in a secure way with the use of a public and private key.

Key Size and Algorithms:

There are RSA, DSA, ECC (Elliptic Curve Cryptography) algorithms that are used to create a public and private key in public key cryptography (Asymmetric encryption). Due to security reason, the latest CA/Browser forum and IST advises to use 2048-bit RSA key. The key size (bit-length) of a public and private key pair decides how easily the key can be exploited with a brute force attack. The more computing power increases, it requires more strong keys to secure transmitting data.

Originator

Under Sec 2(za) of the IT Act, "originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary.

Further, Sec 11 of the IT Act refers to the attribution of the electronic records, it states that any electronic communication can be attributed to the Originator if communication has been sent by originator or by the person authorized by the Originator or through an automatically operated information system.

Its an important element in electronic contract, as it helps to decide the obligation on the Parties. If an information was communicated either through a person authorized on behalf of Originator of through the automatic system, then it is deemed that communication has taken place.

Public Key

"public key" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

Public-key refers to a cryptographic mechanism. It has been named public-key to differentiate it from the traditional and more intuitive cryptographic mechanism known as: symmetric-key, shared secret, secret-key and also called private-key.

Symmetric-key cryptography is a mechanism by which the same key is used for both encrypting and decrypting; it is more intuitive because of its similarity with what you expect to use for locking and unlocking a door: the same key. This characteristic requires sophisticated mechanisms to securely distribute the secret-key to both parties2.

Public-key on the other hand, introduces another concept involving key pairs: one for encrypting, the other for decrypting. This concept, as you will see below, is very clever and attractive, and provides a great deal of advantages over symmetric-key:

- Simplified key distribution
- Digital Signature
- Long-term encryption

However, it is important to note that symmetric-key still plays a major role in the implementation of a Public-key Infrastructure or *PKI*.

Digital Signature and Verification

Digital signature is a mechanism by which a message is authenticated i.e. proving that a message is effectively coming from a given sender, much like a signature on a paper document. For instance, suppose that Alice wants to digitally sign a message to Bob. To do so, she uses her private-key to encrypt the message; she then sends the message along with her public-key (typically, the public key is attached to the signed message). Since Alice's public-key is the only key that can decrypt that message, a successful decryption constitutes a Digital Signature Verification, and meaning that there is no doubt that it is Alice's private key that encrypted the message.

Secure System

"secure system" means computer hardware, software, and procedure that—

(a) are reasonably secure from unauthorized access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

10 safety tips to help you guard against high-tech failure:

Technology continues to be a boon for entrepreneurs, offering increased mobility, productivity and ROI at shrinking expense. But as useful as modern innovations such as smartphones, tablet PCs and cloud computing are to small businesses, they also present growing security concerns.

1. Protect with passwords. This may seem like a no-brainer, but many cyber attacks succeed precisely because of weak password protocols. Access to all equipment, wireless networks and sensitive data should be guarded with unique user names and passwords keyed to specific individuals. The strongest passwords contain numbers, letters and symbols, and aren't based on commonplace words, standard dictionary terms or easy-to-guess dates such as birthdays. Each user should further have a unique password wherever it appears on a device or network. If you create a master document containing all user passcodes, be sure to encrypt it with its own passcode and store it in a secure place.

2. Design safe systems. Reduce exposure to hackers and thieves by limiting access to your technology infrastructure. Minimize points of failure by eliminating unnecessary access to hardware and software, and restricting individual users' and systems' privileges only to needed equipment and programs.

Whenever possible, minimize the scope of potential damage to your networks by using a unique set of email addresses, logins, servers and domain names for each user, work group or department as well.

3. Conduct screening and background checks. While rogue hackers get most of the press, the majority of unauthorized intrusions occur from inside network firewalls. Screen all prospective employees from the mailroom to the executive suite. Beyond simply calling references, be certain to research their credibility as well. An initial trial period, during which access to sensitive data is either prohibited or limited, is also recommended. And it wouldn't hurt to monitor new employees for suspicious network activity.

4. Provide basic training. Countless security breaches occur as a result of human error or carelessness. You can help build a corporate culture that emphasizes computer security through training programs that warn of the risks of sloppy password practices and the careless use of networks, programs and devices. All security measures, from basic document-disposal procedures to protocols for handling lost passwords, should be second-nature to members of your organization.

5. Avoid unknown email attachments. Never, ever click on unsolicited email attachments, which can contain viruses, Trojan programs or computer worms. Before opening them, always contact the sender to confirm message contents. If you're unfamiliar with the source, it's always best to err on the side of caution by deleting the message, then potentially blocking the sender's account and warning others to do the same.

6. Hang up and call back. So-called "social engineers," or cons with a gift for gab, often prey on unsuspecting victims by pretending to be someone they're not. If a purported representative from the bank or strategic partner seeking sensitive data calls, always end the call and hang up. Then dial your direct contact at that organization, or one of its public numbers to confirm the call was legitimate. Never try to verify suspicious calls with a number provided by the caller.

7. Think before clicking. Phishing scams operate by sending innocent-looking emails from apparently trusted sources asking for usernames, passwords or personal information. Some scam artists even create fake Web sites that encourage potential victims from inputting the data themselves. Always go directly to a company's known Internet address or pick up the phone before providing such info or clicking on suspicious links.

8. Use a virus scanner, and keep all software up-to-date. Whether working at home or on an office network, it pays to install basic virus scanning capability on your PC. Many network providers now offer such applications for free. Keeping software of all types up to date is also imperative, including scheduling regular downloads of security updates, which help guard against new viruses and variations of old threats.

9. Keep sensitive data out of the cloud. Cloud computing offers businesses many benefits and cost savings. But such services also could pose additional threats as data are housed on remote servers operated by third parties who may have their own security issues. With many cloud-based services still in their infancy, it's prudent to keep your most confidential data on your own networks.

10. Stay paranoid. Shred everything, including documents with corporate names, addresses and other information, including the logos of vendors and banks you deal with. Never leave sensitive reports out on your desk or otherwise accessible for any sustained period of time, let alone overnight. Change passwords regularly and often, especially if you've shared them with an associate. It may seem obsessive, but a healthy dose of paranoia could prevent a major data breach.

The average cost to an organization to recover from such a breach is $6.75 million, according to Javelin Strategy & Research. And that doesn't count damage to your reputation or relationships. So be proactive and diligent about prevention. An ounce far outweighs a pound of cure.

Verify

"verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether—

(a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

Subscriber

"subscriber" means a person in whose name the [Electronic Signature] Certificate is issued;

Duties of subscriber

1. Generating key pair (Section 40)

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

2. Acceptance of Digital Signature Certificate (Section 41)

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorises the publication of a Digital Signature Certificate-

(a) to one or more persons;

(b) in a repository, or

otherwise demonstrates his approval of the Digital Signature Certificate in any manner,

(2) By accepting a Digital Signature the subscriber certifies to all who reasonable rely on the information contained in the Digital Signature Certificate that-
(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true.;
(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

3. Control of private key (Section 42)

(1) Every subscriber shall exercise shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.
(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without and delay to the Certifying Authority in such manner as may be specified by the regulations.
Explanation- For the removal of doubts, it is hereby declared that the subscriber shall be liable to till he has informed the Certifying Authority that the private key has been compromised.

Information Technology Act, 2000

Introduction to Cyber Crimes in India Crime, in whatever forms it is, directly or indirectly, always affects the society. In today's world, there is immense increase in the use of Internet in every field of the society and due to this increase in usage of Internet, a number of new crimes have evolved. Such crimes where use of computers coupled with the use of Internet is involved are broadly termed as Cyber Crimes.

But under Indian law "Cybercrime" as such has not been defined under any legislation. One legislation that deals with the offences related to such crimes in India is Information Technology Act, 2000, which was also further amended in the form of IT Amendment Act, 2008. But these two important legislations also do not include any definition for "cybercrime". If looked into practicality, it is not at all easy to define this term. In order to define such an offense, when the nature of such offense is seen, it is a combination of crime and computer. So, it can be said that, when in commission of any offense computer is used, that can be termed as "cyber crime". Now, the question arises as to what the term "cyber law" will be compromised of. By looking at the working definition of cybercrime, one can reach a conclusion that cyber law is a term which is related to all the legal issues involving computer and Internet. It is even more difficult to come up with a definition for the term cyber law as it is an intersection of various fields. It involves privacy issues, jurisdiction issues, intellectual property rights issues and a number of other legal questions.

In India, what can basically be termed as cyber law are the IT act 2000 and its amended version in the form of the IT (Amendment) act, 2008.

The Information Technology Act, 2000 basically deals with the legal recognition of electronic documents and that of digital signatures. This Act incorporates a separate Chapter XI entitled "Offences" to deal with various cyber crimes and contraventions. This act also deals with Justice dispensation systems for various cyber crimes. The act was widely criticised on various fronts and due this criticism detailed amendments were brought in the form of IT Amendment Act, 2008. Major of such amendments were the focus on data privacy and information security.

Even though legal recognition of digital signatures was already included under the original Act of 2000, but the Amendment Act, 2008 made the digital signature technology-neutral. Along with, the defining of reasonable security practices to be followed by the Corporate, the role of intermediaries was also redefined. Very importantly, the term "cyber cafe" was defined under this Act. Offences like child pornography and cyber terrorism were also included is the forms of cyber crimes. Cyber terrorism has been made a heinous cyber crime under this Act and has been defined in the widest possible terms and made punishable with imprisonment which may extend to imprisonment for life and fine.

An important change that has been brought forth by the Amendment Act is that the new amendment has replaced Section 43 with Section 66. Under Section 66 the Word "hacking" has been removed, but that does not mean that "hacking" as an offence has been removed; instead hacking still remains an offence by the name of "data theft" in this section. This section has further been widened in the form of Sections 66A to 66F.

66A deals with the sending of offensive messages through communication service, and causing annoyance to any electronic communication, and also includes the offence of misleading the recipient of the origin of such messages. Such offences can be punished with imprisonment for 3 years or fine. 66B deals with dishonestly receiving stolen computers or other communication device and such a crime can be punished with three years of imprisonment or fine of Rs.1 Lakh or both. 66C deals with stealing electronic signature or identity such as using another persons' password or electronic signature, such an offence can be punished with three years of imprisonment or fine of Rs. 1 lakh or both. Similar is the punishment under section 66D for cheating by personation through computer resource or a communication device. 66E covers the offences relating to privacy violation such as publicly publishing the information about any person's location without prior permission or consent. 66F is great importance as it deals with cyber terrorism.

This Section covers a wide range of offences which can be termed as terrorism; Such as, any act denying access to any authorised person to access the computer in order to hamper the unity, integrity, security or sovereignty of the nation. Further, this section also includes the acts of access to a commuter resource without authorisation.

It also covers such acts which can lead to any injury to any person or result in damage or destruction of any property, while trying to contaminate the computer through any virus like Trojan etc. All the offences that are covered under this Section can be punished with life imprisonment. Very importantly, the offences which are covered under section 66 are cognizable and non-bailable. The major transformation from section 43 of the original act to Section 66 of the Amendment Act is that, that all the offences that were covered under Section 43 gave rise to civil liability which had its remedy in either compensation or damages. But under Section 66 of the Amendment Act if such act is done with criminal intention that is mens rea, then it will attract criminal liability having remedy in imprisonment or fine or both.

Moreover, under Sections 71, 72, 73 of the Information Technology Act 2000 some acts or omissions have been made criminally liable with strict liability e.g. Penalty for breach of confidentiality and privacy, penalty for misrepresentation etc. Section 67 of the original Act dealt with publishing or transmitting obscene material in electronic form but the scope of this section was widened by the amendment which included child pornography under section 67-B and also the act of retention of records by the intermediaries. And such offences under section 67-A will be punished with conviction of a term up to 3 years and fine of Rs.5 lakh and in case it is the second conviction then conviction will be for five years and fine of Rs.10 Lack or both. But for offence under section 67-B the provision is for stricter conviction which is for 5 years and fine of Rs. 10 Lakh or both in case of first conviction, and the same will be increased to 7 years and fine of Rs. 10 lakh in case of second conviction.

To conclude it can be said that, it has been provided in the preamble of the Information Technology Act 2000 that this act was passed in order to give legal recognition for transactions done through electronic means, and to improve further, this act has also made amendments to the Indian Penal Code 1860, Indian Evidence Act 1872, The Bankers Books of Evidence Act 1891, and the Reserve Bank of India Act 1934 in order to further the same objective. This act has defined various offences and also has laid down certain penalties as well. This act in a way has characterised the cyber crimes, which were earlier unknown to general public in India. This Act has made Cyber offences to be investigated only by a Police Officer not below the rank of the Inspector((now), Deputy Superintendent of Police((earlier). Even though this piece of legislation has proved to be a big leap in the field of cyber crimes, there still is a need for further changes which can improve its efficacy such as there is lack of effective mechanism for the appropriate retention of electronic evidence. So, an effective methodology in that regard can be chalked out.

Part A (ONE Mark)
Multiple Choice Questions
Online Examination

Part B (2 Marks)

1. What is computer and computer network?
2. What are the characteristics of computer network?
3. Define computer resource.
4. Define Cyber Appellate Tribunal.
5. What is data?
6. Discuss the importance of digital signature.
7. What is Encryption with Digital Signature?
8. Describe the electronic record and its benefits.
9. Give note on i) Information ii) intermediary

Part C (8 Marks)

1. List out the hardware's required to set up a computer network.
2. Write about computer system and how could organized hardware devices to system functions.
3. Describe the Cyber Appellate Tribunal and its procedure and powers.
4. What is a digital signature and explain its process with diagram.
5. List out the six types of electronic forms.
6. Discuss the reasons why E-Forms can transform your Business.
7. What are the advanced challenges available in electronic records?
8. Discuss the role of Intermediaries.
9. Brief note on i) Key Pair ii) Originator
10. Give some safety tips to secure system against high-tech failure.
11. Who is subscriber and discuss their duties?

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed University Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2017 onwards)
DEPARTMENT OF COMMERCE (CA)

SUBJECT: : Cyber Crime and Laws
SEMESTER : VI
SUBJECT CODE: 17CCU604B CLASS : III B.COM CA

UNIT : III

S.NO	QUESTIONS	OPTION 1	OPTION 2	OPTION 3	OPTION 4	ANSWER
1	A computer_____is a system in which multiple computers are connected to each other to share information and resources.	network	internet	web	host	network
2	The most commonly used cable to connect computers is Category 5 cable _____	RJ-35	RJ-25	RJ-45	RJ-55.	RJ-45
3	Which device acts as a central point among computers in a network	Distributor	Router	cable	Network card	Router
4	wireless mode_____are available by using which computers can be connected without any physical cable	Cable	Distributor	Network card	Router	Router
5	Which is also known as Network Interface Card?	Network cable	Network provider	Network adapter	Network link	Network adapter
6	Motherboard has slot, in which_____card is inserted.	internal	secondary	primary	external	internal
7	Peripheral Component Interconnect is a_____type of network card	secondary	primary	internal	external	internal
8	ISA stands for _____	Industry Standard Architecture	Indian Standard Architecture	Indian Server Architecture	Industry Server Architecture	Industry Standard Architecture
9	How many types of internal network cards are available?	three	five	two	four	two
10	Computers automatically install drivers required to support _____card.	ISA	USB	PCI	MSB	USB
11	system resource is any usable part of a computer that can be controlled and assigned by the _____	motherboard	operating system	modem	hardware	operating system
12	Swap file is available in _____	hard disk	Compact disk	Blue ray disk	USB	hard disk
13	Give abbreviation for IRQ _____	Interrupt Request Queue	Internet Renewal Queue	Internet Request Queue	Interrupt Renewal Queue	Interrupt Request Queue
14	Which of the following is not an input device?	keyboards	Optical scanner	Touch screens	printers	printers
15	Which is also known as registers?	Electronic circuit	Processing unit	Main memory	buffer	Electronic circuit
16	Which is required to execute software instructions?	ALU	MLU	CLU	RLU	ALU
17	Output devices are used to convert_____information produced by the computer system into human-intelligible form.	mechanical	electronic	logical	physical	electronic
18	Which is the high speed temporary memory?	cache	primary	secondary	main	cache
19	Programs are collections of_____for manipulating data.	instructions	controls	objects	informations	instructions
20	Which of the following is the processed Data?	object	information	instruction	picture	information
21	In digital signature, public key is also known as _____	Signature key	Internal key	Verification key	Control key	Verification key
22	The data entered in web form is send to_____for further processing	server	Database	browser	client	server
23	How many types of electronic form are available?	seven	five	six	four	six
24	In which form, getting data from the form to a database or system is usually manual	fillable	static	connected	distributed	static
25	Which of the following form does not contains widget?	editable	fillable	Validating	smart	editable
26	Word forms is an example for form _____	Level 2	Level 3	Level 4	Level 1	Level 3
27	The form that modifies itself is come under which level?	Level 5	Level 2	Level 3	Level 1	Level 5

28	_____ form submit data directly to database	Connected	Validating	Editable	Smart	Connected
29	In digital signature verifier uses_____function to authenticate.	vash	bash	hash	thrash	hash
30	The receiver with the_____key can only decode the message	foreign	private	primary	candidate	private
31	PKI stands for_____.	Private key interior	Public key interior	Private key infrastructure	Public key infrastructure	Public key infrastructure
32	CA/Browser forum and IST advises uses_____bit RSA key	2044	2048	2046	2042	2048
33	_____means a person in whose name the 'Electronic Signature' Certificate is issued	subscriber	originator	provider	authority	subscriber
34	By encryption of a text we mean _____	compressing it	expanding it	scrambling it to preserve its security	hashing it	scrambling it to preserve its security
35	The responsibility of a certification authority for digitalsignature is to authenticate the _____	hash function used	private keys of subscribers	Public keys of subscribers	key used in DES	Public keys of subscribers
36	Hashed message is signed by a sender using _____	his public key	his private key	receiver's public key	receiver's private key	his private key
37	An asymmetric-key (or public-key) cipher uses _____	1 Key	2 Key	3 Key	4 Key	2 Key
38	We use Cryptography term to transforming messages to make them secure and immune to _____	Change	Idle	attack	defend	attack
39	In Asymmetric-Key Cryptography, two keys, e and d, have a special relationship to _____	others	Each other	Data	keys	Each other
40	DES stands for _____	Data Encryption Standard	Data Encryption Subscription	Data Encryption Solution	Data Encryption Slots	Data Encryption Standard
41	Cryptography algorithms (ciphers) are divided into ___	2 groups	4 groups	1 groups	No group	2 groups
42	In Encryption, original message, before being transformed, is called _____	Simple Text	Plain Text	Empty Text	Filled Text	Plain Text
43	In symmetric key cryptography, key used by sender and receiver is _____	shared	different	two keys are used	none	shared
44	To exchange_____Symmetric-key cryptography started thousands of years ago.	secret	Packet	file	record	secret
45	Which one of the following statement is not correct for Digital signature?	It is mechanism for authentication	It cannot be duplicated	It is created by encrypting information	It is the scanned image of one's signature	It is the scanned image of one's signature
46	Which of the following is not the duties of subscriber?	Generating key pair	Acceptance of Digital Signature Certificate	Generating Digital Signature	Control of private key	Generating Digital Signature
47	A digital signature needs a _____	Private key system	Public key system	Shared key system	Secret key system	Public key system
48	Encryption and decryption provide secrecy, orconfidentiality, but not _____	Authentication	Integrity	Privacy	warranty	Integrity
49	Message must be encrypted at sender site and decrypted at the _____	Sender Site	Site	Receiver site	conferencing	Receiver site
50	What type of resource is most likely to be a shared common resource in a computer Network	Printers	Speakers	Floppy disk drives	Keyboards	Printers
51	Software is divided into programs and_____.	Data	instructions	coding	memory	Data
52	Bu using computer network we can share resources from computer to another _____	computer	radio	Television	modem	computer
53	The holes in the router are called _____	ports	connectors	plugins	pins	ports

54	_____is the necessary component of a computer without which a computer cannot be connected over a network.	Network card	Distributor	cable	Router	Network card
55	Which of the following is not an in build computer resource?	IRQ lines	CPU	DMA channels	USB	USB
56	Computers gather data by using_____device.	present	input	output	store	input
57	Which of the following is an input device?	scanner	speaker	CD	printer	scanner
58	Pointing device includes the following except _____	mouse	Pen input	keyboard	trackball	keyboard
59	USB refers to :	Port type	Storage device	processor	Serial bus standard	Port type
60	Which of the following contains only input devices.	Mouse,keyboard,monitor	Mouse,keyboard,printer	Mouse,keyboard,plotter	Mouse,keyboard,scanner	Mouse,keyboard,scanner

UNIT-IV

SYLLABUS

Electronic Records : Authentication of Electronic Records; Legal Recognition of Electronic Records; Legal Recognition of Digital Signatures; Use of Electronic Records and Digital Signatures in Government and its Agencies; Retention of Electronic Records; Attribution, Acknowledgement and Dispatch of Electronic Records; Secure Electronic Records and Digital Signatures.

Electronic Records: Authentication of Electronic Records

An electronic record is information recorded by a computer that is produced or received in the initiation, conduct or completion of an agency or individual activity. Examples of electronic records include: e-mail messages, word processed documents, electronic spreadsheets, digital images and databases. Many electronic records are maintained as part of an electronic recordkeeping system, such as geographic information systems (GIS), digital image storage systems, computer aided design (CAD) systems, etc.

1) Subject to the provisions of this section, any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation.- For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible-

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Techniques used for Authentication

Cryptography

The processes of encryption and decryption provide the basis on which digital signature infrastructure depends for maintaining security. This process is known as cryptography. The process of encryption keeps the information concealed for whom it is not intended even for those who can see the encrypted data, thereby, ensures confidentiality. It addresses the data protection and privacy issues, including data integrity and confidentiality and allows secure communication over insecure channels. Basically, encryption is a procedure to convert data into an unintelligible form that cannot be converted back into the original format in the absence of the secret decryption key. The purpose of applying cryptography is to protect vital information from getting into the hands of unauthorized persons, especially when the documents carrying information are transferred over the open networks, such as the internet. In an open system such as the Internet, the asymmetric encryption procedures help to protect and validate digital signatures on electronic documents.

Many countries limit the use of cryptography for confidentiality purposes keeping in mind the issue of national defense on the ground that encryption may make the information confidential in the communication process. However, digital signature by the use of cryptography for authentication purposes does not necessarily imply the same as the encrypted digital signature may have been appended to a non-encrypted message, thereby leading to authenticity not to confidentiality. Hence, it is of utmost importance to recognize the cryptography technique for authentication than confidentiality by the rules on digital signatures. There are various tools available online with the use of which keys may be easily deciphered by unauthorized intermediaries. Hence, the need is to strengthen the key to a secure digital signature in order to prevent the attacks to which the digital signatures are prone to due to high stakes involved.

"Public and Private Keys"

Before digitally signing an electronic communication, the sender has to create a public-private key pair. The two keys used for digital signatures are the Private Key and the public key. Private Key is kept confidential by the signer and used by him only to create the digital signature and the public key, is more widely known and is used to verify the digital signature by the relying party. In case of communication with many people, they need to verify the authenticity of document through the signer‟s digital signatures for which the public key should be accessible or disseminated to all of them, for example by publishing in an on-line repository over the internet or any other form of public directory from where it can be easily accessed. Though public keys are easily available, it doesn‟t mean that private key can be easily deciphered.

Though the keys of the pair are mathematically related, it is virtually impossible to obtain the private key from knowledge of the public key if an asymmetric cryptosystem has been designed and implemented securely.. Hence, despite the knowledge of the public key of a given signer and using it to verify his signatures, cannot discover the private key of the signer and use it to forge digital signatures. In the same way, if data is encrypted by someone using the public key, encrypted data can only be decrypted with the use of the private key. This is used when the person is desirous of letting the holder of the private key only to decrypt the message.

"Hash Function" and "Message Digest"

In addition to the generation of key pairs, the fundamental process used to create and verify a digital signature, is generally called as a "hash function". To apply hash function, the signer first has to delimit precisely the border of the information which is to be signed. This delimited information to be signed is referred to as the "message" to which "hash function" is applied. A hash function is basically a mathematical process created using the binary numbers based on an algorithm which creates a digital representation, or compressed form of the message, often referred to as a "message digest", in the form of a "hash value" or "hash result" of a standard length which is very much smaller than the message but nonetheless substantially unique to it.

The hash functions are public and no private key is required. The message is used as input according to this function which gives back a string making it unique to other messages which will always be the same for that message. These functions map the data to fixed sized hash values in such a way that it would be extremely difficult to come up with the same string of data that would match these particular hash values. The fact behind using the hash function is that a message digest represents concisely the original data from which it was computed. It could be considered as a digital fingerprint of the „larger" data string. Therefore, the hash function is used for both creating and verifying a digital signature, simultaneously, making the software able to work on smaller and predictable amounts of data for creating digital signatures, thereby, providing a strong evidentiary correlation to the original message content.

The digital signature can be verified by comparing the message digest obtained from the decoding of the signature with the message digest of the text. Hence, the security of the hash function is essential for the integrity of digital signatures. Any alteration in the content of the message always generates a different hash result when the same hash function is used. The minutest variation of the original document modification, insertion, deletion) can be instantly traced because there won't be any association between the message digests. In general, a digital signature (a digitally signed hash result of the message) is attached to its message and stored and transmitted with its message. Though, it can also be stored and sent as a separate data so long as it maintains a trustworthy connection with its message. It is also essential to understand that as a digital signature is unique to its message, it is worthless if having no association with its message.

Legal Recognition of Electronic Records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-

1. rendered or made available in an electronic form, and
2. accessible so as to be usable for a subsequent reference.

Recognition of electronic records:

The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and other activities carried out by electronic Information Systems Control and Audit means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

Digital Signature (Amended Vide ITAA 2008):

Section 3 gives legal recognition to electronic records and digital signatures. The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as "hash function" which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature. Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

Electronic Signature:

Electronic signature has also been dealt with under Section 3A of the IT Act, 2000. A subscriber can authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable and may be specified in the Second Schedule. An Amendment to the IT Act in 2008 introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

Electronic Governance:

E-governance or Electronic Governance is dealt with under Sections 4 to 10A of the IT Act, 2000. It provides for legal recognition of electronic records and signature and also provides for legal recognition of contracts formed through electronic means. Filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. Section 4 provides for "legal recognition of electronic records". It provides that where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form.

Section 5 provides for legal recognition of Digital Signatures. Where any law requires that any information or matter should be authenticated by affixing the signature of any person, then such requirement shall be satisfied if it is authenticated by means of Digital Signatures affixed in such manner as may be prescribed by the Central Government.

Section 6 lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. Section 6A talks about the service provider as the appropriate government may authorize any service provider and vary charges as they think fit.

Section 7 provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the information therein remains accessible and represents the original information.

Section 8 provides for the publication of rules, regulations and notifications in the Electronic Gazette. It provides that where any law requires the publication of any rule, regulation, order, bye-law, notification or any other matter in the Official Gazette, then such requirement shall be deemed to be satisfied if the same is published in an electronic form. It also provides where the Official Gazette is published both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form.

However, section 9 of the Act provides that the conditions stipulated in sections 6, 7 and 8 shall not confer any right to insist that the document should be accepted in an electronic form by any Ministry or department of the Central Government or the State Government.

Attribution, Acknowledgement and Dispatch of Electronic Records:

The Act deals with attribution, receipt and dispatch of electronic records. 'Attribution' means 'to consider it to be written or made by someone'. Hence, section 11 lays down how an electronic record is to be attributed to the person who originated it.

Section12 provides for the manner in which acknowledgement of receipt of an electronic record by various modes shall be made. Whereas, Section 13 of the act provides for the manner in which the time and place of dispatch and receipt of electronic record sent by the originator shall be identified. Generally, an electronic record is deemed to be dispatched at the place where the originator has his place of business and received where the addressee has his place of business.

Secure Electronic Records and Secure Electronic Signatures:

Sections 14 to16 deals with securing electronic records and electronic signatures. Section 14 provides where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification. Section 15 provides for the security procedure to be applied to Digital Signatures for being treated as a secure digital signature. Section 16 provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures. In doing so, the Central Government shall take into account various factors like nature of the transaction, level of sophistication of the technological capacity of the parties, availability and cost of alternative procedures, volume of similar transactions entered into by other parties etc.

Legislations in other nations:

As against the lone legislation ITA and ITAA in India, in many other nations globally, there is much legislation that govern e-commerce and cyber crimes going into all the facets of cyber crimes. Data Communication, storage, child pornography, electronic records and data privacy have all been addressed in separate Acts and Rules giving thrust in the particular area focused in the Act. In the US, they have the Health Insurance Portability and Accountability Act popularly known as HIPAA which inter alia, regulates all health and insurance related records, their upkeep and maintenance and the issues of privacy and confidentiality involved in such records. There are a number of laws in the US both at the federal level and at different states level like the Cable Communications Policy Act, Children's Internet Protection Act, and Children's Online Privacy Protection Act etc.

Legal Recognition of Digital Signatures

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (hen, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation.-For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

Legal Recognition of Advanced E-Signatures "The E-Signatures Directive differentiates between basic "electronic signatures" and "advanced electronic signatures."Advanced e-signatures are admissible in legal proceedings and provide a higher level of security than basic e-signatures provide. An e-signature becomes an "advanced" e-signature if satisfy few requirements such as: a unique link to the signatory; ability to identify itself to the signatory; creation of document using signature under the exclusive control of the signatory; and relationship with the data in a way that makes the recipient able to detect any variations to the original document sent by the signatory. The advanced e-signature is that only which is based on a qualified certificate defined in Annex I and Annex II of the Directive. The qualified certificate must also be created using a secure signature creation device complying with the requirements of Annex III. Certified advanced electronic signatures are placed on higher pedestal than other electronic signatures. EU Directive defines „Electronic Signature" and „advanced electronic signature" as follows:„electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication; „advanced electronic signature" means an electronic signature which meets the following requirements:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control;
- and it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The E-Signature Directive does not unequivocally specify the use of any particular technology; apparently, it is technologically neutral.
However, in the guise of attaining the security, the Directive supports covertly the use of more sophisticated and security-minded technologies, such as Public Key Infrastructure.

Levels of Security offered by E-signatures

First and Second Levels When entering into a contract online, four degrees of security are possible. The first level of security exists when a party accepts an offer by merely clicking an "I Agree" button on a computer screen. The second level of security is used when secrets are shared between the two contracting parties such as the use of a password or a credit card number to verify a customer's intention to purchase goods or services.

Third Level: Biometrics The third level is achieved with biometrics. Biometric methods involve a unique physical attribute of the contracting party, and these are inherently extremely difficult to replicate by a would-be cyber-thief. The proposed U.K. identity card would use three types of biometrics: photograph, iris scan, and fingerprints.

India has already started issuing such I-cards in the name of ADHAAR issued by UIDAI capturing unique physical attributes of the concerned person. Indian passport system has also been updated to include biometrics details to verify the records. Other examples of biometrics are a voice pattern, or a digitized image of a handwritten signature that is attached to an electronic message. In all of these examples, a sample would be taken from the person in advance and stored for later comparison for identification. If a person‟s handwriting is being used as the biometric identifier, the "shape, speed, stroke order, off-tablet motion, pen pressure and timing information" during signing would be recorded and this information is almost impossible to duplicate by a cyber-impersonator.

Fourth Level: Digital Signatures with PKI Technology The digital signature is considered the fourth level of security because it is more complex than biometrics. This provides the highest level of security. A digital signature is not merely a digitized version of a handwritten signature as many laymen erroneously assume. The digital signature refers to the entire document. The technology used with digital signatures is known as Public Key Infrastructure, or "PKI". The first step of Public Key Infrastructure technology is to create a public-private key pair, the private key will always be kept confidentially by the sender and the public key will be available online. The second step is the encryption of the message by the sender through digitally "signing" the message by creating a unique digest of the message. The third step is to attach the digital signature to the message and to send both to the recipient. The fourth step is for the recipient to decrypt the digital signature by using the sender's public key.

If decryption is possible, the recipient knows the message is authentic, i.e., that it came from the purported sender. If the recipient creates a second message digest of the communication with some alterations and compare it to the decrypted message digest, it can never match because the digital signature is bound with the document and also changes with every document. If the document gets changed, digital signature will also get changed. The slightest variation in the document will create a new document, thereby, require a new digital signature. Hence, the digital signature makes the recipient sure that the message has not been altered. Because PKI verifies the source of a message and its contents, digital signature is the most advantageous type of e-signature.

Three Models of Electronic Signature Laws

All over the world, the countries have adopted one or the other form of electronic signature law. On the basis of the technology adopted by various countries, these laws may be grouped into three categories.

Prescriptive Model

Countries that have adopted these laws have mandated PKI technology for use in digital signatures. This category includes Germany, Italy, Malaysia and Russia etc. India has also adopted this model by the IT Act 2000, which later shifted to hybrid model by the introduction of electronic signatures as well.

Unlimited liability may be imposed for negligent loss of a private key resulting in loss or damage. However, this model is highly restrictive and overly burdened.

Technological neutrality Model

Countries with technological neutrality model are extremely market oriented and permissive and this Model is exactly opposite to the prescriptive model. Most common law jurisdictions of the world have adopted this approach, including the U.S., Australia and New Zealand. Minimalist laws are adopted as per this model which doesn‟t mandate for any particular type of technology. For example, the U.S. E-Sign and the UETA provide that no electronic signatures of whatever type may be denied legal effect because it is in the electronic form. No special presumptions are made in favor of PKI or to any other particular technology". The disadvantage of this model is that all type of signature cannot be equated to the standard of digital signature whether it is password, a PIN no. or any other type of electronic signature. Hence, critics of this model contend that it is too vague and creates too much legal uncertainty.

Hybrid Model

Hybrid Model is mid-way path of the above mentioned two categories. A per this model a special presumption as to authenticity is created in favour of digital signatures, however, not to the exclusion of other kind of signatures. Examples are the EU Directive, the U.N. Model Law, Singapore (with an e signature law resembling the U.N. Model Law) and Bermuda. These laws have "limited technological neutrality." The only existing technology that appears to meet the requirements of the EU Directive‟s "advanced electronic signature" is PKI.

The Relevance of Signatures

Fundamentally, the signatures were required to prove the fact/ statement happened in past. Evidence law of all countries trust and acknowledge the written words in comparison of oral agreement. The reason for this favor is attributed to the fact that signatures on paper continue to exist as proof wherever required while the spoken word, once uttered, cannot be reproduced as proof. Thus, the need for signatures grew to bind parties to promises that they made In the light of suspicion as to human motives, written signatures are required to ensure non-repudiation.

The Functions of Signatures

Traditionally, hand-written, paper-based signatures perform many functions. Article 7 of the UNCITRAL Model Law on Electronic Commerce is based on the recognition of the functions of a signature in a paper-based environment. In the preparation of the UNCITRAL Model Law on Electronic Commerce, the Working Group discussed the following functions traditionally performed by handwritten signatures:

- to identify a person;
- to provide certainty as to the personal involvement of that person in the act of signing;

- to associate that person with the content of a document
- to attest to the intent of a party to be bound by the content of a signed contract;
- to attest the intent of a person to endorse authorship of a text (thus displaying awareness of the fact that legal consequences might possibly flow from the act of signing);
- to attest the intent of a person to associate itself with the content of a document written by someone else;
- to prove the fact as to the time when a person was present at a given place for the signature

In an electronic environment, everything is written on virtual memory which can be copied any number of times and cannot differentiated from the original. The ease with which a document can be altered and the speed with which it can be disseminated offer the potential of great levels of fraud. To avoid such frauds, it is required to use such electronic techniques which can identify document to its originator and reduce the possibility of alterations without detection. In other words, need is to use such the technical means which can perform some or all of the functions performed by handwritten signatures in an electronic environment. Such techniques are called as "electronic signatures". The volume of electronic transactions taking place every day requires the assurance as to the validity and authenticity of the transactions. The speed with which electronic payments are made demands for a certain online economic environment that electronic signatures can provide by ensuring functional equivalence to hand-written signatures.

For example, Digital signature assures validity and authenticity in e-mail communications, PIN assures the same in electronic payment transfer and password in many other electronic transactions. The key difference between hand written signatures and digital signatures is that your digital signatures are different for every document that is signed. When a document is changed and signed once again, the digital signature will be different. In this way the signature is bound to the document and to the person who has signed it providing assurance of the authenticity and integrity. At International level, United Nations has adopted UNCITRAL Model Law on Electronic Commerce and UNCITRAL Model Law on Electronic Signatures to guide all nations for preparing laws governing electronic signatures in order to create as much unanimity as possible. In India, The IT Act 2000 was passed adopting these two covenants, however, validating only digital signature which is replaced by the IT Amendment 2008 incorporating the rules relating to Electronic signatures with slight modifications wherever necessary.

Use of Electronic Records and Digital Signatures in Government and its Agencies

1. (1) Where any law provides for-
    1. The filing of any form. Application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner.
    2. The issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner.

3. The receipt or payment of money in a particular manner. Then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is affected by means of such electronic form as may be prescribed by the appropriate Government.

2. The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe-
   1. The manner and format, in which such electronic records shall be filed, created or issued.
   2. the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a)

Retention of Electronic Records

1. Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if-
   1. The information contained therein remains accessible so as to be usable for a subsequent reference.
   2. The electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received.
   3. The details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record: Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.
2. Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Establishing Retention Periods for Electronic Records

Information is created and maintained in many forms: paper, microfilm, computer, and optical disk. When establishing a legally valid records management program, most organizations realize that all records, not just paper and microfilm records, must be included. A records retention schedule establishes the retention period for all records, regardless of form. Records Management principles such as records retention and official version designation (Office of Record) also apply to electronic records.

This article reflects upon some major records management issues that affect computer records. Rather than consider all forms of computer-generated information as part of the records management program, the discussion below attempts to apply traditional records management concepts of "record" and "non-record" (work-in-progress) status to help determine the retention of computer records.

The computer industry and the courts refer to all computer information as "records." For purposes of evidence, all computer records would be subject to subpoena by the adverse party under rules of discovery. This could include computer records related to the general ledger, communications in the electronic mail system, or even the word processing files used to create documents.

From an organization's perspective, however, some of these so-called "records" are really tools used to create official company records, not the official records themselves. Computer information may be just "work-in-progress" to facilitate the preparation or revision of the final printed paper documents. For example, computer information such as word processing files are merely tools or work-in-progress used to prepare drafts and the final official paper records. The author does not intend for the work-in-progress to be reviewed by others, to be treated as official records, nor to reflect the official position of the organization. Similarly, electronic mail records and voice mail records provide a convenient substitute for non-documented verbal communication. In short, some of these "computer records" only represent a step in the process of creating official company records.

In order to apply records management principles to computer information, you first determine which computer information is a "record" and which is a "non-record." You may elect to establish some of the following principles:

- Electronic mail is a non-record unless converted to records by some formal process.
- Voice mail is always a non-record.
- Word processing files and superseded printed drafts are non-records. The final printed outputs are records.
  - One set of computer data containing accounting and tax information plus one copy of the visible output (e.g., printed report or computer output microfilm) are records under the Internal Revenue Service's Revenue Procedure 91-59.
- Computer back-up tapes and other duplicate computer files are non-records.
- Databases and other data compilations that are used for multiple purposes are records.

Some of these principles are reflected in the discussion below. The exact implementation will depend on the needs of your organization.

When computer information is characterized as "record" material, it must be retained according to your organization's records retention schedule. When computer information is characterized as "non-record" material, it can be destroyed at the discretion of the user — generally, after a relatively short period of time or after the official record is produced.

Some common types of computer information are discussed below.

Electronic Mail

Most larger organizations have established electronic mail systems. Electronic messages can be sent within the electronic mail network, or between the network and other computers through modems. Once created and sent, these electronic messages will often remain available on the system for many years, until the sender or recipient exercises the option to destroy the electronic records. Electronic mail messages may be printed onto paper at the users option.

Information system managers generally develop elaborate procedures to back up and preserve the electronic mail records for many years. The backups can be used to reconstruct the electronic records in case of system failure or inadvertent destruction of records. Even after the original electronic records have been removed from the primary on-line storage media, many years of electronic mail history remain available on magnetic tapes.

Unfortunately, organizations rarely determine the records retention period for electronic mail. Most believe that "longer is better."

When individuals communicate via electronic mail, they often utilize "loose" language that may be appropriate for internal conversations but would be totally inappropriate for formal written documents. Some people use verbiage that reflects personal opinions or biases, believing that electronic mail is personal or private.

Court cases have now confirmed that electronic mail is neither personal nor private. Electronic mail messages can legitimately be reviewed and used by supervisors without infringing on the rights of employees.

During litigation or government investigation, all electronic files of an organization are subject to subpoena and review by the other party. Electronic mail messages will be treated like records of the organization — reflecting the position and actions taken by the organization! It is possible for the other party to require an organization to examine the entire electronic mail history to identify all communications between certain individuals or related to certain subjects. If electronic mail records have been backed-up over several years, this would represent a significant burden, and a significant legal risk.

The informal nature of the electronic mail messages could also be harmful to the organization. Messages and "loose" language could easily be taken out of context by judges or regulators, leading to inappropriate conclusions and potentially damaging conclusions.

Electronic mail rarely represents the "official" position of the organization. These communications reflect preliminary thought or ideas, have not been reviewed by the organization and typically only reflect the personal opinion of the parties involved. Yet, since employees of the organization created these communications, courts and regulatory agencies can construe these records to reflect the organizational view.

Electronic mail messages should automatically be erased from the system after a short period of time — 15 to 30 days. Backup tapes of the electronic mail should also be destroyed within this period.

Some individuals may need to preserve electronic messages for a longer period of time. The system can allow users to select an option to preserve selected messages for an additional 15 to 30 days.

Alternatively, selected messages can be "formalized" and converted into an official company record by either moving the records to a special electronic storage area on the computer or producing paper prints. The electronic method would require some formal activity such as assigning a record series or records retention code to the records or otherwise identifying the records as official organization records.

Electronic mail systems generally allow the transmission of messages to multiple locations. Rather than reproducing the electronic file at each location, the electronic record is typically maintained at one location on disk but made accessible to multiple users. Other systems may replicate the electronic message in the other locations. The rules established above for electronic mail messages must apply to all locations containing the message.

The discipline of managing electronic mail can readily be accomplished within a network. The problem occurs when stand-alone or multiple networks communicate messages. In these cases, actual copies of the electronic mail message could exist in multiple locations.

Within an organization, procedures can be established to control the retention of each electronic mail message at the source. Even company-operated stand-alone microcomputers could contain an "executive program" or other software product that imposes records retention discipline similar to that discussed for the electronic mail networks. For example, all company-purchased microcomputers could contain identical electronic mail software that would automatically erase electronic mail messages (even those transmitted to or received from an outside source) after the requisite period of time. Additionally, the procedures for formalizing records or converting electronic mail records to official company records could also be incorporated.

An organization, however, has no control over electronic mail messages created by or sent to computer systems outside the organization. This case is similar to when an outside organization creates a document and then submits it to your organization. Both your organization and the outside one would maintain a set of records according to their respective records retention programs.

Due to the potential legal risks associated with electronic mail messages, special care should be taken for messages sent outside the organization. Perhaps, only official company records should be sent outside your organization — regardless of whether the records are in paper or electronic form.

Voice Mail

Voice mail is similar to electronic mail except that the messages consist of voice communication rather than typewritten communication. Voice mail consists of even more informal messages than electronic mail. The potential for misinterpretation or use of loose language is even greater.

Voice mail is typically used to communicate short messages within an organization when the individual is not available to receive a telephone call. Procedures should generally be established to redirect or transcribe voice mail messages when an individual is unavailable for an extended period of time.

Voice mail, including all backups, should automatically be erased within the same 15 to 30 day period. Due to the short-term nature of voice mail, no procedures should be established to allow the formalization of voice mail records nor the preservation of voice mail for a longer period of time.

Electronic Records with Tax Implications

Most organizations now utilize computers as part of their accounting system. Accounting transactions are recorded in the regular course of business and incorporated into the general ledger and other reports that reflect the status of the accounting system.

In Revenue Ruling 71-20, the Internal Revenue Service recognized that computer records meet the requirements for recordkeeping under the Internal Revenue Code. Revenue Procedure 91-59 specifies that taxpayers utilizing computer records must maintain the computer records in both electronic ("machine sensible") and visible format (paper or microfilm) for the period of time they are subject to a tax audit. A taxpayer may be asked to produce the electronic records in a form that is readable on a current computer system and make that data available to the IRS auditor. For this legal reason, computer records related to accounting and tax matters should be treated as official company records.

Taxpayers should then maintain the electronic records related to tax matters for the period of time they are subject to tax audit. According to Title 26, United States Code, Section 6501, the Internal Revenue Service may audit you for the following periods:

- within three years after you file a tax return for normal circumstances,
- within six years after you file a tax return if you understate your gross income by 25% or more, and
- indefinitely, in case of false return, willful attempt to evade tax, no return or extension by agreement.

Most organizations have established a records retention period of six years (and sometimes even the traditional seven years) to protect themselves during the most likely time period during which an audit could occur.

This time period must be extended if the taxpayer signs an agreement to extend the audit with the Internal Revenue Service. The electronic version of records subject to tax review will normally be maintained for the full records retention period.

Revenue Procedure 91-59 describes an exceedingly difficult burden for the taxpayer related to the preservation of electronic records. Taxpayers must maintain the electronic records for the requisite period but also must make the records available on a current computer system. This burden is exceedingly difficult because as taxpayers will usually convert to newer, perhaps, incompatible technologies over time. After a period of just a few years, the organization may not have equipment or software that can read the old tapes. Even if the equipment and software exist, magnetic tapes start to deteriorate and may become unreadable after a few years, even if the tapes are properly stored and periodically rewound.

With the increased use of electronic data interchange, attention to the retention requirements for electronic records becomes even more important. Revenue Procedure 91-59 recognizes electronic data interchange records and specifies that these records may be retained in electronic form unless a visible record is requested by a tax auditor. The taxpayer will be responsible for ensuring the continued preservation and retention of these electronic records for the full period they are subject to the administration of any tax law.

Other than this revenue procedure, no other law known to this author requires an organization to maintain both the electronic and visible form of the same information. You may, therefore, maintain records in any form unless the law either specifies the form or restricts the forms that can be used. In the case of tax records, however, you must maintain both the electronic and visible version of the same information.

Databases

Databases may consist of a number of files and fields of data that provide useful information to the organization. Typically, databases are modified over time through the addition, deletion, or modification of records. Reports are periodically prepared to reflect information from the databases that may be useful for specific purposes. Due to the large volume of information typically maintained in databases, reports rarely reflect “all” the information found on the database. Well-operated systems will provide periodic backups to restore databases in case of accidental erasure or disaster.

Many databases contain tax-related information. Their records retention period will be established based upon the tax issues raised above.

Organizations maintain some databases for reasons other than tax. The information could include mailing lists, customer information, marketing information, parts inventory, etc.

Since reports typically do not reflect the entire content of the database, the electronic form of the database contains different information than the visible reports. Regardless, the electronic databases are often more useful than the paper reports. For this reason, visible reports are not equivalent to electronic databases.

For records retention purposes, most organizations will want to uniquely define a database as an official record of the organization, even though it is a computer record. The retention period might appropriately be established as "until superseded (SUP)" to reflect that only the current version needs to be maintained. Backups can then be destroyed after a relatively short period of time such as one month. Other organizations may elect to maintain a "snapshot" of the database in electronic form on an annual basis and retain the snapshot for a designated retention period to reflect user or operational needs. For example, the annual snapshot of the database may be appropriate to determine the state of certain activity at the close of previous years.

Word Processing Files

Many organizational documents are prepared using word processing. A draft of the document is generally typed into the word processing system from hand-written notes or other materials, or transcribed from automated dictation devices. The word processing document is then printed and revised until the final printed version is accepted by the author.

For records retention purposes, the original notes and recorded media from dictation should be considered non-record material or work-in-progress. This version should be destroyed in a relatively short period of time after the final draft has been accepted. Similarly, successive drafts of a document and the successive revisions of the electronic word processing file should be considered non-record or work-in-progress. Only the final approved, paper record should be considered an official organization document.

If the final product of the word processing process is a communication in an electronic mail system, the communication will only become an official record of the organization if the formalization process discussed above is followed.

For operational reasons, you may want to maintain some of the electronic-word processing files for extended periods of time to facilitate the revision of drafts. These decisions should be made based upon the importance of the final document produced and the likelihood of revision or use of the material for other purposes. The word processing operator would then destroy the computer version when it is no longer needed.

Lawyers often argue for the preservation of multiple drafts of contracts. They argue that problems with a final contract can often be resolved by determining the party's intent through the use of previous drafts. In some cases, the final agreement fails to include provisions that had been included and approved in previous drafts.

Other attorneys argue that the "Parole Evidence Rule" prohibits the consideration of any evidence in court outside of the final written document of the parties. In fact, most contracts contain a clause that prohibits the consideration of previous drafts or other information that has not been incorporated into this final written document.

To meet the needs of attorneys, it may be appropriate for the Legal Department to maintain multiple, printed drafts of contracts as part of the final contract file. This decision must be made based upon the needs of the attorneys and experience in this area. But versions of the computer files related to each draft should not be kept — only the most current version.

Word processing computer information should be treated differently than databases. The computer information from a word processing file is generally printed letter-for-letter onto a final paper document. In essence, the paper document "mirrors" the information in the word processing systems so only the most useful version — the printed, paper version — should be kept.

Finally, Records retention of computer records present difficult challenges. This articles analyzes some common types of computer records. Organizations addressing records retention of computer records should first determine which form of the records will be the official organization records — computer, paper, or microfilm — and what will be the status of the computer records. With this approach, some computer information will be treated as official records of the organization while others will be considered non-records or work-in-progress.

Attribution, Acknowledgement and Dispatch of Electronic Records

11. Attribution of electronic records (Section 11)

An electronic record shall be attributed to the originator -

1. if it was sent by the originator himself.
2. by a person who had the authority to act on behalf of the originator in respect of that electronic record, or
3. by an information system programmed by or on behalf of the originator to operate automatically.

12. Acknowledgment of receipt (Section 12)

1. Where the originator has not agreed with the addressee that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by -
    1. any communication by the addressee, automated or otherwise, or
    2. any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

2. Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.
3. Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

13. Time and place of dispatch and receipt of electronic record (Section 13)

1. Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.
2. Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely :-
    1. if the addressee has designated a computer resource for the purpose of receiving electronic records -
        1. receipt occurs at the time when the electronic, record enters the designated computer resource, or
        2. if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee.
    2. if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.
3. Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.
4. The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).
5. For the purposes of this section -
6. if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business.
7. if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business.
8. "usual place of residence", in relation to a body corporate, means the place where it is registered.

Secure Electronic Records and Digital Signatures

Secure Electronic Records and Secure Digital Signatures:

In the age of e-commerce where the electronic records and digital signatures are of crucial significance for proper functioning of e-commerce and business in the globalised free market economy it is imperative that the transactions of ecommerce in the form of electronic record and digital signatures should be secure, authentic and must be suitably confidential from the general public and third parties. The relevant parties to the electronic records and digital signatures must be confident while conducting e-commerce or business that their transactions are secure and cannot be tampered with by any unrelated persons to the transactions of e-commerce between the relevant parties. Therefore, in order to have proper security procedures to secure electronic records and digital signatures, proper cyber laws are very essential. Many countries in the world have tried to frame such laws suiting to their unique business environment, the political system and the necessity of properly conducting e-commerce or business in the modern world of cyberspace and the internet.

We find that in the new environment of the development of technology of information and communication have witnessed several new legal and moral issues while conducting e-commerce and business. For many of those issues there may not be clear-cut answers but certainly these issues have very important impact on the communication systems and the internet. We find that the internet has given a sudden growth of new and speedy means of communication in the globalised market place. These transactions are very lucrative commercial transactions through the internet and no business which wants to have competitive advantage in the world market can do without the internet for the purposes of e-commerce and business.

IT ACT, 2000 includes the legal norms relating to security of electronic records and electronic signatures. It means when the 'electronic record' and 'electronic signature' are deemed secure

1. Secure electronic record (sec14) An electronic record can be secured for the purposes of the Act if it has been authenticated by means of a secure digital signature.
If any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

2. Secure digital signature (Section 15) Section 15 lies down that an electronic signature shall be deemed to be a secure electronic signature if:

a) The signature creation data, at the time of affixing, was under the exclusive control of signatory and no other person; and

b) The signature creation data was stored and affixed in such exclusive manner as may be prescribed.

3. Security procedure The Central Government may for the purpose of sections 14 and 15 prescribe the security procedures and practices having regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate. The digital signature infrastructure depends largely on process of encryption and decryption for maintaining security. This process is called as cryptography.

Figure: Cryptography

The purpose of encryption is to ensure confidentiality by keeping the information hidden from any one for whom it is not intended and even for those who can see the encrypted addressee of the data protection and privacy issues, including data integrity and confidentiality, allows secure communication over insecure channels.
An important condition for e-commerce's survival is the ability to safeguard all electronic transactions. Unless an electronic transaction is secure it would be difficult to determine its authenticity. Moreover, the users will be hesitant to send confidential information over the net. Existence of safeguards and assurance that such transmission are fool proof will go a long way towards boosting e-commerce and the common way of protecting electronic transactions is through cryptography. Cryptography uses sophisticated mathematical algorithms, particularly a technology which is known as asymmetric cryptography.

Any person would like hid transactions to be confidential and this can be achieved through encryption and decryption techniques. Encryption process would code a message and the coded message would then be transmitted over the net. Thus only users having capacity to decrypt the coded message would have access to the content.

For successful decryption, it is important that the decrypting technique is corresponding to that particular encrypting technique. It is also important that the encryption process is secure enough, so that it cannot be easily cracked. The strength of the encryption depends on the key length used by the encryption software. The techniques of encryption and decryption involve the use of two kinds of keys, public and private keys, both of which are mathematically linked. One key is used for encryption and the other corresponding key is used for decryption. Each user has a pair of keys of which the private key is kept secret and the public key is open to all. Therefore, if X wants to send a message to Y, X will encrypt the message with Y's public key and send it to Y. it is only Y who would be able to access the message.

The nature of digital signature is the importance of digital signature which is also known as advanced or secure electronic signature. Authentication of digital signature and how much reliable and secure the digital signatures are determined with the help of Encryption and Decryption techniques with pairs of keys.

Part A (ONE Mark)
Multiple Choice Questions
Online Examination

Part B (2 Marks)

1. What is authentication of electronic record?
2. Give note on i) Electronic Signatures ii) Electronic Governance
3. Discuss the functions of signatures.
4. What is Retention of Electronic Records?
5. Short note on i) Electronic mail ii) Databases
6. Define Voice mail.
7. Explain the Attribution, Acknowledgement and Dispatch of Electronic Records?

Part C (8 Marks)

1. Describe the techniques used for authentication of the electronic record.
2. Explain Legal Recognition of Electronic Records.
3. Discuss the Legal Recognition of Digital Signatures.
4. Narrate the levels of Security offered by E-signatures.
5. List out the models of Electronic Signature Laws.
6. What are the use of Electronic Records and Digital Signatures in Government and its Agencies?
7. Discuss the reasons to establish the retention Periods for Electronic Records.
8. What are the legal acts given by information technology act, 2000 to secure Electronic Records and Digital Signatures?

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed University Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2017 onwards)
DEPARTMENT OF COMMERCE (CA)

SUBJECT: : Cyber Crime and Laws
SEMESTER : VI
SUBJECT CODE: 17CCU604B CLASS : III B.COM CA

UNIT : IV

S.NO	QUESTIONS	OPTION 1	OPTION 2	OPTION 3	OPTION 4	ANSWER
1	Which of the following is not an electronic record?	e-mail messages	electronic spreadsheets,	digital images	magazines	magazines
2	hash function means an algorithm mapping or translation of one sequence of_____into another	Files	bits	images	words	bits
3	electronic record yields the_____result every time the algorithm is executed with the same electronic record	same	different	encrypted	decrypted	same
4	Any person by the use of a_____of the subscriber can verify the electronic record.	public key	Partial key	secondary	shared	public key
5	In asymmetric key cryptography, the private key is kept by	Sender	All devices connected to network	Sender and receiver	Receiver	Receiver
6	The sender “signs” a message as _____	Digital signature	Artificial signature	Encrypted signature	Decrypted signature	Digital signature
7	Cryptography means _____	Word processing	Secret writing	Parallel processing	Serial writing	Secret writing
8	In cryptography receiver encrypts the message and sender decrypts the message.	Never	True	False	Can’t say	False
9	Cryptography relates to _____	security	editing	testing	tampering	security
10	To check integrity of a message, or document, receiver creates the _____	Hash Table	Hash Tag	Hyper text	Finger print	Hash Tag
11	When data must arrive at receiver exactly as they were sent, it is called _____	Message Confidentiality	Message splashing	Message sending	Message Integrity	Message Integrity
12	Message digest needs to be Kept _____	secret	private	public	shared	secret
13	A(n)_____function creates a message digest out of a message.	encryption	decryption	hash	thrash	hash
14	A_____signature is included in the document; a _____ signature is a separate entity.	conventional; digital	Digital; conventional	Digital;Digital	Conventional; conventional	conventional; digital
15	A hash function does not need_____key	Public	private	partial	primary	private
16	Any alteration in the content of the message always generates a _____hash result when the same hash function is used.	similar	different	duplicate	same	different
17	A(n)_____can be used to preserve the integrity of a document or a message.	message digest	message summary	encrypted message	decrypted message	message digest
18	A digital signature needs a(n)_____system	symmetric-key	Secret key	Partial key	asymmetric-key	asymmetric-key
19	Electronic record is converted into a message digest by using a mathematical function known as _____which digitally freezes the electronic record.	Square function	Linear function	Hash function	Cosine function	Hash function
20	E-governance or Electronic Governance is dealt with under Sections_____of the IT Act,2000.	2 to 6A	4 to 10A	6 to 8A	8 to 10A	4 to 10A
21	Section_____provides for legal recognition of Digital Signatures.	5	4	7	6	5
22	Section 6 lays down the foundation of _____	Digital Signatures	Electronic Governance.	Electronic Gazette.	Electronic form	Electronic Governance.
23	Section_____provides that the documents, records or information which is to be retained	6	5	7	3	7
24	Section 8 provides for the publication of rules, regulations and notifications in the	Electronic media	Electronic form	Electronic Gazette.	Electronic contract	Electronic Gazette.
25	How many levels of security issued by digital signatures?	three	Four	two	five	Four
26	A party accepts an offer by merely clicking an “I	Fourth	Second	First	Third	First

	Agree" button on a computer screen is_____ level of security					
27	Use of a password or a credit card number to verify a customer‟s intention to purchase goods or services is come under which level of security?	Third	Fourth	Second	First	Second
28	Third level of security is achieved with _____	Biometrics	PKI	Digital Signature	password	Biometrics
29	AADHAR,UIDAI are the examples of_____level of security.	Fourth	Second	Third	First	Third
30	Digital Signatures with _ ___Technology is fourth level of security	CKI	PKI	MKI	SKI	PKI
31	How many models in electronic signature laws?	Two	Three	Four	Five	Three
32	Countries that have adopted_____laws have mandated PKI technology for use in digital signatures.	Technologically neutral model	Hybrid model	Prescriptive model	Descriptive model	Prescriptive model
33	Which model of electronic signature law is following in India?	Hybrid model	Descriptive model	Technologically neutral model	Prescriptive model	Prescriptive model
34	Which model of electronic signature law is highly restrictive and over burdened?	Descriptive model	Prescriptive model	Hybrid model	Technologically neutral model	Prescriptive model
35	Market oriented Countries use_____model of electronic signature law.	Prescriptive model	Descriptive model	Technologically neutral model	Hybrid model	Technologically neutral model
36	Which model is exactly opposite to prescriptive model?	Hybrid model	Prescriptive model	Descriptive model	Technologically neutral model	Technologically neutral model
37	Digital signatures are_____for every document that is signed.	different	same	identical	duplicate	different
38	When a_____is changed once again, the digital signature will be different.	computer	document	CD	network	document
39	Validating only digital signature by IT Amendment 2000 is replaced by the IT Amendment_____by incorporating the rules relating to Electronic signatures.	2008	2006	2004	2000	2008
40	Who backup and preserve the electronic mail for several years?	Information system administrators	Information system executives	Information system developers	Information system managers	Information system managers
41	E-mail address is made up of_____parts	three	two	four	five	three
42	The E-mail component of Internet Explorer is called _____	Message box	Outlook Express	Messenger Mailbox	Message outlook	Outlook Express
43	Which one of the following statement is not correct for Digital signature?	mechanism for authentication	cannot be duplicated	created by encrypting information	scanned image of one's signature	scanned image of one's signature
44	Which of these should be avoided in an E-mail?	Wrong E-mail address	Subject line	Smileys	Re-reading	Wrong E-mail address
45	Voice mail, including all backups, should automatically be erased within the same_____day period.	15 to 30	20 to 30	10 to 20	5 to 10	15 to 30
46	Which revenue procedure specifies, taxpayers utilizing computer records must maintain the computer records in both electronic and visible format	90-59	91-59	91-49	90-69	91-59
47	A_____is a collection of information that is organized so that it can be easily accessed, managed and updated	database	Record	Field	attribute	database
48	_____are periodically prepared to reflect information from the databases that may be useful for specific purposes.	Tables	Forms	Reports	Files	Reports
49	Number of personal computers in which word processor is already installed is about _____	60	70	90	80	90
50	The software for compiling a database is a _____	Database manager	Database executive	Database processor	Database query engine	Database manager
51	Attribution of electronic records come under which section?	nine	ten	twelve	eleven	eleven
52	Which of the following is not important to keep the e-commerce survive?	Secure transactions	Confidential transactions	Authenticated transactions	Precarious transactions	Precarious transactions
53	Cryptography uses sophisticated _____	Scientific algorithms	mathematical	e-commerce	Network functions	mathematical

			algorithms	principles		algorithms
54	The strength of the encryption depends on the_____used by the encryption software.	key length	Code length	Key complexity	Code complexity	key length
55	the electronic_____are often more useful than the paper reports.	tables	databases	documents	files	databases
56	_____is typically used to communicate when the individual is not available to receive a telephone call.	E message	Online mail	Voice mail	E mail	Voice mail
57	_____is always a non-record.	E mail	Voice mail	E message	Online mail	Voice mail
58	Singapore following which model of electronic signature law?	Hybrid	Neutral	Prescriptive	Descriptive	Hybrid
59	The advanced e-signature is that only which is based on a _____	Accurate document	Accurate form	Qualified certificate	Qualified report	Qualified certificate
60	Which of the following forms a ‘key pair’ in cryptography?	Private & primary keys	Private & public keys	Private & duplicate keys	Private & unique keys	Private & public keys

UNIT-V

SYLLABUS

Regulatory Framework: Regulation of Certifying Authorities; Appointment and Functions of Controller; License to issue Digital Signatures Certificate; Renewal of License; Controller's Powers; Procedure to be Followed by Certifying Authority; Issue, Suspension and Revocation of Digital Signatures Certificate, Duties of Subscribers; Penalties and Adjudication; Appellate Tribunal; Offences.

Regulatory Framework: Regulation of Certifying Authorities

1. Appointment of Controller and other officers

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purpose of this Act and may also by the same or subsequent notification appoint such of Deputy Controllers and Assistant Controllers as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

2. Functions of Controller

The Controller may perform all or any of the following functions, namely:-

(a) exercising supervision over the activities of the Certifying functions, namely :-

(b) certifying public keys of the Certifying Authorities;

(c) laying down the standards to be maintained by the Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authority should possess;

(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;

(g) specifying the form and content of a Digital Signature Certificate and the key;
(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;
(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;
(m) laying down the duties of the Certifying Authorities;
(n) maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

3. Recognition of foreign Certifying Authorities

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognise any foreign Certifying Authority as a Certifying Authority for the purpose of this Act.
(2) Where any Certifying Authority is recognised under sub-section (1), the Digital Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.
(3) The Controller may, if he is satisfied that the Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub-section (1) he may, for reasons to be recorded in writing in the Official Gazette, revoke such recognition.

4. Controller to act as repository

(1) The Controller shall be the repository of all Digital Signature Certificates issued under this Act.
(2) The Controller shall-
(a) make use of hardware, software and procedures that are secure from intrusion and misuse;
(b) observe such other standards as may be prescribed by the Central Government, to ensure that the secrecy and security of the digital signatures are assured.
(3) The Controller shall maintain a computerised data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

5. Licence to issue Digital Signature Certificates

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a licence to issue Digital Signature Certificates.
(2) No licence shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure

facilities, which are necessary to issue Digital signature Certificates as may be prescribed by the Central Government.

(3) A licence granted under this sections shall-

(a) be valid for such period as may be prescribed by the Central Government;

(b) not be transferable or heritable;

(c) be subject to such terms and conditions as may be specified by the regulations.

6. Application for licence

(1) Every application for issue of a licence shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a licence shall be accompanied by-

(a) a certification practice statement;

(b) a statement including the procedures with respect to identification of the applicant;

(c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

(d) such other documents, as may be prescribed by the Central Government.

7. Renewal of licence

An application for renewal of a licence shall be-

(a) in such form;

(b) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the licence.

8. Procedure for grant or rejection of licence

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the licence or reject the application: Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

9. Suspension of licence

(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has,-

(a) made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;

(b) failed to comply with the terms and conditions subject to which the licence was granted;

(c) failed to maintain the standards specified under clause (b) of sub-section

(2) of section 20;

(d) contravened any provisions of this Act, rule, regulation or order made thereunder, revoke the licence :

Provided that no licence shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1), by order suspend such licence pending the completion of any inquiry ordered by him : Provided that no licence shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No certifying Authority whose licence has been suspended shall issue any Digital Signature Certificate during such suspension.

10. Notice of suspension or revocation of licence

(1) Where the licence of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the data base maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories: Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site shall be accessible round the clock : Provided further that the Controller may, if he considers necessary, publicise the contents of data base in such electronic or other media, as he may consider appropriate.

11. Power to delegate

The Controller may, in writing, authorise the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

12. Power to investigate contraventions

(1) The Controller or any officer authorised by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made thereunder.

(2) The Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 and shall exercise such powers, subject to such limitation laid down under that Act.

13. Access to computers and data

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that nay contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the

purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

(2) For the purpose of sub-section (1), the Controller or any person authorised by him may, by order, direct any person incharge of, or otherwise concerned with the operation of, the computer system, data apparatus or material, to provide him with such reasonable technical and other assistance as he may consider necessary.

14. Certifying Authority to follow certain procedures

Every Certifying Authority shall,-

(a) make use of hardware, software and procedures that are secure from intrusion and misuse;

(b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;

(c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and

(d) observe such other standards as may be specified by regulations.

15. Certifying Authority to ensure compliance of the Act, etc.

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made there under.

16. Display of licence

Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

17. Surrender of licence

(1) Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.

(2) Where any Certifying Authority fails to surrender a licence under sub-section (1), the person in whose favour a licence is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

18. Disclosure

(1) Every Certifying Authority shall disclose in the manner specified by regulations-

(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;

(b) any certification practice statement relevant thereto;

(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and

(d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.
(2) Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall-
(a) use reasonable efforts to notify any person who is likely to be affected by that occurrence; or
(b) act in accordance with the procedure specified in its certification practice statement to deal with such event or situation.

Appointment and Functions of Controller

The Controller may perform all or any of the following function, namely:-

(a) exercising supervision over the activities of Certifying Authorities;

(b) certifying public keys of the Certifying Authorities;

(c) laying down the standards to be maintained by Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(e) specifying the conditions subject to which the Certifying Authority shall conduct their business;

(f) specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key;

(g) specifying the form and content of a Digital Signature Certificate and the key;

(h) specifying the form the manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such system;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a data-base containing the disclosure record of ever Certifying Authority containing such particulars as may be specified by regulations which shall be accessible to public.

License to issue Digital Signatures Certificate

What Is Digital Signature Certificate?

Digital Signature Certificates (DSCs) are the digital equivalent (i.e electronic format) of physical or paper certificates. Examples of physical certificates are Driving License, Passport or Membership Cards.

Certificates serve as proof of identity of an individual for a certain purpose; for example, a Driving License identifies someone who can legally drive in a particular country. Likewise, a Digital Signature Certificate can be presented electronically to prove your identity, to access information or services on the Internet or to sign certain documents digitally.

DSC provides an additional level of safety and security for online banking transactions by digitally verifying the financial transactions and encrypting the information such that only intended parties can read it.

Who issues DSC and what are the different types of DSC?

A licensed Certifying Authority (CA) issues the Digital Signature Certificate. The CA is someone who has been granted a License to issue a DSC under Section 24 of the Indian IT-Act 2000.

The list of licensed CAs along with their contact information is available on the Controller of Certifying Authorities (CCA) portal (www.cca.gov.in).

After procurement of the DSC, the Certificate can be downloaded in to the hard token or can be installed to the PC/Laptop. Please ensure that the token drivers are installed on your system as guided by your Certified Authority.

Standard Chartered Bank Online banking supports Class 3 types of DSCs.

Class 3 Certificates are issued to individuals as well as organisations. As these are high-assurance Certificates primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.

Who issues Digital Signature certificates?

A licensed Certifying Authority (CA) issues the digital signature. Certifying Authority (CA) means a person who has been granted a license to issue a digital signature certificate under Section 24 of the Indian IT-Act 2000. The list of licensed CAs along with their contact information is available on the MCA portal.

Requirements while you apply for a digital signature certificate

1. Submission of DSC Application form duly filled in by the applicant

Any individual applying for a Digital Signature Certificate is required to fill an Application Form for online submission and verification of personal details by the certifying authority

2. Producing Photo ID proof

3. Producing Address proof

Steps to apply for a digital signature certificate

STEP 1: Log on and select your type of entity

Log on to the website of a Certifying Authority licensed to issue Digital Certificates in India.

Having accessed the page, you will be guided to the Digital Certification Services' section.

Now under the 'Digital Certification Services' section, click on the type of entity for which you want to obtain the DSC:' individual or organization', etc.

In case you are applying for an individual DSC, click on 'individual'. A new tab containing the DSC Registration Form will appear. Download the DSC Registration Form on your PC.

STEP 2: Fill the necessary details

Once you have downloaded the form, fill in all the necessary details as required in the form:

1. Class of the DSC

2. Validity

3. Type: Only Sign or Sign & Encrypt

4. Applicant Name & Contact Details

5. Residential Address

6. GST Number & Identity Details of Proof Documents

7. Declaration

8. Document as proof of identity

9. Document as proof of address

10. Attestation Officer

11. Payment Details

On filling up all the necessary details you must affix your recent photograph and put your signature under the declaration. Check thoroughly for completion of the form. Take a print of the completed form and preserve it.

STEP 3: Proof of identity and address

The supporting document provided as proof of identity and address must be attested by an attesting officer. Ensure the sign and seal of the attesting officer is visibly clear on the supporting proof documents.

STEP 4: Payment for DSC

A demand draft or cheque must be obtained towards payment for application of DSC in the name of the Local Registration Authority where you are going to submit your application for verification.

You can find the details of the Local Registration Authority according to your city of residence by searching for a Certifying Authority licensed to issue Digital Certificates online.

STEP 5: Post the documents required

Enclose the following in an envelope.

1. DSC Registration Form duly completed

-Supporting document for Proof of Identity and proof of address attested by the attesting officer

2. Demand Draft/Cheque for payment.

Address the enclosed envelope to the Local Registration Authority (LRA) and post it to the designated address of the LRA for further processing.

On completion of the above-mentioned steps by filling in the DSC Form and providing necessary documents and payment, you have successfully completed the application process for your Digital Signature Certificate.

Renewal of License

Process for Renewal of Digital Certificates

1. The applicant (Government Subscriber) browses APTS website / approaches APTS for knowing the Process of Renewal of Digital Signature Certificate.

2. The following are the steps to be followed by the applicant to acquire the digital certificate:

Obtaining the Enrollment Kit (Consisting of Application & User Manual)

1) The applicant or his/her representative can approach for obtaining the Enrollment Kit from APTS office (or)

The applicant can download the application form from the APTS web site.

For cost of the digital certificate refer Annexure-IV. The amount can be paid in the form of Demand Draft drawn in favor of the Managing Director, APTS. No cash transactions are allowed at APTS.

2) APTS hands over the Enrollment Kit to the applicant or his/her representative, which includes:

i. User Manual for acquiring Digital Certificate

ii. Certificate Request Form (Application for digital certificate)

2.2. Submission of the Application for renewal of the digital certificate (Certificate Request Form): (**Refer** APTS-eMudhra-User Manual for DSC & MANDATORY - Verification Guidelines issued by CCA or CA).

a. The information provided by the applicant in the Request Form, such as Name, Postal addresses, Phone numbers, Email-id etc., should be complete, valid, current and active.

b. The applicant must sign the Request Form.

c. The Request Form should be complete in all respects.

d. The applicant sends the filled-in Certificate Request Form, Payment receipt issued by APTS and validation documents **as per the checklist provided in Annexure-II** to APTS for verification.

e. It should be noted that the filled in Application form and the validation documents should be submitted in duplicate, in person or by post.

f. The applicant should keep a photo copy of the submitted Request Form and Documents with him/her for future references.

2.3. Verification of the Application (Request form & other Documents) at APTS:

(Refer MANDATORY - Verification Guidelines issued by CCA or CA).

a. APTS RA verifies the request form, payment receipt and other documents. The request for renewal of digital certificate will be accepted provided all the necessary information has been filled in by the applicant in the Application form enclosing all attested relevant documents. If APTS RA office finds that the application form is not complete, then request is likely to be rejected.

b. If the request is accepted, the applicant will be notified by APTS via phone using the phone number mentioned in the Request Form. Then the applicant should proceed with the next process step for Certificate enrollment.

c. If the request is rejected, the applicant is notified by APTS via phone using the phone number mentioned in the Request Form and the applicant again has to submit the request.

2.4. Online Enrollment through APTS website:

a. As per the 'APTS-eMudhra-User Manual for DSC', the applicant completes the first three stages - Installation, Registration, and Enrollment.

b. When the Enrolment is completed as per the 'APTS-eMudhra-User Manual for DSC', contact APTS RA / HelpDesk (Refer Annexure I) and forward the Application.

c. RA enters the Certificate Request Number on the Certificate Request Form submitted by the applicant and verifies the Certificate request details online.

i. If the details entered by the applicant, online are complete and as per the Request Form, the RA forwards the request to the APTS Sub-CA.

ii. If the details entered by the applicant, online are not complete and are not matching with the Request Form, the RA rejects the request for the certificate and informs the same to the applicant. The applicant has to again enroll immediately. After completing re-enrollment, the applicant must once again contact the APTS-RA officer.

d. APTS Issuing Authority (Sub-CA Administrator) verifies, digitally signs and releases the request for renewal of the Certificate.

e. After APTS Sub-CA Administrator releases the request, the Certificate will be renewed and download link will be sent to registered eMail ID. The renewal of the Certificate will be provided on Business days (Monday to Friday) between 10.30 AM to 5.00 PM, excluding National holidays and State holidays.

2.5. Downloading the Certificate:

a. After the Certificate is renewed an eMail & SMS notifications are automatically sent to the applicant to the Email address & Mobile number provided during the Certificate request.

b. The User should check his/her eMail & SMS for the notification for every 5 minutes by refreshing the Mailbox / Inbox.

c. Follow the steps defined in the 'MANDATORY - Verification Guidelines issued by CCA or CA' for downloading the Certificate.

Controller's Powers

Powers of CCA

According to the Act, following powers have been conferred on the controller of certifying authority. These powers are enumerated as below:

Power to delegate

According to section 27 of the Act, the controller can delegate any of his powers, and may authorize the Deputy and Assistant controller or any officer to exercise the same.

Power to investigate contraventions

According to section 28 of the Act, investigations can be made by the controller or any officer authorised for any contraventions of the provisions of the ACT.

Access to computers and data

According to section 29 of the Act, the controller may have access to any computer resources, computer system of any person to acquire any information, during the course of exercising his duties helpful in further investigations.

Procedure to be followed by CA Functions and powers of CA

Certifying Authority to issue Digital Signature Certificate (DSC)

Representations to be checked while issuing DSC

Suspension of DSC

Revocation of DSC

Functions and power of certifying Authority

According to the ACT, the following are the functions of certifying authority: To issue the Digital Signature Certificate (section 35) To check the representations while issuing digital signature certificate (Section36) To suspend the digital signature certificate (Section 37) To revoke the digital signature certificate (Section 38)

(a) Certifying Authority to issue Digital Signature Certificate

According to section 35, following steps are required to be followed by the certifying authority to issue digital signature certificate.

Any person can make an application to the Certifying Authority, for the issue of Digital Signature Certificate in such form, as may be prescribed by the Central Government.

Every such application shall be accompanied by such fee, not exceeding twenty five thousand rupees, as may be prescribed by Central Government to be paid to the certifying authority. Provided that while prescribing fees under sub-section (2), different fees may be prescribed for different classes of applicants.

Every such application shall be accompanied by a certification practice statement, or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application

No Digital Signature Certificate shall be granted, unless the Certifying Authority is satisfied that-

The applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

The applicant holds a private key, which is capable of creating a digital signature;

The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant

No application can be rejected unless an applicant has been heard on that matter and given a reasonable opportunity.

Procedure to be followed by Certifying Authority

Certification Practice Statement (CPS)

i) Each licenced certifying authority will bring about a detailed statement of practices and operational procedures proposed to be employed by him in the form of Certification Practice Statement (CPS) for issue of Digital Signature Certificate. Each licensed certifying authority shall use the model the Certification Practice Statement prescribed by the Controller as a guide to prepare his Certification Practice Statement.

ii) Any change in the Certification Practice Statement during the term of licence shall require prior approval of the Controller.

iii) Every licensed certifying authority shall highlight to its subscriber any limitation of their liabilities and, in particular, it must draw the subscriber's attention to the implications of reliance limits on their certificate.

iv) The subscriber identity verification method for issuance, suspension, revocation and renewal of a certificate must be specified in the Certification Practice Statement.

v) A copy of the latest version of Certification Practice Statement together with effective date must be filed with the Controller and published on the certifying authority's Internet website accessible to the public.

vi) After the effective date, the latest version of the Certification Practice Statement filed with the Controller will be the prevailing version for a particular certificate.
vii) Every certifying authority must log all changes to the Certification Practice Statement together with effective date of each change.
viii) The certifying authority shall keep in a trustworthy manner a copy of each version of the Certification Practice Statement, together with the date it came into effect and the date it ceased to have effect.
ix) The certifying authority must disclose information to its subscribers and relying parties on the assurance level(s) of the certificates that it issues and the limitations of its liabilities. This is to enable the users to make informed choices on the types of certificates that meet their usage requirements.
x) Security and risk management controls must be instituted to ensure that security policies and safeguards are in place. Such controls include personnel security and incident handling measures to prevent fraud and security breaches.
xi) The certifying authority shall utilize only trustworthy systems in performing their respective services.
Disclosure : Every certifying authority shall create its own web page on the internet. The home page shall, inter alia, contain the following :
(a) its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;
(b) any certification practice statement relevant thereto;
(c) notice of the revocation or suspension of its Certifying Authority certificate, if any; and
(d) any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

Identity Verification of Subscriber

Certifying authority shall have the sole responsibility of the verification and authentication of the subscriber. Certifying authority, therefore, must enforce an adequate authentication method to verify the identity of the subscriber. Certifying Authority must publish the procedures for verification of the identity of the subscriber in his certification practice statement.

Records Documenting Compliance

i) The certifying authority shall maintain and make available to Controller on his request, records in a trustworthy fashion, including
(a) documentation of their own compliance with the CPS, and
(b) documentation of actions and information that is material to each certificate application and to the creation, issuance, use, suspension, revocation, expiration, and renewal or re-enrollment of each certificate it issues. These records shall include all relevant evidence in the certifying authority possession regarding

- the identity of the subscriber named in each certificate
- the identity of persons requesting suspension or revocation of certificate issued to him.
- time stamps indicating the date and time when the certificate was:
  - issued to subscriber
  - request received for revocation or suspension
  - revocated or suspended
  - notified/published
- other facts represented in the certificate, and
- certain foreseeable material facts related to issuing certificates.

ii) Records may be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate and complete. The certifying authority shall retain the record in a trustworthy manner as prescribed in CPS.

Security Guidelines for Certifying Authorities

The Certifying Authorities that intend to be licensed by the Controller shall comply with the mandatory IT security and digital signature guidelines given at Annexure-II.

Issuance of Certificates

i) In addition to the requirement specified in Section 35 of the Information Technology Act, 2000, every certifying authority shall comply with the requirement in this rule in relation to the issuance of certificates.

ii) The certificate must contain or incorporate by reference such information as is sufficient to locate or identify one or more repositories in which notification of revocation of suspension of the certificate will be listed if the certificate is suspended or revoked.

iii) The subscriber identity verification method employed for issuance of certificate must be specified in the Certification Practice Statement and is subject to the approval of the Controller during the application for a licence.

iv) When the certificate is issued to a person (referred to in this rule as a New Certificate) on the basis of another valid certificate held by the same person (referred in this rule as an Originating Certificate) and subsequently the originating certificate has been suspended or revoked, the certifying authority that issued the new certificate must conduct investigations to determines whether it is necessary to suspend or revoke the new certificate.

v) The licensed certifying authority must provide a reasonable opportunity for the subscriber to verify the contents of the certificate before it is accepted.

vi) If the subscriber accepts the issued certificate, the licensed certifying authority shall publish a signed copy of the certificate in a repository.

vii) If the subscriber does not accept the certificate, the licensed certifying authority shall not publish it.

viii) Once the certificate has been issued by the licensed certifying authority and accepted by the subscriber, the licensed certifying authority shall notify the subscriber within a reasonable time of any fact known to the licensed certifying authority that significantly affects the validity or reliability of the certificate.

Digital Signature Standard

i) The asymmetric cryptographic algorithms used for generation of digital signature shall conform to the IEEE Standard Specifications for public key cryptography.
ii) The cryptographic keys and algorithms shall be sufficiently strong to protect the cryptographic result (e.g. digital signature) from attacks for the life span of the keys.

Digital Signature Certificate Standard

All Digital Signature Certificates issued by the Certifying Authorities shall conform to ANSI X.509 standard. The Certificate shall inter alia contain the following data:
1. Sl. No. (assigning of serial No. to the Digital Signature Certificate by Certifying Authority to distinguish it from other certificate)
2. Signature Algorithm Identifier (which identifies the algorithm used by Certifying Authority to sign the certificate)
3. Issuer Name (name of the CA who issued the certificate)
4. Validity period of the digital signature certificate
5. Name of the Subscriber (whose public key the Certificate identifies)
6. Public Key Information of the Subscriber

Certificate Management

i) To ensure the integrity of its digital certificates, the certifying authority must implement appropriate security controls in the certificate management processes, i.e. certificate registration, generation, issuance, publication, renewal, suspension, revocation and archival.
ii) The certifying authority must implement suspension and revocation procedures to suspend or revoke certificates once such requests have been verified to be valid. Suspension and revocation information must be published within the time interval specified in the Certificate Practice Statement (CPS) of the certifying authority.
iii) The certifying authority must ensure the continued accessibility and availability of its certificate repository to its user community, i.e. its subscribers and relying parties.
iv) The certifying authority must maintain a secure archive of its subscribers' certificates and registration information for the minimum period stipulated in the Rules to facilitate verification of digital signatures after the certificates have expired.
v) Certifying Authority must publish their certificate, revocation date and CPS.

Key pair generation

i) The key pair shall be generated using certifying authority controlled key generation software.

ii) Each subscriber will have control over the generation of his/her own digital signature pairs using application provided by certifying authority.

iii) The key pair generation for subscriber shall be in accordance with the certification practice statement of certifying authority.

iv) The public key parameters shall be generated via certifying authority's authorized software.

v) Certifying authority shall not backup the private signing keys of the subscriber. The subscriber should backup their private signing keys and shall ensure those keys are securely protected.

Key Management

i) The cryptographic keys provide the basis for the functions of the digital certificates, e.g. authentication and digital signature. Hence the keys must be adequately secured at each phase of their life cycle, i.e. key generation, distribution, storage, usage, backup, archival and destruction.

ii) As the cryptographic components of the certifying authority systems are highly sensitive and critical, the components must be subjected to an audit review to ensure their integrity and assurance.

iii) The certifying authority must establish procedures to immediately revoke the affected subscribers' certificates in the event of a compromise of its own digital signature private key.

iv) Adequate backup measures must be implemented to ensure the continued availability of cryptographic keys in the event of loss or corruption of the keys.

v) A certifying authority shall securely generate and protect its own private key(s), using a trustworthy system, and take necessary precautions to prevent its loss, disclosure, modification, or unauthorized use.

vi) Certifying Authority must use trustworthy hardware, software and encryption techniques approved by the controller for all operations requiring the use of their private key.

Systems and Operations

i) Each certification authority shall make and keep in a trustworthy manner the records relating to –

a. activities in issuance, renewal, suspension and revocation of certificates (including the process of identification of any person requesting a certificate from a licensed certifying authority);

b. the process of generating subscribers' (where applicable) or the licensed certifying authority's own key pairs.

c. The administration of a licensed certifying authority's computing facilities

d. Such critical related activity of a licensed certifying authority as may be determined by the Controller.

ii) Certifying Authority shall archive all certificates issued by it and maintain mechanisms to access such certificate for a period of not less than seven years.

iii) Every licensed certifying authority shall retain all records required to be kept under Section (i) above and all logs of the creation of the archive of certificates referred to in Section (ii) above for a period of not less than seven years.

iv) Certifying authority must implement access and integrity controls on the systems that store and process the subscribers' information and certificates.

v) Certifying authority must deploy physical security measures to protect the systems and related assets from physical security threats.

Requirements Prior to Cessation

Before ceasing to act as a certifying authority, a certifying authority must:

(a) Notify the controller of its intention to cease acting as an certifying authority. Such notice shall be made at least ninety (90) days before ceasing to act as an certifying authority. The certifying authority may require additional statements in order to verify compliance with this provision.

(b) Provide to the subscriber of each unrevoked or unexpired certificate it issued ninety (90) days notice of its intention to cease acting as an IA.

(c) Revoke all certificates that remain unrevoked or unexpired at the end of the ninety (90) day notice period, whether or not the subscribers have requested revocation.

(d) Give notice of revocation to each affected subscriber.

(e) Make a reasonable effort to ensure that discontinuing its certification services will cause minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding certificates.

(f) Make reasonable arrangements for preserving its records.

(g) Pay reasonable restitution (not to exceed the certificate purchase price) to subscribers for revoking their certificates before their expiration date.

Personnel

i) Certifying authority shall formulate and follow personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. Such practices shall be consistent with their CPS.

ii) An applicant shall take reasonable measures to ensure that every trusted person –

(a) is a fit and proper person to carry out the duties assigned to him;

(b) is not an undischarged bankrupt in India or elsewhere or has made a composition or an arrangement with his creditors; and

(c) has not been convicted, whether in India or elsewhere, of –

i) an offence, the conviction for which involved a finding that he acted fraudulently or dishonestly; or

ii) an offence under the Act or these Rules.

iii) Every trusted person must –

(a) have a good knowledge of the Act and these Rules;

(b) be trained in the certifying authority's certification practice statement; and

(c) possess the relevant technical qualifications, expertise and experience to effectively carry out his duties.

iv) All employees, contractors, and consultants of a certifying authority (collectively, "personnel") that have access to or control over cryptographic operations that may materially affect the certifying authority issuance, use, suspension, or revocation of certificates, including access to restricted operations certifying authority's repository, shall, for purposes of this CPS, be considered as serving in a trusted position. Such personnel include, but are not limited to, customer service personnel, system administration personnel, designated engineering personnel, and executives who are designated to oversee the Certifying Authority trustworthy system infrastructures.

v) Certifying Authority shall conduct an initial investigation of all personnel who are candidates to serve in trusted positions to make a reasonable attempt to determine their trustworthiness and competence. certifying authority shall conduct periodic investigations of all personnel who serve in trusted positions to verify their continued trustworthiness and competence.

vi) All personnel who fail an initial or periodic investigation shall not serve in a trusted position. The removal of any person serving in a trusted position shall be at the sole discretion of the applicable certifying authority.

Audit

i) Certifying Authority shall implement and maintain trustworthy systems to maintain and preserve record for all material events, such as key generation and certificate application, validation, suspension, and revocation of Digital Signatures. Such record shall be made accessible to the controller, an auditor or an officer authorized by the Controller. A computer security professional accredited by the controller shall audit the operations of certifying authority at least annually, at the sole expense of the audited entity, to evaluate its compliance with this CPS and other applicable agreements, guidelines, procedures, and standards.

ii) The firm or company to which the audit team belongs must be independent of the certifying authority being audited and must not be a software or hardware vendor that is or has been providing services or supplying equipment to the certifying authority.

iii) Auditing fees as specified by the Controller shall be borne by the certifying authority.

iv) A copy of every audit report shall be submitted to the Controller within 4 weeks of the completion of an audit.

v) Failure to pass the audit may be a ground for revocation of a licence.

Issue, Suspension and Revocation of Digital Signatures Certificate, Duties of Subscribers

1. Certifying Authority to issue Digital Signature Certificate

(1) Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applications;

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the Certification practice statement or the other statement under sub-section (3) and after making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application :

Provided that no Digital Certificate shall be granted unless the Certifying Authority is satisfied that-

(a) the application holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;

(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant : Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

2. Representation upon issuance of Digital Signature Certificate

A Certifying Authority while issuing a Digital Signature Certificate shall certify that-

(a) it has complied with the provisions of this Act and the rules and regulations made thereunder;

(b) it has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;

(d) the subscriber's public key and private key constitute a functioning key pair;

(e) the information contained in the Digital Signature Certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

3. Suspension of Digital Signature Certificate

(1) Subject to the provisions of sub-section (2), the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate,-

(a) on receipt of a request to that effect from-

(i) the subscriber listed in the Digital Signature Certificate; or
(ii) any person duly authorised to act on behalf of that subscriber;
(b) if it is of opinion that the Digital Signature Certificate should be suspended in public interest.
(2) A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.
(3) On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

4. Revocation of Digital Signature Certificate

(1) A Certifying Authority may revoke a Digital Signature Certificate issues by it-
(a) where the subscriber or any other person authorised by him makes a request to that effect; or
(b) upon the death of the subscriber; or
(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.
(2) Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that-
(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;
(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;
(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability;
(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.
(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.
(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communication the same to the subscriber.

5. Notice of suspension or revocation

(1) Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.
(2) Where one or more repositories are specified, the Certifying Authority shall publish notice of such suspension or revocation, as the case may be, in all such repositories.

Duties of Subscribers (Section 40 to 42)

Section : 40. Generating key pair.

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

Section : 41. Acceptance of Digital Signature Certificate.

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate—

(a) to one or more persons;

(b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that—

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;

(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;

(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Section : 42. Control of private key.

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation.— For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

Penalties and Adjudication

1. Penalty of damage of computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer or computer network,-

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or other programmes residing in such computer, computer system or computer network;
(e) disrupts or causes disruption of any computer, computer system or computer network;
(f) denies or causes the denial of access to any person authorised to access any computer, or computer network by any means ;
(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder ;
(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.
Explanation.- For the purpose of this section,-
(i) "computer contaminant" means any set of computer instructions that are designed-
(a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
(b) by any means to usurp the normal operation of the computer, computer system, or computer network;
(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed some other event takes place in that computer resource;
(iv) "damage " means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

2. Penalty for failure to furnish information, return, etc.
If any person who is required under this Act or any rules or regulations made thereunder to-
(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
(b) file any return or furnish any information, books or other documents within the time specified therefor in the regulation fails to file return or furnish the same within the time specified therefor in

the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

3. Residuary penalty

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

4. Power to adjudicate

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and-

(6) all proceedings before it shall be deemed to be judicial proceedings within
the meaning of sections 193 and 228 of the Indian Penal Code;

(7) shall be deemed to be a civil court for the purpose of section 345 and .46 of the Code of Criminal Procedure, 1973.

5. Factors to be taken into account by the adjudicating officer

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely :-

(a) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;

(b) the amount of loss caused to any person as a result of the default;

(c) the repetitive nature of the default.

Appellate Tribunal

Cyber Appellate Tribunal

The office of the adjudicating officer is established under S.46 of the IT Act, which provides that the person appointed to such a post must be a government officer of a rank not below that of a Director or an equivalent rank, and must have experience both in the field of Information Technology as well as legal or judicial experience. In most cases, the appointed adjudicating officer is the Principle Secretary to the Department of Information Technology in the state. The decisions of these adjudicating officers determine the scope and meaning of several provisions of the IT Act, and are instrumental in the development of the law in this field and filling a lacuna regarding the interpretation of these important provisions, particularly in areas such as data protection and privacy. However, despite the large number of cyber-crime cases being registered across the country, there is a lack of available judgments on the adjudication of disputes under Sections 43, 43A, 44 and 45 of the Act. Of all the states, only the websites of the Departments of Information Technology in Maharashtra, Tamil Nadu, New Delhi, and Haryana have reported judgments or orders of the Adjudicating Officers. The adjudicating officer in Maharasthra, Rajesh Aggarwal, has done a particularly commendable job, having disposed of 51 cases under the IT Act, with 20 cases still pending.

The first Cyber Appellate Tribunal set up by the Central Government is located at New Delhi. Although a second branch of the Tribunal was to be set up in Bangalore, no efforts seem to have been made in this regard. Further, the position of the Chairperson of the Appellate Tribunal, has been left vacant since 2011, after the appointed Chairperson attained the age of superannuation and retired. Although judicial and technical members have been appointed at various points, the tribunal cannot hold hearings without a chairperson. A total of 17 judgments have been passed by the Cyber Appellate Tribunal prior to the retirement of the chairperson, while the backlog of cases is continuously growing. Despite a writ petition being filed before the Karnataka High Court and the secretary of the Department of IT coming on record to state that the Chairperson would be appointed within 6 months (of September 2013), no action seems to have been taken in this regard, and the lacunae in the judicial mechanism under the IT Act continues. The proper functioning of adjudicating officers and the Cyber Appellate Tribunal is particularly necessary for the functioning of a just judicial system in light of the provisions of the Act (namely, Section 61) which bar the jurisdiction of ordinary civil courts in claims below the amount of Rs. 5 Crores, where the adjudicating officer or the CAT is empowered.

Procedure and powers of the Cyber Appellate Tribunal –

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it ex parte;

(g) any other matter which may be prescribed.

(3) Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of section 193 and 228, and for the purposes of section 196 of the Indian Penal Code(45 of 1860) and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

Offences

The faster world-wide connectivity has developed numerous online crimes and these increased offences led to the need of laws for protection. In order to keep in stride with the changing generation, the Indian Parliament passed the Information Technology Act 2000 that has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The law defines the offenses in a detailed manner along with the penalties for each category of offence.

Offences

Cyber offences are the illegitimate actions, which are carried out in a classy manner where either the computer is the tool or target or both.

Cyber-crime usually includes the following −

- Unauthorized access of the computers
- Data diddling
- Virus/worms attack
- Theft of computer system
- Hacking
- Denial of attacks
- Logic bombs
- Trojan attacks
- Internet time theft
- Web jacking
- Email bombing
- Salami attacks
- Physically damaging computer system.

The offences included in the I.T. Act 2000 are as follows −

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Protected system.
- Penalty for misrepresentation.
- Penalty for breach of confidentiality and privacy.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Publication for fraudulent purpose.
- Act to apply for offence or contravention committed outside India Confiscation.

- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Compounding of Offences

As per Section 77-A of the I. T. Act, any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.

No offence shall be compounded if −

- The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR
- Offence affects the socio economic conditions of the country; OR
- Offence has been committed against a child below the age of 18 years; OR
- Offence has been committed against a woman.

The person alleged of an offence under this Act may file an application for compounding in the Court. The offence will then be pending for trial and the provisions of Sections 265-B and 265-C of Cr. P.C. shall apply.

Part A (ONE Mark)
Multiple Choice Questions
Online Examination

Part B (2 Marks)

1. What are the certain procedures following Certifying Authority?
2. What Is Digital Signature Certificate?
3. Who issues Digital Signature certificates?
4. What are the requirements while you apply for a digital signature certificate?
5. Define Controller's Powers.
6. Give note on i) Key pair generation ii)Key Management
7. Define Audit.
8. Define Cyber Appellate Tribunal.
9. What is Compounding of Offences?

Part C (8 Marks)

1. Discuss the regulations of Certifying Authorities.
2. List out points of Appointment and Functions of Controller.
3. Who issues DSC and what are the different types of DSC?
4. Discuss the steps to apply for a digital signature certificate.
5. What are the processes for Renewal of Digital Certificates? Explain.
6. List out the procedure to be followed by CA and also the functions and powers of CA.
7. Explain the Duties of Subscribers.
8. Describe the Penalties and Adjudication.
9. Discuss the procedure and powers of the Cyber Appellate Tribunal.

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed University Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2017 onwards)
DEPARTMENT OF COMMERCE (CA)

SUBJECT: : Cyber Crime and Laws
SEMESTER : VI
SUBJECT CODE: 17CCU604B CLASS : III B.COM CA
UNIT : V

S.NO	QUESTIONS	OPTION 1	OPTION 2	OPTION 3	OPTION 4	ANSWER
1	certifying public keys of the Certifying Authorities is the functions of	Supervisor	Controller	Executive	administrator	Controller
2	_____are the digital equivalent of physical or paper certificates.	Electronic Signed Certificates	Electronic Signature Certificates	Digital Signed Certificates	Digital Signature Certificates	Digital Signature Certificates
3	The list of licensed CAs along with their contact information is available on website	www.clc.gov.in	www.ccl.gov.in	www.cca.gov.in	www.lca.gov.in	www.cca.gov.in
4	_____provides safety and security for online banking transactions by digitally verifying financial transactions	DSC	ESC	CSC	TSC	DSC
5	Who issues the Digital Signature Certificate?	Certifying controller	Certifying authority	Certifying supremacy	Certifying mastery	Certifying authority
6	Digital signature license come under which section?	24	34	44	54	24
7	Which of the following is not needed for getting Digital Signature?	AADHAR Card	PAN Card	ATM Card	VOTER ID Card	ATM Card
8	A demand draft or cheque must be obtained towards payment for application of DSC in the name of the _____	Local Registration Counseller	Local Registration Certifier	Local Registration Authority	Local Registration Administrator	Local Registration Authority
9	The applicant can approach_____office for obtaining the Enrollment Kit	SPTS	APTS	CPTS	RPTS	APTS
10	Which kit consists of Application and User Manual for getting digital signature?	Enrollment	Registration	Authorisation	licensing	Enrollment
11	_____make use of hardware, software and procedures that are secure from intrusion and misuse.	Certifying Authority	Certifying supremacy	Certifying controller	Certifying mastery	Certifying Authority
12	Who resolves conflict of interests between the Certifying Authorities and the subscribers?	Controller	Provider	Administrator	Applicant	Controller
13	Who holds a private key, which is capable of creating a digital signature?	Administrator	Applicant	Provider	Controller	Applicant
14	Who having the sole responsibility of the verification and authentication of the subscriber?	Certifying mastery	Certifying authority	Certifying authority	Certifying controller	Certifying authority
15	Certifying Authority must publish the_____for verification of the identity of the subscriber	procedures	algorithms	techniques	mechanisms	procedures
16	Which of the following is not indicated by time stamp printed on the digital certificate?	Revocated time	Time of issuing	Suspended time	Printed time	Printed time
17	The subscriber identity verification method employed for issuance of certificate must be specified in the _____	Subscriber document	Provider document	Digital Practice Statement	Certification Practice Statement	Certification Practice Statement
18	Who publishes a signed copy of the certificate in a repository?	Subscriber	Certifying authority	Verifier	Controller	Certifying authority
19	Asymmetric cryptographic algorithm used for creating Digital Signature Certificate follows standard.	IEEE	ACM	ISO	ANSI	IEEE
20	The Information Technology Act 2000 that has been conceptualized on the_____Model Law.	United Nations committee on International Trade Law	Universal Nations Commissions on International Trade Law	Universal Nations committees on International Trade Law	United Nations Commissions on International Trade Law	United Nations Commissions on International Trade Law
21	Which Parliament passed the Information Technology Act 2000?	Russian	Indian	American	French	Indian
22	The office of the adjudicating officer is established under_____of	S.56	S.26	S.46	S.36	S.46

	the IT Act.					
23	Who is Principle Secretary to the Department of Information Technology in the state.	Controller	Subscriber	Certifying Authority	adjudicating officer	adjudicating officer
24	Which of the following state's website is not displaying orders of adjudicating officer?	Tamilnadu	Haryana	Maharashtra	Karanataka	Karanataka
25	The first Cyber Appellate Tribunal set up by the Central Government is located at	Bangalore	New Delhi.	Chennai	Trivandrum	New Delhi.
26	How much penalty should need to pay for not maintaining book of accounts/records	10,000 for each year	20,000 for each day	10,000 for each day	20,000 for each year	10,000 for each day
27	The Rank of adjudicating officer is not below the rank of _____	Director of the Governmen t of India	Director of the State Governmen t	Director of the Nationalis ed Bank	Director of the	Director of the Governme nt of India
28	Whom having the powers of Civil Court?	Certifying Authority	adjudicatin g officer	Verificatio n Authority	Controlli ng Officer	adjudicati ng officer
29	_____means any set of computer instructions that are designed to modify, destroy, record, transmit data or programme residing within a computer,	computer contaminan t	Computer immaculate	computer disfigurem ent	computer smut	computer contamina nt
30	_____means a representation of information, knowledge, facts, concepts or instructions in text, image, audio video that are being prepared	computer disk	computer OS	computer files	computer data base	computer data base
31	No person shall be appointed as an adjudicating officer unless he have experience in the field of _____	Informatio n Technolog y	Criminal justices	Forensics	Genomic s	Informatio n Technolog y
32	Who must publish the procedures for verification of the identity of the subscriber in his certification practice statement.	Controlling Officer	adjudicatin g officer	Certifying Authority	Verificati on Authority	Certifying Authority
33	Who verifies, digitally signs and releases the request for renewal of the Digital Certificate?	MPTS Issuing Authority	APTS Issuing Authority	RPTS Issuing Authority	CPTS Issuing Authority	APTS Issuing Authority
34	If the_____does not accept the certificate, the licensed certifying authority shall not publish it.	verifier	subscriber	provider	controller	subscriber
35	Certifying Authority must publish their certificate,_____date and CPS.	revocation	delivery	suspensio n	Registere d	revocation
36	Certifying authority shall not backup the_____signing keys of the subscriber.	partial	private	primary	public	private
37	How many phases are there in Digital Certificate creation?	six	seven	eight	nine	seven
38	What is the last stage of Digital Certificate?	distribution	backup	destructio n	archival	destructio n
39	Cryptography components must be subjected to an_____to ensure their integrity and assurance.	Formal review	Peer review	Informal review	Audit review	Audit review
40	Which measures are useful in the event of loss or corruption of the cryptographic key.	backup	storage	verificatio n	Validity	backup
41	Certifying Authority must use trustworthy hardware, software and encryption techniques approved by the	Subscriber	Controller	Verifier	Provider	Controller
42	The process of generating subscribers is the duty of _____	Certificatio n authority	Certificatio n controller	Certificati on validator	Certificat ion producer	Certificati on authority
43	Certifying authority must deploy_____measures to protect the systems and related assets	Conceptual security	physical security	Logical control	Access control	physical security
44	Notice shall be made at least_____days before ceasing to act as an certifying authority.	ninety	fifty	forty	thirty	ninety
45	A copy of every audit report shall be submitted to the Controller within_____of the completion of an audit by the certifying authority	2 weeks	4 weeks	3 weeks	5 weeks	4 weeks
46	The persons who apply for digital certificates may pay not exceeding Rs	35000	3500	2500	25000	25000
47	To whom the applicants of digital certificate pay the fee?	Certificatio n authority	Certificatio n controller	Certificati on validator	Certificat ion producer	Certificati on authority
48	Various applicants are collected various fees based under the subsection	2	5	4	3	2
49	Every application of digital certificate shall be accompanied by a	Certificate approving Statement	Certificate verification Statement	Certificate usage Statement	Certificat e practice Statemen t	Certificate practice Statement
50	Certifying authority shall not backup the_____signing keys of the subscriber.	Private	Primary	Public	Partial	Private
51	Who should backup their private signing keys and shall ensure those keys are securely protected?	authority	controller	subscriber	verifier	subscriber

52	RA enters the Certificate Request Number on the Certificate Request Form submitted by the	controller	subscriber	verifier	applicant	applicant
53	Certifying authority follows steps under section ____ to issue digital signature certificate.	25	15	35	55	35
54	Certifying Authority maintain mechanisms to access such certificate for a period of not less than years.	seven	eight	ten	six	seven
55	Digital certificate's auditing fees is specified by the _____	Controller	Verifier	Certifying authority	Certifying practioner	Controller
56	"Publishing of information which is obscene in electronic form" is an offense included in IT ACT	2000	2003	2001	2002	2000
57	Who shall generate the key pair by applying the security procedure?	subscriber	applicant	controller	practioner	subscriber
58	A Digital Signature Certificate is suspended under section	17	37	27	47	37
59	Acceptance of Digital Signature Certificate is duty of	controller	subscriber	applicant	practioner	subscriber
60	Control of private key is come under which section?	42	52	22	32	42