



Cyber Crimes & Laws - safafa

Information Security (University of Delhi)



Scan to open on Studocu

Cyber Crimes and Laws

B.Com. Semester III Paper BC 3.4 (b) and
B.Com. (Hons.) Semester IV Paper BCH 4.5 (d)

Sushila Madan

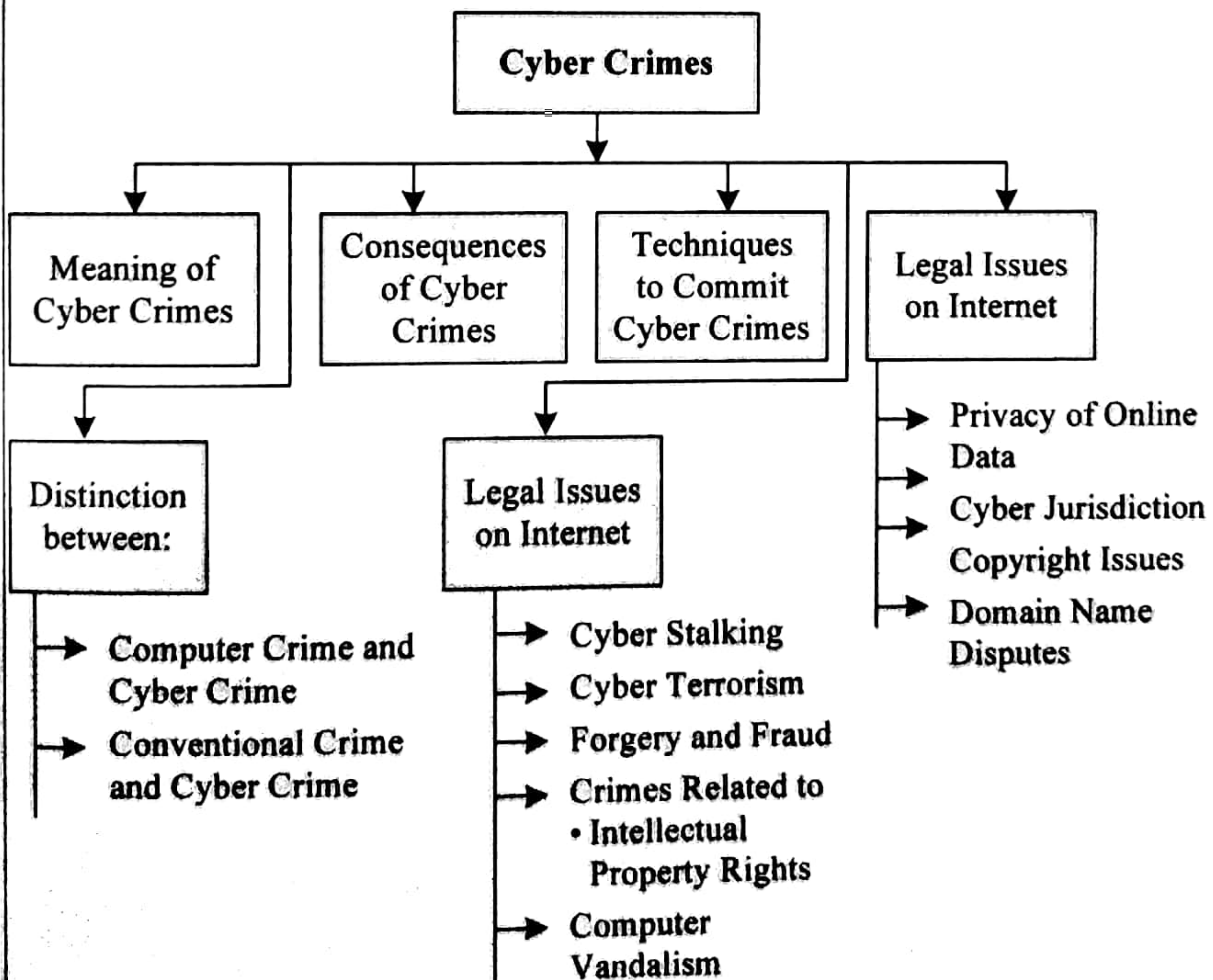


1

Cyber Crimes

➤➤ Objectives ◀◀

In this Chapter, we will learn:



INTRODUCTION

With the advent and increasing use of Internet, the businesses have crossed the barriers of local markets and are reaching out to customers located in any part of the world. Computers are widely used in enterprises not only as a tool for processing information, but also for gaining strategic and competitive advantage. The key business operations in enterprises are performed using computers. Computers can be used both for constructive and destructive reasons.

With the advent of internet, many computer crimes can be committed from any part of the globe, without computer knowledge. Cyber-criminals use false identity and work from remote locations. Even if the real IP address of the cybercriminal is detected, it is difficult to link an IP address to a person and hold them accountable in a court of law.

1.1 WHAT IS CYBERCRIME?

Cybercrime is defined as an unlawful act committed using a computer either as a tool or as a target (or both) for facilitating a crime.

The advancement of technology has increased the scope of cyber frauds. As information around the globe has become more accessible, it has also become more vulnerable to misuse. The major reasons behind the increase in cyber frauds are:

- **Failure of Internal Control System.** Internal controls may be defined as the policies, procedures, practices, and organizational structures that are designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. For example, firewalls and antivirus program. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. Antivirus software should update virus definitions frequently.
- **New Risks.** In the dynamic world of cyber crime, organizations may fail to identify new risks (such as viruses, spyware,

malware) and implement countermeasures against those risks.

- **Smart Fraudsters.** Fraudsters are innovating new smart techniques to target weaknesses in the system even before the organization realizes that such gaps exist in the security system.

In cybercrime, computer is necessary as one of the components of the offence. **Crime committed by using any digital device such as mobiles, pen-drives, CDs is covered under the ambit of cyber-crime.**

1.2 DISTINCTION BETWEEN COMPUTER CRIME AND CYBERCRIME

Cybercrimes typically are those in which special knowledge of cyberspace such as telecommunication devices, protocols and computers is used to commit a crime, whereas computer crimes are those in which the perpetrator uses computer technology to offend.

The terms “cybercrime” and “computer crime” have become nearly synonymous, although there is a difference between these two events.

“**Computer Crime**” encompasses crimes committed against the computer, the materials contained therein such as software and data, and its uses as a processing tool. These include hacking, denial of service attacks, unauthorized use of services and cyber vandalism.

Simply **computer crime** is a criminal breaking into the house/office and taking something of the computer.

“**Cyber Crime**” describes criminal activities committed through the use of electronic communications media. One of the greatest concerns is with regard to cyber-fraud and identity theft through such methods as phishing, pharming, spoofing and through the abuse of online surveillance technology. There are also many other forms of criminal behaviour perpetrated through the use of information technology such as harassment, defamation, pornography, cyber terrorism, industrial espionage and some regulatory offences.

Cyber crime is taking something of the computer over the internet.

Also a computer crime can be doing something illegal with computers like selling illegal software. In cybercrime, computer is necessary as one of the components of the offence.

Examples of cybercrimes where **computers are used to commit crime** are:

- Pornography
- Threatening e-mail
- Assuming someone's identity
- Sexual harassment
- Defamation
- Spam
- Phishing
- Cyber terrorism
- IPR violations
- Software privacy
- Copyright infringement
- Trademark violations
- Cyberstalking

Examples of cybercrimes where **computers become target of crime** are:

- Virus
- Worms
- Hacking
- Email spamming
- Computer theft
- Defacing websites

1.3 DISTINCTION BETWEEN CONVENTIONAL CRIME AND CYBER CRIME

Apparently, there is no distinction between cybercrime and conventional crime. The main difference between conventional crime and cybercrimes is the medium used to commit crime. In cybercrimes, the involvement of computer at any stage of the crime is mandatory. The other points of differences are:

Table 1.1: Conventional Crime vs Cyber Crimes

Point of Difference	Conventional Crime	Cybercrime
Evidences of offences	Conventional criminals usually leave traces of crime through either fingerprints or other physical evidences.	Cyber-criminals leave very little evidence about the cybercrime as the crimes are committed using Internet. These criminals can freely change their identities.
Length of investigation	Conventional crimes can be investigated within a shorter time since the criminals usually leave evidence that can be used to spot them.	It takes longer to identify and apprehend cyber criminals since the perpetrators use false identity and work from remote locations. Even if the real IP address of the cybercriminal is detected, it is difficult to link an IP address to a person and hold them accountable in a court of law.
Force involved	Conventional crimes such as rape, murder, burglary involve the use of excessive force that results in physical injury and trauma on the victims.	Cybercrimes do not require the use of any force since the cybercriminals merely use the identities of their victims to steal from them.
Scale of crime	Conventional criminals come in physical proximity to the victim and therefore conventional crimes take	Cybercriminals need not come in physical proximity to the victim. A single hacker can hack thousands

	place on a relatively limited scale. For example, a criminal must enter a bank to rob it and can probably rob one or two banks in a day.	of computers all over the world.
Efforts involved	Conventional crimes are relatively more difficult to commit than cybercrimes.	Cybercrimes are relatively easier to commit as the criminal can hide his/her identity.
Detection period	Conventional crimes can generally be detected immediately or within a reasonable time.	Cybercrimes may remain undetected for a very long period.

1.4 CONSEQUENCES OF CYBERCRIMES

The consequences of cybercrimes are very serious. They may adversely affect the reputation and morale of the organization. They may even affect the very existence of the organization. **The consequences of cybercrimes are:**

- **Financial Loss:** Financial loss may be direct such as embezzlement due to fraud, or indirect as expenditure incurred for repairing the damaged electronic equipment.
- **Legal Repercussions:** It is very difficult to find the evidence of cybercrime. Even if a hacker is identified, it becomes very difficult to provide evidence against him/her in the Court.
- **Loss of Reputation and Competitive Edge:** Most of the cybercrimes are not reported as they adversely affect the reputation of the organization. If these frauds come to the limelight, the creditability of the organization is shattered.
- **Blackmail/ Industrial Espionage:** The cybercriminal may blackmail the organization as he may possess confidential information, even though it may be obtained by unfair means.
- **Disclosure of Sensitive, Confidential, or Embarrassing Information:** The disclosure of sensitive, confidential and

embarrassing information will adversely affect the reputation of the organization.

1.5 TECHNIQUES TO COMMIT CYBER CRIMES

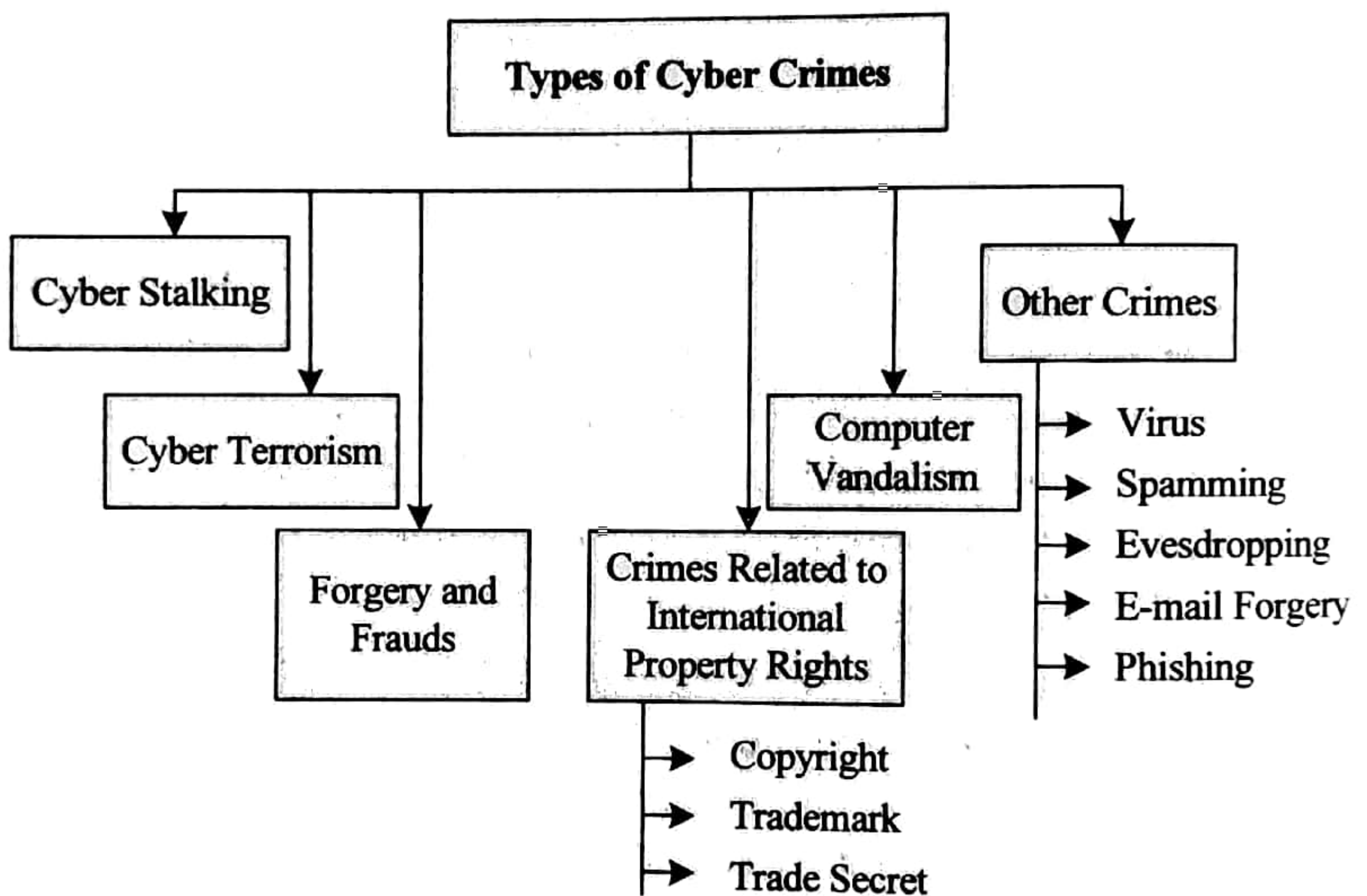
Professional cyber criminals find new ways to commit cyber-crimes and treat cybercrime as business. The different techniques to commit cybercrimes are:

- **Hacking:** “Hacking” refers to “Unauthorized Access to a Computer Network” which may otherwise be called an “Unauthorized Intrusion”. Hackers access the system through unauthorized means to check the security vulnerability of a system. They do not intend to cause damage to the system.
- **Cracking:** Crackers are hackers with malicious intentions. Un-ethical hacking may be called as cracking. There are hackers who are more malicious in nature whose primary purpose or intent is to commit a crime through their actions for some level of personal gain or satisfaction.
- **Data Diddling:** Data diddling involves changing the data going into or out of a computer. For example, an employee breaks into the payroll system and changes the number of days worked, thereby increasing his wage bill.
- **Data Leakage:** Data leakage involves removing copies of confidential data from within the system without any trace.
- **Denial of Service Attack:** Denial of service attacks prevent the system from processing or responding to legitimate traffic or requests for resources and objects. The most common of these attacks are transmitting so many emails to a server that it cannot process them all.
- **Internet Terrorism:** Internet terrorism involves disrupting e-commerce with the use of Internet.
- **Logic/Time Bombs:** These bombs lie in wait until some specified circumstances or a particular time triggers it. This circumstances/time may be like, birthdate of famous person, entering a specific password, or adding or deleting information

to and from certain computer files. On being triggered, the bomb destroys the computer data or programs.

- **Masquerading or Impersonation:** Masquerading involves gaining access to the system by pretending to be an authorized user.

1.6 TYPES OF CYBERCRIMES



The world is coming closer due to increased usage of Internet. At the same time, the Internet has made the commitment of cybercrimes easier. The different kinds of cybercrimes are:

1.6.1 Cyber Stalking

Cyber stalking is a crime to harass someone with the use of technology, particularly the Internet.

Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. Cyberstalking also includes exploitation of minors sexually or otherwise. Cyber stalkers may be either strangers to the victim or

of spam increases, locating or assessing legitimate messages can become difficult. Spams fill up the storage space and prevent legitimate messages from being delivered.

- **Eavesdropping:** It refers to listening of private conversation or accessing data transmitted with the use of wire trap.
- **E-mail Forgery:** It involves e-mail messages that look as if someone else sent it.
- **Phishing:** Phishing is an attempt to acquire sensitive information such as usernames, password, and credit card details by falsely claiming to be an established legitimate enterprise.

1.7 CYBER SECURITY

Internet has opened a variety of threats that emanate from a host of tools in the hands of people who deliberately or otherwise cause damage to the infrastructure. Cyber-attacks are quite frequent and serious. Failure to ensure proper security systems can be extremely costly, disruptive, and embarrassing, resulting in loss of present and future business. Moreover, frequent security failures can cause panic among the potential customers.

Cybersecurity is the protection of internet-connected systems, including hardware, software and data, from cyberattacks. Cyber security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation. The use of cybersecurity can help prevent cyberattacks, data breaches and identity theft and can aid in risk management.

1.7.1 Major Cyber Security Threats and Solutions to Prevent Cyber Security Threats

The major cyber security threats and solutions to prevent cyber security threats are shown in the following Table:

Security Threat	Explanation	Solution
Virus	Virus is a destructive program which disrupts the normal functioning of computer systems. Computer virus is a piece of code attached to a legitimate program that, when executed, infects other programs in the system by replicating and attaching itself to them. In addition to this, a virus may corrupt/erase files. Due to its spreading nature, a virus can cause severe damage to a system. Virus spreads because every time an infected program is executed, it tries to infect other programs.	In order to detect and eliminate virus, anti-virus software must be installed. If updated regularly, anti-virus software would be an effective tool. Virus detection software can be used for continual scanning of the hard disk(s), memory and network interfaces for known viruses and to treat the system by removing the malicious code. Both proxy servers and e-mail system should be running virus detection software. Since new viruses are continually being developed, it is important to regularly update virus detection software to the latest version to ensure detection of any recent additions to the list of known viruses.
Hackers	"Hacking" refers to "Unauthorized Access to a Computer Network" which may otherwise be called an "Unauthorized Intrusion". Hackers access the system through unauthorized means to check the security vulnerability of a system. Crackers are hackers with malicious intentions. -Un-ethical hacking	Authentication procedures provide data confidentiality and protection against unauthorized modification. Both physical access control mechanism (firewall) and logical access control mechanism (a software subsystem) can be used for an access control and authentication.

	may be called as cracking. There are hackers who are more malicious in nature whose primary purpose or intent is to commit a crime through their actions for some level of personal gain or satisfaction.	Firewall is a system or group of systems that enforces an access control policy between two networks. Firewall consists of specialized hardware and software that keep unwanted users and malicious code out of a system. Firewall software filters incoming and outgoing information and blocks unauthorized users. Firewalls prevent outsiders from accessing the data behind the firewall.
Denial of Service Attack	Denial of service attacks prevent the system from processing or responding to legitimate traffic or requests for resources and objects. The most common of these attacks are transmitting so many data packets to a server that it cannot process them all.	Firewall is quite an effective way to protect the network from untrusted, unauthorized outside users.
Eavesdropping	It refers to listening to private conversation or accessing data transmitted with the use of wire trap.	Encryption is the process of scrambling signals that represent data during transmission. It is one of the many methods of securing data by encoding information so that it is only able to be read by the individuals or computers, it was intended for. It is the process of transforming information before communicating it to make it unintelligible to all but the intended recipient.

Trojan Horse	A Trojan horse is a malicious program that is disguised as or embedded within legitimate software. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed. Trojan horse is a hidden malicious code that could alter or delete the information of client computer or perform any other unauthorized function. When a Trojan horse is planted in a computer, its instructions remain hidden. The computer appears to function normally but in fact it is performing underlying functions dictated by the instructive code.	If updated regularly, anti-virus software would be an effective tool in preventing downloading Trojan horses.
Data Leakage	It involves removing copies of confidential data from within the system without any trace. It includes exposing personal information such as email addresses, phone number, account details, etc. on social media, websites, etc.	Encrypting information so that it is only able to be read by the individuals or computers, it was intended for.

1.8 CYBER FORENSIC

Cyber forensics, also called computer forensics or digital forensics, is the process of extracting information and data from computers to serve as digital evidence to prove and legally prosecute cybercrime.

- **Logic/Time Bombs:** These bombs lie in wait until some specified circumstances or a particular time triggers it. This circumstances/time may be like, birthdate of famous person, entering a specific password, or adding or deleting information to and from certain computer files. On being triggered, the bomb destroys the computer data or programs.
- **Masquerading or Impersonation:** It involves gaining access to the system by pretending to be an authorized user.
- **Piggybacking:** It involves tapping into a communication line or standing in line with a card user at ATM and acquiring his PIN. The stolen cards are used to withdraw money from account.
- **Super Zapping:** It involves bye-passing all security systems by means of specialized software packages.
- **Trap Door:** It involves gaining illegitimate access to a computer system by using system's escapes.

SUMMARY

- Cybercrime is defined as an unlawful act committed using a computer either as a tool or as a target (or both) for facilitating a crime.
- Crime committed by using any digital device such as mobiles, pen-drives, CDs is covered under the ambit of cyber-crime.
- “Computer Crime” encompasses crimes committed against the computer, the materials contained therein such as software and data, and its uses as a processing tool.
- “Cyber Crime” describes criminal activities committed through the use of electronic communications media.
- The main difference between these two crimes is the medium used to commit crime. In cybercrimes, the involvement of computer at any stage of the crime is mandatory.

- "Hacking" refers to "Unauthorized Access to a Computer Network".
- Crackers are hackers with malicious intentions. Un-ethical hacking may be called as cracking.
- Data Diddling involves changing the data going into or out of a computer.
- Data Leakage involves removing copies of confidential data from within the system without any trace.
- Denial of service attacks prevent the system from processing or responding to legitimate traffic or requests for resources and objects.
- Internet Terrorism involves disrupting e-commerce with the use of Internet.
- Masquerading or Impersonation involves gaining access to the system by pretending to be an authorized user.
- Cyber stalking is a crime to harass someone with the use of technology, particularly the Internet.
- Cyber Terrorism is the use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically.
- Forgery is the act of altering documents stored in computerized form.
- Fraud is the crime of deceiving another, through the use of objects obtained through forgery.
- Intellectual property (IP) is a category of property that includes intangible creations of the human intellect, and primarily includes Copyrights, Patents, Trademarks, Publicity rights, Artistic work like music and literature, Discoveries, inventions, etc., and Trade secrets.
- Crimes related to Intellectual Property Rights (IPRs) may be defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations.

- A copyright is the legal right of an author, publisher, composer, or other person who creates a work to exclusively print, publish, distribute, or perform the work in public.
- A computer virus is a computer program that can copy itself and infect a computer without the permission or knowledge of the user.
- The term spam describes unwanted e-mail. It may be in the form of advertisement from vendors. Spams fill up the storage space and prevent legitimate messages from being delivered.
- Eavesdropping refers to listening of private conversation or accessing data transmitted with the use of wire trap.
- E-mail Forgery involves e-mail messages that look as if someone else sent it.
- Theft of trade secrets means the theft of ideas, plans, methods, technologies, or any sensitive information from all types of industries including manufacturers, financial service institutions, and the computer industry.
- A trademark violation involves counterfeiting or copying brand name products.
- On the Internet, computer vandalism includes acts such as a cracker replacing the original Web page with some obscene material.
- Cyber security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.
- Cybersquatting 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.
- A hacker is an unauthorized user who attempts to or gains access to an information system.
- Cyber forensics is the process of extracting information and data from computers to serve as digital evidence to prove and legally prosecute cybercrime.

- 'Jurisdiction' is the concept whereby in any legal system, the power to hear or determine a case is vested in an appropriate court.
- Domain names are simply the addresses of the Internet. Domain names are commonly used to find web sites. Domain names are used to identify Internet resources, such as computers, networks, and services.
- Identity thieves are cyber criminals who try to gain access to their victim's personal information such as name, address, phone number, bank account number, email address, credit card information, etc.
- Internet stalkers are individuals who maliciously monitor the online activity of their victims to terrorize and/or acquire personal information.
- Phishers are cyber criminals who attempt to obtain personal or sensitive information through victims' computers.
- Cyber terrorism is a well-developed, politically inspired cyber-attack in which the cyber-criminal attempts to steal data and/or corrupt corporate or government computer systems and networks, resulting in harm to countries, businesses, organizations and even individuals.
- Hackers access the system through unauthorized means to check the security vulnerability of a system. They do not intend to cause damage to the system.
- Crackers are hackers with malicious intentions. Un-ethical hacking may be called as cracking.
- Data diddling involves changing the data going into or out of a computer.
- Data Leakage involves removing copies of confidential data from within the system without any trace.
- Denial of service attacks prevent the system from processing or responding to legitimate traffic or requests for resources and objects.

- Spam involves sending unauthorized emails.
- Masquerading or Impersonation involves gaining access to the system by pretending to be an authorized user.
- Piggybacking involves tapping into a communication line or standing in line with a card user at ATM and acquiring his PIN.
- Super Zapping involves bye-passing all security systems by means of specialized software packages.
- Trap Door involves gaining illegitimate access to a computer system by using system's escapes.

REVIEW QUESTIONS

1. What is a cybercrime? What are the major reasons behind the increase in cyber frauds?
2. Distinguish between 'Computer Crime' and 'Cybercrime'.
3. Explain five examples of cybercrimes where computers are used to commit crime.
4. Explain five examples of cybercrimes where computers become target of crime.
5. Distinguish between 'Conventional Crime' and 'Cybercrime'.
6. What are the consequences of cybercrimes?
7. What are the different techniques to commit cybercrimes?
8. Explain the different types of cybercrimes.
9. Write a short note on 'Cyberstalking'.
10. What do you understand by the term 'Cyber Terrorism'?
11. Explain in brief 'Forgery and Fraud'.
12. What is intellectual property? Explain the different types of intellectual property.

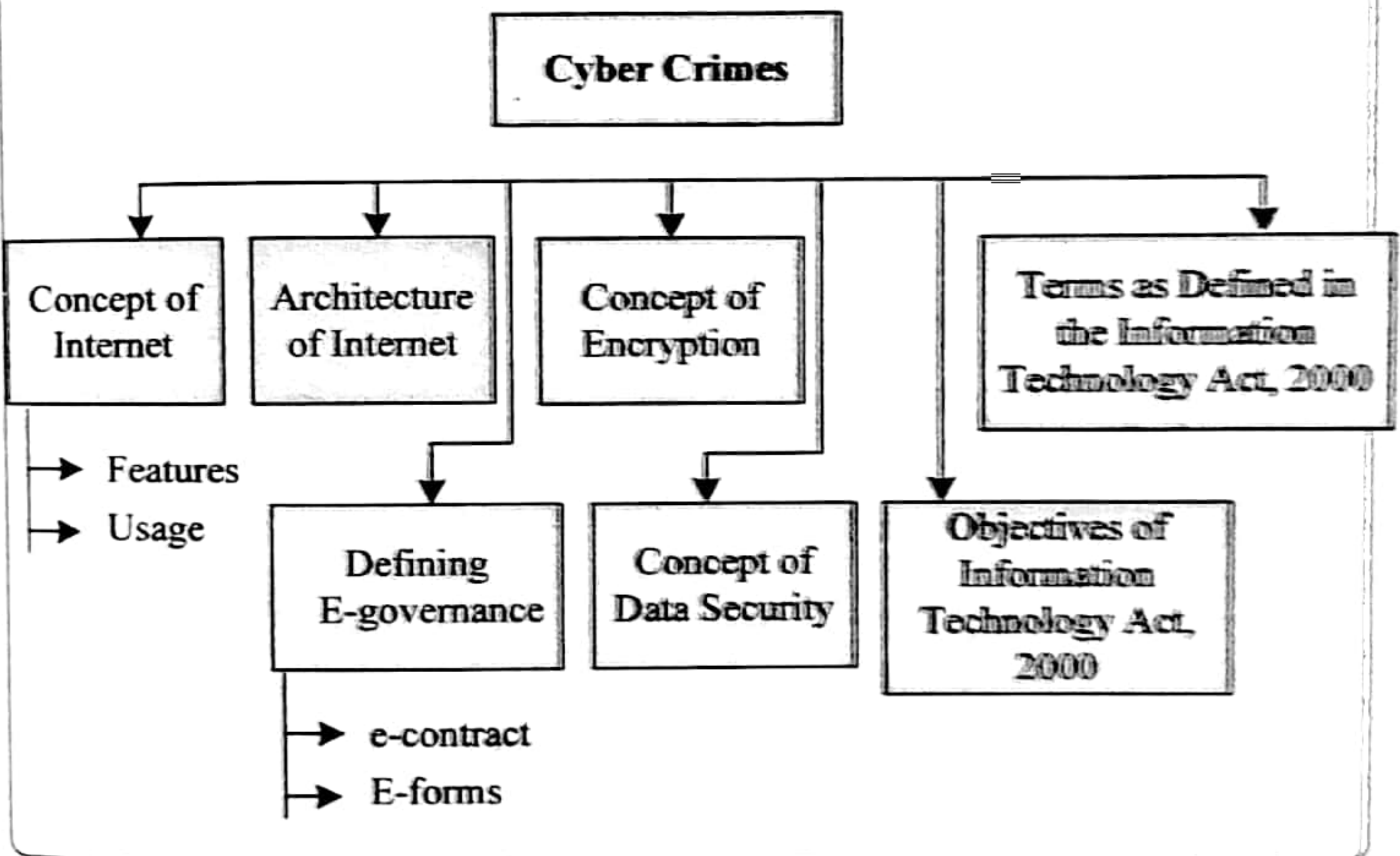
13. Write a short note on crimes related to 'Intellectual Property Rights'.
14. Write a short note on 'Computer Vandalism'.
15. Write a short note on 'Spamming'.
16. Write a short note on 'Computer Virus'.
17. Write a short note on 'Eavesdropping'.
18. Write a short note on 'E-mail Forgery'.
19. What is "cyber security"? Explain the different cyber security threats and the solutions to prevent these threats.
20. Write a short note on 'Cyber Forensic'.
21. Write a short note on 'Privacy of online data'.
22. Write a short note on 'Cyber Jurisdiction'.
23. Differentiate between IPR and Copyright Issues.
24. What is 'Domain Name Disputes'?
25. Explain the different types of domain name disputes. How domain name disputes can be resolved?
26. How domain name disputes can be resolved in India?
27. Write a short note on Internet Corporation for Assigned Names and Numbers (ICANN).
28. Explain different types of cyber criminals.
29. Explain the different techniques to commit cyber-crimes.

2

Definition and Terminology

➤➤ Objectives <<

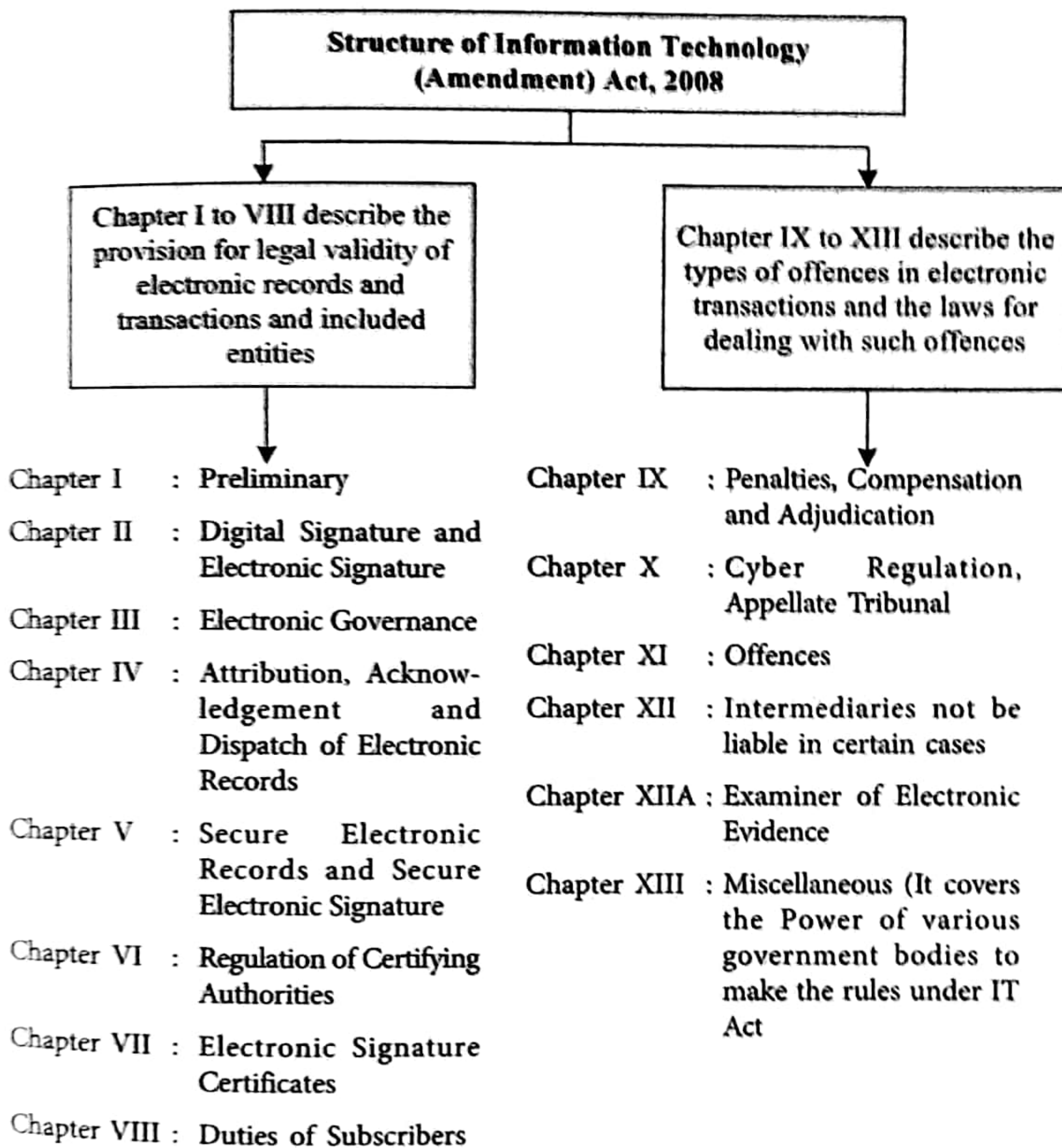
In this Chapter, we will learn:



2.1 CONCEPT OF INTERNET

Internet is a network of networks that allows computers worldwide to connect and exchange information.

and to ensure efficient operation of transactions conducted online. In addition to these, regulatory framework is mandatory to facilitate e-commerce. The IT Act, 2000 is divided into XIII Chapters. The structure of the IT ACT is given on next page.



Note: In our syllabus we will study provisions covered in the following chapters of the IT Act: Chapter I, Chapter II, Chapter III, Chapter IV, Chapter V, Chapter VI, Chapter VII, Chapter VIII, Chapter IX, Chapter X and Chapter XI.

Thus under the provisions of the IT Act, the term "Data" means and includes the following:

1. A representation of information, knowledge, facts, concepts or instructions.
 2. The representation of information, knowledge, facts, concepts or instructions may be in the form of being prepared or they have been prepared in a formalized manner.
 3. The prepared representation in the formalized manner referred under Point-2 is intended to be processed, is being processed or has been processed.
 4. The processing referred to under Point-3 must be in a computer system or computer network.
 5. Data may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes), or
 6. This representation in a formalized manner may also be stored internally in the memory of the computer.
- (p) ***"Digital Signature"*** means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

Thus under the provisions of the IT Act, the term "Digital Signature" refers to:

1. Authentication of any electronic record by a subscriber. The authentication can be done by the subscriber and not by anyone else.
 2. The authentication of electronic records must be done by means of an electronic method or procedure in accordance with the provisions of section 3.
- (q) ***"Digital Signature Certificate"*** means a Digital Signature Certificate issued under sub-section (4) of section 35.

Digital Signature Certificates are issued by a duly authorized Certifying Authority.

- (r) **“Electronic Form”** with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.
- (s) **“Electronic Gazette”** means official Gazette published in the electronic form.
- (t) **“Electronic Record”** means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.
- (ta) **“Electronic signature”** means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature, (Inserted vide ITAA-2008).
- (tb) **“Electronic Signature Certificate”** means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate, (Inserted vide ITAA-2008).
- (u) **“Function”**, in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer.

Thus under the provisions of the IT Act, the term “Function” in relation to a computer includes the following actions:

1. logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication.
 2. The acts explained under Point-1 must be from or within a computer.
- (v) **“Information”** includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche; (Inserted vide ITAA-2008).

(ze) **"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.

(zf) **"Security Procedure"** means the security procedure prescribed under section 16 by the Central Government.

(zg) **"Subscriber"** means a person in whose name the Electronic Signature Certificate is issued.

(zh) **"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.

SUMMARY

- Internet is a network of networks that allows computers worldwide to connect and exchange information.
- The most common tools of Internet include e-mail, listservs, newsgroups, telnet, gopher, FTP, and the World Wide Web.
- The architecture of internet is primarily communication network designed. The failure of individual computers or networks will not affect its overall reliability.

- Internet governance refers to the development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.
- E- Contract is a contract that is formed electronically. When e-contracts which are created online, are authenticated by affixing digital signatures or electronic signatures, are as legal as the traditional contracts entered on the paper.
- An e-form (electronic form) is a computer program version of a paper form. These forms are filled out and submitted electronically.
- Encryption is a technique for preventing the data stored in the databases and when transmitted over networks being intercepted.
- Data security is the practice of keeping data protected from corruption, and unauthorized disclosure, alteration (both addition and deletion) and access.
- Information Technology Act, 2000, legally recognized the transactions carried out by means of electronic data interchange or electronic commerce and gave legal recognition to digital signatures for authentication of any information or matter which requires authentication under any law.

REVIEW QUESTIONS

1. Describe the meaning and usages of Internet.
2. Explain the architecture of Internet.
3. What are the features of Internet?
4. Explain the tasks for which internet can be used.
5. Explain the advantages and limitations of internet.
6. Explain the concept of Internet governance.

7. Write a short note on International Telecommunications Union (ITU).
8. Write a short note on International Electrotechnical Commission (IEC).
9. Write a short note on International Standards organization (ISO).
10. Write a short note on Internet Architecture Board (IAB).
11. Write a short note on Internet Engineering Task Force (IETF).
12. Write a short note on The Internet Society (ISOC).
13. Write a short note on The Internet Assigned Numbers Authority (IANA).
14. Write a short note on Institute for Electrical and Electronics Engineers (IEEE).
15. Write a short note on World Wide Web Consortium (W3C).
16. What is an e-contract? Describe the conditions subject to which an e-contract can be enforced as legal as the traditional contracts entered on the paper.
17. Explain the main parties involved in e-contract.
18. Explain the different type of e-contracts.
19. What are the e-forms? Describe the advantages of using e-forms.
20. Describe the meaning of encryption. What purposes are being served through encryption?
21. Why data security is important? Explain the controls that help in achieving the objective of data security.
22. Write a short note on cryptography.
23. What are the objectives of IT Act, 2000?
24. Define the following important terms as defined in the IT Act, 2000 :
 - Access

- Addressee
- Adjudicating Officer
- Affixing Electronic Signature
- Appropriate Government
- Certifying Authority
- Certification Practice Statement
- Communication Device
- Computer
- Computer Network
- Computer Resource
- Computer System
- Cyber Security
- Cyber Appellate Tribunal
- Data
- Digital signature
- Electronic Form
- Electronic Record
- Electronic Signature
- Information
- Intermediary
- Key Pair
- Originator
- Private Key
- Public Key
- Secure System
- Verify
- subscriber