GUDLAVALLERU ENGINEERING COLLEGE

(An Autonomous Institute with Permanent Affiliation to JNTUK, Kakinada)

Seshadri Rao Knowledge Village, Gudlavalleru – 521 356.

Department of Computer Science and Engineering

HANDOUT

on

CYBER LAWS

Vision

To be a leading Institution of Engineering Education and Research, preparing students for leadership in their fields in a caring and challenging learning environment.

Mission

- To produce quality engineers by providing state-of-the-art engineering education.
- To attract and retain knowledgeable, creative, motivated, and highly skilled individuals whose leadership and contributions uphold the college tenets of education, creativity, research and responsible public service.
- To develop faculty and resources to impart and disseminate knowledge and information to students that will enhance educational level, which in turn will contribute to social and economic betterment of society.
- To provide an environment that values and encourages knowledge acquisition and academic freedom, making this a preferred institution for knowledge seekers.
- To provide quality assurance.
- To partner and collaborate with industry, government, and R & D institutes.
- To develop new knowledge and sustainable technologies and serve as an engine for facilitating the nation's economic development.
- To impart personality development skills to students that will help them to succeed and lead.
- To instill in students the attitude, values and vision that will prepare them to lead lives of personal integrity and civic responsibility.

- To promote a campus environment that welcomes and makes students of all races, cultures and civilizations feel at home.

- Putting students face to face with industrial, governmental, and societal challenges

Program Educational Objectives

PEO1 : Identify, analyze, formulate and solve Computer Science and Engineering problems both independently and in a team environment by using the appropriate modern tools.

PEO2 : Manage software projects with significant technical, legal, ethical, social, environmental and economic considerations.

PEO3 : Demonstrate commitment and progress in lifelong learning, professional development, leadership and Communicate effectively with professional clients and the public.

CYBER LAWS

Class & Sem. : III B.Tech – I Semester Year : 2018-19

Branch : CSE Credits : 3

==========

1. Brief History and Scope of the Subject

Cyber law is that stream of law where all the cyber-crimes such as theft, fraud, etc. all of which are subject to the Indian Penal Code are addressed by the Information Technology Act, 2000. With advanced technology and changing times, almost all the processes are now going on IT platform. This is giving rise to increase of cyber-crimes in India as well as abroad.

The rapid development of information technology posed certain challenges for the law that are not confined to a particular category of law but arises in diverse areas of law, such as criminal law, intellectual property law, contract and tort. Of late, owing to the rapid development of the internet and the World Wide Web, various unprecedented problems have emerged. These problems concern the issues of free speech, intellectual property, safety, equity, privacy, e-commerce and jurisdiction and are governed by the Cyber Law. The branch of law which regulates the technological aspects of information or information processing is called Cyber Law.

It has a wide and great scope in the corporate field. Students who are experts in cyber law are huge in demand and are paid handsomely. The rapid growth of the information technology has lead to a situation where the existing laws are challenged. It deals with computer hackers and people who introduce viruses to the computer. Cyber Law prevents or reduces the damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet, World Wide Web (WWW), email, computers, cell phones, software and hardware.

2. Pre-Requisites

- Information about new technologies and communications.
- Importance and necessity of Cyber law.
- Knowledge about cyber crimes and frauds.

3. Course Objectives:

- To expose the need of cyber laws to prosecute cybercrimes in the society
- To understand the IT Act 2000 for cyber crime and cyber justice
- To introduce the criminal Activities based on Internet.
- To familiarize various Licensing Issues Authorities for Digital Signatures.

4. Course Outcomes:

Students will be able to:

CO1: outline the pros and cons of Internet

CO2: operate On Confidential data in a precautious manner

CO3: demonstrate about the Criminal Justice in India and its Implications

CO4: define the cyber consumers Under the Consumer Protection Act

CO5: devise the legal framework for Confidential Information.

CO6: outline e-commerce issue for copyright protection and Defend Personal Data from being hacked.

5. Program Outcomes:

Graduates of the Computer Science and Engineering Program will have

a) an ability to apply knowledge of mathematics, science, and engineering
b) an ability to design and conduct experiments, as well as to analyze and interpret data
c) an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability
d) an ability to function on multidisciplinary teams
e) an ability to identify, formulate, and solve engineering problems
f) an understanding of professional and ethical responsibility
g) an ability to communicate effectively
h) the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context
i) a recognition of the need for, and an ability to engage in life-long learning,
j) a knowledge of contemporary issues

k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.

6. Mapping of Course Outcomes with Program Outcomes:

	a	b	c	d	e	f	g	h	i	i	k
CO1						√	√				
CO2						√			√	√	√
CO3								√			
CO4							√				
CO5							√			√	√
CO6						√					√

7. Prescribed Text Books

1. Vivek Sood, " Cyber Law Simplefied", Tata McGraw Hill.
2. Marjie T. Britz, "Computer Forensics and Cyber Crime", Pearson

Reference Text Books

1. Cyber Laws Texts and Cases, Ferrera, CENGAGE.

URLs and Other E-Learning Resources

- Cyber Crimes: http://www.legalindia.com/cyber-crimes-and-the-law/
- Cyber Laws: http://www.cyberlawsindia.net/
- Legal Services: http://www.legalserviceindia.com/cyber/cyber.htm
- Digital Signatures: http://searchsecurity.techtarget.com/definition/digital-signature

8. Digital Learning Materials:

- http://cyber.law.harvard.edu/media/files/copyrightandeducation.html
- http://www.tutorialspoint.com/information_security_cyber_law/quick_guide.htm
- https://books.google.co.in/books/about/Cyber_Law_Simplified.html?id=Wxk89dMjxIQC

9. Lecture Schedule / Lesson Plan

Topic	No. of Periods	
	Theory	Tutorial
UNIT – I: The IT Act, 2000- A Critique		
Crimes in this Millennium	1	1
Section 80 of the ITAct, 2000 – A Weapon or a Farce?	2	
Forgetting the Line between Cognizable and Non - Cognizable Offences	2	
Arrest for "About to Commit" an Offence Under the ITAct	1	1
A Tribute to Draco, Arrest But No Punishment.	1	
UNIT – II: Cyber Crime and Criminal Justice		
Penalties, Adjudication and Appeals Under the IT Act, 2000: Concept of Cyber Crime and the IT Act, 2000	1	1
Hacking, Teenage Web Vandals	1	
Cyber fraud and Cyber Cheating	2	
Virus on Internet Deformation	1	1
Harassment and E- mail Abuse	2	
UNIT – III: Cyber Pornography		
Cyber Pornography, Other IT Offences	2	1
Monetary Penalties, Adjudication and Appeals Under IT Act 2000	2	
Network Service Providers, Jurisdiction and Cyber Crimes	2	1
Nature of Cyber Criminality Strategies to Tackle Cyber Crime and Trends	1	1
Criminal Justice in India and Implications	1	
UNIT – IV: Digital Signatures, Certifying Authorities and e-Governance		
Introduction to Digital Signatures, Certifying Authorities and Liability in the Event of Digital Signature compromise	2	1
E - Governance in the India	1	1
A Warming to Babudom, Are Cyber Consumers Covered under	2	

the Consumer Protection		
Goods and Services	1	1
Consumer Complaint Defect in Goods and Deficiency in Services Restrictive and Unfair Trade Practices	2	
UNIT – V: Traditional Computer Crime		
Early Hacker and Theft of Components Traditional problems	1	1
Recognizing and Defining Computer Crime	1	
Phreakers: Yesterday's Hackers, Hacking	2	1
Computers as Commodities, Theft of intellectual Property	1	
UNIT – VI: Web Based Criminal Activity		
Interference with Lawful Use of Computers, Malware	1	1
DoS (Denial of Service) and DDoS (Distributed Denial of Service) Attacks	1	
Spam, Ransomware and Kidnapping of Information, Theft of Information	1	
Data Manipulation, and Web Encroachment Online Gambling Online Fraud	2	1
Securities Fraud and stock Manipulation, Ancillary crimes	2	
Total Number of Periods:	**42**	**14**

UNIT-1

Objectives:

To familiarize with cyber crimes and IT Act 2000.

Syllabus

UNIT – I: The IT Act, 2000- A Critique

Crimes in this Millennium, Section 80 of the IT Act, 2000 – A Weapon or a Farce?, Forgetting the Line between Cognizable and Non - Cognizable Offences, Arrest for "About to Commit" an Offence Under the IT Act, A Tribute to Draco, Arrest But No Punishment.

Outcomes:

Students will be able to:

- Identify various crimes in the millennium and measures taken to reduce them.
- Explain the meaning and definition of section 80 of the IT act 2000.
- Identify the applicability of Section 80
- Conclude whether Section 80 is a weapon or a Farse?
- Explain cognizable offences and Non - Cognizable Offences.
- Distinguish cognizable offences and Non - Cognizable Offences.
- Explain the offences that lead to arrest.
- Amendments that should be done to Section 80 of IT Act, 2000.

Learning Material

1. Crimes in this Millennium:

Introduction:

- **Cyber crime** is the deadliest widespread problem that is being faced by our planet this millennium.
- Cybercrime, computer crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, and target place of a crime.
- Cyber crime is broadly used term to describe criminal activity committed on computers or the Internet.
- Cyber crime is a criminal activity involving an information technology infrastructure, including illegal access, illegal interception, data interference, system interference, misuse of devices and electronic fraud.
- The weapon with which cybercrime are committed is **technology.** Cybercrimes are the work of technology and thus cyber criminals are technocrats who have deep understanding of the Internet and Computers.
- Cybercrime is extremely efficient i.e., it takes place in real time. It may take seconds or a few minutes to hack websites or do cyber frauds.
- Cybercrime has no geographical limitations, boundaries or distances. A cyber criminal in the one corner of the world can commit hacking on a system in other corner of the world.
- The act of cyber crime takes place in cyberspace which makes the cybercriminal being physically outside cyberspace. All the components of cyber criminality from preparation to execution, take place in the cyber space.
- Cybercrime has the potential of causing harm and injury which is of an unimaginable magnitude. It can easily destroy websites created and maintained with huge investments or hack into websites of backs and the defence department's websites.
- It is extremely difficult to collect evidence of cybercrime and prove the same in the court of law, due to the anonymity and invisibility of cybercriminal.

- Cyber crimes such as hacking, planting computer viruses and online financial frauds have the potential of shaking economies.

Various cyber crimes:

- February 6th, 7th and 8th of 2000 were the days of cyber criminal and darkest nights ever for Internet and e-commerce.Some of the big web-sites such as **Yahoo, Buy.com, Amazon.com and E-Trade** were shut down for hours.
- After this, the criminal activity did not stop. Again in the month of May 2000, cyber criminal attacked the Internet community by virus"**I Love You"**, which was deadlier than all its ancestors, causing a loss of US $10 billion. This proved that the technology grows equally for the IT industry and the cyber criminal.
- In December 1999, 300,000 credit card numbers were snatched from an online music retailer **"CD Universe"**.
- In March 1999, the virus called **"Melissa"** paralyzed e-mail systems around the world, causing an estimated damage of US $80 million.
- In India, the magnitude of cyber crime is less when compared to the world. Some of them are:
    - Hackers from Pakistan, named "**G Force Pakistan**" hacked the websites of following Indian Organizations: Indian Science Congress, Asian Age Newspaper, National Research Centre, Agricultural University of Maharashtra, IIM Ahmadabad, Gujarat Government, GloxoWelcome, Centre of Electronics Design and Technology, IIT Madras.
    - Other hacker group named "**Pakistan Hackerz Club"** led by Docter Nuker hacked the following sites: Indian Parliament, Ahemdabad Telephone Exchange, Engineering Export Promotion Council, United Nations (India).
    - Third hacker group named **"night man",** hacked both government owned websites and Indian Companies. Among those are: Lal Bahadur Shastry National Academy of Administration, Blue star Infotech, Mahindra & Mahindra.
    - Other cyber include: Web-defacement of Bhabha Atomic Research Centre, theft of telephone numbers and related information from the system of the Chief Manager of Department of Telecom, hacking SEBI(securities and Exchange Board of India) and a link of pornographic site was inserted into it, harassment caused to retired government official by over 4000 phone calls.

- Israli websites were crashed down by Palestinian hackers. A cyber war was done by a lone individual in a basement with a laptop as his weapon.

Measures Taken:

- The FBI has estimated losses of upto US $ 10 billion a year due to cyber crime.
- According to **CERT (Computer Emergency Response Team)** Coordination centre, which is an agency focused on computer security issues, four million computer hosts were affected due to computer viruses.
- In 1999, America spent US $4.4billion on Internet Security software which includes:
  - Firewalls
  - Intrusion-detection programs
  - Authentication and authorization software.
- President of US had announced a public-private sector joint initiative to protect US information infrastructure from hackers and viruses.
- About Rs.15,330 crores was spent on Indian web-sites for e-security, but they remain vulnerable to threat of hackinh and cyber crimes.

Effect of growing cyber crime:

- Cyber crime is growing at a rate of 4.1% per week.
- If this situation continues, many Internet users, cyber consumers, e-retailers would feel vulnerable for using e-transactions and e-commerce would start to shrink faster.

2. Section 80 of the IT Act, 2000 – A Weapon or a Farce?

Introduction:

- With the threat of cyber criminality, our legislature has inserted **Section 80 in the Information Technology Act, 2000.** It is as follows:

  "80. Power of police officer and other officers to enter, search, etc.-"

  (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a **Deputy Superintendent of Police**, or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any **public place*** and search and **arrest without warrant any person** found therein who is reasonably **suspected of having committed or of committing or of being about to commit any offence** under this Act.

***public place:** includes any place conveyance, any hotel, any shop or any other place intended for use by or accessible by public.

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974), shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

- Section 80 applies only to offences defined under the IT Act 2000.It is not applied to cyber crimes under other laws. For example: Defamation(damage of good reputation) through e-mail is not an offence under the IT Act 2000, so section 80 doesn't apply to such a case.

Ingredients of sub-section(1) of section 80:

- An accused can be arrested without warrant under section 80 of Act 2000, **only from a public place and no other place.**
- He can be arrested either for **having committed or for committing or for being about to commit** any offence (illegal act or crime) under the IT Act.
- The following are the confusions in the law:
    - A person is alleged (said or thought that he did an illegal act) to have committed an offence under the IT Act 2000 in a place other than a public place, but is found in a public place.
    - A person is alleged to have committed an offence under the IT Act 2000 in a public place, but found in some other public place.
    - The person is alleged to have committed or is committing or is about to commit an offence under the IT act, in a public place and is found in that very public place.

  The application of section 80 is restricted only to the **third situation.**
- Section 80 is then modified as:

  "80. Power of police officer and other officers to enter, search, etc.-"

  (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a **Deputy Superintendent of Police**, or any other officer of the Central Government or a State Government

authorized by the Central Government in this behalf may enter any **public place** and search and **arrest without warrant any person** found therein who is reasonably **suspected of having committed or of committing or of being about to commit any offence** under this Act **in such public place.**

Applicability of section 80:

- As section 80 is restricted to the power of arrest without warrant only in a public place, the following are the situations where section 80 becomes vulnerable:
  - **Example1**: A is reasonably suspected of having committed the offence of hacking under IT Act from his (A's) house. After committing the offence, he (A) goes to a hotel. As per section 80, A can be arrested without warrant from the hotel which is a public place. However, if he (A) remains in his house after committing the said offence of hacking, he cannot be arrested without warrant as per section 80.
  - **Example 2**: If A is reasonably suspected of having committed the offence of hacking under IT Act from a cyber cafe, he can be arrested without warrant under section 80 only if he is found in the cyber cafe itself or in some other public place. But if he (A) goes home and stays there, after committing the cyber crime in the cyber cafe, then he cannot be arrested without warrant.
  - **Example 3:** If A from a cyber cafe in Bombay is alleged to have hacked the defence systems installed in the computer network in the Defense Ministry at Delhi, he can be arrested without warrant , only if he remains in the cyber cafe or is found in some other public place. If he is not in a public place, the power of arrest without warrant cannot be exercised. In this case, the following are the questions raised:
    - Would the accused wait there in the cyber cafe or any other public place for being arrested, till the Defense Ministry comes to know of the hacking, then complains to the police who registers a case, investigates the offence, tracks down the hacking to the cyber cafe and sends a team to Mumbai for arrest under section 80?
    - Is it that the investigation of cyber crime is so efficient and easy that the accused would be arrested within a short time during which he is likely to be found in cyber cafe?

Cyber crimes that do not permit to immediate arrest:

Section 80 has been legislated without any consideration for the nature of Internet and cyber criminality. The following are some characteristics of cyber crimes that do not permit to immediate arrest of the accused:

- **Geographical distances and borders are irrelevant** to cyber crime. A cyber criminal sitting in one corner of the globe may hack the victim's bank's computer system located in another corner and transfer funds to some other corner of the world.
- A cyber criminal is **almost invisible**. He is here, there, everywhere.
- The cyber criminal **does not come face to face with the victim nor he is physically present at the place** where he commits the offence.
- It is extremely **difficult to collect evidence** of a cyber crime, and **investigation is a time- consuming process**.
- While cyber crime investigation is time-consuming, but **performing a cyber crime is vert efficient. It may take only a few seconds or minutes** to plant virus into computer systems.Ex: "I Love You" virus took only two hours to spread all over the globe.

Section 80 is impotent-A Farce:

The logic of **restricting the power of arrest without warrant only from a public place** has the following issues:

- Before the victim even realizes that he has been hit by a cyber crime, **the criminal would be far away from the public place.**
- The DSP could arrest the accused without warrant from a public place only if the **accused slips into coma in that place or only if the accused is a fool** to stay there itself after committing the crime.
- The power of arrest without warrant can be exercised effectively where crimes under IT Act are committed from work places, which are also public places, by **those who work there and thus visit regularly i.e., employers and employees.**
- Cyber cafes are run by businessmen for profit and not by detectives or police informers. A cyber cafe must grant privacy to its customers and satisfy them; otherwise they have to shut down their business. In this situation, **it is impossible for the cyber cafe manager to know whether the user is hacking a computer system**

or has a secured access. Even the records that identify the users from time to time does not help section 80, as the criminals would not wait outside the cafe until the DSP comes arrests them.

***impotent-(not strong)**

***A Farce-(uses improbable situations, physical humor and silliness to entertain)**

Therefore, cases where the cyber criminals were caught under section 80 of IT Act were very few.

3. Forgetting the Line between Cognizable and Non - Cognizable Offences

- Offences in which arrest without warrant is provided are called **"Cognizable offence"** and others are **"non-cognizable offences".**
- A cognizable offence means a case where a police officer has the power to arrest without warrant. A Non cognizable offence means a case where a police officer has no authority to arrest without warrant*.

  *warrant-section 2(1) of Criminal Procedure code (Cr.P.C)
- If a case is related to two or more offences of which one at least one is cognizable, the case termed as **cognizable**.
- It is only in a cognizable case that a **FIR (First Information Report)*** can be registered. FIR cannot be registered for a non cognizable case.

  *FIR- It is the earliest and the first information of a cognizable offence recorded by an officer-in-charge of a police station.

Cognizable Offences:

- An **FIR** case implies that the **victim/informant is the only witness for prosecution**. If the cognizable offence has been committed, the informant may report to the concerned Police station within whose jurisdiction* the offence has been committed, and gives the information of the offence.

  *jurisdiction- the territory or sphere of activity over which the legal authority of a court or other institution extends.
- **Section 154 of Cr.P.C(Code for Criminal Procedure)** contains the procedure for registration of FIR. It is as follows:

  "154. Information in cognizable cases.-

  (1) Every information relating to the commission of a cognizable offence, if given orally to an officer in charge of a police station, shall be reduced to writing by him

or under his direction, and be read over to the informant; and every such information, whether given in writing or reduced to writing as aforesaid, shall be signed by the person giving it, and the substance thereof shall be entered in a book to be kept by such officer in such form as the State Government may prescribe in this behalf.

(2) A copy of the information as recorded under Sub-Section (1) shall be given forthwith, free of cost, to the informant.

(3) Any person, aggrieved* by a refusal on the part of an officer in charge of a police station to record the information referred to in Sub-Section (1) may send the substance of such information, in writing and by post, to the Superintendent of Police concerned who, if satisfied that such information discloses the commission of a cognizable offence, shall either investigate the case himself or direct an investigation to be made by any police officer subordinate to him, in the manner provided by this Code, and such officer shall have all the powers of an officer in charge of the police station in relation to that offence.

*aggrieved-unfairly treated

- As per the **section 156 of Cr.P.C ,** any officer-in-charge of Police station, without the order of a Magistrate, may investigate any cognizable case falling within the jurisdiction of police station.
- Section 157 of Cr.P.C states the procedure of investigation in cognizable offences. It is as follows:

"157. Procedure of investigation.-

(1) If, from information received or otherwise, an officer in charge of a police station has reason to suspect the commission of an offence which he is empowered under section 156 to investigate, he shall forthwith send a report of the same to a Magistrate empowered to take cognizance of such offence upon a police report and shall proceed in person, or shall depute one of his subordinate officers not being below such rank as the State Government may, by general or special order, prescribe in this behalf, to proceed, to the spot, to investigate the facts and circumstances of the case, and, if necessary, to take measures for the discovery and arrest of the offender; Provided that-

(a) when information as to the commission of any such offence is given against any person by name and the case is not of a serious nature, the officer in charge of a police station need not proceed in person or depute a subordinate officer to make an investigation on the spot;

(b) if it appears to the officer in charge of a police station that there is no sufficient ground for entering on an investigation, he shall not investigate the case.

(2) In each of the cases mentioned in clauses (a) and (b) of the proviso to sub- section (1), the officer in charge of the police station shall state in his report his reasons for not fully complying with the requirements of that sub- section, and, in the case mentioned in clause (b) of the said proviso, the officer shall also forthwith notify to the informant, if any, in such manner as may be prescribed by the State Government, the fact that he will not investigate the case or cause it to be investigated.

- According to section 80 of IT Act 2000, the police officer must not be below the rank of a DSP.
- In cognizable cases, the investigating police officer has the power to initiate and proceed with the investigation without a judicial order. During investigation, the investigating officer (IO) has the power of to require the attendance of persons who appear to be acquainted with the facts and circumstances of the case, for recording their their statements.
- After completing the investigation, the police is required to file a Charge Sheet/Challan/Police Report against the accused before the criminal court.
- After the Charge-Sheet has been filed, charges are framed against the accused followed by Prosecution evidence, defence evidence, final arguments and judgment.

Non Cognizable Offences:

- No FIR can be registered for a non cognizable case.
- The complainant can only file a criminal complaint in the Court of Magistrate.
- In non cognizable case, if the informant makes a complaint to the police station, the police would record the substance of the information as a **"Non-cognizable Report (NCR)"** and refer the informant to the Magistrate.
- The Magistrate on receiving a criminal complaint examines the compliant and his witnesses, the substance of which shall be reduced to writing. The recordings of these

statements by the Magistrate are referred to as **"preliminary complainant's evidence".**

- The Magistrate will then apply his mind to the preliminary evidence on behalf of the complainant and if he is of the opinion that there is sufficient ground for proceeding, he will issue process for the accused for facing trail.
- This process may take a very long time, even years, for the case to reach a stage of issuance of process to the accused.
- The court may postpone the issuance of process to the accused and may direct an investigation to be made by the police for the of deciding whether or not there is sufficient ground for proceeding against the accused.

Line between Cognizable and non-cognizable cases:

Cognizable cases	**Non-Cognizable cases**
An **FIR is registered** with the police	A **criminal complaint** is to be filed in the court
The police initiates the investigation on its own and **does not require the permission of court**	No investigation can be carried out by the police without the **order of the court.**
The State investigates the case and fights against the accused. The State is the prosecutor and the only responsibility of a complainant /victim/informant is as a prosecution witness	It is the complainant who seeks to prosecute the accused.
The burden of proving the allegations against the accused lies upon the **prosecution i.e., State**.	The burden of proving the allegations against the accused lies upon the **complainant.**
No procedure of preliminary evidence in the Court.	Preliminary evidence is compulsory.
The criminal procedure is **faster.**	The criminal procedure is **slower** and it is structured in such a way to reduce the burden on police.
Police has the **power of arrest without**	Police has **no power of arrest without**

warrant.	**warrant.**
Crimes like rape, murder, theft etc. are considered cognizable	Public nuisance, simple hurt, mischief etc. are considered non-cognizable.

Classification of offences against other laws:

Offence	Cognizable or non-cognizable	Bailable or non-bailable	By what court triable
If punishable with death, imprisonment for life or imprisonment for more than 7 years.	Cognizable	Non-bailable	Court of Session.
If punishable with imprisonment for 3 years and upwards but not more than 7 years.	Ditto	Ditto	Magistrate of the first class.
If punishable with imprisonment for less than 3 years or with fine only.	Non-cognizable	Bailable	Any Magistrate.

Classification of IT Act Offences:

Section	**Offence**	**Punishment**	**Bailability and Cognizability**
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Non-Bailable, Cognizable
66	Hacking with computer System	Imprisonment up to 3 years or fine up to Rs 5 lakhs	Non-Bailable, Cognizable

67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Non-Bailable, Cognizable
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Non-Bailable, Cognizable
69	Failure to assist the agency referred to in sub section (3) in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine	Non-Bailable, Cognizable
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine	Non-Bailable, Cognizable.
71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.	Bailable, Non-Cognizable.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.	Bailable, Non-

			Cognizable.
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Bailable, Non-Cognizable.
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Bailable, Non-Cognizable.

Section 80 of IT Act 2000 with cognizable and Non-cognizable:

- When the accused is found in a public place, all the IT Act offences become cognizable and the accused can be arrested without warrant.
- If the accused move away from the public place, all the offences of IT Act become non-cognizable.
- Whether the FIR process or criminal complaint procedure depends on where the accused is found.
- If the accused is in the public place, he can be arrested without warrant even if the IT Act offence is not serious. If he is not in the public place, the accused cannot be arrested without warrant even if the offence is serious.

  The following are the examples of the above cases:

  - **Example 1:** A is found in a public place and is accused of the offence of tampering with computer source documents under section 65 of the IT Act, 2000 which prescribes a punishment of imprisonment up to 3 years. As per section 80, A can be arrested without warrant.
  - **Example 2:** A is not found in a public place and is accused of the offence of gaining access to a protected system which entails a punishment which can extend upto 10 years under section 70 of IT Act, 2000. The offence is very serious but A cannot be arrested without warrant.

Confusions raised in case of IT Act:

- Should the informant/victim complain to the police station or file a complaint before judicial Magistrate?
- If the victim/informant goes to the police station, should the police register an FIR or refer the informant/victim to the Magistrate for a complaint to be filed?
- Should the victim/informant or the police check whether the accused is still waiting to be arrested in the public place, and then decide the course of action between a FIR and the complaint procedure?
- How should be the case be categorized (cognizable or non cognizable) till it is checked whether the accused is in the public place or nor?
- Upon whom out of the police and the victim/informant would be the responsibility lie to show that the accused is waiting to be arrested in a public place?

4. Arrest for "About to Commit" an Offence Under the ITAct, A Tribute to Draco:

- **Section 80 of the IT Act, 2000** seeks to penalize citizens**" about to commit"** any offence under the Act.
- **Section 216A** penalizes a person for harboring persons "about to commit" with a rigorous imprisonment for a term which may extend up to 7 years.
- The component of "about to commit" of section 80 is wide open for misuse. Innocents can easily be put on the grounds of being about to commit an offence under the IT Act, 2000.
- Many innocents can be misinterpreted as "being about to commit" an IT Act offence. The following are some instances:
    - If a person visits a porno-web-site which sends an e-mail of dirty material to friends, it can be alleged that he was about to commit the offence under **Section 67 of the IT Act**, even though he may have accessed the site only for personal viewing, without any intension og transferring the material.
    - If a person visits a web-site which gives ideas on modes of hacking computer systems, he can be arrested on the allegation of being about to commit hacking under **section 66**, though he is just visiting the site for fun.
- In law, a **preparation for the commission of an offence** is different from **an attempt to commit it**.

- Preparation consists in devising or arranging the means or measures necessary for the commission of offence.
- Attempt to commit the offence is a direct movement towards the commission after preparations are made.

  Example case: A truck was carrying paddy to Delhi from Punjab , against Punjab Paddy Export Control Order. The truck was stopped by the Sub Inspector of the Food and Supplies Department at Samalkha which is 32 miles from Delhi. Prosecution was launched against the accused. The question was whether the offence of attempt had been committed? The Supreme court acquitted the accused saying that- it is quite possible that the accused might have been warned they are having no license to carry the paddy and they might have changed their mind at any place between Samalkha barrier and Delhi border and not have proceeded in their journey further. The offence of attempt had not been committed. The acts of the accused were only up to preparation.

5. Arrest, but NO Punishment:

- Section 80 covers three grounds of arrest:
  - Of having committed or
  - Of committing or
  - Of being about to commit
- **"having committed"** refers to a situation where the offence has been concluded i.e., all the acts of the offence have been done.
- **"of committing"** refer to a situation where a person is caught in the process of commission of an offence which has not yet concluded.
- **"about to commit"** refer to a stage of preparation. It is a stage prior to "of committing".
- If a person is **about to commit** hacking of a computer system or **is committing** it, he **can only be arrested under Section 80, but cannot be punished** under Section 66 for the offence of hacking because it does not cover either "of committing" or "of being about to commit" within its ambit(range).\
- A section similar to **Section 151 of Cr.P.C** should be included in the IT Act which treats "of committing" and "of being about to commit" as substantive offences.

  "151. Arrest to prevent the commission of cognizable offence-

(1) A police officer knowing of a design to commit any cognizable offence may arrest, without orders from a Magistrate and without a warrant, the person so designing, if it appears to such officer that the commission of the offence cannot be otherwise prevented.

(2) No person arrested under sub- section (1) shall be detained in custody for a period exceeding twenty- four hours from the time of his arrest unless his further detention is required or authorized under any other provisions of this Code or of any other law for the time being in force.

Conclusion

The following amendments necessary in section 80 of the IT Act:

- The word **"public"** should be removed from sub-section (1).
- The words **"any offence under this Act"** in sub-section (1) should be substituted with the words **"any cognizable offence under this Act"**.
- The words **"reasonably suspected of having committed or of committing or of being about to commit"** in sub-section(1) should be substituted by the words **"reasonably suspected of being concerned".**
- A police officer not below the rank of a DSP must be assisted by an IT professional.

UNIT-1
Assignment-Cum-Tutorial Questions
SECTION-A

I. *Objective Questions*

1. The weapon with which cybercrime are committed is _____.
2. CERT stands for _____.
3. Cyber crimes such as _____have the potential of shaking economies. [ ]

A) Hacking B) planting computer viruses

C) online financial frauds D) All the above.

4. Internet Security software which includes: [ ]

A) Firewalls B) Intrusion-detection programs C) Authentication and authorization software D) All the Above

5. _____ is the deadliest virus that attacked the Internet world.
6. Under section 80 of IT Act 2000, a person can be arrested from_____. [ ]

A) Private place B) public place C) Any place D) none

7. FIR stands for _____.
8. FIR is registered in _____ case. [ ]

A) Cognizable B)non-Cognizable C) Both A&B D) None

9. _____ of Cr.P.C contains the procedure for registration of FIR. [ ]

A) Section 154 B) section 156 C) section 157 D) None

10. Cr.P.C stands for _____.
11. As per the _____ of Cr.P.C , any officer-in-charge of Police station, without the order of a Magistrate, may investigate any cognizable case falling within the jurisdiction of police station [ ]

A) Section 154 B) section 156 C) section 157 D) None

12. _____ of Cr.P.C states the procedure of investigation in cognizable offences. [ ]

A) Section 154 B) section 156 C) section 157 D) None

13. Preliminary complainant's evidence is taken in _____ case. [ ]

A) Cognizable B) non-Cognizable C) Both a & B D) None

14. A type of cyber crime that occurs in pay per click online advertising when a person, automated script or computer program imitates a legitimate user of a web browser clicking on an ad, for the purpose of generating a charge per click without having actual interest in the target of the ad's link. [ ]

A)Phishing B) Zombie C) Click fraud D) none of these

15. which one of the following is not an example of using computer as a weapon'? [ ]

A) Cyber Terrorism B) I PR violations

C) Credit card frauds D) All of these

16.The use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization is termed [ ]

A)Cyberspace B) Cyber stalking C) Pornography D) none of these

17.The attempt acquires information (and sometimes, indirectly, money) such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication is termed:

[ ]

A)Spamming B) Phishing C) Spoofing D) None of these

18. _____is a computer connected to the Internet that has been compromised by a hacker, Computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction.

[ ]

A)Server B) Zombie C) Symbian D) None of these

19.Which one of the following is an example of denial of service attack'?

[ ]

A) Attempts to flood a network, thereby preventing legitimate network traffic

B) Attempts to disrupt connections between two machines, thereby preventing access to a service

C) Attempts to prevent a particular individual from accessing a service

D) All of these

21. In cyber law terminology 'DoS' means: [ ]

A)Denial of Service B) Disc operating System

C) Distant Operator service D) None

22. The Indian Parliament passed the Information Technology Bill ,which is regarded as the mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format , in the year: [ ]

A)2000 B) 2001 C) 2002 D) 2003

23. The seat of the Asian School of Cyber Laws: [ ]

A)New Delhi B) Pune C) Chennai D) Hyderabad

24.Which one of the following is not an example of using computer as a weapon'? [ ]

A) Cyber Terrorism B) I PR violations

C) Credit card frauds D)All of these

SECTION-B

II) Descriptive Questions

1. List various cyber crimes that affected Internet world and what are the measures taken by the government.
2. Explain section 80 of IT Act, 2000.
3. Explain the differences between cognizable and non-cognizable cases.
4. List the classification of IT Act Offences.
5. Explain various issues of cognizable cases.
6. In law, how a preparation for the commission of an offence is different from an attempt to commit it. Justify with a case study?
7. Discuss various cases where innocents are misinterpreted as “being about to commit” an IT Act offence.
8. Discuss the reasons for delay in non-cognizable cases.
9. How section 80 is becoming a FARCE by restricting it to arrest the accused only from a public place?
10. List the characteristics of cyber crimes that do not permit to immediate arrest of the accused.

UNIT-2

Objectives:

To identify the areas in cyber crimes and criminal justice under Act 2000.

Syllabus:

UNIT – II: Cyber Crime and Criminal Justice

Penalties, Adjudication and Appeals under the IT Act, 2000: Concept of Cyber Crime and the IT Act, 2000, Hacking, Teenage Web Vandals, Cyber fraud and Cyber Cheating, Virus on Internet, Deformation, Harassment and E- mail Abuse

Outcomes:

At the end of the unit, students will be able to:

- Understand the concept of cyber crime and the IT Act.
- Explain the characteristics and classification of hacking and its effects.
- Understand the reasons for teenage web vandals.
- Explain the effects of cyber fraud and cyber cheating in Internet.
- Understand the effects of viruses on Internet and liable punishments by law.
- Explain defamation, harassment and e-mail abuse in Internet and punishments.

Learning Material

1.Concept of Cyber Crime and the IT Act

Introduction:

- The IT Act, 2000 doesn't define "cyber crime", but only provides the definition of punishment for certain offences.
- As per the IT Act cyber crimes are restricted to tampering with the computer source code, hacking and cyber pornography. Cyber fraud, defamation, harassment, e-mail abuse and IPR thefts are not classified as cyber crimes according to this Act. So, according to IT, Act 2000, only certain offences are punished and is not applicable for all cyber crimes.
    - Example 1: If a person through Internet threatens any person abd causes death or hurt, it is an offence under section 506 of IPC (Indian Penal Code, 1860) but it is not an offence under IT Act.
    - When a person cheats another on the Internet, it is an offence under section 420 of IPC but not under IT Act, 2000.

Classification of cyber crimes:

- Cyber crimes are classified as:
    - **Old crimes, committed through Internet.** For example, cheating, fraud, misappropriation, defamation, pornography, threats etc committed through or with the help of Internet, come under this category. Internet with its speed and global access has made these crimes much easier, efficient, risk-free, cheap and profitable to commit. These are called **"Crimes on the Internet".**
    - **New crimes committed with the Internet itself.** These include hacking, planting viruses and IPR thefts. These are called "**Crimes of the Internet".**
    - **New crimes used for commission of old crimes.** For example, hacking is used to perform cyber fraud.
- **Computer crimes are classified by the nature of usage of computers**
    - For computer crimes such as hacking, **computer and network** are essential for the commission of the offence.

- **Computer assisted crimes**, such as cyber pornography where the medium of Internet is used.
- Crimes where the computer is only **incidental for commission**, such as cyber fraud.

Necessity of Document:

- Though IT Act, 2000 specifically defines and punishes only a few cyber crimes, it recognizes that there are other crimes which are provided in the IPC, 1860. But, in IPC, the definition of "document" did not include **"electronic records"** within its scope.
- **Definition of Document:**
  - According to IPC, document denotes "any matter expressed or described upon any substance by means of letters, figures or marks, which may be used as evidence of that matter"
  - "Electronic record"(of IT Act, 2000) means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film.
- In IPC, a document is "paper based".
- The following table specifies various sections of IPC , regarding document:

Section in IPC	Offence
167	Public servant framing an incorrect document with intent to cause injury
172	Absconding to avoid service of summons, etc. to produce a document in a court of justice.
173	Preventing service of summons, etc. to produce a document in a court of justice.
175	Omission to produce document to public servant by person legally bound to produce it
192	Fabricating false evidence
204	Destruction of document to prevent its production as evidence
463	Forgery
464	Making a false document
466	Forgery of record of court or of public register, etc
468	Forgery for purpose of cheating

469	Forgery for purpose of harming reputation
470	Forged document
471	Using as genuine a forged document
474	Having possession of document described in section 466 or 467, knowing it to be forged and intending to use it as genuine
476	Counterfeiting device or mark used for authenticating documents other than those described in section 467, or possessing counterfeit marked material
477 A	Falsification of accounts

2. Hacking

Definitions' of Hacking:

- A person who enjoys exploring the details of programmable systems and how to stretch their capabilities as opposed to most users who prefer to learn only the minimum necessary, or one who programmes enthusiastically, is described as **hacker.**
- Breaking into computer systems is called "Hacking".

Classification of Hackers:

- Hackers have been classified as:
  - **Code Hackers**: Those who have knowledge of the intricacies (complex and detailed information) of computer systems and their operations.
  - **Phreakers:** Those who have deep knowledge of the Internet and telecommunication systems.
  - **Cyber-Punks:** Those who specialize in cryptography.
  - **Crackers:** Those who break into computer security systems.

Characteristics of Hacking:

- Criminal hacking is one of the biggest threats to the Internet and e-commerce because it has the effect of gradually destroying the credibility of the Internet.
- Hacking creates a perception in the minds if neitizens that the Internet is vulnerable and weak.
- Hacking makes e-commerce costlier because of huge investments required to install systems to guard against hackers.

- Rampant (uncontrollable) hacking is questioning the technology and survival of e-commerce and is dampening the spirits of web entrepreneurs from entering into IT industry.
- In India, hacking is a major problem where Indian web-sites are being hacked by Pakistani hackers (inserted a pornographic web-site link of SEBI).

Types of Hacking prevalent:

Four types of hacking are most prevalent today:

- For fun as a hobby, mostly by teenagers obsessed with the Internet.
- To damage the business of competitors.
- With the intension of committing offence such as a fraud and misappropriation.
- By Internet Security companies to test their clients systems and win their confidence.

Why hacking is simple:

- Hacking is simple to execute because there are websites which specialize in hacking.
- There are virtual schools which teach methods of hacking.
- There are 1900 web-sites which offer weapons for free to crash computers and hijack control of computer systems.

Section 66 of IT Act, 2000:

- "66 Hacking with computer system.-
  (1) Whoever 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 hacking.
  (2) Whoever commits hacking shall be punished with imprisonment up to three years or with fine which may extend up to two lakh rupees, or with both".
- According to the definition , innocent errors of commission which may destroy or delete or alter any information residing in a computer resource or diminish its value or utility or affect it injuriously, even though it may cause or likely to cause a loss or damage to the public or any person, **would not amount to hacking**.
- Damages for hacking can be claimed by the victims from hacker.
- In 2001, two persons, Amit Parsai(computer engineer) and Kapil Juneja(Computer diploma holder) were arrested by Delhi police on allegations of hacking under section 66,

for blocking the access to the complainants' web site on the ground of non-payment of charges for hiring web space.

Acts of Hacking:

- The following acts done by any person without the permission of the owner or any person who is in charge of a computer, come under hacking:
  - Access to computer, computer system,. Computer network.
  - Damage to any computer, computer system or computer network, data, computer data base or any other program's residing in computer.
  - Disruption of any computer, computer system or computer network.
  - Assistance to any person to facilitate access to a computer, computer system or computer network against IT Act, rules or regulations.

3. Teenage Web Vandals

- Cyber crime has become fashionable and a hot favorite of teenaged netizens in India.
- How-to-hack CD's are easily and cheaply available for only Rs 100-300 which is affordable for any student and those CD's contain ways of cracking a game, hacking an Internet account and hijacking a computer.
- The Internet has thrown up opportunities which were unimaginable before. Marc Anderson (Netscape), Jerry Yang (Yahoo), sabir Bhatia (hotmail), Jonathan Ivie(Apple-designed Macintosh computer) are examples of billionaires who achieved below the age of 35.
- Today's teenagers do not even wait up to the age of 35 to become a billionaire. This is the power and attraction of IT, which is giving birth to teenage cyber criminal.
- Though the acts of defacing web-sites or putting tags appear to be harmless, they are creating fear in the Internet community and are gradually becoming bigger crimes.
- Cyber criminals of today are becoming future Dons of cyber underworld of hacking and fraud.

Significant motivating factors and causes of teenage cyber criminality:

- **Global fame and publicity**, due to world wide access of internet.
- **Excitement of making a difference in the world** i.e., a sense of achievement and greatness.

- **Assertion of knowledge** of the internet and computer programming.
- **Lack of sensitivity to the adverse consequences** of act of hacking and defacing. They think that no loss is being caused b y their acts.
- **Lack of fear of Law.**
- **Cheap and easy availability** of the weapons of committing hacking.

Controlling teenage cyber criminality:

- Imparting information to the teenagers, about the adverse consequences of cyber crime to the IT industry and society.
- Parents and elder members of the family should at least check the acts of their adolescents.

4. Cyber fraud and Cyber Cheating

Introduction:

- Fraud on Internet consumes about one-third of all cyber crimes. It is most profitable business on the Internet.
- Cyber frauds wait for e-commerce because their profitability is directly linked with the **growth of e-commerce**.
- Most cyber frauds are not revealed by the victims because of fear of loss of public trust, confidence, image and business.

Major areas of fraud and cheating:

- Misuse of credit cards by obtaining passwords through hacking.
- Bogus investments with rich schemes.
- Deceptive investment newsletters containing false information about companies.
- Non-delivery of goods purchased from online auctions and web-sites.
- Misappropriation and transfer of funds.

Definition of fraud:

The following acts that are committed by a party to deceive another party come under fraud:

- The suggestion, as a fact, of that which is not true, by one who does not believe it to be true.
- Active concealment of a fact by one having knowledge or belief of fact.

- A promise made without any intension of performing it.
- Any other fact to deceive.
- Any act that is specifically declared to be fraudulent by the law.

Offence of cheating:

- **Section 415 of IPC** defines cheating.
- A representation is made by a person which is false and which he knows is false at the time of making the representation.
- The false representation is made with the dishonest intention of deceiving the person to whom it is made.
- The person deceived id induced to deliver any property or to do or omit to do something which he would otherwise not have done or omitted.

Examples of cheating:

(Imprisonment which may extend up to one year or with fine, or with both)

- A, exhibiting a false sample of article to Z, intentionally deceives Z into believing that article and dishonestly induces Z to buy and pay for the article. A cheats.
- A, by tendering a cheque of a bank with which he keeps no money and intentionally deceives Z, intending not to pay for it. A cheats.
- A, intentionally deceives Z into believing that A means to repay money that Z may lend to him and thereby dishonestly induces Z to lend him money, while not intending to repay it. A cheats.
- A intentionally deceives Z into a belief that A has performed his part of a contract made with Z, which he has not performed, and dishonestly induces Z to pay money. A cheats.

(Imprisonment which may extend up to three years or with fine, or with both)

- When a person cheats another by pretending to be some other person or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is, it is **cheating by personation**.

(Imprisonment which may extend up to seven years or with fine, or with both)

- Whoever cheats and dishonestly induces a person deceived to deliver any property to any other person.

5. Virus on Internet

- **"Computer virus"** has been defined as "any computer instruction, information, data or program that destroys damages, degrades or adversely affects the performance of a computer resource".
- Computer virus attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in computer resource.
- **"Damage"** means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
- **"Computer contaminant"** is defined as any set of computer instructions that are designed to modify, destroy, record, and transmit data or program residing within a computer, computer system or computer network that deviates the normal operation of computer.
- The law of IT imposes a monetary liability of damages as compensation to the victim, upon any person who introduces any computer virus or computer contaminant into any computer, computer system or computer network, irrespective of whether it is done intentionally, negligently, erroneously, inadvertently or innocently.
- It is a responsibility and legal duty upon every person to ensure that he does not introduce any computer virus or contaminant into the computer or computer network.
- Though the introduction of virus does not entail any corporal punishment, as the virus destroys or deletes or alters any information residing in a computer resource, it amount to hacking which is punishable up to 3 years and extend a fine up to 2 lakhs.
- The act of planting a virus and other computer contaminants amount to the criminal offence "mischief":
    - **"Mischief-**

      Whoever, with the intent to csuse, or knowing that he is likely to cause, wrongful loss or damage to the public or to any person, causes the destruction of any property, or any such change in any property or diminishes its value or utility, or affects it injuriously, commits 'mischief'.

- The following are the **ingredients of mischief**:
  - Destruction of any property, or any such change in any property which destroys or diminishes its value or utility, or affects it injuriously.
  - Wrongful loss or damage to the public or to any person by any acts above.
- **Example: "I love you" virus on Internet.** This virus initiated from Philippines and infected computers in about two dozen countries. It affected thousands of companies including AT&T, Microsoft etc. Many companies had to shut down their e-mail systems. This virus spread by duplicating itself sending copies to everyone on a victim's e-mail address book
- **Worms, Trojan Horses** are cousins of virus and contaminants which specialize in destroying computer systems, programs and information residing there.
- The IT Act, 2000 provides that whoever introduces or causes to be introduced any computer contaminant or computer virus into any computer or computer network, shall be liable to pay damages by way of compensation not exceeding rupees one crore to the person so affected.

6. Defamation, Harassment and e-mail Abuse

Introduction:

- The internet promotes democracy by providing a very efficient, easy and cost-friendly medium to all its users to communicate globally.
- Internet provides many forums such as chat rooms, for netizens to voice their views freely. But this is also being misused.

Defamation:

- Defamation is the injury done to the reputation of a person.
- The following are the ingredients of defamation:
  - Making or publishing an **imputation (bad rumor)** concerning any person.
  - The imputation is made with the intention of causing harm to the person and knowing that imputation will harm the reputation of a person.
  - The imputation is made by words, which are either spoken or read, or by signs or by visible representations.

- **Example:**
  - An Engineering and Management graduate who harassed his wife for dowry was caught by Delhi Police for sending obscene e-mails containing pornographic material, extremely vulgar language and asking people to chat with her, in his wife's name to her relatives, friends and others. The Police registered a case for defamation, criminal intimidation and acts intended to insult the modesty of women, under sections 500, 506 and 509.
  - Some web-sites post the morphed photographs of famous people and film stars.
- According to law, imputation does not harm a person's reputation, unless that imputation directly or indirectly lowers the character of that person in respect to his caste or lowers the credit of that person.
- For example: If A writes a letter to B which is derogatory (insulting) of B, it does not amount to defamation. However, if A writes a letter to C containing derogatory remarks about B which damage's B's reputation, then it amounts to defamation.
- The punishment for defamation is simple imprisonment for a term which may extend to two years, or with fine, or both.
- Publishers and editors of newspapers, journals etc. containing defamatory matter, irrespective of author of the article, are also liable for defamation.
- According to law, whoever prints or engraves any matter, knowing that such matter is defamatory of any person, is liable to be punished.

Imputations that not amount to defamation:

- Imputation which is true concerning any person, if it is for the public good. But if the imputation is true about a person and is not good for the public, then it is defamatory.
- An opinion in good faith regarding the conduct of a public servant in the discharge of his public functions, or regarding his character, only so far as his character appears in that conduct..
- Publishing the true report of the proceedings of a Court of Justice.
- Regarding the conduct of a person as a witness in any case, only so far as his character appears in that conduct.

- An opinion in good faith regarding the merits of any performance which its author has submitted to the judgment of the public or regarding the character of the author so far as his character appears in such performance.
    - A says of a book published by Z- "Z's book is foolish; Z must be a weak man, Z's book is indecent; Z must be a man of impure mind.(not defamating)
    - A says- "I am not surprised that Z's book is foolish and indecent, for he is a weak man. (Defamation)
- Passing in good faith by a person having authority over another. (Ex: judge, blaming the witness).
- Accusations made in good faith against any person to any of those who have lawful authority over that person with respect to the subject matter of the accusation.
    - A, in good faith accuses Z before a Magistrate
    - A, in good faith complains of the conduct of Z, a servant to Z's master.
    - A, in good faith complains of the conduct of Z, a child to Z's father.
- Conveying a caution (care taken to avoid danger) in good faith to a person against another, for the good of the person to whom it is conveyed.

Conclusion:

- By the above exceptions, the law of defamation tries to balance the democratic freedom of speech and expression for public good with the malicious and dishonest imputations harming the reputation of a person.
- Due to speed and global access of the Internet, criminal netizens got the opportunity to threaten a person with violent minds, which is punishable under IPC with imprisonment up to seven years, or with fine, or with both.
    - To cause death or grievous hurt
    - To cause destruction of any property by fire.
    - To impute unchastity to a woman.

Harassment:

- Serious cases of harassment came into light before IT Act 2000.
- A retired government official complained to the local police ststion that people were harassing him constantly over phone, with enquiring about the call girls. The caller

claimed that a message was displayed on their cell phone which said “Delhi college girls for Rs.500/- contact at phone number …..”. He received about 4000 phone calls over six weeks. The accused, Sunish Kapoor was arrested under sections 506(criminal intimidation) and 292(transmitting obscene material).

E-mail abuse:

- In e-mail abuse, women are being targeted by criminal netizens for the sake of revenge or for harassment.
- Delhi police arrested Manish, an Engineer and MBA degree holder, who posted the telephone number of his former boss’s wife on a chat room and asked netizens to get in touch late in the night. His motive was to take revenge on hos ex-boss who was responsible for his dismissal from his previous job.

UNIT-II
Assignment-Cum-Tutorial Questions
SECTION-A

Objective Questions

1. Hacking requires_____ [ ]

a) Computer b) Network c) both d) none.

2. _____ denotes “any matter expressed or described upon any substance by means of letters, figures or marks, which may be used as evidence of that matter”. [ ]

a) Document b) Electronic record c)FIR d) none

3._____ means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film. [ ]

a) Document b) Electronic record c)FIR d) none

4. Breaking into computer systems is called _____ [ ]

a) Cheating b) fraud c) Hacking d) all the above

5. _____ have deep knowledge of the Internet and telecommunication systems.

6. _____ who have knowledge of the intricacies (complex and detailed information) of computer systems and their operations. [ ]

a) code hackers b) Phreakers c) Cyber prunks d) crackers.

7. _____ specialize in cryptography. [ ]

a) Code hackers b) Phreakers c) Cyber prunks d) crackers.

8. Hacking with computer system is defined in_____ [ ]

a) Section 67 b) section 66 c) section 68 d) section 69

9. The main target of cyber fraud is_____.

10. Section _____ of IPC defines cheating.

11. _____ is defined as any set of computer instructions that are designed to modify, destroy, record, and transmit data or program residing within a computer.

12. Making or publishing an imputation concerning any person is called _____ [ ]

a) Defamation b) Harassment

c) e-mail abuse d) all the above

13. Internet protection makes sure that children don't do anything illegal online. [ ]

A. True B. False

14. A situation in which an individual makes another person feel uncomfortable online is hacking. [ ]

A. True B. False

15. Which computer virus records every movement you make on your computer? [ ]

a) Malware Android b)Key logger c) DoS d)Trapper

16. Which one is not a malicious software [ ]

a) Time bomb b) Mac c) Rabbit d) Trojan Horse

17. Which of the following is known as harassing and individual or a group of individuals by using internet or mobile phone? [ ]

a) Cyber Defamation b) Cyber Squatting

c) Cyber Stalking d) Cracking

18. What category of software is designed to cause detriment to your computer? [ ]

a) Bugs b) Malware c) Systems software d) Network snakes

19. What type of virus describes the awful consequences of not acting immediately? [ ]

a) Android b) Spoofing c)Misleading e-mail d) Phishing

20. What is the most likely problem with unsolicited investment advice? [ ]

a) You might not earn as much as claimed.

b) The advice might not be truly unbiased.

c) The advice might not be from a legitimate firm.

d) You might lose money.

21. Artificially inflating a stock in order to sell it at a higher value is referred to as what? [ ]

a) Bait and switch b) The Nigerian fraud

c) Pump and dump d) The Wall Street fraud

21. What is the top rule for avoiding Internet fraud?

a) If it seems too good to be true, it probably is. [ ]

b) Never use your bank account numbers.

c) Only work with people who have verifiable email addresses.

d) Don't invest in foreign deals.

22. What can you do on your local computer to protect your privacy?

a) Install a virus scanner. [ ]

b) Install a firewall.

c) Set your browser's security settings.

d) Set your computer's filter settings.

23. What program would you use to gain administrative rights to someone's computer? [ ]

a) Bot b) Executive Android c) Rootkit d) Trojan horse

SECTION-B

Descriptive Questions

1. List the classification of cyber crimes.
2. Define hacking and explain the characteristics and classification of hacking.
3. Explain Section 66 of IT Act, 2000.
4. Explain teenage web criminality and what measures can be taken to reduce teenage web vandals.
5. Explain the effects of virus on Internet.
6. Explain Defamation and its characteristics.

7. A says of a book published by Z- “Z’s book is foolish; Z must be a weak man, Z’s book is indecent; Z must be a man of impure mind.

A says- “I am not surprised that Z’s book is foolish and indecent, for he is a weak man. Do these offences amount to defamation, Justify?

8. If A writes a letter to B which is derogatory (insulting) of B

If A writes a letter to C containing derogatory remarks about B which damage’s B’s reputation.

Which of the above cases amount defamation and which one do not. Justify your answer.

9. Illustrate how the growth of e-commerce, profitable for cyber frauds?

With the Internet, is there a need for a hijacker to board an aircraft to hijack it? Quote some cases to support your answer.

10. Can the protective measures taken by the government stop the cyber fraud? Quote some fundamental changes to be made in the functioning of Internet.

11. Explain some international cyber frauds and technological battles around the world.

12. “A introduces water into an ice house belonging to Z, and thus causes ice to melt, intending wrongful loss to Z”. Does A commit mischief?

13. Quote some preventive measures to protect your personal computer from computer viruses.

UNIT-3

CYBER LAWS

Objectives:

To demonstrate about the Criminal Justice in India and its Implications.

Syllabus:

Cyber Pornography, Other IT Offences, Monetary Penalties, Adjudication and Appeals Under IT Act 2000, Network Service Providers, Jurisdiction and Cyber Crimes, Nature of Cyber Criminality Strategies to Tackle Cyber Crime and Trends, Criminal Justice in India and Implications.

Outcomes:

Students will be able to:

- Identify the problems with cyber pornography.
- Understand offences, other than those specified in IT Act.
- Explain onetary penalties and adjudicating authorities.
- Explain different types of network service providers and their liabilities for law.
- Understand the nature of cyber crime.
- Explain various strategies of tackling cyber crimes.
- Explain reasons for delayed justice in case of cyber crime.

Learning Material

1.Cyber Pornography

- Cyber Pornography is a difficult problem due to the difference in the acceptable limits of morality in different countries.
- Cyber crimes like hacking, cyber frauds, implanting virus threaten the credibility of the Internet, where as cyber pornography promotes the use of Internet.
- The reasons why cyber pornography has become so big are:
    - The easy, free, efficient, convenient and anonymous accessibility to pornographic material through the Internet.

- The anonymity of the cyber pornography industry, global accessibility, problems of jurisdiction, different and standards of morality in different countries, made the laws and their enforcement, useless.

- Cyber pornography has the caught the eye of even peons in offices who know only two things i.e., games and pornography.
- Attempts to control, restrict and regulate cyber pornography have completely failed.
- In 1996, the Communications Decency Act was legislated in USA for the purpose of regulating the pornographic content on the internet to protect minors, but that met a severe criticism.
- Nothing can be done against cyber pornography, because of global access of the Internet and different legal treatments to pornography in different parts of the world.
- Due to the three click access to cyber pornography from anywhere and its invisibility, the law makers and the law enforcement have no choice but to continue with contradiction.
- State has to try to attain social maturity through education and then it should be left to the individual choice as to what and how much of cyber pornography the individual wants to see.
- Child pornography can be directly avoided with laws which may permit hacking of these web-sites by the State. This would at least check child pornography even if it cannot erase it completely.
- Section 292 of IPC treats “sale of obscene books” as an offence. Section 67 of IT Act extends this and treats “publishing of information which is obscene in electronic form” as an offence.
- Cyber porno sites in foreign lands, publishing pornographic material would not be liable under 67 because section 75 of IT Act applies only to an offence involves a computer, computer system or computer network located in India.
- If an Indian surfer visits a pornographic web-site based in a foreign land, the site is not liable under section 67 because it is the visitor’s act which gives him access to the web-site and the web-site did not commit any offence.

- If a web-site in a foreign land transmits lascivious material to a person in India or if it advertises its services on a computer network in India, it would be liable under section 67 of IT Act.
- Search engines are also not liable under section 67 because they neither publish nor transmit any material.
- Though there are prohibitive and penal laws for punishing cyber pornography, the real problem lies in the implementation of these laws by the law enforcement agencies.
- Due to dualism in India, there are difficulties in applying these laws honestly, fairly and without bias upon the medium of Internet.

2. Other IT Offences

- Any person who knowingly or intentionally destroys or alters any computer source code used for a computer, computer program, computer system or computer network , is said to commit the offence of tampering with computer source documents and is punishable with an **imprisonment up to 3 years or with a fine which may extend to Rs. 2 lakh, or with both**. This is applicable if he fails to be in the limits of Controller of Certifying Authorities.

Controller of Certifying Authority:

- The Controller of Certifying Authorities may direct any agency of the government to intercept any information transmitted through any computer resource if it thinks that it is necessary for the sovereignty and integrity of India.
- Every subscriber or person in charge of the computer resource should extend all facilities and assistance to decrypt the information. Whoever fails to assist the agency in this regard is **punishable with imprisonment for a term which may extend to 7 years.**
- A person who unathorizedly secures access or attempts to secure access to a protected system as declared by a notification in a official gazette by the appropriate Government is liable for a **punishment with imprisonment up to 10 years and also is liable to fine.**
- A person who makes any misinterpretation to, or suppresses any material fact from Controller of Certifying Authorities for obtaining any certificate is liable for a **imprisonment which may extend up to 2 years or fine which may extend to Rs. 1 lakh or with both.**

- Any person who secures access to any electronic record, book, register, correspondence, information, document or other material, without the permission of the person concerned and discloses the same to any other person, is liable with **imprisonment for a term which may extend to two years or with fine which may extend to Rs 1 lakh, or with both.**
- A person who publishes a Digital Signature Certificate with the knowledge that the Certifying Authority listed in the certificate has not issued it or the subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended, is liable with **imprisonment for a term which may extend to 2 years or fine up to 1 lakh or with both.**
- A person, who knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose, is liable with **imprisonment extending up to 2 years, or with fine extending up to Rs. 2 lakh or both.**
- If a company commits an offence (or contravention), then every person who at the time of the contravention, shall be guilty of the contravention and is liable for the punishments accordingly. If the officer of the company proves that the contravention took place without his knowledge, he is not liable for the punishment.

3. Monetary Penalties, Adjudication and Appeals Under IT Act 2000

- Besides defining and punishing various cyber crimes with imprisonment/fine/both, the IT Act provides that the person would be liable to pay damages by way of compensation to the victim or penalty for non-compliance of certain requirements.

Acts those are liable for compensation:

- Any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network, is liable to pay damages by way of compensation not exceeding Rs 1 crore to the person affected(i.e., victim) if he does any or more of the following acts:
    - **Accesses or secures access** to computer, computer system or computer network.
    - **Downloads, copies or extracts any data**, computer database or information from a computer, computer system or computer network including information or data held or stored in any removable storage medium.

- **Introduces** or causes to be introduced any computer contaminant or computer virus into any computer, computer system or any computer network.
- **Damages** or causes to be damaged any computer, computer system or any computer network.
- **Disrupts** or causes disruption of any computer, computer system or any computer network.
- **Denies** or causes the denial of access to any person authorized to access any computer, computer system or any computer network.
- **Provides any assistance** to any person to any person to facilitate access to a computer, computer system or any computer network by any means.

Monetary Penalties:

- The following monetary penalties have been provided in the IT law for non-compliance of certain requirements:
  - Not exceeding Rs. 1.50 lakh for every failure to furnish any document, return or report to the Controller of Certifying Authority which is required to be furnished under the IT law.
  - Not exceeding Rs 5,000 for every day during which the failure to file any return or furnish any information, books or other documents within a stipulated time frame, continues.
  - Not exceeding Rs 10,000 per day during which the failure to maintain books of accounts or records as required, continues.
- As per section 45 of the IT Act, whoever violates any rules or regulations made under the Act, for the contravention of which no penalty has been separately provided, is liable to pay a compensation not exceeding Rs 25,000\- to the person affected by such contravention.

Adjudicating Authority:

- An adjudicating authority has been separately created for the purpose of adjudication of contraventions for which compensation and monetary penalties are provided.

- Contraventions punishable with imprisonment are trialable exclusively by criminal courts, where as contraventions entailing compensation or penalty under sections 43, 44 and 45 are left for adjudication by an adjudicating officer.
- The Central Government appoints any officer, not below the rank of a Director to the Government of India or an equivalent officer of a State Government, as an adjudicating officer for holding inquiries.
- No person can be appointed as an adjudication officer unless he possesses experience in the field of Information Technology.
- An adjudicating officer, upon considering the evidence produced, can impose penalty for the person who is liable to penalty under sections 43, 44 and 45.
- The adjudicating officer has been granted the powers of a civil court, upon the **Cyber Appellate Tribunal.**
- No appeal can be filed before the tribunal against an order made by the adjudicating officer with the consent of parties. An appeal should be filed within 45 days before the tribunal, from the date on which a copy of the order is received by the aggrieved person.
- Any appeal against any decision or order of the Cyber Appelate Tribunal has to be made to the High Court within 60 days from the date of communication to the aggrieved person.

4. Network Service Providers

- **Network service providers** are intermediaries who provide network technology services to users of the Internet.
- **Section 79 of IT Act**, 2000 is included in the legislature to protect network service providers from liability in certain cases.
- **Different types of network service providers:**
    - **Internet Access Providers**- who specialize in offering access to the Internet.
    - **Internet Service Providers**- who offer additional services such as hosting content produced by themselves or by users or by third parties.
    - **Online Service Providers**- who provide proprietary content for subscribers on their closed systems
- All ISP's are network service providers but vice versa is not true.

- Section 79 says that a person providing any service as network service provider would not be liable under IT Act, if
  - He proves that the offence or contravention was committed without his knowledge.
  - He had exercised all due diligence (voluntary investigation) to prevent the commission of such offence or contravention.

Issues of section 79:

- Section 79 reduces the hardships of network service providers only to a very limited extent and imposes a heavy duty upon them to exercise due diligence to prevent the commission of offence or contravention under IT Act. They have been given the roles of censor boards and the police by law.
- It is practically impossible and commercially not viable(affordable) for the ISP's who merely provide access or provide hosting services to web-sites, to manage and control Internet content and transactions and exercise diligence over the content of all interactions and millions of web pages on the Internet.
- Section 79 may be appropriate for those ISP's who are content providers, as they provide content themselves but not for those who provide access to Internet or host web sites.
- Section 79 makes no distinction between various kinds of ISP's.
- Section 79 implies that network service providers are liable for an offence or contravention, if they do not exercise due diligence to prevent the commission of an offence or contravention for any third party information or data made available by them.
- Therefore section 79 is imposing very heavy responsibility on all network service providers, irrespective of the nature of their services, failing which; they shall be liable under IT Act.
- Section 79 does not apply to offences, violations and contraventions under the laws other than the IT Act.
- It is unfair to accuse and penalize the Internet Service Providers for crimes committed by users over which they have no control.

- Most ISP's provide the technology and do not manage or control the content or transactions on the Internet. These are like telephone companies which provide the technology and have no control over the conversation or the manner of use of telephone. But unlike Newspaper, who have direct control over the content.
- To expect the ISP's to exercise diligence to prevent the commission of offences and contraventions, is unreasonable, even if liability is imposed on them. It is neither possible nor viable for them to keep track of all the transactions and content by acting as watch-dogs. It will directly affect their business and cause harassment to them.
- It would be reasonable to allow the ISP's who provide only technology without content, to operate freely without fear and to seek their cooperation in any investigation.
- ISP's and NSP's which do not provide content themselves must take steps to protect themselves against the allegations in the commission of offences by the users to whom they only provide technological services.
- ISP's have to clarify in their agreements that they have no control and accept no responsibility for any transaction or content or any other act done by the user to whom they only provide technological services.
- The real solution lies in the amendment of the law which must protect the network service provider's which only provide access or technology and no content, from criminal and civil liabilities.

5. Jurisdiction and Cyber Crimes

- The IT Act 2000, specifically states that unless otherwise provided in the Act, the Act applies to any offence or contravention committed **outside India by any person irrespective of his nationality.**
- The IT Act will apply to an offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention, **involves a computer, computer system or computer network located in India.**
- The words "act or conduct constituting the offence or contravention, involves a computer, computer system or computer network located in India" are very important to determine the jurisdiction of IT Act over acts committed outside India.

- For an offence or contravention under IT Act which is committed outside India, it has to be proved that the act involves a computer, computer system or computer network located in India.

Jurisdiction of IT Act:

- If a web-site is created in US, which contains illegal material, it is not possible for the IT Act jurisdiction to question the site unless the creation or maintenance or running of the site involves a computer, computer system or computer network located in India, under section 67.
- If a person from US hacks a computer system or network in India, the accused can be punished for hacking under section 66 of IT Act, because his act involves a computer in India.
- If a person plants a virus into a computer system located in India, he will be liable under section 43© of IT Act to pay damages, not exceeding 1 crore to the victim.

Basic principle of Jurisdiction:

- Every offence shall ordinarily be inquired into and tried by the court within whose local jurisdiction it was committed.
- The principles of Cr.P.C 1973 are applied for determining jurisdiction in trail by courts as well as in investigation by the police.
- If an offence is committed in more than one place, or partly in one place and partly in another,, or where it is continuing and continues to be committed in more than one local area, or where the offence consists of several acts done in different local areas, then it may inquired into or tried by a court having jurisdiction over either of such areas.
- If an act is done in one jurisdiction and its consequence is ensued in another jurisdiction, the offence can be inquired into or tried by a court within either of the local jurisdiction. For example:
    - The place from where the defamatory letter was e-mailed and the place at which it was received are different.
    - If an employee of a company based at Delhi, operates a bank account of his employer company in a Bombay bank, transfers funds to his account at Calcutta,

this case can be tried at Delhi or Bombay where the offence was partially committed or at Calcutta where the money was received and retained.

- In case of cheating that is done by means of letters or telecommunication messages, it may be inquired into or tried by any court within whose jurisdiction such letters or messages were sent or where they are received.

- In case where there are two or more courts for the offence and a question arises as to which of the courts has jurisdiction t6o inquire into, that is decided by the High Court, under which these courts function.
- When two are more courts have jurisdiction over an offence, the choice of the court for the case can be done by the complainant. He chooses the court which is most convenient for him and most inconvenient for the accused.

Cyber crimes:

- The Internet by its nature and purpose operates when the parties are not physically face to face with one another.
- Due to the global access of the Internet, cyber crimes involve two or more places, one from where the cyber criminal inflicts and other where the victim is inflicted.
- Every criminal makes all attempts to conceal his identity and place of operation.

6. Nature of Cyber Criminality, Strategies to tackle cyber crime and trends

Characteristics of cyber crime which distinguishes it from other forms of criminality:

- The weapon of cyber crime is **Technology**. Cyber crimes are the work of technology and are performed by technocrats who have a deep understanding if Internet and computers.
- Cyber crime is **extremely efficient**. It operates and affects within no time. It takes only a few seconds or a few minutes to hack websites.
- Cyber crime has **no geographical limitations**, boundaries or distances.
- The act of cyber crime takes place in cyber space which makes the cyber criminal almost **invisible**. All the components of cyber criminality, from preparation to execution, take place in cyber world. The **degree of risk in cyber criminality is less** when compared to traditional criminalities due to disregard of geographical distances.

- The **harm and injury caused by cyber crime is of unimaginable magnitude**. It can easily destroy web-sites created and maintained with huge investments. It can hack confidential zones like defense systems and can shake economies.
- It is extremely **difficult to collect evidence** of cyber crime and prove the same in Court of law, due to its efficiency and potential that can affect several countries at the same time.
- Cyber crimes are **easy to commit** because the weapons to commit are easily and freely available in CD's and Internet.

Strategies to tackle cyber crimes:

- The IT Act, 2000 provides the most prevalent and convenient method to deal with cyber crime: **deterrence.** The general policy is to use deterrent punishments as a strategy for controlling the crime.
- But deterrence is not only the answer for the cyber crime. It is only one of the several strategies to tackle cyber crime.
- Information Technology Security Procedure And Guidelines are framed, which are enclosed in Annexure II Certifying Authorities Rules made under IT Act, 2000.
- The characteristics of cyber crime need to be considered while devising measures of checking, preventing and punishing cyber crimes.
- The following strategies are adopted to tackle the cyber crimes:
    - Since the cyber crimes are crimes of technology, a cyber cop has to be at least a half IT engineer, to be a competent cyber crime investigator. The cyber cops must learn to use technical weapons and tools such as trace and trap devices to detect cyber crimes.
    - The cyber criminal has the tendency of jumping geographical borders, called **"jurisdictional jumping"**. So there has to be cooperation between law enforcement agencies of different countries.
    - Effective laws of **extradition** (the surrender of an accused or convicted person by one state or country to another) and their implementation are necessary to bring cyber criminals to trail. The existing extradition need to be strengthened by cooperation in the international community.

- The most effective weapons to counter cyber crime is the use of encryption and other security technologies. We need better locks on computer to prevent cyber crime.
- The IT industry has to the responsibility of protecting its own computer systems and networks by using secure technologies instead of depending on law enforcement agencies, for which it is extremely difficult to track the anonymous cyber criminals.
- The government should encourage the use of security technologies and should work in close partnership with the private sector. Government should fund and support R&D and facilitate education about the measures to counter cyber crime.
- Cyber are not reported by the victims for the fear of losing confidence of customers and the loss of business. But suppressing the information encourages the cyber crime. The private sector must share the information about the cyber crime so as to understand its various forma so that it can be dealt even effectively.
- Technological methods that easily identify the netizens, must be used while investigating a cyber crime.

Conclusion:

- There is great rise in cyber criminality committed by the **employees and other insiders** in the organization besides system penetration by an external party.
- Virus related and denial-of-service attacks have increased. Cross-national attacks are raised.
- There is disappearance of Intellectual Property for personal benefit or to sell the same to a competitor or any other interested buyer.
- Due to the growth of cyber consumers, cyber crime is mainly affecting web-sites and portals.

7. Criminal Justice in India and Implications on Cyber Crime

- **"Delayed justice"** has been a part of the criminal and civil justice systems of our country. The reasons for delayed justice are as follows:
  - Growth of population
  - Disproportionate ratio between the number of cases and the number of judges

- Inaction by the government
- lack of accountability and sensitivity and dilatory attitude(slower processing)

- The State must take pro-active measures to ensure speedy criminal justice, which should not take 120 days to conclude.
- Due to more liberalization and enforcement of fundamental rights, it is difficult to detect the crimes committed by hardened criminals, and hence they would go unpunished and the society would suffer. The society expects that the Police must deal with criminals in an efficient and effective manner and book those who are involved in the crime.
- The judiciary has become strict on the grant of bail. It is not as liberal as stated in the legal principles. The media also substantially contributes to te criminal cases and highlights the cases as if the accused are criminal before the start of the trail.
- Many of the cyber crimes such as hacking, planting virus, cyber fraud or defamation are committed over several geographical areas, which adds delay in the investigation and trail of cyber crimes.
- Witnesses are scattered over different places, leading to time consuming investigation and trail.

UNIT-III
Assignment-Cum-Tutorial Questions
SECTION-A

Objective Questions

1. Cyber pornography _____ the use of Internet. [ ]

   (a) Threatens (b) Promotes (c) Rises (d) all the above
2. _____ of IPC treats “sale of obscene books” as an offence.
3. _____ of IT Act extends this and treats “publishing of information which is obscene in electronic form” as an offence.
4. The _____ may direct any agency of the government to intercept any information transmitted through any computer resource if it thinks that it is necessary for the sovereignty and integrity of India.
5. For every failure to furnish any document, return or report to the Controller of Certifying Authority which is required to be furnished under the IT law, the penalty is _____ lakh.
6. A _____ has been separately created for the purpose of adjudication of contraventions for which compensation and monetary penalties are provided.
7. An adjudicating officer, upon considering the evidence produced, can impose penalty for the person who is liable to penalty under sections _____ [ ]

   (a)43 (b) 44 (c) 45 (d) All the above
8. _____ are intermediaries who provide network technology services to users of the Internet.
9. _____ are those who specialize in offering access to the Internet. [ ]

   (a) Internet Access Providers (b) Internet Service Providers

   (c) Online Service Providers (d) All the above

10._____ are those who offer additional services such as hosting content produced by themselves or by users or by third parties. [ ]

(a) Internet Access Providers (b) Internet Service Providers

(c) Online Service Providers (d) All the above

11._____who provide proprietary content for subscribers on their closed systems [ ]

(a) Internet Access Providers (b) Internet Service Providers

(c) Online Service Providers (d) All the above

12.Section _____ deals with network service providers.

13.The cyber criminal has the tendency of jumping geographical borders, called _____.

14._____ of the Information Technology Act, 2000 prohibits sending of offensive messages through communication service"

(a)section 66A (b) Section 66E [ ]

(c) Section 67A (d) Section 67B

15._____ of the Information Technology Act, 2000 prohibits capturing, transmitting or publishing the image of a private area of a person without consent. [ ]

(a) section 66A (b) Section 66E

(c) Section 67A (d) Section 67B

16._____ of the Information Technology Act, 2000 specifically prohibits, transmission or publication of obscene material in electronic form. [ ]

(a) section 66A (b) Section 66E

(c) Section 67 (d) Section 67B

17._____ of the Information Technology Act, 2000 prohibits transmission or publication of material containing sexually explicit act in electronic form. [ ]

(a) section 66A (b) Section 66E

(c) Section 67A (d) Section 67B

18._____ of the Information Technology Act, 2000 prohibits storying, private viewing, transmission or publication of material containing child pornography in electronic form. [ ]

(a)section 66A (b) Section 66E

(c) Section 67A (d) Section 67B

19.The _____ Government has instructed ISPs to filter legal pornography and other adult subjects **"by default".** **[ ]**

(a)United Kingdom (b) Australia

(c) Japan (d) America

20.The best way to control cyber crimes is provided by _____[ ]

(a)Cross-Domain Solutions (b) Laws of Extradiction

(c) Educating people (d) None

21.The State must take pro-active measures to ensure speedy criminal justice, which should not take _____ to conclude. [ ]

(a)150 days (b) **120 days** (c) 200 days (d) None

22.The majority of computer crimes are committed by _____

(a)outsiders (b) insiders [ ]

(c) Hackers (d) Overseas criminals

23.The typical computer criminal is_____

(a) young hacker [ ]

(b) trusted employee with no criminal record

(c) trusted employee with long but unknown criminal record

(d) Overseas young hacker.

24.There are about _____ cases pending in India.

25.If a person plants a virus into a computer system located in India, he will be liable under _____ of IT Act to pay damages, not exceeding 1 crore to the victim. [ ]

(a)Section 43 C (b) Section 46 (c) Section 47 (d) none.

SECTION-B

Descriptive Questions

1. Explain about Controller of Certifying Authority.
2. Discuss about monetary penalties and adjudication authority?
3. Explain how section 79 imposes an extra burden on network service providers?
4. Explain jurisdiction and cyber crimes.
5. Explain the nature of cyber criminality and the strategies to tackle the cyber crimes.
6. Discuss about criminal justice in India?
7. How the jurisdiction limits effect cyber crimes? Quote a real time example.
8. Analyze the reasons for delayed justice in case of cyber crimes in India.
9. Can a government legitimately prohibit citizens from publishing or viewing pornography, or would this be an unjustified violation of basic freedoms?
10. Discuss the necessary amendments to Information Technology Act, 2000 for better Regulation, prosecution and conviction as far as Cyber Pornography Offences are concerned.
11. Discuss the Practicality of banning Cyber Pornography & Role of an Intermediary in India
12. How far the awareness Campaigns for Educating Parents on Parental Control , curb Cyber Pornography.
13. The State of Tamil Nadu v/s Suhas Katti.

Facts: This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the victim for information by the accused through a false e- mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the complaint police nabbed the accused. He was a known family friend of the victim and was interested in marrying her.

She married to another person, but that marriage ended in divorce and the accused started contacting her once again. And her reluctance to marry him he started harassing her through internet.

Held: The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000 and the accused is convicted and is sentenced for the offence to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offence u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently." The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered the first case convicted under section 67 of Information Technology Act 2000 in India.

Discuss the case study and the judgment in the above case

14. Discuss top 4 cases of delayed justice in India.

15. "Justice delayed is justice denied"- Explain with case studies.

UNIT – IV

Objective:

To understand Digital Signatures, responsibilities of certifying authorities and consumer services.

Syllabus:

Digital Signatures, Certifying Authorities and e-Governance

Introduction to Digital Signatures, Certifying Authorities and Liability in the Event of Digital Signature compromise, E - Governance in the India. A Warming to Babudom, Are Cyber Consumers Covered under the Consumer Protection, Goods and Services, Consumer Complaint Defect in Goods and Deficiency in Services Restrictive and Unfair Trade Practices.

Outcomes:

Students will be able to:

- Explain how a digital signature is created and verified.
- Understand the responsibilities of Certifying Authority.
- Explain the outcomes of e-governance.
- Understand Consumer Protection Act.
- Extend the rights of consumers in case of defect in goods.
- Illustrate cases of deficiency in services and measures taken.

1. Digital Signatures

- **"Signature"** refers to the writing of one's name or putting a mark for authenticating or executing a document by the signatory.
- The following are the main functions performed by a signature:
    - **Identification:** By signing the document, the signatory identifies himself by the unique style of writing his name or the mark.
    - **Authentication:** By performing the act of signing a document, the signatory acknowledges that he authorizes and adopts the text in some meaningful way.
    - **Security:** The individuality of the style of writing or the mark grants security against forgery.

- **Binding:** A signature signifies intent of the signatory to be bound by the signed document.
- **Evidence:** A signature is an evidence of the aforesaid identification, authentication and of being bound to the signed document.

- The above functions performed by a signature are significant for commercial transactions. But, with e-commerce, a system is necessary to give confidence to the parties indulging in e-transactions.
- An alternative to a physical signature on paper had to be developed for the cyber world. That is "Digital Signature".
- The functions and purposes of digital signature are same as the normal signature but the act of digitally signing the documents is different from physical signatures on paper.
- **Significant different between a physical signature and digital signature:** Physical signature is the direct act of the human hand without any external dependence whereas digital signature is an external system of technology applied by the subscriber of an electronic record.
- The concept of digital signature has been recognized by the IT Act, 2000, which is the creation of technology.
- **Definition:** "Digital Signature" under the IT Act, 2000 means authentication of any electronic record by a subscriber by means of electronic method or procedure in accordance with Section 3 of the IT Act. It is as follows:

Section 3 of IT Act, 2000:

- **Authentication of electronic records.-**

  (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 the 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.

Asymmetric crypto system:

- "Asymmetric crypto system" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature. This system involves the processes of encryption and decryption of the data on which it is applied.
- Asymmetric crypto system of a process of transforming plain text data into an unintelligible form(cipher-text) such that the original data cannot be recovered without using an inverse decryption process.
- Cryptography is a mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be retrieved into the original format with the use of the decryption process.
- The process of decryption permits the person concerned for whom the encrypted information is indented, to verify the digital signature and access the data.
- The Internet is a very open system of communication. So it is necessary to protect data, maintain its integrity, preserve privacy and confidentiality between the concerned parties, and the processes of encryption, decryption and hash function seek to satisfy these conditions.

Asymmetric cryptography:

- It involves the use of two keys, which form a key pair for the purposes of encryption and decryption.
- A **"key pair"** means a private key and its mathematically related public key.
- A public key can verify a digital signature created by the private key.
- **"Private Key"** is used to create a digital signature.
- **"Public key"** is used to verify a digital signature and is listed in the Digital Signature Certificate.
- **Verifying an electronic record means:**
    - The initial electronic record was affixed with the digital signature by the use of the private key corresponding to the public key of the subscriber.
    - The initial electronic record id retained intact or has been altered since such an electronic record was so affixed with the digital signature.
- The public key is intended to freely available to the public and may be published in a directory or an online repository or may even shown on a visiting card of the subscriber.
- The private key is confidential to the subscriber.
- Any data which is encrypted with a particular private key can only be decrypted by using the corresponding public key.

Security of the private key:

- The security and confidentiality of the private key are very crucial for the safety of the system of digital signatures.
- If the system of asymmetric cryptography is well designed, it is impossible to decode or derive the private key from the knowledge of public key.
- A safe method for ensuring the security and confidentiality of the private key is to store the private key in a floppy or a CD or a card. It is not recommended to store a private key in the hard-disk of the computer because of the risk of it being hacked.
- There is a methodology by which the private key does not enter the memory or the processor of the computer, when used from a floppy or CD.
- The private key which is stored in a floppy or CD is protected through a password assigned by the subscriber.

- The key pair must be generated by the subscriber by applying security procedure on **a key generation system.**
- The key generation system must generate statiscally random key values that are resistant to known attacks.
- The generated keys are to be transferred from key generation system to the storage device using secure mechanism that ensures confidentiality and integrity.

Creation of a Digital Signature:

- **Affixing digital signature** means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature.
- The process of creation of Digital Signature has been explained in **Rule 4 of Information Technology (Certifying Authorities) Rules**, 2000.
- The subscriber would first be required to delimit the information intended to be signed digitally.
- On this information the **"hash function"** is applied, which compresses the information in a digital form which is represented by the **"hash result".**
- The application of hash function and its result are unique to every information/message intended to be signed digitally.
- The system of hash function is used for creation as well as verification of a digital signature. Application of hash function would verify that the information is the same as it was originally and there has been no tampering with the original electronic record.
- The hash function computes a hash result of standard length , which is unique.
- The software of the signatory then transforms the hash result into a Digital Signature by using his private key, which encrypts the information/data.
- The result of the process is unique to the message as well as to the subscriber/signatory and thus can be used as a Digital Signature.

Verification of Digital Signature:

- The process of verification of Digital Signature has been explained in **Rule 5 of Information Technology (Certifying Authorities) Rules**, **2000.**
- The verification is done with the help of the hash function and the public key corresponding to the private key used for creating Digital Signatures.

- By applying the hash function on the original electronic record, a new hash result is computed. At the time of verification, by comparing the new hash result with the hash result computed at the time of applying the process of digital signatures, it can be verified if the original electronic record is the same as that received.
- To verify the identity of the sender, his public key is applied by the recipient of the electronic record. This would verify whether the digital signature was created by the sender's private key.

Secure digital signature:

A secure digital signature should satisfy the following conditions:

- **1. It should be unique to the subscriber affixing it**. A digital signature is unique and is based upon the message that is signed and the private key of the signer.
- **2. It should be capable of identifying such subscriber**. What this implies is that the digital signature should be verifiable by the public key of the signer and by no other public key.
- **3. It should be created in a manner or using a means under the exclusive control of the subscriber.** This implies that the signer must use hardware and software that are completely free of any unauthorized external control.
- **4.** It should be linked to the electronic record to which it relates in such a manner that if the electronic record were altered, the digital signature would be invalidated.

Certifying Authority:

- In e-transactions, the parties do not come face to face with one another, so third party is required. This is in the form of a **"Certifying Authority".**
- **Defnition:**A Certifying Authority is a body, either public or private, that seeks to fill the need for trusted third party services in e-commerce by issuing Digital Signature Certificates.
- A certifying Authority grants **Digital Signature Certificates** to subscribers after proper identification and verification.
- Any person can make an application to the Certifying Authority (CA) for the issue of a Digital Signature Certificate.

2. Digital Signature Certificate

- Each application to CA for Digital Signature Certificate is required to be accompanied by:
  - **The prescribed fee** (not exceeding twenty-five thousand rupees) to be paid to the CA.
  - A **Certification practice statement** or a statement containing specified particulars.
- On receipt of an application the Certifying Authority may grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application.
- A Digital Signature Certificate cannot 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 for issuance of a Digital Signature Certificate can be rejected unless the applicant is given a reasonable explanation.

Issuance of Digital Signature Certificate:

- **Before the issuance of Digital Signature Certificate**, the Certifying Authority must:
  - Confirm that the user's name does not appear in its list of compromised users.
  - Comply with the procedure as defined in his Certification Practice Statement including verification and/or employment.
  - Comply with all the privacy requirements.
  - Obtain consent of a person requesting the Digital Signature Certificate that the details of such Digital Signature Certificate can be published on a directory service.

Issuing a Digital Signature Certificate:

- **While issuing a Digital Signature Certificate** a Certifying Authority must certify that:
  - The subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same.
  - It has published the Digital Signature Certificate and made it available to such person relying on it and the subscriber has accepted it.
  - The subscriber's public key and private key constitute a functioning key pair.
  - The information contained in the Digital Signature Certificate is accurate.

Suspension of Digital Signature Certificate:

- The Certifying Authority, which has issued a Digital Signature Certificate, may suspend such Digital Signature Certificate:
  - On a request from the subscriber listed in the Digital Signature Certificate.
  - On a request from any person duly authorized to act on behalf of that subscriber.
  - If it is of opinion that the Certificate should be suspended in public interest.
  - A Digital Signature Certificate cannot be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity of being heard in the matter.
  - On suspension of a Digital Signature Certificate the Certifying Authority shall communicate the same to the subscriber.

Revocation of Digital Signature Certificate:

- A Certifying Authority can revoke a Certificate issued by it on the:
  - Request of the subscriber.
  - Request of any person authorized by him.
  - Upon the death, of the subscriber.
  - Upon the dissolution or winding up of the firm or a company.
- A Certifying Authority may revoke a Digital Signature Certificate issued by it at any time, if it is of the opinion that:
  - A material fact represented in the Digital Signature Certificate is false or has been concealed.
  - A requirement for issuance of the Digital Signature Certificate was not satisfied.

- The Certifying Authority's private key or security system was compromised in a manner materially affecting the Digital Signature Certificate's reliability,
- The subscriber has been declared insolvent or dead, has been dissolved, wound-up or otherwise ceased to exist.

- A Digital Signature Certificate may not be revoked unless the subscriber has been given an opportunity of being heard in the matter.
- On revocation of a Digital Signature Certificate under this section, the Certifying Authority is required to communicate the same to the subscriber.

3. Certifying Authorities and Liability in the Event of Digital Signature compromise

Role of Certifying Authority:

- Certifying Authorities plays a very important role in the environment of Digital Signatures.
- IT Act simply defines “Certifying Authority” as a person who has been granted a license to issue a “Digital Signature Certificate”. But the role of Certifying Authority begins with the license to issue Digital Signature Certificates and extends to managing the functioning of the system of digital signatures and giving evidence of the proof of digital signatures in legal disputes, wherever necessary in the Court.
- The integrity and safety of the system of digital signatures depends on the Certifying Authorities.
- Certifying Authorities are very important witnesses in digital signature disputes, because they are global corporations located all over the map and hence can reduce delay in legal proceedings.
- The appointment and regulation of Certifying Authorities are very significant due to the imperative necessity of their honesty and professionalism.
- The Central Government appoints a **Controller of Certifying Authorities**, by notification in the Official Gazette. It may also appoint **Deputy Controllers and Assistant Controllers** as needed.
- The **Controller of Certifying Authorities** discharges his functions under the IT Act subject to general control and directions of the Central Government. The **Deputy**

Controllers and Assistant Controllers perform the functions which are assigned to them by the Controller of Certifying Authorities.

- The Central Government specifies
  - Qualifications, experience & terms and conditions of service of the Controller, Deputy Controllers and Assistant Controllers
  - The places where the Head Office and Branch Office of the Controller shall be located.

Controller of Certifying Authorities:

- The Controller of Certifying Authorities is empowered to perform the all or any of the following functions:
  - Exercising supervision over the activities of the Certifying Authorities.
  - Certifying public keys of Certifying Authorities.
  - Laying down the standards to be maintained by the Certifying Authorities.
  - Specifying the qualifications and experience which employees of the Certifying Authority should possess.
  - Specifying the conditions subject to which the Certifying Authorities shall conduct their business.
  - 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.
  - Specifying the form and content of a Digital Signature Certificate and the key.
  - Specifying the form and manner in which accounts shall be maintained by the Certifying Authority.
  - Specifying the terms and conditions subject to which auditors mat be appointed and the remuneration to be paid to them.
  - Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulating of such systems.
  - Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers.

- Laying down the duties of Certifying Authorities.
- Maintaining a database containing the disclosure record of every Certifying Authority, specified by the regulations, which shall be accessible to the public.

➢ Rule 8 of the Certifying Authorities Rules provides the financial criteria for being eligible to be appointed as a Certifying Authority.

Recognition of Foreign Certifying Authorities:

➢ Any **Foreign Certifying Authority** can be recognized by notification by the Controller of Certifying Authorities, with the approval of the Central Government. Digital Signature Certificate issued by such Certifying Authority is valid under the law, after recognition.

➢ The Controller has the power to revoke the recognition of a Foreign Certifying Authority, if the Controller proves that such Certifying Authority contravenes(against law) any conditions and restrictions subject to recognition.

➢ The Controller of Certifying Authorities, must record his reasons in writing, before revocation and the revocation shall be notified in the Official Gazette.

Granting license for Certifying Authority:

➢ **Sections 21 and 22 of the IT Act, 2000 and Rule 10 of Certifying Authorities Rules** provide the procedure and requirements for moving an application by an applicant before the Controller for appointment as a Certifying Authority.

➢ **Rule 11** prescribes non-refundable fees of Rs 25,000\- payable to the Controller, which is required to accompany the application for the grant of license of Certifying Authority.

➢ For renewal of a license, a non-refundable fee of 5000/- is payable.

➢ **Section 24 of IT Act, 2000 and Rule 16 of the Certifying Authorities Rules** provides that the Controller can grant or reject the application for license, within four weeks from the date of receipt of the application, after considering the documents accompanying the application. In exceptional cases, the period can be extended but not more than 8 weeks.

➢ The applicant of the Certifying Authority has to fulfill the requirements of qualifications, expertise, manpower, financial resources and infrastructural facilities for the issuance of Digital Signature Certificate.

Refusing the grant of license or renewal of Certifying Authority:

- **Rule 17** empowers the Controller to refuse to grant or renew a license if-
  - 1. The applicant has not provided the Controller with such information relating to its business, and to any circumstances likely to affect its method of conducting business, as the Controller may require.
  - 2. The applicant is in the course of being wound up or liquidated.
  - 3. A receiver and / or manager have been appointed by the court in respect of the applicant.
  - 4. The applicant or any trusted person has been convicted, whether in India or out of India, of an offence the conviction for which involved a finding that it or such trusted person acted fraudulently or dishonestly, or has been convicted of an offence under the Act or these rules.
  - 5. The Controller has invoked performance bond or banker's guarantee.
  - 6. A Certifying Authority commits breach of, or fails to observe and comply with, the procedures and practices as per the Certification Practice Statement.
  - 7. A Certifying Authority fails to conduct, or does not submit, the returns of the audit in accordance with rule 31.
  - 8. The audit report recommends that the Certifying Authority is not worthy of continuing Certifying Authority's operation.
  - 9. A Certifying Authority fails to comply with the directions of the Controller.

Rules of Certifying Authorities:

- **Rule 3** provides for the **use of public key cryptography** to authenticate information by means of digital signatures.
- **Rule 4 and Rule 5** contain provisions relating to the **creation and verification of digital signatures.**
- **Rule 10** provides that every application for a **licensed Certifying Authority** must be made to the Controller in the **prescribed form.**
- **Rule 11** provides for a non-refundable fee of twenty-five thousand rupees to be paid along with the application for grant of license. For renewal of license a non-refundable

fee of five thousand rupees is payable. The fee is not refundable in the event of suspension or revocation of the license.

- **Rule 12** says that Licensed Certifying Authorities are required to have arrangements for cross certification with other licensed Certifying Authorities within India. Such arrangements have to be submitted to the Controller before the commencement of operations. This rule provides that any dispute arising as a result of an arrangement between the Certifying Authorities or between the Certifying Authority and the subscriber must be referred to the Controller for arbitration or resolution.
- **Rule 13** lays down that the **license issued** to a certifying authority will be **valid for a period of 5 years from the date of issue** and that the license is not transferable.
- **Rule 14** empowers the Controller to **suspend the license** in accordance with the provisions of section 25(2) of the Act.
- **Section 23 of IT Act and Rule 15** contains provisions relating to **renewal of the license of a certifying authority**. A certifying authority is required to submit an application for the renewal of its license at least 45 days prior to the expiry of the validity period of the license.
- **Rule 16** contains provisions relating to **Issuance of License**. The Controller may, within four weeks from the date of receipt of the application grant or renew the license or reject the application. This period of 4 weeks may be extended to a maximum of eight weeks under special circumstances.
- **Rule 19** lays down the **security guidelines for Certifying Authorities**. Certifying Authorities have the sole responsibility of integrity, confidentiality and protection of information and information assets employed in its operation.
- **Rule 20** provides that the licensed Certifying Authority will not commence commercial operation of generation and issue of digital signature certificates before
    - 1. Confirming to the Controller the adoption of Certification Practice Statement.
    - 2. Generation of its key pair
    - 3. Audit of installation of facilities and infrastructure associated with all functions of generation, issue and management of digital signature certificate

- 4. Submission of the arrangement for cross certification with other licensed Certifying Authorities within India to the Controller.

- **Rule 21** contains provisions relating to the requirements prior to **cessation as Certifying Authority**. Before ceasing to act as a Certifying Authority, a Certifying Authority is required to give notice to the Controller of its intention to cease acting as a Certifying Authority. The notice has to be made ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of license. The Certifying Authority is also required to advertise his intention sixty days before the expiry of license or ceasing to act as Certifying Authority in daily newspapers or newspapers specified by the Controller.
- **Rule 22** provides that the Controller has to **maintain a database** of the disclosure record of every Certifying Authority, Cross Certifying Authority and Foreign Certifying Authority.
- **Rule 23** says that the Digital signature certificate can be granted only after a Digital signature certificate application has been submitted by the subscriber to the Certifying Authority and the same has been approved by it.
- **Rule 24** contains provisions relating to the **generation of Digital signature certificates**.
- **Rule 26** contains provisions relating to the **life of a digital signature certificate**. A Digital signature certificate has to be granted with a designated expiry date. It expires automatically upon reaching the designated expiry date at which time it must be archived.
- **Rule 27** says that Certifying Authorities are required to archive the following for a minimum period of seven years:
    - 1. Applications for issue of digital signature certificates.
    - 2. Registration and verification documents of generated Digital signature certificates.
    - 3. Digital signature certificates.
    - 4. Notices of suspension.
    - 5. Information of suspended digital signature certificates.
    - 6. Information of revoked digital signature certificates.
    - 7. Expired digital signature certificates.

- **Rule 29** provides for **revocation of digital signature certificates.**
- **Rule 30** lays down the **fees for issue of digital signature certificate**. The Central Government can prescribe the fees that Certifying Authorities can charge for the issue of digital signature certificates.
- **Rule 31** says that Certifying Authorities must **get their operations audited annually** by an auditor.
- **Rule 32** provides that the **auditor has to be independent of the Certifying Authority** being audited and cannot be a software or hardware vendor which is, or has been providing services or supplying equipment to the said Certifying Authority.
- **Rule 33** says that the following information must be kept confidential:
    - 1. Digital signature certificate application, whether approved or rejected.
    - 2. Digital signature certificate information collected from the subscriber or elsewhere as part of the registration and verification record but not included in the Digital signature certificate information.
    - 3. Subscriber agreement
- **Rule 34** lays down that the **access to confidential information**, by the operational staff of a Certifying Authority, is to be on a **"need-to-know" and "need-to-use"** basis. paper based records, documentation and backup data containing all confidential information must be maintained in secure and locked container or filing system, separately from all other records.

Licensed Certifying Authorities in India:

- The licensed Certifying Authorities in India include:
    - 1. Safescrypt
    - 2. NIC
    - 3. IDRBT
    - 4. TCS
    - 5. MTNL
    - 6. Customs & Central Excise
    - 7. (n)Code Solutions CA (GNFC)

4. E- Governance in the India. A Warning to Babudom

- Electronic records and digital signatures have been granted legal recognition.
- Any matter is authenticated by a Digital Signature affixed in manner prescribed the Central Government.
- **Section 6: Use of electronic records and [electronic signatures] in Government and its agencies.** -Where any law provides for-

  (a) 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;

  (b) The issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;

  (c) The receipt or payment of money in a particular manner,
- **Section 7 :Retention of electronic records.-**
  - 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-
    - (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
    - (b) 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;
    - (c) 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
- **Section 8** of IT Act, 2000 enables publication of rules, regulations, bye-laws, notifications, etc. to be published in the Electronic Gazette.
- **Section 9** says that the provisions of Sections 6, 7 and 8 not to confer right to insist document should be accepted in electronic form. Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or

under any law or controlled or funded by the Central or State Government should accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

Some Initiatives in the field of e-governance -Government to Citizen (G2C) Initiatives:

- **Computerization of Land Records**: In collaboration with NIC. Ensuring that landowners get computerized copies of ownership, crop and tenancy and updated copies of Records of Rights (RoRs) on demand.
- **Bhoomi Project**: Online delivery of Land Records. Self-sustainable e-Governance project for the computerized delivery of 20 million rural land records to 6.7 million farmers through 177 Government-owned kiosks in the State of Karnataka
- **Gyandoot:** It is an Intranet-based Government to Citizen (G2C) service delivery initiative. It was initiated in the Dhar district of Madhya Pradesh in January 2000 with the twin objective of providing relevant information to the rural population and acting as an interface between the district administration and the people.
- **Lokvani Project in Uttar Pradesh:** Lokvani is a public-private partnership project at Sitapur District in Uttar Pradesh which was initiated in November, 2004. Its objective is to provide a single window, self-sustainable e-Governance solution with regard to handling of grievances, land record maintenance and providing a mixture of essential services.
- **Project FRIENDS in Kerala:** FRIENDS (Fast, Reliable, Instant, Efficient Network for the Disbursement of Services) is a Single Window Facility providing citizens the means to pay taxes and other financial dues to the State Government.The services are provided through FRIENDS *Janasevana Kendrams* located in the district headquarters.
- **e-Mitra Project in Rajasthan:** e-Mitra is an integrated project to facilitate the urban and the rural masses with maximum possible services related to different state government departments through Lokmitra-Janmitra Centers/Kiosks.
- **e-*Seva* (Andhra Pradesh):** This project is designed to provide 'Government to Citizen' and 'e-Business to Citizen' services. The highlight of the e*Seva* project is that all the services are delivered online to consumers /citizens by connecting them to the respective

government departments and providing online information at the point of service delivery.

- **Admission to Professional Colleges – Common Entrance Test (CET):** With the rapid growth in the demand as well as supply of professional education, the process of admission to these institutions became a major challenge in the early 1990s. Recourse was then taken to ICT to make the process of admission transparent and objective. One of the pioneering efforts was made by Karnataka. The State Government decided to conduct a common entrance test based on which admission to different colleges and disciplines was made.

5. Are Cyber Consumers Covered under the Consumer Protection?

- A cyber consumer is no different from an ordinary consumer.
- A cyber consumer purchases goods and hires services using the Internet whereas a ordinary consumer uses traditional methods.
- The definition of consumer according to **Consumer Protection Act, 1986** is as follows:

  "Consumer" means any person who,—

  (i) buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other than the person who buys such goods for consideration paid or promised or partly paid or partly promised, or under any system of deferred payment, when such use is made with the approval of such person, but does not include a person who obtains such goods for resale or for any commercial purpose; or

  (ii) hires or avails of any services for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such services other than the person who hires or avails of the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment, when such services are availed of with the approval of the first mentioned person
- **A consumer is a person who buys goods or hires services, for a consideration.** Consideration means something of value. A person who obtains goods or avails services, which are free i.e., without consideration, is not a consumer as per definition.
- Supreme Court says that a tax on income, etc paid by a person cannot be treated as a consideration or a charge for availing services rendered by the Government

hospitals/health centers/ dispensaries. These services are not free of charge and the person availing of the service is a tax payer.

- The tax is meant for a public purpose without any reference to any special benefit to the tax payer.
- Anyone who purchases goods for private purpose or hires services for a consideration is called as a consumer.
- According to Supreme Court, if an authority performs statutory duties as sovereign functions of the state, which may be administrative, judicial, tax/revenue to a person, then he is not a consumer. (Sovereign functions are those actions of the state for which it is not answerable in any court of law. For instance, acts such as defense of the country, raising and maintaining armed forces, making peace or war, foreign affairs, acquiring and retaining territory, are functions which are indicative of external sovereignty and are political in nature. Therefore, they are not amenable to jurisdiction of ordinary civil court.)
- The users of goods are also called as consumer, provided if the use is made with the approval of the person who has brought the goods for consideration.
- A beneficiary of services is a consumer provided the services are availed of with the approval of the person who has hired or availed of the services for consideration. For example: when an young child id taken to the hospital by his parents and the child is treated by the doctor, the parents are treated as consumers having hired the services and the young child would also be a consumer, being a beneficiary of the services.
- The definition of consumer broadly classifies the consumers into two categories:
  - **Those who purchase goods including approved users.** A person who buys goods for resale or for any commercial purpose is not a consumer.
  - **Those who hire or avail of services including approved beneficiaries.**
- The intention of consumer protection law is to protect only the people who consume goods at the end of production chain and not for the industry which uses goods for commercial purposes.
- **"Commercial purpose"** does not include purchase and use of goods by a person exclusively for the purposes of earning his livelihood by means of self employment.
- **According to National Consumer Commission**,
  - If a person purchases goods with a view to using such goods for carrying any activity on a large scale for the purpose of earning profit, then he will definitely not be a consumer.
  - If the goods are purchased by a person exclusively for the purposes of earning his livelihood by means of self-employment, he would be a consumer.

Examples:

- If a person buys a type writer or a car and uses them for his personal use, he is a consumer. But if a person who buys a typewriter for typing others works for consideration or for plying the car as a taxi, he is said to be using it for commercial purpose and he is not a consumer.
- If the commercial use is by the purchaser himself for the purpose of earning his livelihood by means of self-employment, such a purchaser of goods is a consumer.
- A purchaser of a truck who purchases it for plying it as a public carrier by himself is a consumer. But if he purchases the truck to be operated exclusively by another person, he is not a consumer.
- A person who purchases a machine to operate it himself for earning his livelihood is a consumer. If he takes the assistance of one or two persons for operating the machinery, he is a consumer. But if the machine is operated exclusively by another person, then he is not a consumer.
- A person purchased three generating sets from the respondent for use in his factory. His case was that the sets that were supplied were defective and hence he suffered business losses. He approached the State Consumer Commission for recovery of the cost of the machines and damages. The State Consumer Commission held the case since the generators were purchased by the person for generating electricity in his factory for operating the machinery for the purpose of commercial production, and hence the person is not a consumer.
- A person running a typing institute and purchased carbon photocopier. The question is whether the photo copier had been purchased for commercial purpose. This case was held by the National Commission that since the photocopier had no connection with any large scale profit making activity, it cannot be said that it was purchased for a commercial purpose and hence the person is treated as a consumer.
- A charitable trust was running a Diagnostic center where the patients were taking the advantage of CT scan etc. for which they are required to pay and only 10% of the cases were provided free services. The machines purchased for this purpose are said to be for commercial purpose and hence the trust is not a consumer.

Conclusion:

- The National Commission distinguishes the ordinary consumers purchasing goods either for their own consumption or for use in small venture and the consumers of large scale manufacturing or processing activity carried on for a profit.
- It’s the responsibility of consumer to prove that goods were purchased exclusively for the purpose of earning the livelihood by means of self employment.

Hiring services:

- A person, who hires services for consideration, is a consumer whether or not the same are hired for any commercial purpose.
- In case of services the law does not provide any exclusion as in the case of goods.
- If a company engages the services of an architect to design its factory building, the company is a consumer even though the services are hired for a commercial purpose.
- As far as services are concerned, all persons who hire services for a consideration are said to be consumers, irrespective of whether they are manufacturers or traders requiring the services for a commercial purpose.

6. Goods and Services

- **Goods means** "every kind of movable property other than actionable claims and money, and includes stock and shares, growing crops, grass and things attached to or forming a part of the land".
- **Service is defined as "**any service which is made available to potential users and includes the provision of facilities in connection with banking, financing, insurance, transport, processing, supply of electrical or other energy, boarding or lodging or both, housing, construction, entertainment, amusement or the purveying of news or other information.
- All the services of any nature are considered as a service, except free service or under a contract of personal service.
- Government companies, bodies and local authorities rendering services or selling goods are covered under CPA (Consumer Protection Act).
- All services rendered through the Internet come under CPA. But free services which are countless on the Internet are not covered under CPA.
- Duties which are judicial, quasi-judicial and statutory in character are not services under CPA.
- The officers implementing the Registration Act and Stamp Act do not render any service under CPA as they perform statutory duties for collecting State revenue.
- The Supreme Court recently decided that the Provident Fund Commissioner is said to be rendering **"services"** and a member of the Employees Provident Fund Scheme is a **"consumer".**
- A subscriber of a Digital Signature is a consumer to whom Certifying Authority is rendering its services. Therefore a Certifying Authority can be taken to consumer court for deficiency in services by the subscriber of a digital signature.

Difference between "contract of service" and "contract for service":

- A **"contract for service"** implies a contract where one party undertakes to render services to or for another, professional or technical, in which he is not subject to detailed direction and control but he exercises professional or technical skills and uses his own knowledge.
- A **"contract of service"** implies a relationship of master and servant and involves an obligation to obey orders in the work to be performed and also the mode and manner of performance.
- "Contract of service" is not covered under CPA. So if an employ6ee does not perform his duties properly, he cannot be taken under CPA.

7. Consumer Complaint

- **Consumer Protection Act, 1986** is an Act of the Parliament of India enacted in 1986 to protect the interests of consumers in India. It makes provision for the establishment of consumer councils and other authorities for the settlement of consumers' disputes.
- The **Consumer Protection Act, 1986** can be invoked if the complainant consumer makes any or more of the following allegations:
    - The goods bought or agreed to be bought suffer from one or more defects.
    - The services hired or availed of or agreed to be hired or availed of, suffer from deficiency in any respect.
    - An unfair trade practice or a restrictive trade practice has been adopted by any trader i.e., who sells or distributes goods for sale or manufacturer.
    - A trader has charged excess price than the price fixed for the goods or displayed excess price on the goods or any package containing such goods. This includes cases where prices are above MRP (Maximum Retail Price).
    - Goods which are hazardous to life and safety when used are being offered for sale to the public.
- Consumer forums would not interfere in the cases that are serious and that require examination of witnesses. Civil Courts are more appropriate for these cases.
- According to National Consumer Commission, the consumer can seek his remedy under the CPA if he found that loss has been caused in hiring of service for consideration and that loss has been caused to him due to the negligence and deficiency in rendering the service.
- The grievances relating to loss or injury caused on account of negligence and deficiency in the performance of services which are hired for consideration are considered specially under the CPA and the consumer can approach any consumer forum in his jurisdiction.

8. Defect in Goods and Deficiency in Services

- Defect means any fault, imperfection or shortcoming in the quality, quantity, potency or standard which is required to be maintained under any contract.
- **Tamilnadu Housing Board:**
  - Defects are found in the construction of a flat after use but the opponent-Tamilnadu Housing Board denied its liability on the ground that it was provided in the agreement that the occupation of the flat by the purchaser would be with knowledge of its nature of construction and its condition.
  - Neither the purchaser nor anybody on his behalf would have any right for compensation in any manner from the vendor for defects in construction.
  - The defects were found not during the occupation but only after the flat was used by the consumer.
- **Eye surgeon in a hospital:**
  - A machine was purchased by the respondent Doctor from the vendor for the professional purpose of his practice as an eye surgeon in the hospital run by him. It was alleged that the machine was defective.
  - The vendor contended that the machine was purchased for commercial purpose and hence the Doctor was not a consumer.
  - The contention was rejected by the National Commission on the ground that the Doctor was a professional working by self-employment by using his knowledge and skill to earn his livelihood. So he is a consumer.
  - The vendor contended that the machine was not defective but the Doctor was incompetent to use and maintain it. He submitted that a foreign expert had taken the machine to Australia and sent it back after servicing and certifying that it was working perfectly but the Doctor had failed to properly maintain it.
  - The vendor also contended that since the machine had been used for more than a year, it could not be defective. If it is a defective instrument it could not be at all.
  - The National Commission rejected his contention on the ground that there was no evidence to prove the allegation that the machine had not been maintained properly and the certificate from the foreign expert is not proper evidence.
  - The National Commission agreed that the machine supplied to the Doctor was defective as it did not render the service for which it was purchased even after it had been sent to Australia for repairs.
  - The vendor also contended that he was not a regular dealer but only a representative of its manufacturer. This contention was rejected on the basis that the machine was imported by the vendor and supplied to the Doctor, received payment and also changed the circuit in the instrument after the complaint was lodged.

- The state commission directed the vendor to refund the price of Rs 71000/- for the machine with interest @18%.

- Cause of action for defect in the product, deficiency in service, unfair trade practice or restrictive trade practice cannot in all cases be avoided by the manufacturer, trader or service provider.
- The vendor may get a document containing the statement of the consumer that he is completely satisfied by the product or service. The **"Discharge Voucher"** does not deprive the consumer from preferring his claim with respect to deficiency in service.
- The consumer can approach any consumer forum in case of fraudulent discharge vouchers. He can claim for appropriate relief from the vendor if the discharge voucher was obtained by fraud, misinterpretation.

9. Restrictive and Unfair Trade Practices

- **Restrictive trade practice** has been defined in CPA as "any trade practice which requires a consumer to buy, hire or avail of any goods or services as a condition precedent for buying, hiring or availing of other goods or services".
- Restrictive Trade Practices (RTP's) are used by traders and manufactures so as to boost the sale of slow-moving goods which are tied with the sale of goods in demand.
- The law of consumer protection regards such practices as restrictive and exploitative of consumers. For example, a gas distributor imposing a condition that for a gas connection, a gas stove also had to be bought is a restrictive trade practice.
- **"Unfair trade practice"** is defined as a trade practice which uses any unfair method or unfair or deceptive practice for the purposes of promoting the sale of any goods or for the provision of services,
    - Falsely represents that the goods are of a particular standard, quality, quantity, grade, composition, style or model.
    - Falsely represents that the services are of a particular standard, quality or grade.
    - Falsely represents any re-built, second-hand, renovated, reconditioned or old goods as new goods.
    - Represents that the goods or services have sponsorship, approval, performance, characteristics, accessories, uses or benefits which such goods or services do not have.

- Represents that the seller or the supplier has a sponsorship or approval or affiliation which such seller or supplier does not have.
- Makes a false or misleading representation concerning the need for, or the usefulness of, any goods or services.
- Gives to the public any warranty or guarantee of the performance, efficacy or length of life of a product or of any goods that is not based on an adequate or proper test thereof.
- False or misleading warranties and guarantees or promise to replace, maintain or repair an article or repeat or continue a service until it has achieved a specified result.
- False and misleading statements concerning the price of the goods or services.
- Permitting the publication of any advertisement in a news paper or otherwise containing false and misleading representations for sale or supply of goods or services at bargain price.
- Permitting the offering of gifts, prizes etc by creating an impression that something is given free of charge where it is fully or partly covered by the amount charged in the transaction as a whole.
- Permitting the conduct of contests, lotteries, games of chance or skill for the promotion of any product or business interests.
- Permitting the sale or supply of goods knowing or having reason to believe that the goods do not comply with the standards prescribed by competent authority relating to performance, composition, contents, design, constructions, finishing or packaging as are necessary to prevent or reduce the risk of injury to the person using the goods.
- Permitting the hoarding or destruction of goods, or refuses to sell the goods or to make them available for sale or to provide any service, if such hoarding or destruction or refusal raises the cost of those or other similar goods or services.

Instances of unfair trade practices:

- Making false representations through advertisements that TV sets were manufactured in collaboration with a foreign company.
- Misleading representation about the performance of Awanti scooters by not mentioning about the surface and other attendant factors under which the scooters would give 55km per liter.
- False representation claiming treatment of white patches, stomach ailments, premature graying of hair etc.
- False claims about treatment related to reducing weight and the size of the body just in one hour.
- Non-rendering of after sales service as per terms and conditions of warranty.
- An advertisement claiming 100% success to those who joined the college for some examinations held.
- Use of word “Recognized” after the name of an educational institute giving an impression that its courses were Government recognized which was false.
- Making false claims about rendering free after-sales service during the period of warranty and when found defects; it was neither replaced nor repaired.
- False and deceptive investment schemes that are unfair trade practices under the law.

UNIT-IV
Assignment-Cum-Tutorial Questions
SECTION-A

Objective Questions

1. _____ under the IT Act, 2000 means authentication of any electronic record by a subscriber by means of electronic method.
2. Which one of the following is the responsibility of a Digital Signature? [ ]

   (a) Identification (b) Authentication

   (c) Security (d) All the above
3. _____is a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.
4. _____ is used to create a digital signature. [ ]

   (a) Public key (b) private key (c) Both (d) None
5. _____ is used to verify a digital signature and is listed in the Digital Signature Certificate. [ ]

   (a) Public key (b) private key (c) Both (d) None
6. _____ as a person who has been granted a license to issue a "Digital Signature Certificate".
7. A non-refundable fee of _____ rupees has to be paid along with the application for grant of license as a certifying Authority and rupees of _____ for renewal of license.

   (a) 20000, 10000 (b) 25000, 5000 [ ]

   (c) 20000, 5000 (d) 30000, 10000
8. _____ provides for revocation of digital signature certificates. [ ]

   (a) Rule 29 (b) Rule 30 (c) Rule 11 (d) Rule 12
9. Section _____ deals with the use of e-governance by government agencies. [ ]

(a) 7 (b) 6 (c) 5 (d)3

10._____ "every kind of movable property other than actionable claims and money, and includes stock and shares, growing crops, grass and things attached to or forming a part of the land".

11._____- is not covered under CPA. [ ]

(a) Contract of service (b) Contract for service

(c) Both (d) None.

12._____is "any trade practice which requires a consumer to buy, hire or avail of any goods or services as a condition precedent for buying, hiring or availing of other goods or services".

13. _____ helps in ensuring non-fraudulent transactions on the web.

a. Certificate authority b. Digital authority [ ]

c. Dual authority d. Digital signature

14. Who will be responsible for processing the payment from the customer's account to the merchant account? [ ]

a. Acquirer b. Merchant

c. Issue d. Payment gateway

15. _____ refers more to asymmetric key cryptography. [ ]

a. Timing attack b. Meet in middle attack

c. Virus attack d. Worms attack

16. Customer uses _____ key for decryption. [ ]

a. public key b. private key c. secret key d. hash key

17.The E-commerce domain that involves business activity initiated by the consumer and targeted to businesses is known as: [ ]

a. Business to Business (B2B) .b.Consumer to Business (C2B).

c.Business to Consumer (B2C). d.Consumer to Consumer (C2C).

18. Which segment do eBay, Amazon.com belong? [ ]

a. B2Bs b. B2Cs c. C2Bs d. C2Cs

19. The best products to sell in B2C e-commerce are: [ ]

a. Small products b. Digital products

c. Specialty products d. Fresh products

20. What is the percentage of customers who visit a Web site and actually buy something called? [ ]

a. Affiliate programs b. Click-through

c. Spam d. Conversion rate

21. Public key encryption uses multiple keys. One key is used to encrypt data, while another is used to decrypt data. The key used to encrypt data is called the _____ key, while the key used to decrypt data is called the _____ key. [ ]

a. encryption, decryption b. private, public

c. encryption, public d. public, private

22. _____ provides that the auditor has to be independent of the Certifying Authority being audited and cannot be a software or hardware vendor. [ ]

a. Rule 30 b. Rule 31 c. Rule 32 d. Rul2 33

23. The purchase of goods or services for use by an organization in producing other goods and services or to support the daily operations of the organization or for resale is called: [ ]

a. wholesale marketing b. business-to-business marketing

c. corporate marketing d. distribution marketing.

24. Consumer Protection Act was introduced in: [ ]

a. 1987 b. 1986 c. 1988 d 1989

SECTION-B

Descriptive Questions

1. 1. Explain about Digital Signature and Asymmetric crypto system for generating keys.

2. Explain the process of creating and verifying a digital signature.
3. What is Digital Signature Certificate? Explain the process of issue, suspension and revocation of a digital Signature Certificate.
4. What is the role of Certifying Authority and powers of Controller of Certifying Authority?
5. Explain the process of granting and refusing license/ renewal for Certifying Authority.
6. List any ten rules of Certifying Authorities.
7. Give some case studies of e-governance.
8. Explain the definition of a consumer with one or two case studies.
9. Define “Good” and “service”. What is meant by restrictive and unfair trade practice?
10. List some e-governance research centers and illustrate their activities. (Centre for Electronic Governance, Ministry of Information and Technology, Govt. of India, Centre for Electronic Communities, Commonwealth Secretariat's Centre for Electronic Governance)
11. Write any case studies that illustrates defect in services offered and how they are reimbursed.
12. List some unfair trade practice articles with brief explanation. How unfair trade practice promotes the sale of goods. List some real world examples.
13. List the precautionary measures for safekeeping the Digital Signature.
14. How is my Digital Certificate's private key protected?
15. How can we transfer your Digital Certificate to a new computer?

CYBER LAWS

UNIT-5

Objectives:

To understand traditional computer crime and identify various ways of hacking.

Syllabus:

UNIT – V: Traditional Computer Crime

Early Hacker and Theft of Components Traditional problems, Recognizing and Defining Computer Crime, Phreakers: Yesterday's Hackers, Hacking, Computers as Commodities, Theft of intellectual Property

Outcomes:

Students will be able to:

- Identify traditional problems associated with computer crime.
- Explore traditional rationales for phreakers and hackers.
- Explore the evolution of hacking.
- Learn the value of computers as marketable commodities.
- Explain the current state of computer crimes.

Learning Material

1.Traditional Problems

- The **advent of digital communications** and the **advances in technology** have significantly improved the quality of life for many individuals across the country. These advances have substantial side effects.
- Traditional criminalities were spatially based and hence the identification of jurisdiction is not a problem. But, in **cyber worlds which have global connectivity**, it is difficult to identify the actual **vicinage** (location) of jurisdiction.
- For example, an individual in Washington DC by using a sever in Canada, sends a threatening e-mal to the President of US and he uses a **anonymizer** located in Germany ,though the criminal and the victim both are located in same area. The cooperation of

authorities in Canada and Germany is essential to determine this "anonymous" individual.

- **International cooperation** must be created to eradicate the anonymity which confuses the simplest of criminal investigations.
- **Online harassment, stock manipulation and child pornography** have been increased exponentially due to the increase in anonymous e-mail accounts and re-mailers (A **remailer** is an Internet site to which you can send e-mail for forwarding to an intended destination while concealing your own e-mail address. E-mail sent through a **remailer** is sometimes known as anonymous e-mail).
- Many individuals create cyber identities to get engaged in harmless role-playing. But some individuals create false identities for stalking innocents and committing fraud.
- The individuals who create false identities for harmless entertainment fail to recognize that **privacy is a double edged sword**. The same portals which failed to verify their subscriber information also fail to verify those with whom they are communicating.
- **Anonymous re-mailers increase the susceptibility and vulnerability** of naive users and frustrate the efforts of law enforcement.
- The anonymizers are designed to strip the source address information from e-mail messages.
- **Re-mailers** target or direct their services to those individuals claiming that their site protects users from law enforcement and intelligence agencies.
- **Anonymity and lack of international cooperation** encourage criminal activity independent of user sophistication.
- **"Digital Encryption"** that transforms structured data into cipher code was used to protect the online confidentiality. It was employed by financial institutions, government entities, retail establishments etc to prevent the theft of personal and financial information.
- Encryption programs become increasingly available for public consumption. However they are also utilized by the criminals to hide their activities. The growth of encryption software, coupled with the increasing awareness of Internet security result in greater usage.

- Law enforcement agencies **lack adequate resources** to even identify the presence of criminal activity. Such agencies are unable to detect the criminal violations until it is too late.
- Detection of computer crime is delayed due to **self-same masking devices**. Technology is changing at a rate most favorable to the criminal mind. It is always difficult to identify the source and destination of communication on computers.
- **"Digital evidence"** is proven to be capable of being **easily modified or deleted** and its **voluminous nature is quite daunting** (difficult) to investigate for criminal investigators.
- The investigation of computer crime is accompanied by many obstacles like lack of judicial interest, administrative apathy (lack of interest, enthusiasm and concern). A complete picture of criminal landscape has yet to emerge.
- Law enforcement agencies should look to traditional statutes and federal legislation to prosecute computer crimes in the absence of technology-specific legislation.

2.Recognizing and Defining computer crime

Categorization of computer crime:

- There are three general categories of computer crime: **targets, means and incidentals.**
- These are not mutually exclusive. For example, an insider may target a computer system for destruction and at the same time he may use the computer as a means of committing crime.
- An individual may gain unauthorized access to a computer to steal information which resides in it. Thus he/she is targeting a computer while using it as an instrument to commit criminal activity.
- It is unclear exactly when and where the first "computer crime" actually occurred.
- The first documented computer destruction occurred in nineteenth century, when a textile manufacturer named Joseph Jacquard invented an automation of a series of steps in the weaving of special fabrics. This was not popular among the workers, who feared for their continued employment and they dismantled the invention. But this is not considered as a criminal activity involving computers.

- Even a residential burglary where computers were stolen, hijacking of entire shipment of computer hard drives is not considered as a computer crime.
- The theft of millions of dollars via computer hacking is considered as a computer crime.

Three incidents:

- Computer crime was ignored until a variety of cases exposed the vulnerability of data systems and outlined the national security.
- **First event:**
  - It occurred in 1986 when an accounting error of less than one dollar was investigated by a dedicated employee at the University of California at Berkeley.
  - The internal investigation revealed that a German hacker has tapped into military database and obtained sensitive information.
  - Using only a personal computer and a basic modem, this hacker was able to connect to Berkeley computers via an independent data carrier (Tymnet). Once connected, the hacker was able to move about the MILNET with remarkable ease.
  - The fact that such vulnerability existed within the data systems was not known to the administrators.
  - It is highly impossible that this activity would be discovered without the efforts of this employee. This resulted in the recognition of information risks associated with open systems.
  - Government entities initiated measures to protect electronically stored information especially military secrets. But they continued to overlook the economic dangers associated with computer networking.
- **Second Event:**
  - In 1988, they recognized additional threats to computer security after a program developed by a Cornell University student hanged over 6,000 computers and caused between $5 and $100 million in damages.
  - This program is called “Morris worm” (inventor Robert Morris) and was intended to attack computers via the Internet.

- This incident was the first of its kind and exploited security holes in the UNIX operating system, infecting 10 percent of all computers connected to the Internet. Such a wide scale damage created for a newly emerging medium was unforeseen by all, even its creator.
- When Morris recognized the possible damage of his actions, he released an anonymous message to programmers which instructed them how to disable the worm. Unfortunately, this message did not reach many of the intended recipients s the worm had already overloaded many systems.
- Morris was convicted of violating the cyber fraud and abuse act(CFAA) and was sentenced to three years of probation and a fine of $10,000.

➢ **Third event:**

- The crash of AT&T, America's number-one telephone company.
- The problem that caused the crash had nothing to do with hackers at all, but was actually the responsibility of AT&T software. But there is a possibility that the hackers could disrupt vital services.

3. Phreakers: Yesterday's Hackers

➢ Phreakers were the precursors of today's computer hackers. Initially the motivation was simply to break the system which is impenetrable.

➢ Phreakers routinely held conferences in which they discussed their exploits and shared their success.

➢ Phreakers would build "bridges", illegal conference calls of numerous individuals around the world.

➢ But these incidents were overlooked by the law enforcement due to the increase in predatory crime and a lack of personnel, economic resources and political assistance.

➢ This situation allowed the phreakers and hackers to grow and 1980's and 1990's became a virtual playground for hackers and phreakers.

What is Phreaking ?

- Phreaking involves the manipulation of telecommunications carriers to gain knowledge of telecommunication and theft of applicable services.
- Phreaking includes any activity that incorporates the illegal use or manipulation of access codes, access tones, PBX's and switches.
- The theft of telephone access codes is an example of phone phreaking which does not require a technical expertise. The easiest way to steal code is to steal access code from unsuspecting individuals while they are dialing. This is called **"shoulder surf"**
- The more sophisticated approach is **"war dialing".** This involves random number generators which test numerous codes until one is successful. One of these programs running throughout night will generate several hits, which are then compiled into a large database.
- The programs which enable these computerized code thefts have quickly found their way to the Internet and are readily available for downloading.

The war on phreaking:

- By the mid 1990's, AT&T was tired of excessive losses to phone phreaking and telecom fraud and created ANI (Automatic Number Identification) trace capability. This technology dampened the spirits of many phreakers
- Phreakers soon found easier targets and entered into locally owned PBX's and voice mail systems and diverted messages, thus saving the long-distance charges.
- The victim suffered from two problems: Intrusion and Fraud.
- This strategy brought a loss f &300,000 and $ 400,000 to Unisys and IBM.
- The economic benefits attracted many phreakers. The phreakers often hack vulnerable systems and delete voice messages and deny users access,
- Many companies were threatened by the criminals that they obey to any demands made by them.
- The law enforcement authorities tend to minimize the seriousness of phreaking and even deny their existence. But there was no evidence that phreaking is outdated and decreasing its popularity.

Phreaking to Hacking:

- Many of the methods employed by early phreakers are now being used within the hacker community.
- Innovative ways of utilizing stolen PBX codes are being employed by individuals. Pre-paid calls are being sold using stolen-access or PBX codes.
- These scams are highly organized and telecommunications get a very high damage.
- The cellular technology also suffered the same problem due to its reprogrammable nature.

4. Hacking:

- Computers are the target of the criminal and represent the instrumentality of crime.
- The **methodology employed, the motivation expressed and the sophistication displayed** are the characteristics of hacking.
- At the lower end, the individuals may be entering into the systems for making fun of it. Their activities may range from snooping around their neighbors to searching the top secrets of government databases. At the high end, the individuals use the same systems for destruction.
- Hacking is global phenomenon and is not restricted to a particular country. It is virtually available in every country where computer technology is available.

Defnition of Hacking:

- Initially hacking was used by Massachusets Institute of Technology (MIT) and refers to **either the development of novel techniques to identify computer short cuts or clever pranks.**
- The increase in accessibility and connectivity dramatically increased the number of individuals engaged in hacking activity.
- The newcomers were young and started the use of computers and computer technology for playing games. Such entertainment necessitated excessive downloads and led to manipulate telephone exchanges.

- **Early hackers** emphasized the virtuality of cyber space and argued that the Internet is a sphere of unreality, where nothing is concrete and everything is simulated.
- **Traditional hackers** around the globe shared a sense of destroying in which they were the keepers of all knowledge.
- The concepts of **easy money, revenge and personal notoriety** have tampered the righteous ideology. The lack of ideological consistency has resulted in an increase in hacking for profit.
- The availability of **private hacking toolkits and software** motivated the unskilled individuals and intruders.
- The virtual explosion of remote access software released in the market has dramatically changed the characterization of hackers.

Motivation to hacking:

- The six primary motivations for computer intrusion or theft of information in society are:
  - Boredom
  - Intellectual Challenge (mining for knowledge: pure hackers)
  - Revenge (Insiders)
  - Sexual gratification (stalking, sexual harassment)
  - Economic (criminals)
  - Political (terrorists, spies)
- The least destructive are **Boredom users** and these are easily identified by the law enforcement authorities.
- The most overlooked danger to the information security are current and former employees referred to as **Insiders.** These individuals have authorized access to a computer system but they exceed that authorization. Some insiders intentionally hack for personal and financial gain.
- The main problem to the institutional security and integrity result from
  - Careless log-in practices.
  - Employees, who post passwords in public places, allow others to shoulder surf.
  - Using common names for passwords.

- Disclosing passwords to strangers.

- Many employers change their locks after someone resigns or is terminated. But some fail to change security codes, patters of codes due to claiming the expenses associated with retraining and the impractical nature to change the systematic practices. for example many Universities do not change codes for student records systems and rely on individual passwords and deleting user accounts upon termination.
- Financial institutions are also responsible for inadequate security, who fail to change the codes. A former employee at the financial institution knows the codes to system entries, password policies, and the details of his/her co-workers.
- The last two categories are not quite prevalent and are motivated for personal or political gain. **Criminals,** those who utilize computer technology for personal gain are increasingly common. Though any activity that involves unauthorized access violates the traditional ideology, criminals must be separated from the traditional criminal hackers.

Hierarchy of cyber-criminals:

- There are four general categories of cyber criminals:
  - script kiddies
  - cyber punks
  - hackers/crackers
  - cyber criminal organizations
- **Script Kiddies:**
  - Also known as **sidiots, skiddie, Vector skill Deficiency(VSD)**
  - These are the lowest life form of cyber criminal.
  - These are inexperienced hackers who employ scripts or other programs authored by others to exploit security vulnerabilities.
  - These are technologically least sophisticated cyber-criminals and are not capable of writing their own programs and even do not fully understand the programs which they are executing.
  - They are not capable of targeting a specific system but they are limited to systems with identified vulnerabilities.

- Examples: college students use Trojans to remotely "hide" their friends, users capturing bank account and password information to access a victim's account.

➢ **Cyber Punks:**

- These are the individuals who intent to cause damage via Internet by using destructive programs, viruses, worms and general mischief for no economic gain.

➢ **Hackers/Crackers:**

- These are sophisticated computer criminals who are capable of programming, writing code and entering into complex systems.
- These employ their knowledge for personal gain.

➢ **Cyber-criminal Organizations:**

- These are the groups comprised of criminally minded individuals who have used the Internet to communicate, collaborate, and facilitate cyber-crime.
- Their activities are never innocent and include those activities associated with political or economic gain.
- The sophistication of the methods employed and the technical expertise of their members range from elementary to highly complex.

5. Computers as Commodities

➢ The **theft of computer hardware and software copyrights** have been overlooked but have become quite popular as computer components became smaller and more valuable.

Hardware:

➢ Computer components are more worth than gold but these components tend to be less protective than metal commodities.

➢ Computers accessible to students, employees and public are extremely vulnerable to theft. Many valuable computer components worth several hundred dollars are so small that they can be concealed in shirt pocket, within a briefcase or a small wallet.

➢ A simple screw-driver and a little knowledge is enough to successfully steal thousands of dollars of material.

- The **increase of internet auctions** has possibly increased to market the stolen goods. Auction sites such as eBay carry no responsibility for facilitating the transfer of stolen computer components.
- The term "**computer component"** represents smallest portions of computer technology like integrated circuits. Larger components such as CPU's, storage media are not easy targets due to their size.
- Theft of circuitry found within computer systems is more profitable than to steal a CPU. Motherboards, ether cards give more profit due to the inability to trace these components. Integrated chips, serial ports and drives are almost impossible to trace.
- The theft and resale of integrated chips may return as much as ten times on their investment. The reason for this is due to **basic law of supply and demand.**
- Americans have a ready supply of the latest technologies, but other portions of the globe do not have. This led to the emergence of global market places.

Black market dealers:

- These are the most organizing groups trafficking in stolen computer components.
- These individuals or groups carefully service the orders and prepare the merchandise as requested.
- Their targets are selected only after they receive an order for particular merchandise.
- These groups actively participate in the theft itself.

Gray market dealers:

- These are the dealers for illegal practices.
- They represent a major customer for thieves and a ready outlet for illegal wares.
- Buying the components at a significant discount and resell those components to other dealers.
- Gray market dealers involve fraudulent sale of goods. These items are marketed and packaged and often labeled as higher performance and expensive components.

6. Theft of Intellectual Property

Software:

- In August 2001, the FBI arrested four men and seized $10 million worth of counterfeit Microsoft software. These arrests are the result of a 14-month investigation and this revealed the increasing sophistication and organization displayed by computer criminals.
- To prevent software counterfeiting (duplicate), Microsoft designed new hologram technology which resulted in high costs associated with obtaining licensed copies.
- **"Data Piracy"** refers to the reproduction, distribution and use of software without the permission or authorization of the owner of the copyright.
- Making multiple copies for personal use or distributing copies to friends or colleagues has become so commonplace that many individuals fail to recognize the illegality of their actions.
- The ease of replication greatly enhanced through the advent of CD-RW's and users find expensive programs readily transferable.
- The reason for this activity is simply lack of knowledge regarding software licensing.
- Most retail programs are licensed for use at just one computer site or only one user at a time. By buying the software, an individual becomes a licensed user rather than an owner. While this individual user may be allowed to make copies of the program for backup purposes, it ie against law to distribute copies to friends and colleagues.
- **"Software Piracy"** is impossible to stop although software companies are launching more and more lawsuits to stop software piracy by copy-protecting their software,
- **Shareware publishers** encourage users to give copies of programs to friends and colleagues but ask everyone who uses a program regularly to pay a registration fee to the program's author directly.
- **Commercial programs** that are made available to the public illegally are called as "**WareZ".**
- **WareZ sites** are extremely popular on Internet**.** These sites enable visitors to download software illegally, violating copyright protections. Many of these sites are created and maintained by highly sophisticated, well-educated administrators.

UNIT-V
Assignment-Cum-Tutorial Questions
SECTION-A

Objective Questions

1. _____ transforms structured data into cipher code was used to protect the online confidentiality.
2. The three general categories of computer crime: _____,_____ and _____.
3. _____ are the precursors for hackers. [ ]
   a) Cyber punks b) Phreakers c) pre-hackers d) none
4. _____ involves the manipulation of telecommunications carriers to gain knowledge of telecommunication and theft of applicable services.
5. _____is a process to steal access code from unsuspecting individuals while they are dialing.
6. _____ is a process of using random number generators which test numerous codes until one is successful.
7. List the characteristics of Hacking?
8. What activity is referred to as Hacking in early 1990's at MIT?
9. List the six primary motivations to hacking?
10. The most dangerous category of hacking is:
    a) Boredom users b) Insiders c) Criminals d) all the above
11. _____ refers to the reproduction, distribution and use of software without the permission or authorization of the owner of the copyright.
12. Commercial programs that are made available to the public illegally are called as _____.

Multiple Choice Questions:

1. A person who uses his expertise to gain access to other peoples computers to get information illegally or to do damage is called: [ ]

   a) **Hacker** b)Spammer c) Analyst d) programmer

2. _____ has traditionally encompassed abuses and misuses of computer systems or computers connected to the Internet, resulting in direct and concomitant losses. [ ]

   a) Digital crime b) computer related crime

   c) cyber crime d) computer crime

3. _____ includes any criminal activity which involves the unauthorized access, dissemination, manipulation, destruction, or corruption of electronically stored data. [ ]

   a) Digital crime b) computer related crime

   c) cyber crime d) computer crime

4. Which of the following is NOT a reason why many businesses and corporations under report computer crimes? [ ]

   a) consumers don't care about confidentiality

   b) exposure to financial losses

   c) Data

   d) damage to brand

5. Which of the following is a valid reason why a corporation might welcome federal assistance to help catch a cyber criminal? [ ]

   a) Government investigations of corporate cybercrime can boost consumer/client confidence.

   b) Criminals access different services to disguise their location.

   c) Judicial system lets corporations hide the results of law enforcement investigations.

   d) Government agencies have the advantage of being able to ignore the chain of custody.

6. Which of the following is an example of computer-initiated criminal activity? [ ]
   a) Spreading viruses b) Stealing home addresses
   c) Wire transfers d) Spamming
7. One of the earliest examples of computer crime is _____, which consists of an activity in which telecommunications systems are manipulated and ultimately compromised. [ ]
   a) Phreaking b) Spamming c) Hacking d) Cracking
8. Which of the following allows perpetrators to commit multinational cybercrime with little fear of judicial sanctions?
   a) The presence of traditional jurisdictional demarcations [ ]
   b) The lack of physical boundaries
   c) An extensive array of equipment or tools
   d) The widespread acceptance of world passports
9. _____is a act of copying or downloading a program from a network and making multiple copies of it. [ ]
   a) Network piracy b) Plagiarism
   c) Software piracy d) None
10. Collecting personal information and effectively posing as other individual is known as a crime of _____ [ ]
    a) Spoofing b) Density theft c) Spooling d) Hacking
11. Software Piracy can be best described as:
    a) theft b) copying software [ ]
    c) taking from the rich d) infringing copyright.
12. Software where users are encouraged to distribute copies but must pay the owner if they continue to use the product is:
    a) commercial b) shareware **[ ]**
    c) open source d) public domain
13. Falsely claiming ownership of someone else□s work is:

[ ]

a) piracy b) **plagiarism** c) counterfeiting d) theft.

SECTION-B

Descriptive Questions

1. Explain the traditional problems of Hacking?
2. Explain the three incidents of Computer Crime.
3. Explain about Phreaking?
4. What is hacking and what are the factors that motivate to hacking?
5. Explain the hierarchy of cyber criminals?
6. How computers are treated as commodities?
7. Explain about theft of intellectual property?
8. Explain how phreaking laid steps to hacking?
9. Is it possible for hackers to access my computer's webcam?

10 Which are the most concerning cyber threats for private businesses and government organizations?

11. Which are the industry's most exposed to cyber attacks and why?
12. Is hacking a cyber crime?
13. What Resources Are Available to Combat Cyber or Computer Crimes?
14. What Are the Categories of Computer Crimes?
15. Is there any recent case which demonstrates the importance of having Cyber law on Cybercrime within the national jurisdictions of countries?
16. Why is preventing piracy important?

UNIT-6

Objectives:

To understand the lawful use of computer hardware and software.

Syllabus:

Interference with Lawful Use of Computers, Malware, DoS (Denial of Service) and DDoS (Distributed Denial of Service) Attacks, Spam, Ransomware and Kidnapping of Information, Theft of Information, Data Manipulation, and Web Encroachment Online Gambling Online Fraud, Securities Fraud and stock Manipulation, Ancillary crimes

Outcomes:

Students will be able to:

- Understand web-based criminality.
- Analyze the effect of viruses, worms and malware.
- Explain about DoS attacks.
-

Leaning Material

1.Web-based criminal Activity

- Almost everyone have online bank accounts and one-third of the workpeople are online.Bussiness and multinational corporations are relying on technology systems and Internet for the distribution of goods and materials, communication, billing and account management. So criminals are increasingly focusing their efforts in this area.
- The developments made in electronic communication and the increasing emphasis on point-and-click platform has enabled a variety of criminally minded individuals to expand their horizons.
- Traditionally computer crime was comprised mainly of trafficking in stolen equipment or falsification of records. But the clubbing of computer and telecommunications has resulted in the explosion of crime.
- **"Web",** with its characteristic of anonymity has encouraged criminal activity among the people.

- Individuals who never walk into a adult book store started downloading their such materials in the privacy of their home.
- The people who are unwilling to walk into a bank with a gun may feel comfortable altering bank records or manipulating stock records.
- **Computer dependency and globalization of communication** have been exploited by the individual, group and government hacking entities.
- A group known as **Global Hell** hacked into a variety of government sites including the US Army, the FBI and the White House. Though they do not want to destruct government property, it includes the following implications of computer crime:
    - financial losses
    - personal security
    - industrial espionage(spying)
    - international security
    - public safety

Six categories of online crime:

- **Interference with lawful use of computers-**DOS attacks, viruses, worms, malware, cyber vandalism, cyber terrorism, SPAM etc.
- **Theft of information and copyright infringement-** industrial espionage, ID theft, ID fraud etc
- **Dissemination of contraband or offensive materials-** pornography, child pornography, online gaming, racist material etc.
- **Threatening- communications-** extortion, cyber stalking, cyber harassment etc.
- **Fraud-** auction fraud, credit card fraud, theft of services, stock manipulation etc.
- **Ancillary crimes-** money laundering, conspiracy etc.

2. Interference with Lawful use of computers

- Industrial and corporate competition has led to the malicious destruction of data.
- Traditional methods of destruction included attacks on physical structures (headquarters, research laboratories, file cabinets etc).

- The virtuality of cyber space has altered the traditional modes of communication, education and commerce. The interconnectivity of technological devices has increased the vulnerability of corporations.
- The impact of traditional bombs was limited to the physical area but the implications of e-mail bombs are limitless in their application and may completely dismantle the company's informational infrastructure.

3. Malware

- **Malware or malicious programming code** refers to code that causes damage to computer systems.
- Malware includes **back doors, Trojan Horses, Viruses, Worms and DoS attacks.** All these are employed by terrorists, hackers, corporate spies, criminals.
- The range of their utilization includes **black mail, extortion and espionage.** The destruction ranges from **nuisance to destruction.**
- Some viruses may simply insert, delete or scramble text within MS Word documents. Destructive viruses like **Chernobyl** may attack by erasing a portion of the hard disk that makes it impossible to access the disk even after booting. They may attack the File Allocation Table (FAT) of the first partition, making it impossible for the disk to assemble data logically.

Viruses and Worms:

- The first recognized computer virus is **"the rabbit"** in 1960's. These programs diminished the productivity of the computer systems by cloning themselves and occupying system resources.
- The rabbits were strictly local phenomena, and are incapable of copying themselves across systems and they are the mistakes done by system programmers.
- The first virus attached to an executable file was in 1970's on the Univac 1108 system and required to the computer user to answer a series of questions regarding animals.
- **Four Distinct Eras of computer viruses:**
    - **Classical Era (1960's – 1970's)** - in which system anomalies occurred accidentally or were a result of pranks by programmers or system administrators.

- **Floppy Era (1980's-1990's)** - was largely characterized by infection of DOS machines spread by removable media.
  - ❖ The spread if computer viruses were relatively limited and the evolution of viruses was relatively slow.
  - ❖ Viruses during this period were easy to detect, isolate and eliminate due to their lack of sophistication.
- **Macro Era (1990's to 2000's)** -These infect documents and templates, not programs.
  - ❖ In early 1990's polymorphic viruses were emerged, which easily defeated early antivirus software and were not easy to detect.
  - ❖ By the mid 1990's, end users became aware of the risk of viruses and many people stopped sharing programs or running executable files.
  - ❖ The explosion of Internet, the electronic mail and the Windows OS proved irresistible to virus creators.
  - ❖ Embedding the malicious code into the macro programming language that is found in popular Microsoft and Macintosh applications, the virus infects the system when the opens the document.
  - ❖ Once executed the virus will become embedded in both recent and future documents. The virus is then propagated via e-mail, networks and the internet.
  - ❖ The **Melissa** virus caused more than $80 million in damages to computers across the globe. Users infected their computers by downloading and opening the document. The virus then propagated itself by sending e-mail to the first 50 addresses in the computer users's address book.
- **Internet Era (2000- present) –**began with the introduction of a group of publicized infections: **CodeRed, SirCam and w32/Nimbda.A-mm**
  - ❖ All these are capable of using system's address book to infect other computers.
  - ❖ **CodeRed** scanned the Internet for vulnerable machines and then infected them.

- **Nimda ("admin spelled backwards)** infected computers even when the infected e-mail was simply viewed through MS outlook's preview window.
- An increasing expansion of these worms is continuing to cause damages and worms are increasingly utilized for large scale Dos attacks.

4. DoS (Denial of Service) and DDoS (Distributed Denial of Service) Attacks

- The primary objective of Dos attack is to disable a large system without necessarily gaining access to it.
- The most common Dos attack is **"mail-bombing"** i.e., jamming system's server with voluminous e-mail.
- These attacks were directed at some most popular portals of web such as www.amazon.com, www.eBay.com and www.yahoo.com.

Enter Botnets and Zombie Armies:

- Criminals have recognized and developed a new methodology for Dos attacks.
- **Zombies and Bots** are compromised computers attached to the Internet which are used to remotely perform malicious or criminal tasks.
- They are used in batches called **Zombie armies and Botnets.**
- A **botnet** is a number of Internet-connected computers communicating with other similar machines in which components located on networked computers communicate and coordinate their actions by command and control (C&C)
- The majority of owners of zombie computers are unaware of their usage.
- Unfortunately, the botnets employing zombie computers are difficult to identify and shut down and require the disassembly and tracing of an individual who committed the crime is absolutely difficult.
- In 1999, the first known DDoS attacks occurred with tools known as **Trinoo** and **Tribe Flood Network (TFN).** These attacks have become common from that time and were employed by a variety of individuals or groups such as extortionists (a person who obtain things by force and violence), business competitors and terrorists.
- Many business and corporations are so fearful of the potential economic loss caused by such an attack and obey the demands of cyber extortionists.

- In June 2007, The Department of Justice and FBI announced that an ongoing Cybercrime initiative "**Operation Bot Roast"** had identified over one million compromised computer IP addresses.
- Recognizing that the majority of victim's remained unaware of their computer's victimization, the FBI announced that they would join with industry leaders and other government agencies to inform and educate computer users about the damage.
- **Botnets and Zombie armies** are increasingly popular and are providing significant risk to individual users, business and national security.

5. Spam

- **Spamming is defined as "**the abuse of electronic messaging systems to randomly or indiscriminately send unsolicited (without being requested or asked) bulk messages".
- Spam is found in many applications like Instant Messaging, Usenet newsgroup, blogs, mobile messaging etc, but it is familiar with e-mail.
- Spam is increasingly employed by advertisers to reduce operating costs and escape accountability (answerable).
- It is mostly employed by criminals who perform DDoS attacks, irrespective of primary motivation.
- The effects associated with spamming include:
    - human time reading or deleting the messages
    - purchase of anti-spam software
    - Consumption of computer and network resources.
- The exact costs of spam are difficult to determine. It is estimated that it is almost $22 billion in 2005.
- Electronic spam was most commonly used by advertisers or by business themselves.
- The amount of spam continuously increased and is currently used to :
    - spread viruses,
    - deliver Trojans and other malware,
    - initiate DDOS attacks,
    - commit identity theft,
    - facilitate Internet fraud,

- promote political extremism,
- Online crime like extortion and blackmail.

CAN-SPAM Act of 2003:

- The law "**Controlling the Assault of Non-solicited Pornography and Market Act"** was created in 2003 by Congress and came into effect from January, 2004.
- It imposed criminal penalties for individuals and entities that violated any of the Act's provisions.
- **Important elements of Act:**
  - **Don't use false or misleading header information.** Your "From," "To," "Reply-To," and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message.
  - **Don't use deceptive subject lines.** The subject line must accurately reflect the content of the message.
  - **Tell recipients how to opt out of receiving future email from you.** Give a return email address or another easy Internet-based way to allow people to communicate their choice to you. You may create a menu to allow a recipient to opt out of certain types of messages,
  - **Requirement of notification of advertisement and physical postal address of sender.**
  - **Enhances penalities for individuals who gain unauthorized access to a computer for the purpose of sending spam.**

6. Ransomeware and the Kidnapping of information

- **Ransomware** is a new type of malware, which originally surfaced in 1989 with **Imformation Trojan,** but became popular to both criminals and law enforcement only in 2005.
- Ransomware is defined as **" a malware program which encrypts or otherwise renders computer or digital resources inoperable or inaccessible to facilitate illegal operations"**

- Ransomeware is solely designed by criminals and is often used to extort money from its victims.

Effects of Ransomware:

- **User Education:** Ransomware is most successful when the victim lacks knowledge of system security. For example users may protect themselves from potential extortion efforts simply by employing good backup policies or by implementing system restoration software.
- **Sophistication of product:** Ransomeware is most successful when the level of data destruction is not recoverable using commercially available software or simple backup ractices. For example ransomware which incorporates itself into machine's operating system would require payment form the victim.
- **Victim urgency:** For ransomware to be successful, the compromised data must be very important for the victim. For example a victim may be unwilling to pay a ransom for the return of vacation photos but may be willing to pay for income-tax documents.
- **Secure method of payment:** The ultimate goal of ransomware can only be realized in situations where a secure method for payment is available.

7. Theft of Information, Data Manipulation, and Web Encroachment

- The introduction of global communications, digital automation, and the **information** has become the black markets platinum currency.

Traditional Methods of Proprietary Information Theft:

- Whether the motivation is personal, economic, or political, the method of theft of information has remained unchanged over the past several decades.
- Criminals usually focus on system vulnerabilities or employee weaknesses to steal or gain unauthorized access to privileged information.
- Research indicates that uninformed or careless employees are the greatest threat. Data security and inadequate training of personnel is given less priority at all the institutions, including government entities.
- Due to this, criminals steal passwords and enter even the most complex systems.
- The easiest and the most popular method for stealing passwords involve **Social Engineering.**

- Criminals employ traditional confidence scams to gain access to company computers or telephone systems. They persuade employees to volunteer their usernames and passwords.
- Information thieves gather personal information about the employee from the employee themselves or their co-workers as many individuals personalize their passwords even though advised by the IT security administrator.
- Employees are the biggest liability in terms of data security. Many employees post their passwords in public places which lead to **shoulder surfing.**
- Employees who fail to follow proper security procedures for disposing of personal correspondence and company paperwork are responsible for security risk to an institutions digital technology.
- Sensitive information such as old technical manuals, internal phone lists, organizational charts and correspondence etc that is dumped into trash become worthful information for a malicious hacker.
- Emergence of **private e-mail accounts, removable media, instant messaging** are increasingly responsible for theft of information and are the elements that effect digital security.
- Due to increase in insider theft of proprietary information and destruction of data, many organizations have prohibited the use of removable media.
- More sophisticated approaches were employed by hackers to gain unauthorized access to **secured data.** some of them are **remote access to system for routine maintenance like updating, systems administrator's negligence(never changing defaults in the network)**

Trade Secrets and copyrights:

- The increasing commercialization of knowledge has increased the theft and trafficking of proprietary information.
- Some criminals do this for extorting money from the organization while some do it for sale of important information to other competitors.
- These criminals range from corporate criminals, crackers to organized cyber gangs. For example, one employee at a company in Boston used company equipment t0 get bids for

the design specifications of a product. Such practices are not limited to common criminals or corporate insiders. They are also committed by industry competitors or even government entities.

- Government agencies engage in such behavior for personal gain and use patriotic arguments to justify their behavior.

Political Espionage (Practice of spying):

- Technology has the potential for sophisticated attacks on a country's national security and public infra structure.
- Government entities have not invested adequate resources to protect secrets that are technologically stored and collected.
- In1988, while Benjamin Netanyahu was Israel's Prime Minister, intelligent agents gained access to **Telrad** (subcontracted by Nortel, an American telecommunications conglomerate (a large corporation formed by the merging of separate and diverse firms)). By installing undetectable chips during the manufacturing process, agents were granted access to top secret information which included conversations between President Clinton and senior staff officials within the National Security Council. This arrangement sent weekly reports to Israel, which was made possible due to multi-million dollar contract to replace communication equipment Nortel, Telrad and Israel Air Force.
- **Laptop Computers** became the solution to the problem faced by employees. These facilitate home based work environments, work on vacation. But it also had lots of problems associated.
- The **portability** of laptops is the strength and at the same time greatest weakness making them, the prime targets of data black market.
- In London, two government laptops filled with top secret information were stolen from same railway station in a period of two months. Many laptops were stolen due to employee carelessness. One location which is proven to be most popular for thieves is airports. They simply replace the targeted laptop with one of their own. Another method which is proven successful involves a pair or team of thieves, where one will divert the owner after the laptop is placed on the belt. But is risky as the degree of detection is more. But these are due to individual victim's carelessness.

- Employers must address the vulnerability and subsequent security of laptops during training

Data Manipulation-Political Terrorism:

- The event of September 11, 2001has awakened the American public and other government institutions to the dangers posed by terrorism.
- International terrorist groups are increasingly using advances in technology to increase their effectiveness and efficiency.
- They are using Internet to formulate plans, communicate and terrorize their intended target. Internet is a wonderful tool for creating fear. The threat feels more real to the individuals who were not directly involved in a traditional attack.
- The wide-scale panic that has resulted from a variety of recent computer viruses had far more impact on daily behavior than the events of September 11, 2001.
- **Cyberterrorism** is defined as" a deliberate, politically or religiously motivated attack against data compilations, computer programs and information systems which is intended to disrupt or deny service or acquire the information which disrupts the social, physical, or political infra structure of the target".
- Cyber terrorists employ technology to target information systems and data. Computers are becoming both targets and weapons. As a target, computer acts as a best information server. As a weapon, it is used as a tool for mass destruction.
- Cyber terrorism may lead to electric black outs, disrupted communications which cause a greater danger to the public due to interconnectivity. This destroys public trust and social integrity.

Web Encroachment:

- **Cyber squatting** is another form of criminal activity which is specific to the technological age. It is defined as **"the practice of infringing (to violate or to break) on-trademarked property via electronic means".**
- The first method of cyber squatting involves the purchase of domain names consistent with the names of established companies or business.

- Second is the purchase of domain names which are the same as such business but with common misspellings or typographical errors in them (Ex: www.toysrus.com as www.toyserus.com) .
- **Anti-cyber squatting Consumer Protection Act** was laid in 1997.
- An individual named **John Zuccarini,** who purchased thousands of domain names which represented common misspellings of popular business and mouse trapped accidental visitors.

8. Online Gambling

- In 1995, Internet Casinos.Inc (ICI) launched the first online casino with 18 games. Since that time, Internet gaming has increased.
- In 2005, the revenues from online gambling were close to &10 billion dollars and that figure is expected to quadruple by 2010.
- There are several factors which make online gambling attractive to consumers. These include:
    - The lack of physicality and geographical location makes online casinos accessible to any user with a computer, PDA or cell Phone. Users can access a gambling site from home, hotel rooms, libraries, sporting events, anywhere.
    - The continuous operation of online casinos makes them accessible 24 hours a day.
    - The accessibility to minors' increases consumer base for online gambling as proper age verification is not attempted.
    - The increase in e-banking allows users to access and add a fund without ever leaving their chair.This encourages customers to over spend.
- The **Internet Gambling Prohibition and Enforcement Act of 2006(IGEPA)** attempts to reduce the flow of money to online gambling sites by regulating payment systems. It concluded that online gambling debts incurred on credit cards were unenforceable.
- In addition to decreasing the ready availability of funding to online gamblers, the IGPEA authorized state law enforcement to take action against persons or entities which facilitated illegal Internet gambling.
- Even though the government effort to reduce the online casino operation, many gambling sites appear regularly.

- American consumers spend more money on recreational activities, including gambling than any other country.

Lack of International Cooperation and the WTO

- The **World Trade Organization (WTO)** is designed to settle the disputes between nations, while maintaining a variety of multilateral agreements.
- A complaint was given to WTO against the United States for the increasingly restrictive measures against online gambling, by the government of Antigua and Barbuda.
- They argued that there are several gambling and services in United States, but they prohibited international gambling. Such prohibitions were leading causes for the decline of the internet gaming industry in Antigua.
- They alleged that America's Cohen and World Sports Exchange significantly reduced the desirability of operating online casinos in Antigua which directly harmed the nation's economy.
- WTO recognized that a long history of prohibition of gambling existed in the United States; they told United States to promote the restrictions within the country's boundaries.

9. Online Fraud

- The amount of money being lost by the consumers due to Internet fraud is increasing dramatically.
- Over 200,000 complaints were filed with the Internet Crime Complaint Center (IC3).Out of these; Internet Auction Fraud comprises 44.9 percent of the complaints, 19% about merchant payments and 5% of complaints involved check fraud.
- Among the perpetrators (criminals), more than three forth's were male and approximately half were located in one of the following states: California, New York, Florida, Texas, Illinios, Pennsylvania and Tennesse.

Web-Cramming/ ISP Jacking:

- **Web-Cramming** is most often accomplished when criminals develop new Web pages for small businesses and non-profit groups for little or no expense.
- While advertising their service as free, these criminals actually engage in unauthorized phone charges on their victim's accounts.

- The most common scam is use of "**rebate checks**". These checks when cashed, transferred the consumer's ISP, placing the monthly service charges on their telephone bill. This is possible because telephone companies depend on other companies that sell telecommunication services to provide billing and collection services.
- **ISP jacking** involves disconnecting individual users from their selected Internet service providers and redirecting them to illegitimate servers. Users are disconnected from their chosen Internet Service Provider, silence their modem, and reconnect them to the remote server.
- **Telecommunication Fraud** is given low priority among local and state authorities, this result in auction fraud, credit card fraud, get-rich-quick schemes and "work at home" scams.
- Internet scams have taken a variety of appearances and appear quite innovative for the users.

Fraud via Data Manipulation:

- Non-traditional methods of fraud are emerging due to advances in technology.
- **Data Diddling** is becoming increasingly popular and can be committed by anyone having access to an input device. It is **any method of fraud via computer manipulation.** Data Diddling refers to **manipulation of an existing program to redirect or reroute data representing money or economic exchanges.** It is very hard to recognize this criminal activity.
- Most dangerous case of data diddling is **salami technique** which redirects thin slices of accounts to a designated location.
- **IP spoofing** involves manipulation of packets or messages that exchanged between computers. These communications are indirectly routed across varying systems and addresses attached to these messages verify the sender and the recipient organization.
- Technically savvy individual mimic innocent victim and gain access to large amounts of money by disguising their computers.

10. Securities Fraud and Stock Manipulation

- **Licensed traders** were the only individuals with the capability of accessing real-time trading information. But Internet has made it possible for untutored individuals to instantly access stock values and statistics.
- There is lot of increase in the number of individuals engaging in **day trading (**the process of buying and selling highly speculative stocks within one day). But many of these individuals do not fully understand the securities in which they are investing or the market conditions which bear upon stock prices.
- Many day traders are relying on bulletin boards or web pages which claim to provide expert investment advice. Though majority of these pages are created by and subscribed by stock novices, some are actually created by criminals.
- **False information** is another method in which false data is circulated regarding a particular company.
    - By posting fraudulent information regarding the takeover of the company by an Israli company and by providing a link to the fraudulent web site which is an illegal news server, an individual caused the stock to increase by 30 percent. The individual was found guilty by securities fraud and sentenced to five years of probation and a fine of $90,000.
    - An individual named Jakob made over $200,000 by posting following information regarding a company:
        - Emulex was under investigation by SEC
        - Emulex's CEO was resigning
        - Company's revised earnings showed a loss.

    This information caused the stock to tumble from $110 to $43.
- **Insider trading** is increasing due to the popularity of day trading.
    - In 2000, 19 people were arrested in a massive insider trading scheme. This scheme was predicted on a advice of one "insider" who invite interested individuals to chat rooms, offering them inside advice for a percentage of their profits.

- Over a 2.5 tear period, this individual communicated insider information via chat rooms and instant messages, netting a profit of $ 170,000 for himself and $500,000 for his partners.
- Some of the individuals involved in this scheme were punished but many of them are left.
- Most of this fraud is conducted electronically; these actually involve threats of violence.

11. Ancillary Crimes

Money Laundering:

- **Money laundering** refers to the cleaning of money i.e., it refers to an enterprise or price of engaging in deliberate financial transactions to conceal the identity, source or destination of income.
- It refers to illegal concealment of illicit profits by individuals, small business, corporation, criminal syndicates, corrupt officials and even corrupt government.
- It is the backbone of both domestic and international black markets and underground economies.
- Internet has exponentially increased both the amount of revenue concealed and the ease of transaction.

Process of Money Laundering

- The process of money laundering occurs in 3 stages: **placement, layering and integration.**
  - **Placement:** the initial point of entry for illicit funds.
  - **Layering:** the development and maintenance of complex networks of transactions designed for illegal funds.
    - This involves layering of financial and commercial transactions and assets.
    - Layering of funds is accomplished by conducting multiple transactions by developing complex hierarchies of assets.
  - **Integration:** the return of funds into the legal economy.
- Due to **decreased detection and prosecution**, criminals are increasingly turning to the Internet to facilitate money laundering.

- **The lack of physicality and bulk** associated with e-money or e-funds eliminates the need for the identification and maintenance of physical structures to store.
- The risk of detection is reduced as criminals no longer have to physically possess the **illegal goods.** With a simple click, they can move their money without ever touching it.
- E-money provides criminals with higher degree of anonymity as there are no serial numbers or identifying marks.
- **First,** the placement of funds involves the establishment of e-money accounts. Such accounts enable them to exchange digital currency without physical interaction.
- **Second,** the online launderers electronically layer their money. This may be accomplished through the transfer of funds between a network of offshore companies or accounts; the purchasing of foreign currency; or the purchase of high-end merchandise for resale.
- To increase consumer interest and customer convenience, many e-banking sites now allow individuals to open accounts with no physical interaction or without a link to the pre-existing traditionally established account.
- **Finally phase** is reintroduction of money into legal economy. This includes production of false invoices for goods and services

Fighting Money Laundering:

- The prosecution of e-laundering must follow traditional methods: **finding, freezing and forfeiture.**
- International forums must communicate with and provide education to consumers, e-merchants, banks, and Internet service providers.
- The Financial action Task Force has suggested the following requirements for ISP's:
    - Maintenance of reliable subscriber registrations with appropriate identification information.
    - Establishment and maintenance of log files with traffic data relating Internet-protocol number to subscriber and to telephone number used in the connection.
    - Assurances that the information will be maintained for a reasonable period of time and that it will be made available to the law enforcement authorities during criminal investigations.

- Monitoring procedures for online transactions include the following:
  - Unusual requests, timing of transactions or e-mail formats.
  - Anomalies in types, volumes or values of transactions.
  - Incomplete online applications accompanied by refusal for additional information and cooperation.
  - Inconsistencies or conflicts of information on online applications such as physical address and location etc.
  - Multiple online applications.
  - Multiple online transactions involving inter-bank transfers between multiple accounts.

UNIT-VI
Assignment-Cum-Tutorial Questions
SECTION-A

Objective Questions

1. The most important characteristic of web that leads to criminal activity is_____ [ ]
   a) Information hub b) Anonymity
   c) eases of committing d) none.
2. Code that causes damage to computer systems is called _____
3. _____virus erases a portion of hard disk and damages the system.
4. The first recognized computer virus is _____.
5. The era of computer virus in which viruses are limited is_____ [ ]
   a) Classical b) floppy c) macro d) Internet.
6. _____virus belongs to Macro era of computer virus.[ ]
   a) Melissa b) Rabbit c) codeRed d) all the above
7. _____is a DoS attack that jams system's server with voluminous e-mail.
8. _____and _____ are compromised computers attached to the Internet which are used to remotely perform malicious or criminal tasks.
9. The first known DDoS attack is named as _____.
10. Define Spamming.
11. Define Ransomeware.
12. _____ is defined as" a deliberate, politically or religiously motivated attack against data compilations, computer programs and information systems which is intended to disrupt or deny service or acquire the information which disrupts the social, physical, or political infra structure of the target".

Multiple choice Questions:

1. _____ is a type of software intended to deliver advertising, but quite often it tracks user behavior as well. [ ]
   a) ransomware b) adware c)shareware d)none
2. This is an attack in which multiple compromised systems attack a single target, causing users to be denied normal services. [ ]
   a) DDoS attack b) DoS attack c) destruction d) none
3. This is a type of malware that is activated by some trigger, such as a specific date. [ ]
   a) logic bomb b) virus bomb c) ransomeware d) none
4. This is a type of malware that is activated by some trigger, such as a specific date. [ ]
   a) logical bomb b) ethical bomb c) virus bomb d) none
5. This is self-replicating malware that spreads through instant messaging networks. [ ]
   a) IM worm b) Virus c) Trojan d) none
6. This is malicious coding that combines virus' ability to alter program code with the worm's ability to reside in live memory and to propagate without any action on the part of the user.
   a) hybrid virus/worm b) Trojan [ ]
   c) malware d) none
7. This is a means of access to a computer system put in place by either an authorized person or a cracker. [ ]
   a) front door b) modware c) Back door d) none
8. This is malware that is hidden within apparently harmless code to take the user by surprise. [ ]
   a) Trojan Horse b) virus c) worm d) none

9. .____This is a non-technical approach to getting unauthorized access, usually by tricking silly humans into giving up their passwords. [ ]

a) Stealing b) surfing

c) Social Engineering d) none

10.In 1999, Melissa virus was a widely publicized: [ ]

a) e-mail virus b) trojan horse c) Micro virus d) Bomb

SECTION-B

Descriptive Questions

1. Explain the six categories of cyber crime.
2. Explain about Malware.
3. Explain the four era's of computer virus.
4. Explain about DoS and DDoS attacks.
5. Explain about SPAM and CAN-SPAM act.
6. Explain about theft of information?
7. What is Data manipulation and explain about web encroachment.
8. Explain about Online gambling.
9. Explain about online fraud?
10. Explain about Ancillary crimes?
11. Is it possible to block bot communications with traffic analysis solutions?
12. Explain about securities fraud and stock manipulation?
13. Is there a reliable way to detect the bots that communicate with the C&C server?
14. List the steps to detect a malware detected?
15. What kind of actions can a malware bot perform?
16. How does a botnet emerge?