UNIT 12 IT ACT 2000

Structure

12.0 OBJECTIVES

After studying this unit, you should be able to:

- understand the meaning and significance of Information Technology Act;
- explain how IT Amendment Act 2008 came into force;
- describe different provisions of the Act; and
- recognize the meaning of cybercrime and various offences.

12.1 INTRODUCTION

The Information Technology Act was passed as a response to the developments in the IT Sector, to facilitate e-commerce and e-governance, and to control cybercrimes. Internet has become a necessity today and with its increased penetration, clarity was needed in the domain, IT Act was an attempt to provide much needed clarity and direction. This unit discusses various facet of IT Act 2000 and IT Amendment Act 2008.

12.2 DEFINITION

The Information Technology Act, 2000 is the law pertaining to information technology. IT Act, 2000 was the result of passing of the IT the Bill by both the houses of Parliament. The Act is grounded on the United Nations Commission on International Trade Law (UNCITRAL). It deals with E-commerce and cybercrimes. It is, *"An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce"*. The Act came into force on 17.10. 2000.

12.3 FORMULATION OF IT ACT 2000

The advent of internet and then the growth in internet-based business transactions necessitated the formulation and implementation of law to regulate the field. The digital technology has transformed our lives, more and more individuals and businesses are adopting it and are conducting several activities with help of it. Before the formulation of IT Act 2000, the overall environment was of apprehension. Individuals and businesses were aware of the advantages this digitalisation brought along, but at the same time they were hesitant to conduct activities, especially monetary transactions owing to the lack of a legal framework which would protect them from some untoward incidents. To match steps with the strides being taken in digital world, the UNCITRAL adopted the Model Law on Electronic commerce in the year 1996. India was also a signatory to this and hence was expected to introduce laws as per the Model Law. Keeping in view, these factors the IT Bill was introduced to facilitate E-commerce as well as E-governance.

The IT Bill was drafted in the year 1998. Then the bill was then put in front of Parliamentary standing committee wherein, certain modifications were suggested. Finally, the IT Ministry suggested some changes and the approved modifications were retained in the bill and the rest were discarded. The bill was approved by the Union cabinet and then both the houses of Parliament. The President of India also provided his assent to the Bill and it became an Act that came into force on 17th October, 2000. The IT Act, 2000 brought in amendments into the Indian Penal Code 1860, the Indian Evidence Act 1872, Bankers Book Evidence Act 1891 and the Reserve Bank of India Act 1934, thereby incorporating the issues related to crimes and evidences based on

electronic mode and to address the need for regulations pertaining to electronic transfer of funds.

12.4 AMENDMENTS IN IT ACT 2000

The Information Technology Act was enacted in the year 2000 to bring in the necessary changes for growth of digitalisation and e-commerce transactions, and ensure safety and security of such transactions, thereby preventing crimes. The act was then amended to account for the developments in the domain, these amendments were passed by both the houses of Parliament in 2008 and received President's assent on 5th February, 2009, thus becoming the Amendment Act. It introduced various positive developments. It was seen as an effort by the Government of India to create a policy that is able to maintain pace with the evolving technology. The Indian Computer Emergency Response Team (CERT-In) is responsible for administration of the Act. The amendment attempted to fill in the gaps left by the earlier Act, and address the security concerns.

The Act was the need of the hour as with increasing digitalisation, the crimes in the digital space or with the help of digital aids also proliferated. Sending/sharing offensive content, phishing, identity theft, frauds, etc. were crimes which had to be brought within the ambit of penal provisions. All these factors led to the amendments in IT Act 2000, thus paving the way for IT Act 2008. The IT Act 2008 revolutionized the cyber law framework of the nation. The Act addressed various issues such as incorporating electronic signature, inclusion of greater number of cyber offences, addressing the concerns pertaining to data protection, privacy, and also dealt with the issues related to use of digital/cyber medium for terrorism.

12.4.1 Amendment Act, 2008 IT Act 2008

The significant contributions of the Amendment Act 2008 are as follows:

- The Act introduced several definitions to bring in more clarity and make it more inclusive:

  i) Electronic signature "means authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature"

  ii) Communication Device "means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image."

  iii) Cyber cafe "means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public."

  iv) Cyber Security "means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction."

v) The Act also revised the definition of "Intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes. (Substituted vide ITAA-2008)".

- The Act also brought in changes while addressing the penalties and compensations for damage to computer, computer system, etc. If an individual "destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage; he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected."
- Computer Related Offences inserted sections relating to "punishment for sending offensive messages through communication services". It further said, "any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008) shall be punishable with imprisonment".

Several other changes were also introduced. These major changes have been discussed in upcoming sections.

Check Your Progress A

1. What was the need for IT Act 2000?

   .....

   .....

   .....

   .....

   .....

2. What prompted the amendments in IT Act, 2000?

   .....

   .....

   .....

   .....

   .....

3. Fill in the blanks:

   i) The IT Act came into force on_____.

   ii) IT Act 2000 was amended in the year _____.

iii) The _____is responsible for administration of the Act.

iv) _____means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image

12.5 DIGITAL SIGNATURE & ENCRYPTION

Under the provisions of IT Act 2000, digital signature may be used by any subscriber for the purpose of authentication of an electronic record. The electronic record is authenticated with the help of "*asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record*. (Section 2(1)(p) of the Information Technology Act, 2000)."

Traditionally, the signature by an individual on any document helps in authentication of the document and provides an assurance to the receiver regarding its trustworthiness. This is possible in case of a paper-based document, but in case of electronic document, just mentioning the name at the end of document or email provides almost no reassurance regarding its authenticity. The IT Act, 2000 recognizes public key cryptography for the safeguarding of electronic documents. The Section 3 of the Act further provides a user the power for authentication of an electronic record by affixing his digital signature. The authentication process will apply "asymmetric crypto system and hash function that envelops and transforms the initial electronic record into another record". The electronic record can be verified by any other person who is in the possession of the public key. Furthermore, every subscriber has a private as well as a public key which are unique to him and which constitutes a functioning key pair. The creation of digital signature requires application of encryption to specific information. The process involves following steps:

- The message that has to be signed using digital signature is outlined, and then processed with the help of an algorithm called hash function. The processed output thus received is called the hash result which is unique to the message.
- This hash result so produced is encrypted using the private key of the sender. This is the Digital Signature.
- The Digital Signature is then attached to the message which is then transmitted over to the receiver through internet.
- Once the message is received at the receiver's end, he uses the public key of the sender to decrypt the message. If the sender's message is successfully decrypted using his public key and the hash result is computed and compared with the output of the digital signature, then the receiver is assured of the authenticity and integrity of the message.

12.6 ATTRIBUTION

The communication taking place through electronic medium does not have any tangible component. Therefore, it becomes difficult to affix responsibilities and define associations. The term attribution means "the action of ascribing a work or remark to a particular author, artist, or person." The IT Act 2000 (Section 11) lays down the guidelines about how an electronic document can be attributed to the individual from whom it originated. It says that the electronic document will be attributed to the originator under following conditions:

- If the originator himself sent the electronic record
- If an individual who was given the authority by the originator to act on his behalf in respect of that particular electronic record has sent it.
- If it was sent by using information system which was programmed by the originator himself or on his behalf to automatically send the electronic record

For example, if an email was sent to B from A, then A will be the originator of the electronic record and B will be the addressee in this case.

12.7 ACKNOWLEDGEMENT AND DISPATCH OF ELECTRONIC RECORDS

Section 12 of the IT Act deals with the manners in which acknowledgement of the receipt of electronic record may be made and Section 13 of the IT Act discusses the time of receipt of an electronic record.

If the originator of the electronic record has not specified any particular mode of acknowledgement to be given by the receiver regarding the receipt of the record, the acknowledgement can be given by "any communication by the addressee, automated or otherwise" or "any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received." For example, if an individual receives a mail for a meeting, the individual can send a mail to the sender saying thank you for the information, or sends an automated response or shows interest by joining the meeting. These activities show acknowledgement from the receiver end.

Also, in cases where the originator of the electronic record has "stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator." But in cases where the originator has not specified that the electronic record will be binding only upon the receipt of acknowledgement and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by

him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent."

The section 13 of the IT Act talks about dispatch of electronic record. It is stated that, the time at which an individual sends the electronic record and it enters a computer outside the ambit of control of the sender, is the time of dispatch. Also, the place of origin of dispatch is the place of business of the sender and the place of receipt is the place of business of the receiver.

12.8 REGULATION OF CERTIFYING AUTHORITIES

The Information Technology Act specifies that the "Controller of Certifying Authorities" may be appointed by Central Government. The controller of certifying authorities has the authority regarding the regulation of certifying authorities. The Government at the Centre may also appoint Deputy Controllers, Assistant Controllers, other officers and employees as they deem fit.

The authority need to assign tasks and functions to the Deputy Controllers and Assistant Controllers lies with the Controller. The Controller's functions include: supervising the activities of the Certifying Authorities, specifying their duties, certifying their keys, laying down standards for them, taking decisions regarding the requirements pertaining to the desired qualification and relevant experience of the Certifying Authorities, etc. The Controller has to certify the public keys of Certifying Authorities and also has to resolve the conflict of interests between them and the subscribers.

The Controller has the authority for the recognition of foreign Certifying Authority as a Certifying Authority with the prior approval of the Central Government, the Controller may also revoke the recognition if he is satisfied "that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition". The Act also provides that any individual can apply for license to the Controller for the purpose of issuing Electronic Signature Certificates in India. The license may be issued if the concerned person satisfies the requirements laid down by the Central Government and is valid only for the period prescribed by the Central Government. For renewing the license, the application has to be accompanied by prescribed fees and the application has to be made forty five days before the date of expiry of the existing license. The application for license may be approved or rejected depending on the merits of the case and the documents accompanying the application. The Controller has the authority to suspend the license, if he is satisfied after an enquiry that false and incorrect statements have been made by the Certifying Authority and the conditions under which the license was issued have not been complied with, but before revocation the Certifying Authority has to be given a reasonable chance of being heard.

The Controller also has the power for the delegation of any of his powers to the Deputy Controller, Assistant Controller or any other officer. The Controller or any other official, who has been authorised by him, has the authority to start the investigation/enquiry regarding any infringement of the IT Act, any other rules or regulations. They will also have access to: "any computer system, any apparatus, data or any other material connected with such system" for the purpose of information retrieval. Also, "the Controller or any officer authorised by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-tax Act, 1961 (43 of 1961), and shall exercise such powers, subject to such limitations laid down under that Act."

In case of the Certifying Authorities, they have to make sure that they are following the procedures and protocols as prescribed by the Act and they also have to ensure that their employees also abide by the procedures and protocols. They are expected to adhere to security protocols and use resources which are secure from malicious attacks. They also have to display the license at a conspicuous place within their premises and in case the license is suspended or revoked; they are expected to submit it immediately. It also has to adhere to the disclosure norms so as to maintain sanctity of the process and in case of a situation where in the integrity of their computer systems may be affected; they should notify the concerned stakeholders.

12.9 DIGITAL SIGNATURE CERTIFICATES

The IT Act 2000 talks about digital signature certificates which is a digital key which validates and certifies the identity of the person holding it, and is issued by the certifying agencies. The digital signature certificate verifies the authenticity of the electronic record and ensures that it wasn't altered during the transit. The important characteristics of digital signature certificates are:

- These certificates help in authentication of the message source as the ownership is bound to a specific user.
- They help in providing an assurance that the message was not altered during the transit.
- Non-repudiation is ensured as the sender can not deny sending a message bearing his digital signature.

Any individual can apply for the issue of digital signature certificate by filling up the form and depositing the required amount of fee (not to exceed INR 25,000). The certifying authority may issue the certificate if it finds the application to be in required order. These certificates can only be issued by certifying authority.

12.10 DUTIES OF SUBSCRIBERS

After the issuance of Digital Signature Certificates, the subscribers are expected to perform certain duties as prescribed by the Act. The subscriber

has to take utmost care to hold the control of the private key which corresponds to the public key listed in the Digital Signature Certificate. It is important that he takes all necessary precautions to avoid the leak of the private key, and in case the private key gets compromised he should immediately communicate this to the certifying authority. The subscriber shall be held liable till the time the certifying authority has been informed regarding the breach.

12.11 PENALTIES AND ADJUDICATION

The Information Technology (Amendment) Act, 2008 added several crimes related to cyber space and also introduces penalties for control of such crimes. With increasing penetration of digitalization, the flow of information has been transformed. While there are myriads of advantages of usage of digital media, it is not untouched by increasing crimes. The cyberspace has removed the barriers of geography and has made knowledge/information volatile. To prevent the misuse of information and thus losses accruing out of it, the IT act introduced penalties. The chapter IX of the IT Act discusses Penalties, Compensation and Adjudication.

The penalties for various offences are as follows:

- **Section 43:** "Penalty and Compensation for damage to computer, computer system, etc (Amended vide ITAA-2008)". This section says, if any individual who is not authorised to access/use a computer, computer system or computer network accesses it ,or extract data from it in any form, introduces virus in it or is responsible for some action rusting in virus attack, disrupts it, tampers it, or destroys , deletes or alters any information contained therein will be held responsible for the payment of damages by the way of compensation to the affected person. The compensation should not exceed one crore rupees. This is also applicable in cases wherein he denies the access to authorised person, provides assistance to other for malicious activities, or steals, conceals or destroys the source code of the computer resource with the intention of causing damages.

- **Section 43 A:** "Compensation for failure to protect data (Inserted vide ITAA 2006, Change vide ITAA 2008)".This section deals with cases of negligence, and says "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected."

- **Section 44:** "Penalty for failure to furnish information, return, etc"

  This section discusses penalties resulting from the failure to furnish information, or record, file return, maintain books of account or records. If an individual who is required by the Act to provide information or

return or report to controller or certifying authority, fails to fulfill the requirement, he will be held, "liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure". If he fails to "file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues" and if he is required by the Act to maintain a book of account or maintain certain records, fails to do so, "he shall be liable to a penalty no exceeding ten thousand rupees for every day during which the failure continues."

- **Section 45:** "Residuary Penalty":

  If an individual acts in opposition to any rule and regulation that has been laid down by the IT Act, for which any specific penalty has not been mentioned in the Act, he will be held liable for the payment of compensation of an amount not exceeding 25000 rupees to the individual who gets impacted by the action or a penalty of an amount not exceeding 25000 rupees.

Adjudication

For adjudication pertaining to the matters discussed in the chapter, Central Government has the power to appoint an adjudicating officer. The "Adjudicating Officer should not be below the rank of a director to the GoI or an equivalent officer of a state". An individual should be appointed adjudicating officer only if he has relevant "experience in the field of IT and legal or judicial experience as prescribed by the Central Government". While imposing penalties or awarding compensation, the adjudicating officer shall give reasonable opportunities for representation and should award compensation or penalise only when he is fully satisfied. The adjudicating officer "shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section (2) of section 58." Section 47 of the Act discusses the factors which should be considered by the adjudicating officer while awarding compensation. It says that the officer should be mindful of the gains of unfair advantage which resulted from the default, "the amount of loss caused to the aggrieved party as a result of the default, and the repetitive nature of the default."

Check Your Progress B

1. What are Digital Signature Certificates?

   .....

   .....

   .....

   .....

   .....

   .....

2. What do you mean by Attribution?

.....

.....

.....

.....

.....

3. Fill in the blanks:

i. The IT Act, 2000 recognizes _____cryptography for the safeguarding of electronic documents.
ii. Section ___ of the IT act discusses Penalty and Compensation for damage to computer, computer system, etc.
iii. Section _____ of the IT Act discusses Residuary Penalty.
iv. The subscriber shall be held liable till the time the certifying authority has been informed regarding the breach. **(True/False)**

12.12 PROCEDURE, WORKING & LEGAL POSITION IN DIGITAL SIGNATURE

Digital Signatures have been recognised by Indian legal system under the guidelines issued by IT Act 2000. The Act was an outcome of increased focus on improving the ease of doing business in India and to bring in necessary changes to facilitate the digital transactions. The digital signature ensures that the electronic record is authentic and the content/message has not been tampered with. The IT Act 2000 talks about Digital Signature, while in the ITAA 2008 electronic signature has been mentioned. Digital Signature has been defined as "authentication of electronic record" which happens as per the procedures laid down by the Act. But the IT Act of 2000 included the use of "asymmetric crypto system, public key infrastructure and hash function", thus making it dependent on limited infrastructure only. The introduction of Electronic Signature in IT Act, 2008; brought in technological neutrality and broadened the ambit by covering digital signature as well as other forms such as biometric. Also, it is important to understand that digital (or electronic) signature is not same as scanned copy of signature or a digitized copy, or any other conventional form of signature, it pertains to the authentication of electronic record as per the procedures laid down by Section 3 of the IT Act.

The digital signatures use Public Key Infrastructure and are created and verified with its help. To encrypt and decrypt these signatures, two keys namely are required: public key and private key. The public key is required to encrypt the data which is then decrypted with the help of private key. The public key is shared but the private key used for decrypting is known only to the possessor of the key. The system is based on cryptography.

The signature of an individual is a representation of his identity. It holds a significant legal position and represents the identity as well as intent of the concerned person. The IT Act provided same legal status to digital/electronic signature as the hand-written signature. The concept is based on UNCITRAL Model Law on Electronic Signatures, 2001. These signatures serve the same purpose as traditional signatures. In the digital world wherein, electronic records are being transmitted, the digital signature ensures the authenticity and legitimacy of the electronic record. They are safer than traditional signatures and can not be forged. It is far more convenient to use digital signature.

12.13 APPELLATE TRIBUNAL

The IT Act 2000 provides for the establishment of Cyber Appellate Tribunal. The Act states: "The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal." The central government also has the power to specify the matters and places w.r.t. which the Tribunal may exercise its jurisdiction.

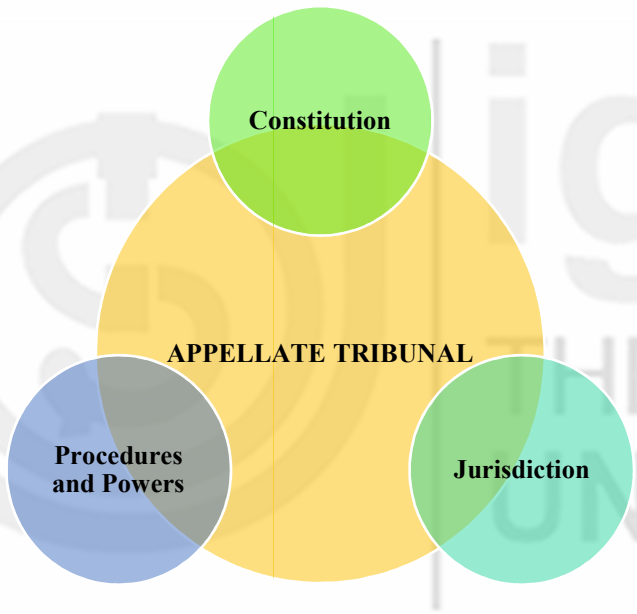

Fig 12.1: Appellate Tribunal

- **Constitution:** The Tribunal shall consist of only one person: The Presiding Officer of the Cyber Appellate Tribunal. The Presiding officer is appointed by the Central Government, and the necessary qualifications for the same are: he will be qualified for the appointment only if he "is, or has been, or is qualified to be, a Judge of a High Court; or is or has been a member of the Indian Legal Service and is holding or has held a post in Grade I of that Service for at least three years." The Presiding officer shall hold the position for 5 years or until he is 65 years of age (Whichever is earlier). The Central Government, in consultation with the Chief Justice of India will be responsible for the selection of chairperson and members of the Tribunal. Also, "The Central Government shall provide the Cyber Appellate Tribunal with such

officers and employees as the Government may think fit" and these people will work under the superintendence of the Presiding Officer.

- **Jurisdiction:** Any individual who is aggrieved pertaining to the orders of a controller or an adjudicating officer may appeal to the Cyber Appellate Tribunal. The appeal has to be filed within 45 days from the date when the order was received by the concerned person. If the aggrieved individual is not satisfied by the decision of Tribunal, he may file an appeal with the High Court.
- **Procedures and Powers:** The Act states that, "The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.". The Tribunal will have same power as civil court (as vested under Code of Civil Procedure, 1908) for the purpose of carrying out its functions in matters such as: summoning and enforcing attendance, requiring the discovery and production of records, receiving evidence, reviewing decisions, etc. The proceedings before the tribunal will be deemed "to be a judicial proceeding within the meaning of sections 193 arid 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973."

12.14 OFFENCES AND CYBER-CRIMES

The advent of internet has transformed our lives. People in every sphere of life are using computers and internet to create, transmit and store information. The information is volatile in nature and is often misused by miscreants, thereby causing harm to others. With increasing penetration of internet and adoption of digital tools and techniques, global connectivity has reached new heights, but at the same time has become even more vulnerable resulting in increased numbers of crimes. To control such malicious activities and deter the miscreants the IT Act was introduced with provisions for addressing these issues. Chapter XI of the IT Act discusses criminal offences which are punishable by fine or imprisonment or both.

Cybercrimes is an umbrella term which includes the criminal activities involving computer/internet/cyberspace. It is basically criminal exploitation of computer and/or internet. These crimes are of sophisticated nature and in these crimes the computer is usually the tool or target or both. It includes:

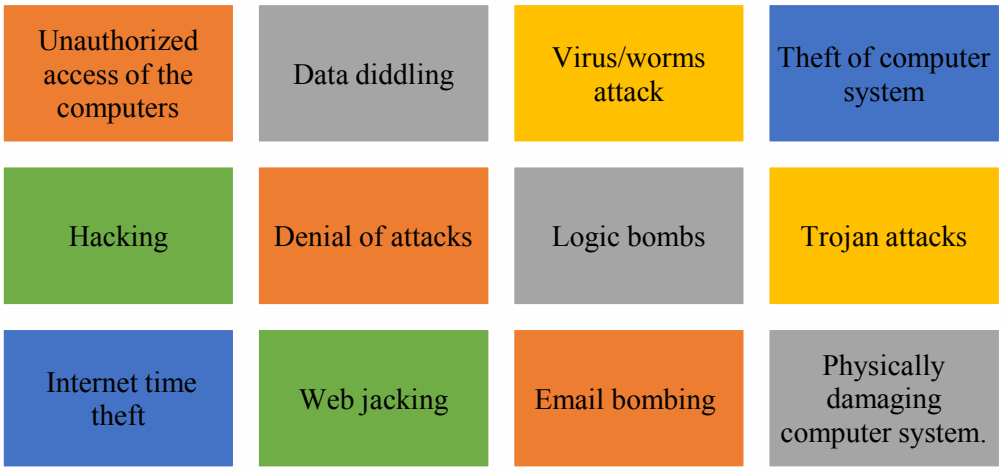

Fig 12.2 : Cyber Crimes

The Indian law does not provide any specific definition of cybercrime, but the term cyber security has been defined, it "means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction." Even though cyber-crime has not been defined in the IT Act but offences and crimes relating to computers and cyberspace have been dealt in detail in the IT Act. Following offences have been included in IT Act:

Table 12.1: Offences and their punishments

Section	Offence	Punishment
Section 65	Tampering with computer source documents	Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
Section 66	Computer related offences	Imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
Section 66 B	Punishment for dishonestly receiving stolen computer resource or communication device	imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.
Section 66 C	Punishment for identity theft	Imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.
Section 66 D	Punishment for cheating by personation by using computer resource	Imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66 E	Punishment for violation of privacy	Imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.
Section 66 F	Punishment for cyber terrorism	Imprisonment which may extend to imprisonment for life
Section 67	Punishment for publishing or transmitting obscene material in electronic form	Imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.
Section 67 A	Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form	Imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.
Section 67 B	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	Punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.
Section 67 C	Preservation and retention of information by intermediaries	Punished with an imprisonment for a term which may extend to three years and also be liable to fine.
Section 68	Power of Controller to give directions	Imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both.
Section 69	Power to issue directions for interception or monitoring or decryption of any information through any computer resource	Imprisonment for a term which may extend to seven years and shall also be liable to fine.

Section 69 A	Power to issue directions for blocking for public access of any information through any computer resource	Imprisonment for a term which may extend to seven years and also be liable to fine.
Section 69 B	Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security	Imprisonment for a term which any extend to three years and shall also be liable to fine.
Section 70	Protected system: 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 for a term which may extend to ten years and shall also be liable to fine.
Section 70 B	Indian Computer Emergency Response Team to serve as national agency for incident response	Imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.
Section 71	Penalty for misrepresentation	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
Section 72	Penalty for Breach ofconfidentiality and privacy	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
Section 72 A	Punishment for disclosure of information in breach of lawful contract	Imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.
Section 73	Penalty for publishing[electronic signature] Certificate false in certain particulars	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
Section 74	Publication for fraudulent purpose	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

The Act will also apply to contraventions conducted outside India if it involves computer, computer system or computer network based out of India.

12.15 E-SIGNATURE AND DIGITAL SIGNATURE

The IT Act of India discusses two types of signatures:

- Electronic Signature, and
- Digital Signature.

Important points for comparison have been summarised below:

- Section 2(1) (ta) of the IT Act 2008 defines Electronic Signature as: "electronic signature means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature". The section 2(1) (p) of the IT Act 2000 talks about Digital Signatures and defines it as "digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3" of the Information Technology Act.
- Electronic Signatures are technologically neutral and the act does not specify any particular technology for the purpose of creation of electronic signature while digital signature follows specific technology-based approach. For example, usage of hash functions, use of public key cryptography system, etc.
- Electronic Signature can be biometric, name typed at the end of a mail, digitalized version of conventional signature. Digital signature uses two-way protection system with encryption and decryption.
- Digital Signatures are more authentic than electronic signatures.
- Electronic signatures are used for the purpose of verification of document while Digital Signatures are used for securing the document.
- Digital Signatures have limited validity of maximum three years, while electronic signatures have no such limits on validity.

12.16 ENCRYPTION

A Digital Signature is used for the authentication of an electronic record. These signatures are created and verified with the help of cryptography. The authentication process involves two other processes: Encryption and Decryption.

Encryption involves transformation of simple messages into cipher text while the process of decryption reverses the coded texts into the actual simple message.

Encryption-Decryption has two forms:

- Symmetric Encryption: It is the most basic kind of encryption involving only one secret key for the purpose of encryption and decryption of information. The key is known to both: the sender as well as the receiver of the message.
- Asymmetric Encryption: There are two keys involved in this case for encrypting/decrypting messages: public key and private key or secret key. Section 2(1)(f) of the Information Technology Act 2000 talks about this kind of encryption. The encryption is done using the public key which is known to many but decryption can only be done by the individual who has the private key known to the receiver only. It helps in protecting the digital signature from forgery. Asymmetric encryption is a relatively modern method.

Check Your Progress C

1. What are the different kinds of encryption?

   ……
   ……
   ……
   ……
   ……
   ……

2. Explain the constitution and jurisdiction of Cyber Appellate Tribunal.

   ……
   ……
   ……
   ……
   ……
   ……

3. Fill in the blanks:

   i) Digital Signatures have been recognised by Indian legal system under the guidelines issued by _____.

   ii) _____is the most basic kind of encryption involving only one secret key for the purpose of encryption and decryption of information.

   iii) There are two keys involved in the case of _____for encrypting/decrypting messages: public key and private key or secret key

   iv) The Tribunal shall consist of only one person: The _____of the Cyber Appellate Tribunal.

12.17 LET US SUM UP

The Information Technology Act, 2000 is the law pertaining to information technology. IT Act, 2000 was the result of passing of the IT the Bill by both the houses of Parliament. The Act is grounded on the United Nations Commission on International Trade Law (UNCITRAL). It deals with E-commerce and cybercrimes.

Under the provisions of IT Act 2000, digital signature may be used by any subscriber for the purpose of authentication of an electronic record. The electronic record is authenticated with the help of "*asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record*. (Section 2(1)(p) of the Information Technology Act, 2000)."

The communication taking place through electronic medium do not have any tangible component. Therefore, it becomes difficult to affix responsibilities and define associations. The term attribution means "the action of ascribing a work or remark to a particular author, artist, or person." The IT Act 2000 (Section 11) lays down the guidelines about how an electronic document can be attributed to the individual from whom it originated.

If the originator of the electronic record has not specified any particular mode of acknowledgement to be given by the receiver regarding the receipt of the record, the acknowledgement can be given by : " any communication by the addressee, automated or otherwise" or "any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received." For example, if an individual receives a mail for a meeting, the individual can send a mail to the sender saying thank you for the information, or sends an automated response or shows interest by joining the meeting. These activities show acknowledgement from the receiver end.

The IT Act 2000 talks about digital signature certificates which is a digital key which validates and certifies the identity of the person holding it, and is issued by the certifying agencies. The digital signature certificate verifies the authenticity of the electronic record and ensures that it wasn't altered during the transit.

12.18 KEY WORDS

Attribution: The action of ascribing a work or remark to a particular author, artist, or person.

Digital Signatures: Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

Digital Signature Certificate: The digital signature certificate verifies the authenticity of the electronic record and ensures that it wasn't altered during the transit.

Electronic Signature: Authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature.

Encryption: Encryption involves transformation of simple messages into cipher text while the process of decryption reverses the coded texts into the actual simple message.

IT Act: An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce.

12.19 ANSWER TO CHECK YOUR PROGRESS

A) i. 17.10. 2000 ii. 2008 iii. Indian Computer Emergency Response Team (CERT-In) iv. Communication Device

B) i. Public key ii. 43 iii. 45 iv. True

C) i. IT Act 2000 ii. Symmetric Encryption iii. Asymmetric Encryption iv. Presiding Officer

12.20 TERMINAL QUESTIONS

1. Write brief notes on following:
   i) Certifying Authority
   ii) Duties of Subscribers
   iii) Appellate Tribunal
   iv) Encryption
2. Differentiate between the following:
   i) Digital Signature and Electronic Signature
   ii) IT Act 2000 and IT (Amendment) Act 2008
3. Explain the process of encryption in Digital Signatures.
4. Explain the process pertaining to Acknowledgement and dispatch of electronic records.
5. What are cyber-crimes?

Note	These questions are helpful to understand this unit. Do efforts for writing the answer of these questions but do not send your answer to university. It is only for your practice.