DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

Govt College of Engineering Kalahandi

Cyber Law & Ethics

B.Tech., Semester -VII

Prepared By
Dr. Soumya Das
Asst Prof Dept of CSE

Cyber Laws and Ethics

UNIT - 2

Information Technology Act

Outline....

- Overview of IT Act, 2000
- Amendments and Limitations of IT Act
- Digital Signatures
- Cryptographic Algorithm
- Public Cryptography
- Private Cryptography
- Electronic Governance
- Legal Recognition of Electronic Records
- Legal Recognition of Digital Signature
- Certifying Authorities
- Cyber Crime and Offences
- Network Service Providers Liability
- Cyber Regulations Appellate Tribunal
- Penalties and Adjudication

Overview of IT Act

- The Information Technology Act, 2000 provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend The Indian Penal Code, The Indian Evidence Act, 1872, The Banker's Books Evidence Act, 1891 and The Reserve Bank of India Act, 1934 and for matters connected therewith or incidental there to.
- The Information Technology Act, 2000 extend to the whole of India and it applies also to any offence or contravention thereunder committed outside India by any person.

Salient Features of The IT Act, 2000

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- The Information Technology Act defines in a new section that cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- The Information Technology Act is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.

Applicability and Non-Applicability of the Act

- **Applicability**
- According to Section 1 (2), the Act extends to the entire country, which also includes Jammu and Kashmir. In order to include Jammu and Kashmir, the Act uses Article 253 of the constitution. Further, it does not take citizenship into account and provides extra-territorial jurisdiction.
- Section 1 (2) along with Section 75, specifies that the Act is applicable to any offence or contravention committed outside India as well. If the conduct of person constituting the offence involves a computer or a computerized system or network located in India, then irrespective of his/her nationality, the person is punishable under the Act.
- Lack of international cooperation is the only limitation of this provision.

Applicability and Non-Applicability of the Act

- **Non-Applicability**
- According to Section 1 (4) of the Information Technology Act, 2000, the Act is not applicable to the following documents:

1. Execution of Negotiable Instrument under Negotiable Instruments Act, 1881, except cheques.
2. Execution of a Power of Attorney under the Powers of Attorney Act, 1882.
3. Creation of Trust under the Indian Trust Act, 1882.
4. Execution of a Will under the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called.
5. Entering into a contract for the sale of conveyance of immovable property or any interest in such property.
6. Any such class of documents or transactions as may be notified by the Central Government in the Gazette.

Amendments Brought in the I.T Act

- The I.T. Act has brought amendment in four statutes vide section 91-94. These changes have been provided in schedule 1-4.
  - The first schedule contains the amendments in the Penal Code. It has widened the scope of the term "document" to bring within its ambit electronic documents.
  - The second schedule deals with amendments to the India Evidence Act. It pertains to the inclusion of electronic document in the definition of evidence.
  - The third schedule amends the Banker's Books Evidence Act. This amendment brings about change in the definition of "Banker's-book". It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device. Similar change has been brought about in the expression "Certified-copy" to include such printouts within its purview.
  - The fourth schedule amends the Reserve Bank of India Act. It pertains to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institution.

Highlights of the Amended Act

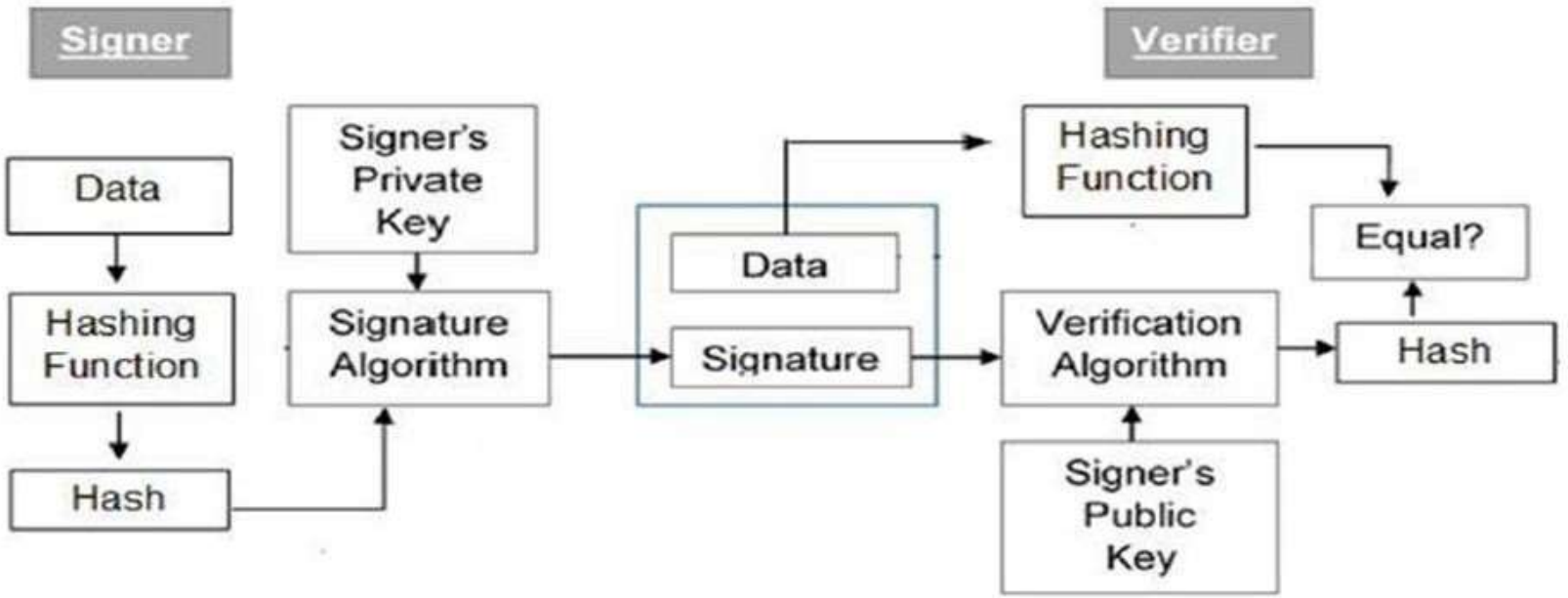
- The newly amended act came with following highlights.
  - It stresses on privacy issues and highlights information security.
  - It elaborates Digital Signature.
  - It clarifies rational security practices for corporate.
  - It focuses on the role of Intermediaries.
  - New faces of Cyber Crime were added.

Digital Signatures

- Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.
- Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.
- Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.
- In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Model of Digital Signature

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



Importance of Digital Signature

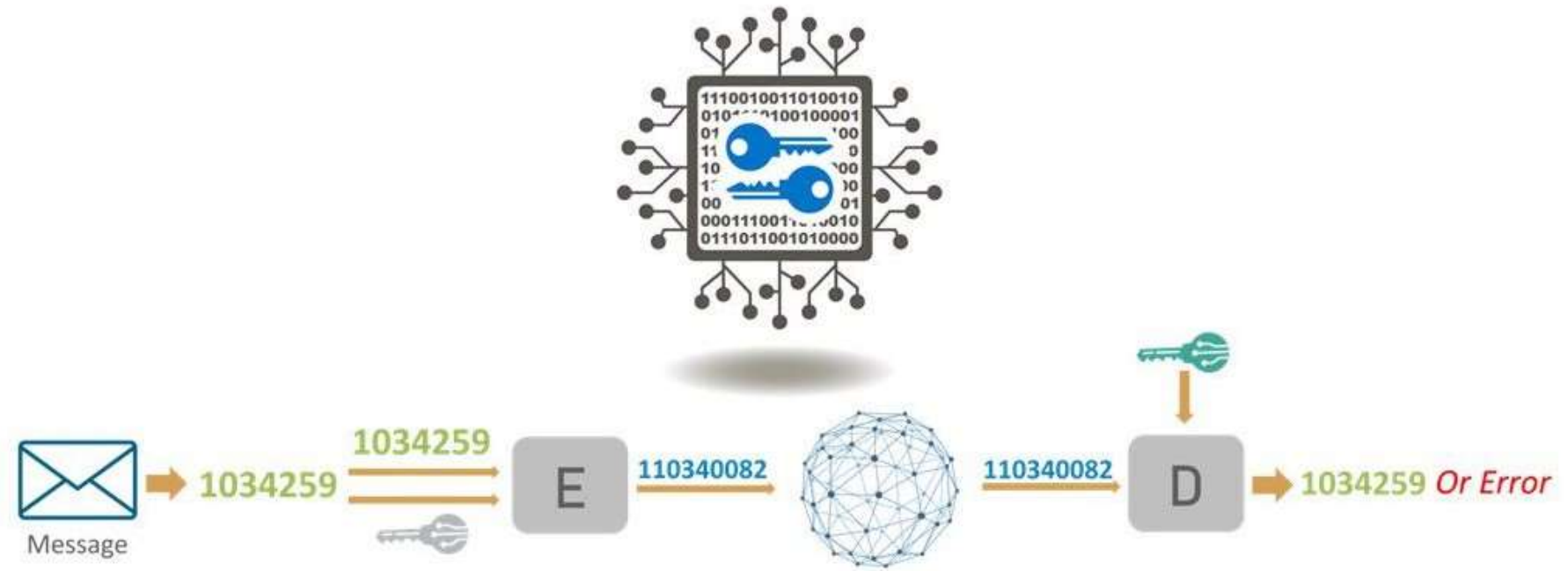
- Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.
- **Message authentication** – When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** – In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.

Importance of Digital Signature

- **Non-repudiation** – Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

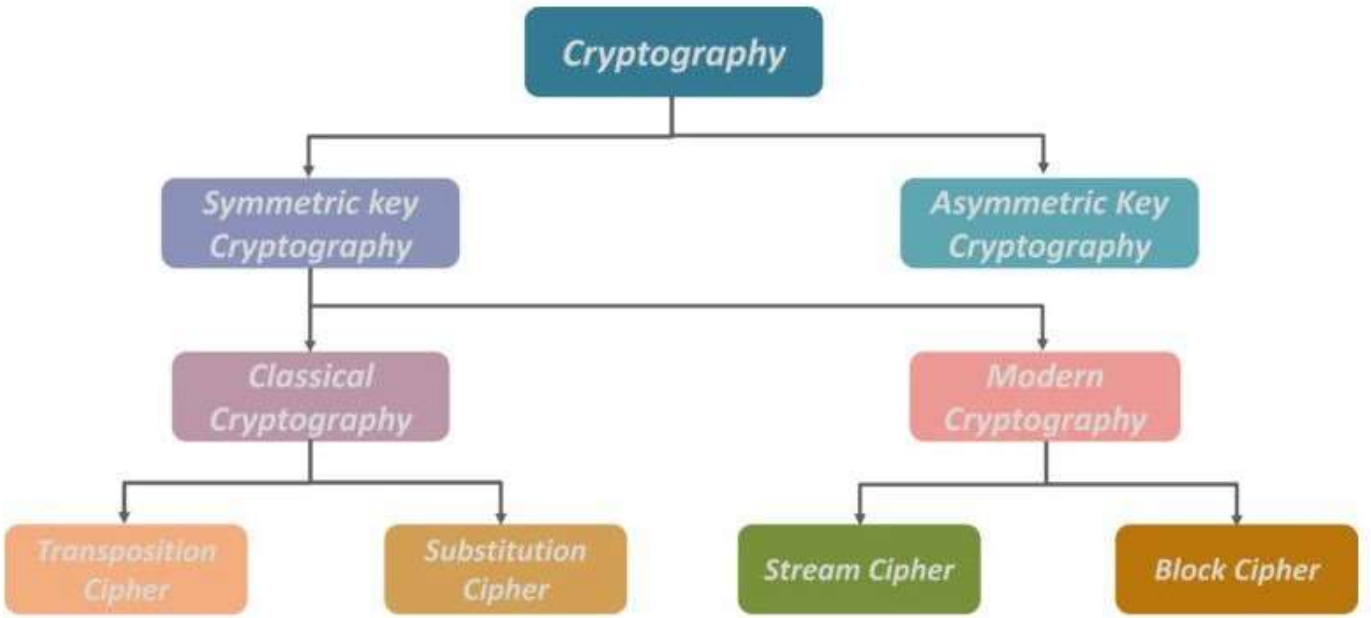
Cryptographic Algorithm

- **Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries.**



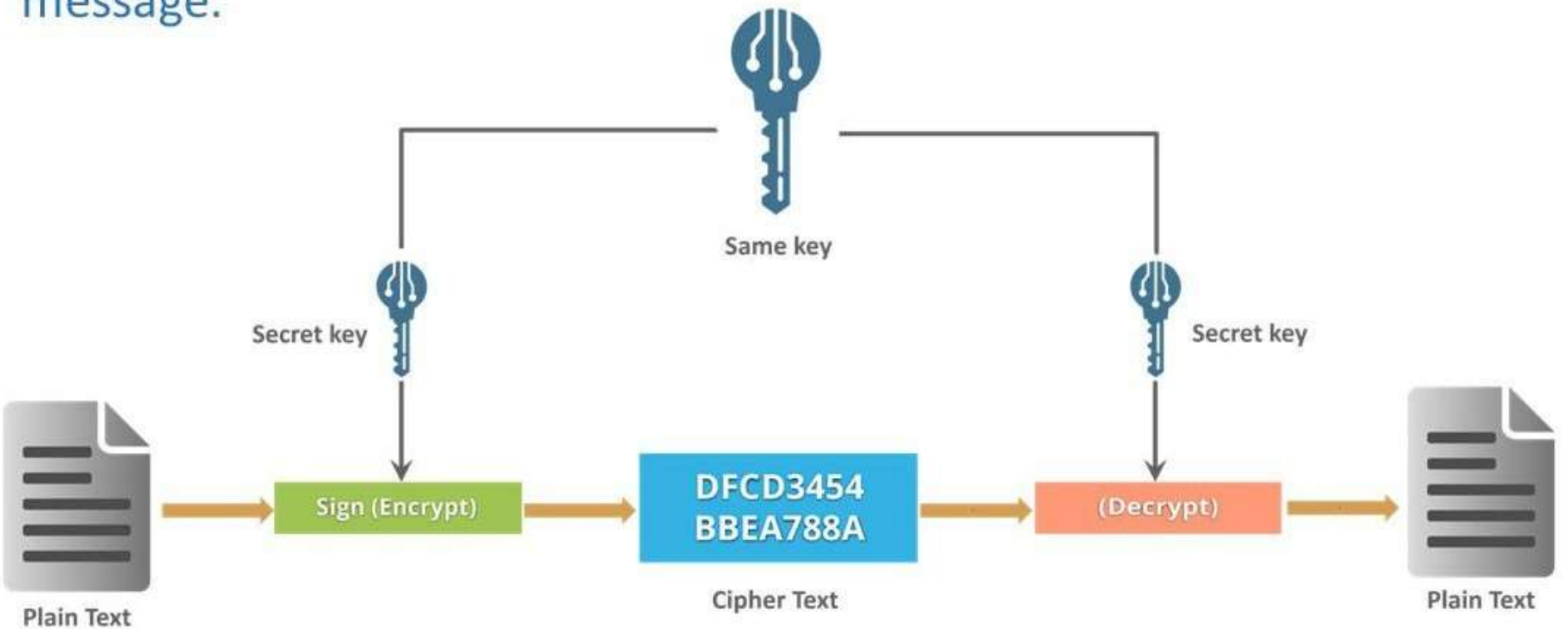
Cryptographic Algorithm

- Cryptography is broadly classified into two categories: Symmetric key Cryptography and Asymmetric key Cryptography (popularly known as public key cryptography).



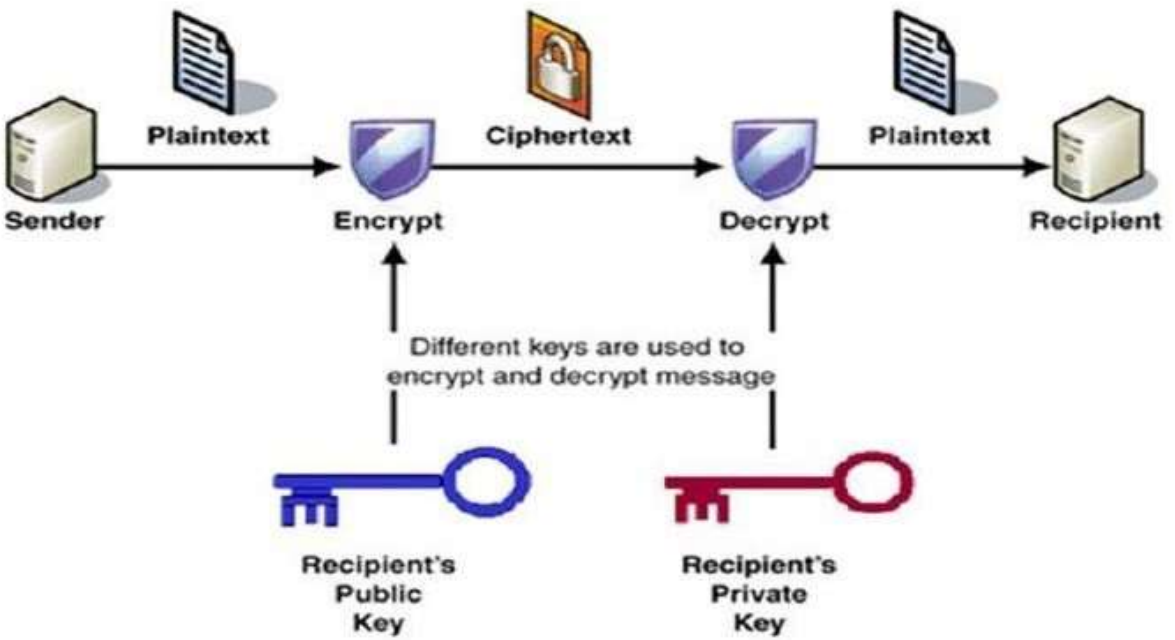
Symmetric Key Cryptography

- An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.



Asymmetric Key Cryptography

- Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key -- to encrypt and decrypt a message and protect it from unauthorized access or use.



Classical Cryptography

- Classical cryptography is based on the mathematics and it relies on the computational difficulty of factorizing large number. The security of classical cryptography is based on the high complexity of the mathematical problem for the instance factorization of large number.
- It manipulates traditional characters, i.e., letters and digits directly.
- It is mainly based on 'security through obscurity'. The techniques employed for coding were kept secret and only the parties involved in communication knew about them.
- It requires the entire cryptosystem for communicating confidentially.

Modern Cryptography

- Modern cryptography is the cornerstone of computer and communications security. Its foundation is based on various concepts of mathematics such as number theory, computational-complexity theory, and probability theory.
- It operates on binary bit sequences.
- It relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secrete key which is used as the seed for the algorithms.
- Modern cryptography requires parties interested in secure communication to possess the secret key only.

Transposition Cipher

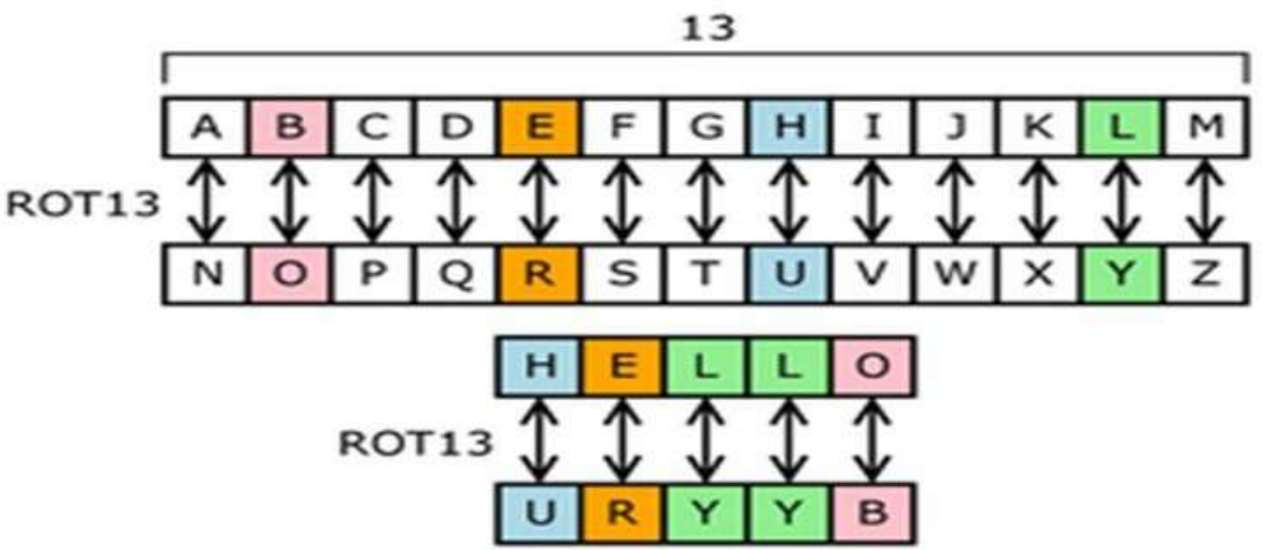
- Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.
- A simple example for a transposition cipher is columnar transposition cipher where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.
- Consider the plain text hello world, and let us apply the simple columnar transposition technique as shown below

h	e	l	l
o	w	o	r
l	d		

- The plain text characters are placed horizontally and the cipher text is created with vertical format as : holewdlo lr. Now, the receiver has to use the same table to decrypt the cipher text to plain text.

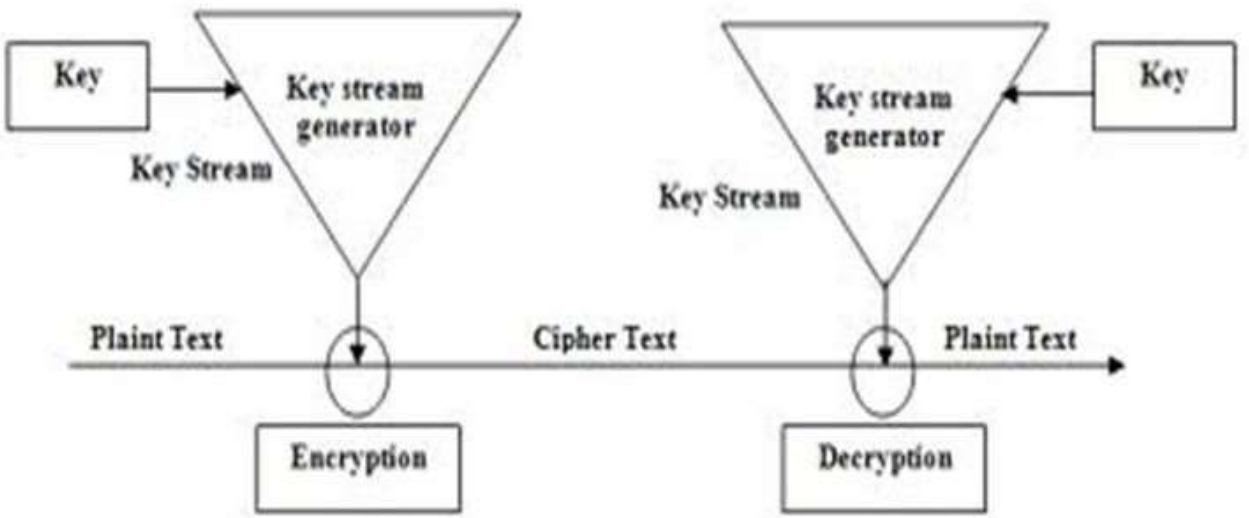
Substitution Cipher

- In cryptography, a substitution cipher is a method of encrypting in which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth.



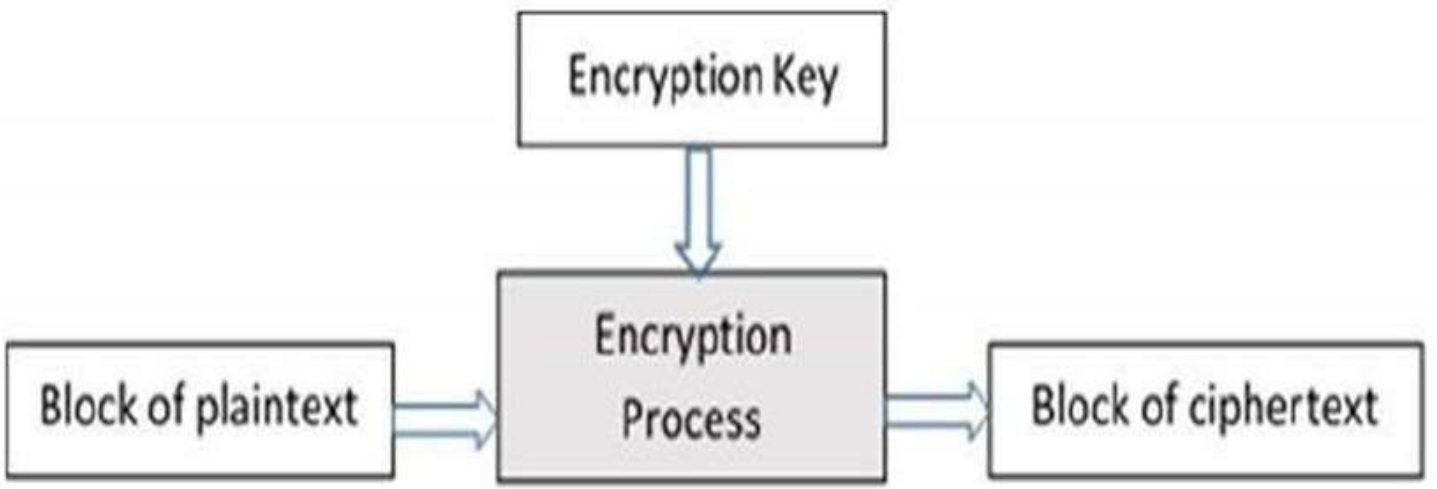
Stream Cipher

- A stream cipher is a method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time. This method is not much used in modern cryptography.



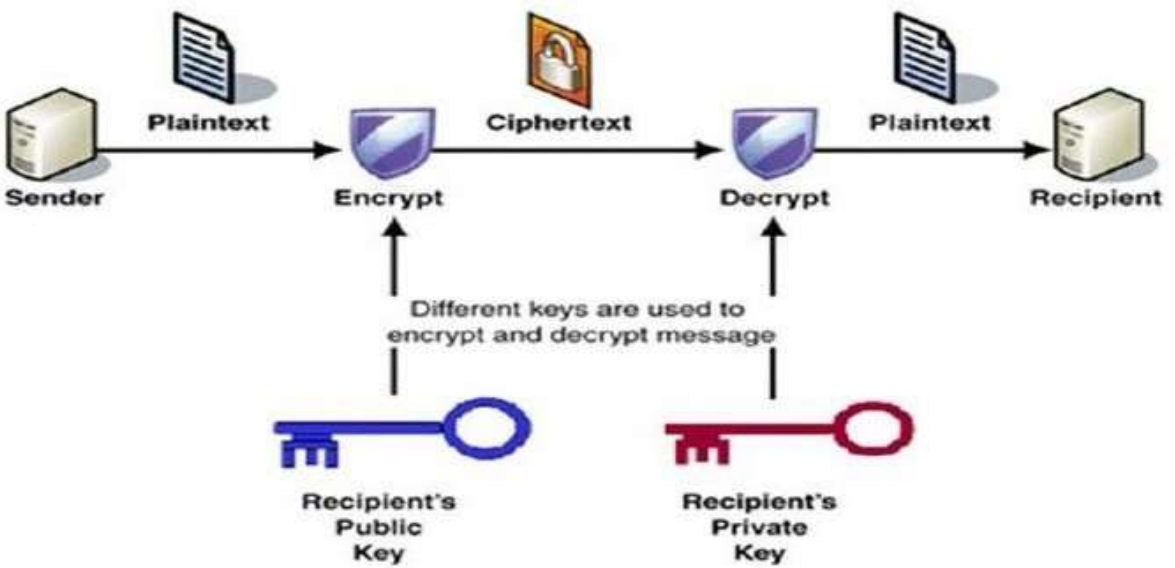
Block Cipher

- A block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers.



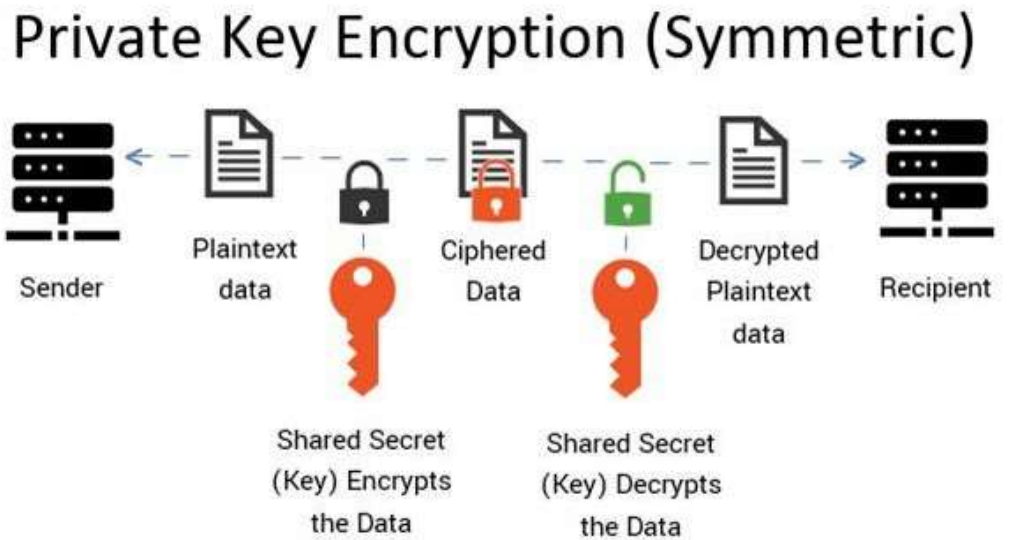
Public Cryptography

- Public key cryptography uses a pair of keys to encrypt and decrypt data to protect it against unauthorized access or use. This key is used to encrypt the message, and to send it to the recipient. When the message arrives, the recipient decrypts it using a private key, to which no one else has access.



Public Cryptography

- Private key encryption is the form of encryption where only a single private key can encrypt and decrypt information. It is a fast process since it uses a single key. However, protecting one key creates a key management issue when everyone is using private keys.



E-Governance

- Electronic governance or e-governance is the application of IT for delivering government services, exchange of information, communication transactions, integration of various stand-alone systems between government to citizen (G2C), government-to-business (G2B), government-to-government (G2G), government-to-employees (G2E) as well as back-office processes and interactions within the entire government framework.
- Through e-governance, government services are made available to citizens in a convenient, efficient, and transparent manner.
- The three main target groups that can be distinguished in governance concepts are government, citizens, and businesses/interest groups. In e-governance, there are no distinct boundaries.

Advantages of E-Governance

- **Speed**
- Technology makes communication swifter. Internet, smartphones have enables instant transmission of high volumes of data all over the world.
- **Saving Costs**
- A lot the Government expenditure goes towards the cost of buying stationery for official purposes. Letters and written records consume a lot of stationery. However, replacing them with smartphones and the internet can saves crores of money in expenses every year.
- **Transparency**
- The use of e-governance helps make all functions of the business transparent. All Governmental information can be uploaded onto the internet. The citizens access specifically access whichever information they want, whenever they want it, at the click of a mouse, or the touch of a finger.
- However, for this to work the Government has to ensure that all data as to be made public and uploaded to the Government information forums on the internet.

Disadvantages of E-Governance

- **Loss of Interpersonal Communication**
- The main disadvantage of e-governance is the loss of interpersonal communication. Interpersonal communication is an aspect of communication that many people consider vital.
- **High Setup Cost and Technical Difficulties**
- Technology has its disadvantages as well. Specifically, the setup cost is very high and the machines have to be regularly maintained. Often, computers and internet can also break down and put a dent in governmental work and services.
- **Illiteracy**
- A large number of people in India are illiterate and do not know how to operate computers and smartphones. E-governance is very difficult for them to access and understand.

Legal Recognition of Electronic Records

- Let's say that a certain law requires a matter written, typewritten, or printed. Even in the case of such a law, the requirement is satisfied if the information is rendered or made available in an electronic form and also accessible for subsequent reference.
- The Information Technology Act, 2000 also aims to provide the legal framework under which legal sanctity is accorded to all electronic records and other activities carried out by electronic Information Systems Control and Audit means.
- The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

Legal Recognition of Digital Signature

- Let's say that the law requires a person's signature to authenticate some information or a document. Notwithstanding anything contained in such law, if the person authenticates it with a digital signature in a manner that the Central Government prescribes, then he satisfies the requirement of the law.
- The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as "hash function" which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record.
- Any tampering with the contents of the electronic record will immediately invalidate the digital signature.

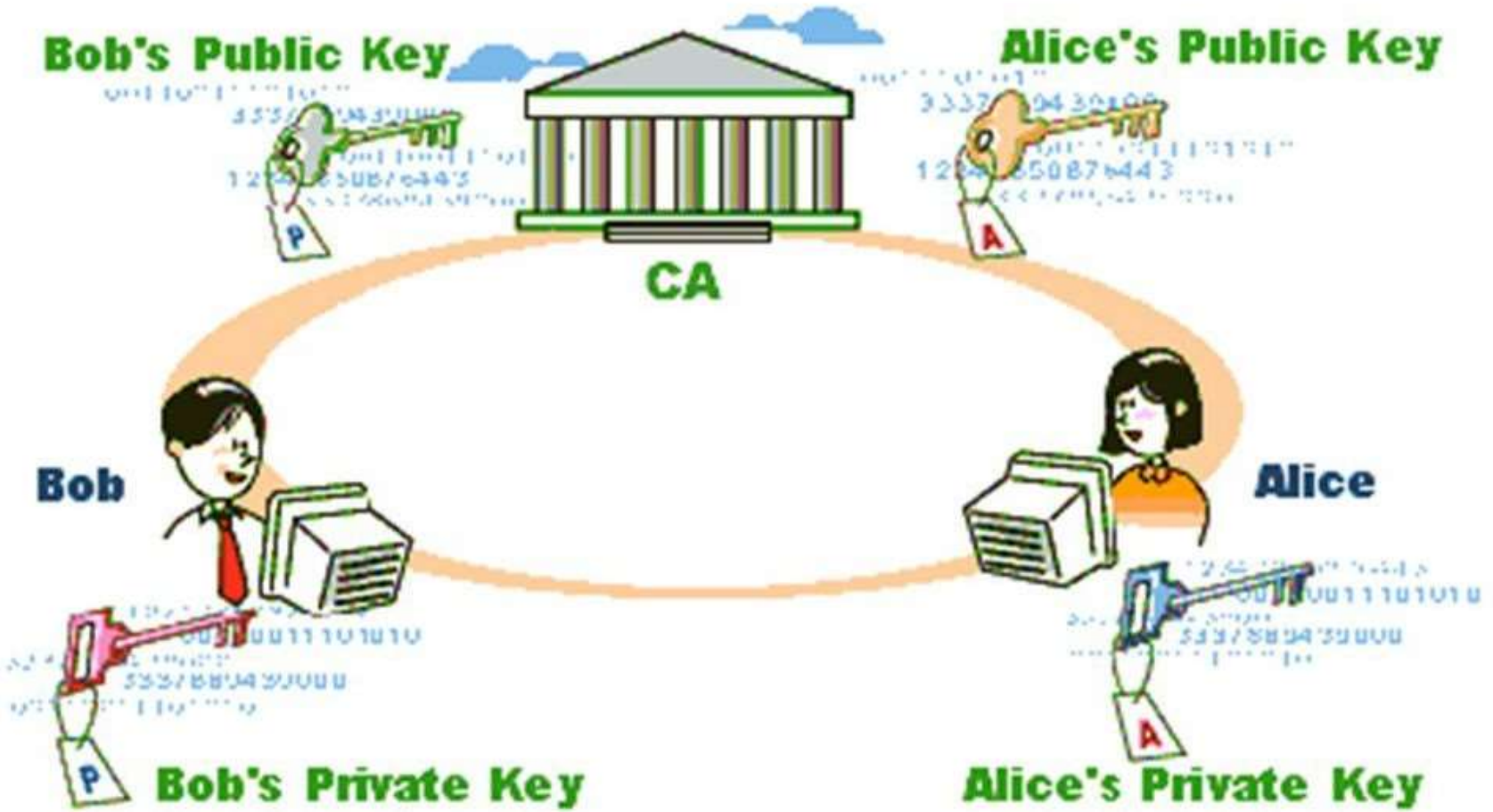
Legal Recognition of Digital Signature

- Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key.
- This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature.
- It will also enable a person who has a public key to identify the originator of the message.

Certifying Authorities

- In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key.
- A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.
- It will also enable a person who has a public key to identify the originator of the message.

Certifying Authorities



Cyber Crime

- Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.
- Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.
- Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.
- Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

Types of cybercrime

- Email and internet fraud.
- Identity fraud (where personal information is stolen and used).
- Theft of financial or card payment data.
- Theft and sale of corporate data.
- Cyberextortion (demanding money to prevent a threatened attack).
- Ransomware attacks (a type of cyberextortion).
- Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- Cyberespionage (where hackers access government or company data).

CLASSIFICATION OF CYBER OFFENCES

- The increased rate of technology in computers has led to the enactment of Information Technology Act 2000. The converting of the paperwork into electronic records, the storage of the electronic data, has tremendously changed the scenario of the country.
- Offenses: Cyber offenses are the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both. Cybercrime usually includes:
- (a) Unauthorized access of the computers (b) Data diddling (c) Virus/worms attack (d) Theft of computer system (e) Hacking (f) Denial of attacks (g) Logic bombs (h) Trojan attacks (i) Internet time theft (j) Web jacking (k) Email bombing (l) Salami attacks (m) Physically damaging computer system.

The offenses included in the IT Act 2000

1. Tampering with the computer source documents.
2. Hacking with computer system.
3. Publishing of information which is obscene in electronic form.
4. Power of Controller to give directions
5. Directions of Controller to a subscriber to extend facilities to decrypt information
6. Protected system
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offense or contravention committed outside India
12. Confiscation
13. Penalties or confiscation not to interfere with other punishments.
14. Power to investigate offenses.

Network Service Providers Liability

- The Indian ITAct,2000 stipulates that Network service providers are not liable in certain cases, for any third party information or data made available by an ISP, if it proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commissioning of such offence.
- A 'network service provider' means any person who provides access to information service in electronic form. For example: Internet service provider, cellular mobile services, customer access services, mobile satellite services etc.
- It essentially performs two tasks-to provide access to the network and to act as intermediary between an originator and addressee with respect to any particular electronic message.

Network Service Providers Liability

- According to section 79 of the IT ActFor the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made thereunder for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention.

(a) "network service provider" means an intermediary.

(b) "third party information" means any information dealt with by a network service provider in his capacity as an intermediary.

Cyber Regulations Appellate Tribunal (Section 48)

- The Central Government notifies and establishes appellate tribunals called Cyber Regulations Appellate Tribunal.
- The Central Government also specifies in the notification all the matters and places which fall under the jurisdiction of the Tribunal.
- **QUALIFICATIONS**
- To be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal, a person has or qualified to be a judge of a High Court.
- Judicial members of the Cyber Appellate Tribunal so appointed from amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for a period of not less than one year or Grade I post of that service for a period of not less than five years.
- Members other than judicial member should have special knowledge and professional experience in information technology, telecommunication, industry, management or consumer affairs.

Cyber Regulations Appellate Tribunal (Section 48)

- **TERM**
- Section 51 (1) provides a five year term for the Chairperson or Member of the Cyber Appellate Tribunal.
- The term states from the date on which he enters upon his office. It will last for five years or until he attains the age of 65 years, whichever is earlier.
- **POWERS**
- As per section 52A the Chairperson being the Head of the Cyber Appellate Tribunal has both executive and administrative powers of general superintendence and directions in the conduct of the affairs of that Tribunal which may include presiding over the meetings of the Tribunal.

Cyber Regulations Appellate Tribunal (Section 48)

- To exercise and discharge such powers and functions of the Tribunal as may be prescribed.
- The Chairperson has the power of the to transfer cases after either following the laid down procedure or suo moto may transfer any case pending before one Bench, for disposal to any other Bench.

The CYBER APPELLATE COURT shall have the powers of

1. Summoning and enforcing the attendance of any person and examining him on oath.
2. Requiring the discovery and production of documents or other electronic records.
3. Receiving evidence on affidavits.
4. Issuing commissions for the examination of witness or documents.
5. Reviewing its decisions.
6. Dismissing an application for default or deciding it ex parte.
7. Any other matter, which may be prescribed.

PENALTIES

- Penalty for damage to computer, computer system, etc
- If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network
- accesses or secures access to such computer, computer system or computer network.
- downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium.
- introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network.

PENALTIES

- damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network
- disrupts or causes disruption of any computer, computer system or computer network
- denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means.
- provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder

PENALTIES

- charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network.

Power to Adjudicate

- For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder, the Central Government shall, subject to the provisions of sub-section(3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.
- The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty as he thinks fit in accordance with the provisions of that section.

Power to Adjudicate

- No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and Legal or Judicial experience as may be prescribed by the Central Government.
- Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.
- Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section 58, and
  - all proceedings before it shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code
  - shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973.