U-II INFORMATION TECHNOLOGY 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", 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 Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental there to.

PURPOSE OF ACT

- To establish a regime for the responsible collection and handling of personal information in the Victorian public sector;
- To provide individuals with rights of access to information about them held by organizations, including information held by contracted service providers;
- To provide individuals with the right to require an organization to correct information about them held by the organization including information held by contracted service providers;
- To provide remedies for interferences with the information privacy of an individual;
- To provide for the appointment of a Privacy Commissioner.

NATURE OF RIGHTS CREATED BY THIS ACT

- Gives rise to any civil cause of action
- Without limiting paragraph (a), operates to create in any person any legal right enforceable in a court or tribunal - otherwise than in accordance with the procedures set out in this Act.

A contravention of this Act does not create any criminal liability except to the extent expressly provided by this Act.

IN SHORT:

- India becomes 12th nation in world having cyber Law due to IT ACT2000
- India comes among top 10 country who are having fully updated cyber law
- IT ACT-2000 is first law in India applicable throughout country including Jammu & Kashmir
- Promotes trust in electronic world
- Promotes e-commerce
- Acceptance of electronic document as evidence is possible due to IT ACT
- Acceptance of digital signature become possible

IT ACT-2000 HAS DONE THE AMENDMENTS IN:

- Indian Penal code (IPC) –1860
- Indian evidence ACT-1872
- The bankers books evidence ACT-1891 and
- RBI ACT-1934

Whenever one touches computer knowingly or unknowingly he/she shall be within the ambit of IT ACT-2000

IT ACT-2000 CHAPTERS AND SECTIONS:

Chapter I : Preliminary
1 Short title, Extent, Commencement and application
2 Definitions
Chapter II : Digital Signature
3 Authentication of electronic records
Chapter III Electronic Governance
4 Legal recognition of electronic records
5 Legal recognition of digital signatures
6 Use of electronic records and digital signatures in Government and its agencies
7 Retention of electronic records
8 Publication of rule, regulation, etc., in Electronic Gazette
9 Sections 6,7 and 8 not to confer right to insist document should be accepted in electronic form
10 Power to make rules by Central Government in respect of digital signature
Chapter IV : Attribution, Acknowledgement and Despatch of Electronic records
11 Attribution of electronic records
12 Acknowledgement of receipt
13 Time and place of despatch and receipt of electronic record
Chapter V : Secure Electronic records and secure digital signatures
14 Secure electronic record
15 Secure digital signature
16 Security procedure
Chapter VI : Regulation of Certifying Authorities
17 Appointment of Controller and other officers
18 Functions of Controller
19 Recognition of foreign Certifying Authorities
20 Controller to act as repository
21 Licence to issue Digital Signature Certificates
22 Application for licence
23 Renewal of licence
24 Procedure for grant or rejection of licence
25 Suspension of licence
26 Notice of suspension or revocation of licence
27 Power to delegate
28 Power to investigate contraventions
29 Access to computers and data
30 Certifying Authority to follow certain procedures
31 Certifying Authority to ensure compliance of the Act, etc.
32 Display of licence
33 Surrender of licence
34 Disclosure

85 Offences by companies
86 Removal of difficulties
87 Power of Central Government to make rules
88 Constitution of Advisory Committee
89 Power of Controller to make regulations
90 Power of State Government to make rules
91 Amendment of Act 45 of 1860
92 Amendment of Act 1 of 1872
93 Amendment of Act 18 of 1891
94 Amendment of Act 2 of 1934

Schedules

Schedule 1 Amendments to the Indian Penal Code
Schedule 2 Amendments to the Indian Evidence Act, 1872
Schedule 3 Amendments to the Bankers' Books Evidence Act, 1891
Schedule 4 Amendments to the Reserve Bank of India Act, 1934

SUMMARY:

- **13** - chapters as above
- **94** sections
- Major sections Dealing with crime are 43, 65, 66, 67
- **Section - 43** Penalty for damage to computer, computer system, etc.
- **Section - 65** Tampering with computer source documents
- **Section - 66** Hacking with Computer system
- **Section - 67** Publishing of information which is obscene in electronic form

AMENDMENTS AND LIMITATIONS OF IT ACT – 2000:

Expansion scope:

With the technology and communication boom, the mobile phones have quickly made their presence inevitable in today's life. While the IT Act 's definition of computers can accommodate mobile phones too, but I still think making explicit declaration of mobile phones and handhelds to be covered under this act will be fine. .. So the offences involving mobile phones be also covered under this act…

The need for Anti Spam policies:

With email and sms becoming such popular, unsolicited mails and sms have also grown rapidly .. We should make an anti spam law apropos CanSpam Act which will ensure that these unsolicited mails or sms are dealt with .. There should be a national "Do not email" and "Do not call" registry and the address listed there shouldn't be sent spam emails or sms …

The need for Privacy policies:

With camera phones becoming more common, events like Kareena & Shahid kissing video mms will increase too .. Now without getting into voyeurism debate, I would like to point out the digital aspect of the problem. Any information can be distributed or shared over the Internet without the concerned parties being unknown… More people downloaded the clip from Mid Day website than people who read that particular issue of the tabloid… This was a complete breach of privacy and

a new Privacy Act should be devised.. It should also cover digital privacy so that the netizens can have the right to control their personal data

Cyber Squatting:

Cyber Squatting is simply registering a domain name for exploiting it later.. Although ICANN can resolve the disputes but we should have a law that covers this here … And as now we have started issuing Country level top domain (.in), the registrar should have more responsibilities …

Spoofing:

I was surprised to learn that the IT Act doesn't specifically cover spoofing .. Spoofing is disguising your identity over the Internet...It can be anything from spoofing the IP address or spoofing the email address to send fake mails.. Although it can be held as fraud but it would be difficult to cover it under IPC … So it should also be included in the IT Act …

Mail or Forum bombing:

After being a moderator of a forum for such a long time, I have learnt what tactics people use to disrupt and to bother the forum admins .. The best and most used method is using Bots .. Bots are computer programs that post automatic replies on websites and / or send automatic emails just to create havoc or spam .. Although the IT Act covers malicious software under Virus but the definition of virus is complete only when it causes any damage .. Bots don't do any damage … they just create problems for admins and site owners ..So Bots (be it forum bots or chat bots or email bots) should also be covered in the Act …

Misleading search words:

Now this is a trivial issue … Like this search query for Failure, the first result is Autobiography of George W Bush .. So .. Pages can be created to cajole searchers to direct to some page that has no relation to the search terms .. Now this was a derogatory attempt, but there can be other uses too .. Like users searching for a specific products are redirected to products of competitor's site .. So steps should be taken to minimize such search hijacking …

Pornography & Derogatory sites:

While pornography has been covered in the IT Act but sites that contain derogatory or misleading information about respected persons should also be covered .. I didn't found any mention to this regard in the Act … Maybe it collides with Right to Freedom of expression .. But still I found it quotable. There should be proper implementation of it too .. Consider the case of DPS MMS scandal .. It resulted in jailing of Bazee CEO Avnish Bajaj .. On what basis? .. If it was because that he was the owner of the site, which hosted the clip, then why don't we jail CEO of BSNL or other telephone companies when terrorists use their network for their business? … There are a million other reasons on why he shouldn't be convicted but Police thought otherwise … So .. Their should be a proper policy on what to do and what not to .. and proper implementation of that policy .

WHAT IS CRYPTOGRAPHY?

Is art or science of Secret writing? It concerned with the developing algorithms to

- To conceal the content of messages from all except sender and recipient
- To verify the correctness of message or its sender and recipient

Cryptography is art or science of transforming intelligible message to unintelligible and again transforming that message back to the original form

Terminologies

- **Encryption(Enciphering) :**Process of encoding the message so that meaning is not obvious or not in understandable form
- **Decryption(Deciphering):** Reverse process of encryption
- **Plaintext:** The original form of the message
- **Cipher text:** Disguised(encrypted) message

  P- plain-text

  C- Cipher text

  E- Encryption algorithm

  D- Decryption algorithms

  C= E (p)

  P= D(C)

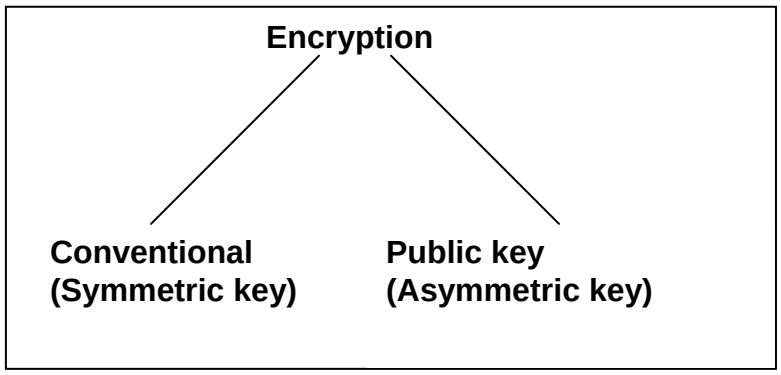
  P= D(E (P))

- **Key :** Critical (secret) information used in cipher and known only to sender and receiver
  - Symmetric – Shared key
  - Asymmetric – Public key
- **Code:** Algorithm used for transforming the intelligible (plain text) to unintelligible (cipher text)
- **Cipher:** Is algorithm /Code used for transforming plaintext to cipher text
- **Cryptanalysis (Code breaking):** Study of method for transforming cipher text to plaintext without having knowledge of any key
- **Cryptology :** Area of cryptography and cryptanalysis together is called as cryptology

Types of ciphers:

There are two types of ciphers

1. Stream cipher : Converts plaintext to cipher text one bit at time
2. Block cipher : It takes a given length of data as input and produces different length of encrypted data



Conventional (Symmetric key) Cryptography:

Symmetric key cryptography Is also termed as private or secret key encryption because secret key is shared between sender and receiver

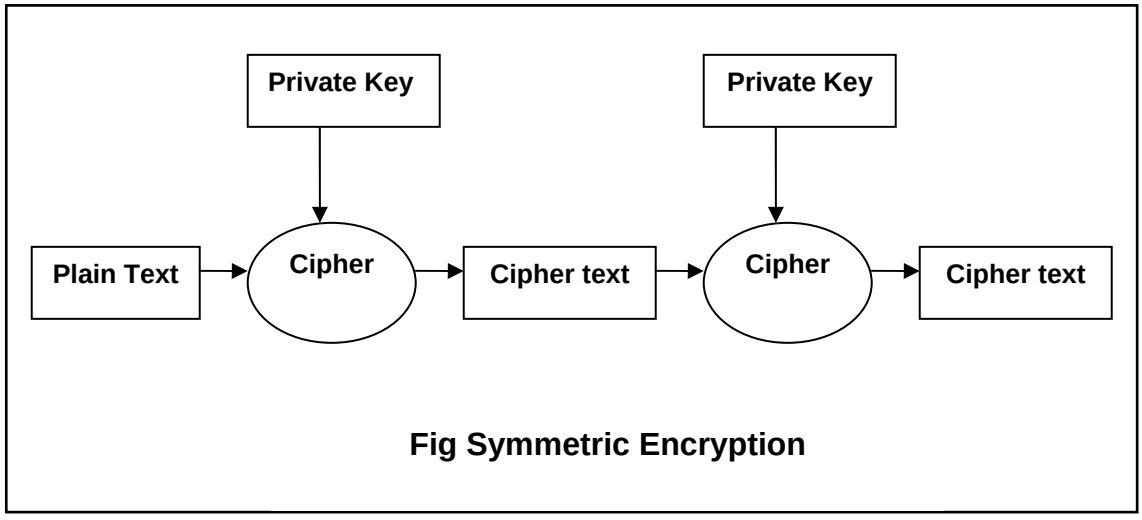


Fig Symmetric Encryption

Caesar's Cipher

The earliest known use of substitution cipher was given by Julius Caesar for exchanging military secret information before 2000 years

An extremely simple example of conventional cryptography is a substitution cipher. A substitution cipher substitutes one piece of information for another.

The Caesar cipher involved in replacing each letter of alphabet with the letter standing three places further down the alphabet

For example, if we encode the word “SECRET” using Caesar’s key value of 3, we offset the alphabet so that the 3rd letter down (D) begins the alphabet.

Where D=A, E=B, F=C, and so on.

So starting with ABCDEFGHIJKLMNOPQRSTUVWXYZ and sliding everything up by 3, you get DEFGHIJKLMNOPQRSTUVWXYZABC

i.e.

P.T.:	A	B	C	D	E	F	G	……..	Z
C.T.:	D	E	F	G	H	I	J	……	C

Now let’s assign numerical value (NV) to each letter

P.T.:	A	B	C	D	E	F	G	……..	Z
N.V.:	0	1	2	3	4	5	6	……..	25

The algorithms can be expressed as

For plaintext letter p, substitute the ciphertext letter c3

C= E (p) = (p+3) mod 26

A shift may be of any amount so general Caesar algorithm is

C=E(P) = (P+K) mod(26)

Where K takes a value in the range of 1 to 25 and decryption algorithm is

P = D(C) = (C – K) mod 26

Drawback of Caesar Cipher:

Major problem of Caesar cipher is language regularity due to which there is possibility that cryptanalysis may guess the message present in CT

Language regularity is based on the frequency of letter occurrence

- Letter **E** is more frequent then
- T R I O A S Then
- Rarely used is J K Q X Z
- Letter **E** is **25** times more frequent than the **Q**

Example of language Regularity: (Caesar Monoalphabetic Substitution)

P.T.:	A	B	C	D	E	F	G	……..	Z
C.T.:	D	E	F	G	H	I	J	……	C

C.T.: W T I G M E P W T I E O I V G S Q M R R

P.T.: S P E C I A L S P E A K E R C O M I N G

As shown appearance frequencies of letters words and pairs of letters accelerates the identification of certain letters

Asymmetric cryptography:

- Developed in 1970
- Two keys are involved in asymmetric encryption
- One key is used by sender to encrypt the data and other by receiver to decrypt the data
- Both the keys are reversible also
- Generally public keys are used for encryption of data while private keys are used for decryption of data

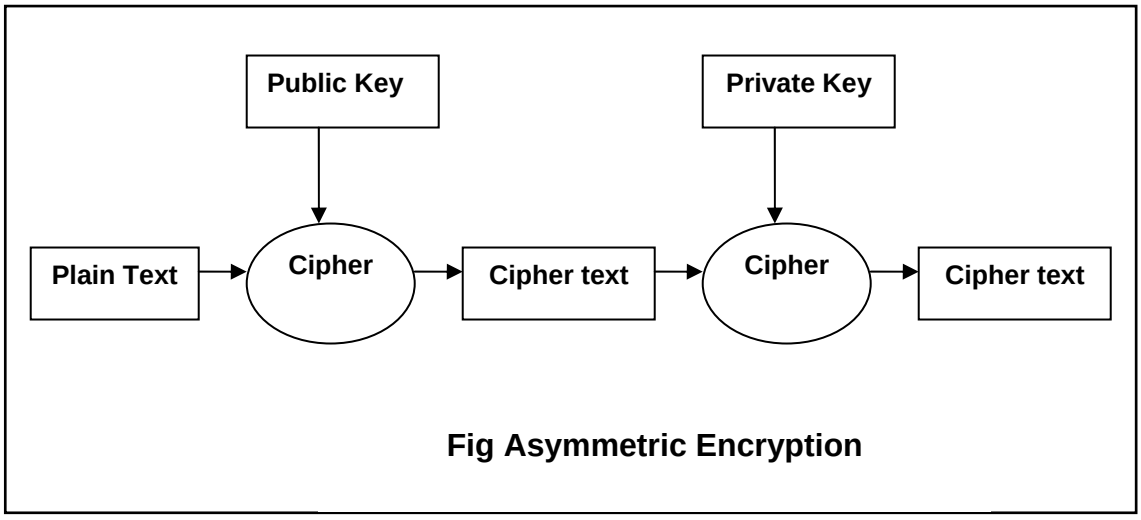


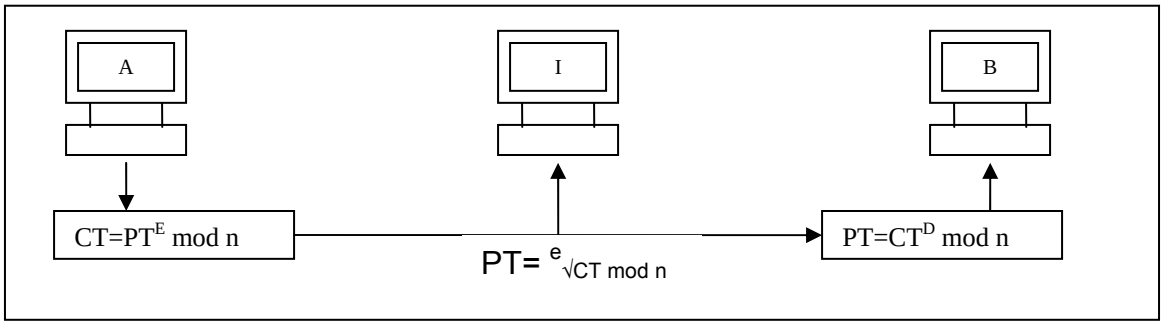
Fig Asymmetric Encryption

RSA ALGORITHM:

- Developed by **R**ivest, **S**hamir, **A**dleman
- Most popular asymmetric key cryptographic algorithm
- RSA algorithm is based on mathematical fact that it is easy to find and multiply to large prime numbers together but it is extremely difficult to factor their products
- The public and private key in RSA are based on very large prime number(made of 100 or more digit prime number)
- Algorithm is quiet simple however challenge was related with selection and generation of public and private key

Algorithm:

1. Select two large prime numbers let **P** and **Q**
2. Calculate **N= P * Q**
3. Select the public key (i.e. Encryption key) E such that it is not the factor of **(P – 1)** & **(Q – 1)**
4. Select private key (i.e. Decryption key) D such that the following equation becomes true **(D * E) mod (P – 1) * (Q – 1) = 1**
5. For encryption calculate Cipher text CT from plain text PT as follows **$CT=PT^E$ mod N**
6. Send **CT** i.e. cipher text to receiver
7. For decryption calculate PT from CT i.e. **$PT= CT^D$ Mod N**



As shown for user A & B there is polynomial complexity while for intruder I there is logarithmic complexity i.e. hard to break cipher by Intruder

Example:

1. Take P=7 and Q=17 as two prime numbers
2. N=P * Q =7*17 =119
3. (P-1)* (Q-1)=6*16=96 so factors are 2,2,2,2,2 and 3 so public key should not have factor of 2 and 3 let us choose public key value as 5
4. Select private key D such that (D *E) mod (P-1)*(Q-1)=1 so choose 77 as D because it satisfies the equation
5. i.e. (5*77) mod 96 => 385 mod 96=1 which satisfy our condition
6. E=5 and D=77

DIGITAL SIGNATURE:

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

- DSS make the use of algorithm called digital signature algorithm (DSA)
- Similar to RSA, DSA is also based on asymmetric key cryptography. However their objectives are totally different
- As we know RSA is primarily used for encrypting the message but we can use RSA to produce digital signature
- DSA can only be used to perform digital signature , it cannot be used for encryption

RSA and Digital Signature:

Lets assume sender **A** wants to send a message **M** to receiver **B** along with digital signature **S** calculated over message **M** following steps occur for preparation of message

Step I:

Sender A uses SHA-1 Message digest algorithm for calculating the MD1 of original message M as shown below

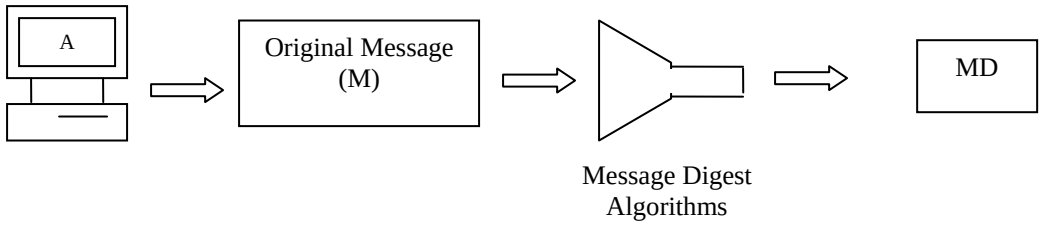


Fig. Message Digest Calculation

Step II:

Sender A now encrypts the MD with his private key and the output of this process is called digital signature (DS)

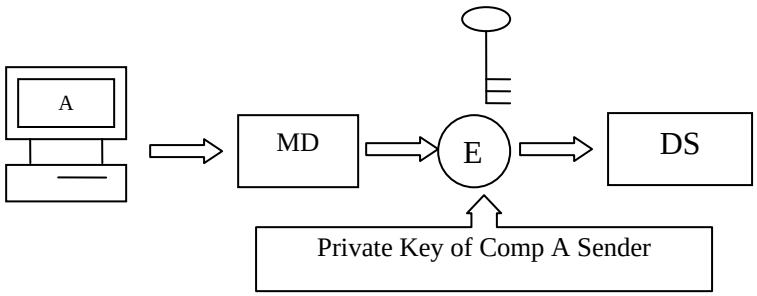


Fig. Digital Signature Creation

Step III:
Now sender A sends original message M along with digital signature DS to receiver B as shown below

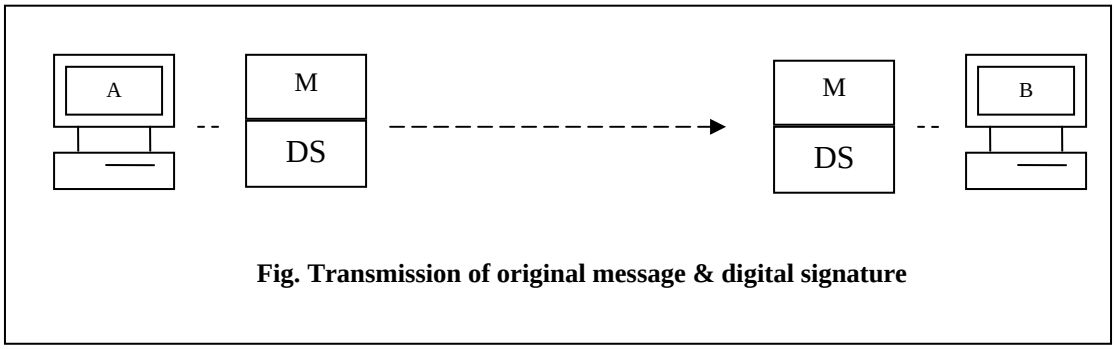


Fig. Transmission of original message & digital signature

Step IV:

- **B** receives original message (M) from **A** and digital signature DS
- **B** uses same message digest algorithm used by **A** and calculates MD2 of received message as shown below

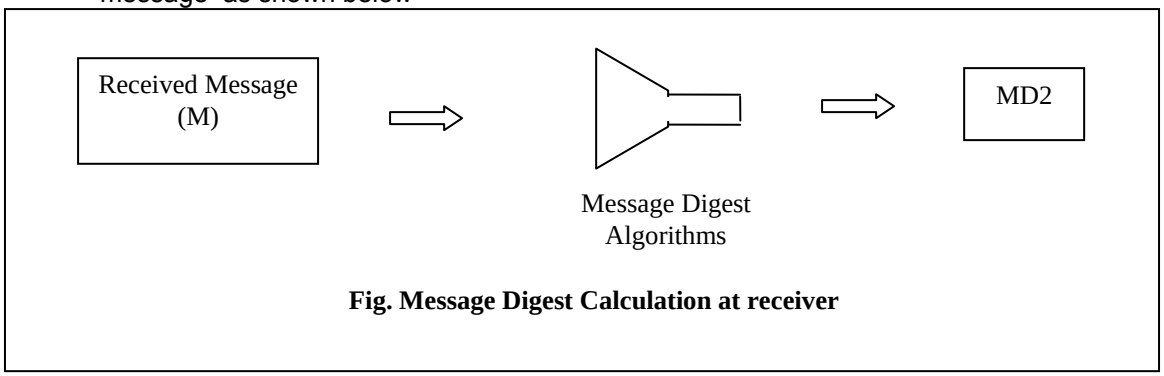


Fig. Message Digest Calculation at receiver

Step V:

- Now receiver uses A's public key to decipher(decrypt) the digital signature
- Output of above step is the original message digest (MD1) calculated by A.

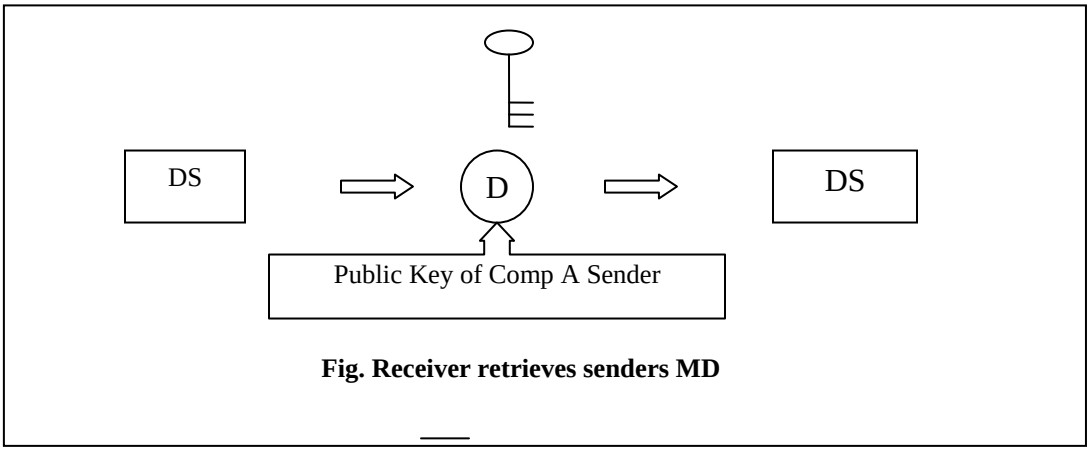


Fig. Receiver retrieves senders MD

Step V:

- ✓ B now compares two message digest i.e. MD2 –calculated in step-4 and MD1- retrieved from A's digital signature in step5
- ✓ If MD1=MD2 then – B accepts original message (M) as the correct unaltered message from A
- ✓ i.e. B is assured/confirmed that message came from A not from someone else posing as A

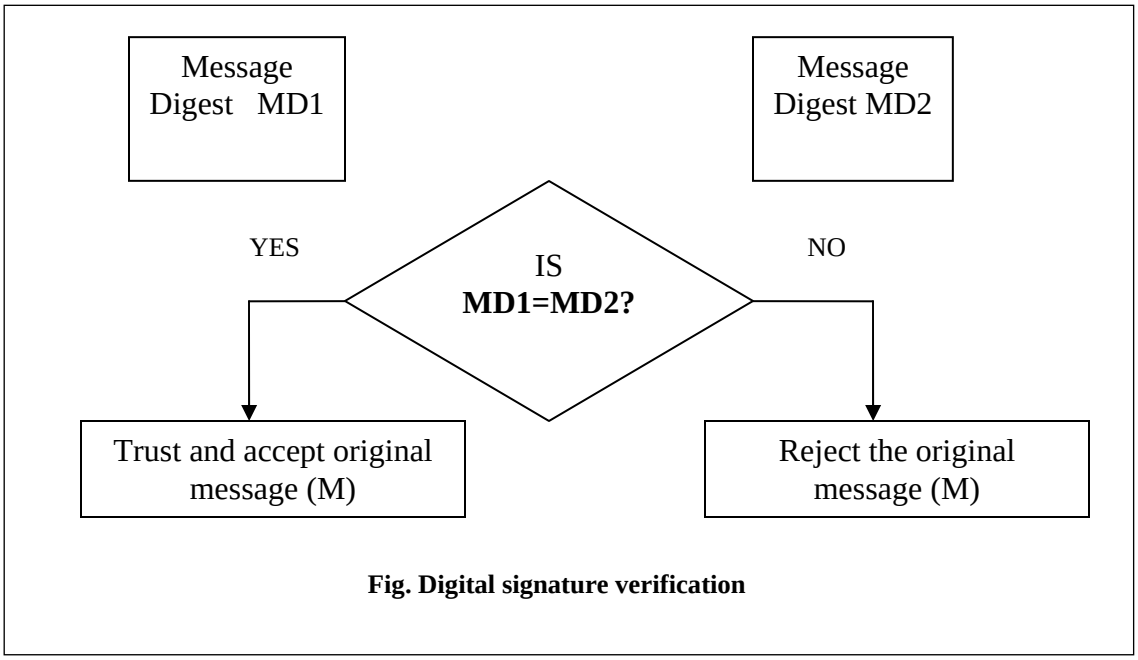


Fig. Digital signature verification

Section-3: 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, 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.

Section-4: Legal recognition of electronic records

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is—
(a) rendered or made available in an electronic form; and
(b) accessible so as to be usable for a subsequent reference.

Section-5: Legal recognition of digital signatures
Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (hen, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

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

Section-6: Use of electronic records and digital signatures in Government and its agencies
(1) 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,
then, notwithstanding anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

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

Section-7: Retention of electronic records
(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if—
(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 despatch or receipt of such electronic record are available in the electronic record: Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

Section-8: Publication of rule, regulation, etc., in Electronic Gazette
Where any law provides that any rule, regulation, order, bye-law, notification or any other matter shall be published in the Official Gazette, then, such requirement shall be deemed to have been satisfied if such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette: Provided that where any rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or Electronic Gazette, the date of publication shall be deemed to be the date of the Gazette which was first published in any form.

Section-9: 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 monetarytransaction in the electronic form.

Section-10: Power to make rules by Central Government in respect of digital signature.
The Central Government may, for the purposes of this Act, by rules, prescribe—
(a) the type of digital signature;
(b) the manner and format in which the digital signature shall be affixed;
(c) the manner or procedure which facilitates identification of the person affixing the digital signature;
(d) control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments; and
(e) any other matter which is necessary to give legal effect to digital signatures.

CHAPTER –6 REGULATION OF CERTIFICATION AUTHORITY (SECTION 17-39)

Appointment of Controller and other Officers.

- The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.
- The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
- The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.
- The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.
- The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.
- There shall be a seal of the Office of the Controller.

FUNCTIONS OF CONTROLLER

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

- Exercising supervision over the activities of the Certifying Authorities;
- Certifying public keys of the Certifying Authorities;
- Laying down the standards to be maintained by the Certifying Authorities;
- Specifying the qualifications and experience which employees of the Certifying Authorities 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 Authorities;
- Specifying the terms and conditions subject to which auditors may 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 regulation of such systems;
- Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
- Resolving any conflict of interests between the Certifying Authorities and the subscribers;
- Laying down the duties of the Certifying Authorities;
- Maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

SECTION –19: RECOGNITION OF FOREIGN CERTIFYING AUTHORITIES.

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

CONTROLLER TO ACT AS REPOSITORY.

The Controller shall be the repository of all Digital Signature Certificates issued under this Act.The Controller shall:

- Make use of hardware, software and procedures that are secure from intrusion and misuse;
- Observe such other standards as may be prescribed by the Central Government, to ensure that the secrecy and security of the digital signatures are assured.

The Controller shall maintain a computerized data base of all public keys in such a manner that such data base and the public keys are available to any member of the public.

LICENSE TO ISSUE DIGITAL SIGNATURE CERTIFICATES.

Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a license to issue Digital Signature Certificates.

No license shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Digital Signature Certificates as may be prescribed by the Central Government

A license granted under this section shall:

- Be valid for such period as may be prescribed by the Central Government;
- Not be transferable or heritable;
- Be subject to such terms and conditions as may be specified by the regulations.

Application for License

Every application for issue of a license shall be in such form as may be prescribed by the Central Government.
Every application for issue of a license shall be accompanied by:

- A certification practice statement;
- A statement including the procedures with respect to identification of the applicant;
- Payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;
- Such other documents, as may be prescribed by the Central Government.

Renewal of License

An application for renewal of a license shall be-

- In such form;
- Accompanied by such fees, not exceeding five thousand rupees,

as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the license.

Procedure for Grant or Rejection of License

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the license or reject the application:

Provided that no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

Suspension of License.

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

- Made a statement in, or in relation to, the application for the issue or renewal of the licence, which is incorrect or false in material particulars;
- Failed to comply with the terms and conditions subject to which the licence was granted;
- Failed to maintain the standards specified under clause (b) of sub-section (2) of section 20;
- Contravened any provisions of this Act, rule, regulation or order made thereunder, revoke the licence:

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

The Controller may, if he has reasonable cause to believe that there is any ground for revoking a licence under sub-section (1), by order suspend such license pending the completion of any inquiry ordered by him:

Provided that no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

No Certifying Authority whose license has been suspended shall issue any Digital Signature Certificate during such suspension.

Notice of Suspension or Revocation of License

Where the license of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the database maintained by him.

Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories:

Provided that the data base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock:

Provided further that the Controller may, if he considers necessary, publish the contents of database in such electronic or other media, as he may consider appropriate.

Power to Delegate

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

Power to Investigate Contraventions

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

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

Access to Computers and Data

Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorised by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this Act, rules or regulations made thereunder has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system.

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

Certifying Authority to follow Certain Procedures.

Every Certifying Authority shall:

- Make use of hardware, software and procedures that are secure from intrusion and misuse;
- Provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
- Adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and
- Observe such other standards as may be specified by regulations.

Certifying Authority to Ensure Compliance of the Act, etc.

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

Display of License

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

Surrender of License.

- Every Certifying Authority whose license is suspended or revoked shall immediately after such suspension or revocation, surrender the license to the Controller.
- Where any Certifying Authority fails to surrender a license under sub-section (1), the person in whose favour a license is issued, shall be guilty of an offence and shall be punished with imprisonment which may extend up to six months or a fine which may extend up to ten thousand rupees or with both.

Disclosure

Every Certifying Authority shall disclose in the manner specified by regulations:

- Its Digital Signature Certificate which contains the public key corresponding to the private key used by that Certifying Authority to digitally sign another Digital Signature Certificate;
- Any certification practice statement relevant thereto;
- Notice of the revocation or suspension of its Certifying Authority certificate, if any; and
- Any other fact that materially and adversely affects either the reliability of a Digital Signature Certificate, which that Authority has issued, or the Authority's ability to perform its services.

Where in the opinion of the Certifying Authority any event has occurred or any situation has arisen which may materially and adversely affect the integrity of its computer system or the conditions subject to which a Digital Signature Certificate was granted, then, the Certifying Authority shall:

- Use reasonable efforts to notify any person who is likely to be affected by that occurrence; or
- Act n accordance with the procedure specified in its certification practice statement to deal with such event or situation.

Digital Signature Certificates

Certifying Authority to issue Digital Signature Certificate.

- Any person may make an application to the Certifying Authority for the issue of a Digital Signature Certificate in such form as may be prescribed by the Central Government
- Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority:

- Provided that while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants'.
- Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.
- On receipt of an application under sub-section

The Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section
After making such enquiries as it may deem fit, grant the Digital Signature Certificate or for reasons to be recorded in writing, reject the application:

Provided that no Digital Signature Certificate shall be granted unless the Certifying Authority is satisfied that:

- The applicant holds the private key corresponding to the public key to be listed in the Digital Signature Certificate;
- The applicant holds a private key, which is capable of creating a digital signature;
- The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant:

Provided further that no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

Representations upon Issuance of Digital Signature Certificate.
A Certifying Authority while issuing a Digital Signature Certificate shall certify that:

- It has complied with the provisions of this Act and the rules and regulations made thereunder,
- It has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;
- The subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate;
- The subscriber's public key and private key constitute a functioning key pair,
- The information contained in the Digital Signature Certificate is accurate; and
- It has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

Suspension of Digital Signature Certificate.
Subject to the provisions of sub-section (1) the Certifying Authority which has issued a Digital Signature Certificate may suspend such Digital Signature Certificate:

On receipt of a request to that effect from -

- The subscriber listed in toe Digital Signature Certificate; or
- Any person duly authorized to act on behalf of that subscriber,

If it is of opinion that the Digital Signature Certificate should be suspended in public interest

A Digital Signature Certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

On suspension of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

Revocation of Digital Signature Certificate.

A Certifying Authority may revoke a Digital Signature Certificate issued by it:

- Where the subscriber or any other person authorized by him makes a request to that effect; or
- Upon the death of the subscriber, or
- Upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section (1), a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time, if it is of opinion that:

- A 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 or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

A Digital Signature Certificate shall 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 shall communicate the same to the subscriber.

Notice of Suspension or Revocation.

Where a Digital Signature Certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the Digital Signature Certificate for publication of such notice.

Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may he. in all such repositories.

Duties of Subscribers

Generating Key Pair.

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

Acceptance of Digital Signature Certificate.

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

- To one or more persons;
- In a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate 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;
- All representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
- (All information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Control of Private Key

- Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorised to affix the digital signature of the subscriber.
- If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by .the regulations.

Explanation.- For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

CYBER CRIME AND OFFENCES:

Cyber crime refers activities done with criminal intent in cyberspace or by using the medium of Internet, Cyber crime could be either criminal activity in the conventional sense or may be activities newly evolved with growth of new medium

- Any offence under law in which an electronic document is involved can be termed generally as a "Cyber Crime". Such an electronic document can be a tool of Crime or an object of Crime.
- The crime can be an "Internet Crime" where a website or an e-mail might be used as a tool or a crime involving a LAN or even a single computer. A Crime using a Mobile or ATM is also generally covered under the term "Cyber Crime" since electronic documents are involved.
- Out of the crimes some crimes come under Information Technology Act 2000 and some may come under other statutes such as IPC.
- For the purpose of determining the jurisdiction of specially designated Cyber Crime Police Stations, offences under ITA 2000 alone may be considered as "Cyber Crime". This is a limited definition.

  eg: A defamatory/threatening message sent through e-mail or SMS is an offence under IPC and not under ITA 2000. If the message is "Obscene" it may be an offence under Section 67 of ITA 2000.

- A Fraud committed using web or e-mail such as the Nigerian Fraud or a Lottery fraud is an offence under IPC and not under ITA 2000.
- Any offence in which an Electronic Document is accessed or altered causing a wrongful harm to some body may be an offence under Section 66 of ITA 2000.
- Various cyber offences are defined in IT ACT, cyber offences(attacks) to be investigated only by a police officer not below the rank of deputy superintendant of police

CYBER OFFENCES:

Tampering with computer source documents – Section 65
Hacking - Section 66
Publishing of information which is obscene in electronic form - Section 67

SECTION 65: TAMPERING COMPUTER SOURCE DOCUMENTS

- Tampering with computer source documents
- Knowingly or intentionally concealing, destroying or altering or intentionally or knowingly causing another to conceal, destroy or alter any computer source code used for computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force

PUNISHMENT FOR TAMPERING COMPUTER SOURCE DOCUMENTS

- Imprisonment up to three years, or with fine, which may extend up to two lakh rupees, or with both.

SECTION 66:HACKING WITH COMPUTER SYSTEM

- Occurs when there is intent to cause or knowledge that one is likely to cause wrongful loss or damage to the public or any person by destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility or affecting it injuriously by any means

PUNISHMENT FOR HACKING

- Imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

SECTION 67: PUBLISHING OF INFORMATION, WHICH IS OBSCENE IN ELECTRONIC FORM

- Publishing or transmitting or causing to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it

PUNISHMENT FOR PUBLISHING OBSCENE INFORMATION IN ELECTRONIC FORM

- **On first conviction -** imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees

- **Second or subsequent conviction -** imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

LIABILITY OF NETWORK SERVICE PROVIDERS

According to section 79 of the IT Act

For 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 there under 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.

Explanation. —For the purposes of this section, —

(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;

This section seeks to restrict the liabilities of a network service provider in certain cases. Let us first understand the term “network service provider” (NSP). Section 79 says that an NSP is an intermediary. The IT Act has defined the term “intermediary”.

According to section 2(1)(w) of the IT Act

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

An NSP, in respect of a particular electronic message, therefore has the following characteristics:

1. It **receives** the message on behalf of another person, or
2. It **stores** the message on behalf of another person, or
3. It **transmits** the message on behalf of another person, or
4. It **provides any service** with respect to that message.

Now let us examine the restrictions on the liabilities of NSPs. An NSP is not liable for any third party information or data made available by him if:

1. The NSP proves that the offence or contravention was committed without his knowledge, or
2. The NSP proves that he had exercised all due diligence to prevent the commission of such offence or contravention.

The important terms used in this section are:
Knowledge implies “clear perception of a fact” or “specific information”.

Liability of ISPs in India

- In respect to ISPs in India, their liabilities are also determined by the **License for Internet Services** based on guidelines dated 24th August 2007.

- The license as applicable on 30th October 2007
- According to **clause 33** of this license:

    1. ISPs must prevent unlawful content, messages or communications from being carried on their network. This includes objectionable, obscene, unauthorized and other content..
    2. Once specific instances of such content are reported to the ISP by the enforcement agencies, they must immediately prevent the carriage of such material on their network.

3. ISPs must ensure that content carried by them does not infringe “international and domestic cyber laws”.
4. The use of ISP networks for anti-national activities would be construed as an offence punishable under the Indian Penal Code or other laws.
5. ISPs are required to comply with the IT Act provisions. They are responsible for any damages arising out of default in this compliance.
6. ISPs must ensure that their networks cannot be used to endanger or make vulnerable a networked infrastructure.
7. ISPs must ensure that their services are not used to break-in or attempt to break-in to Indian networks.
8. ISPs must provide, without any delay, all the tracing facilities to trace nuisance, obnoxious or malicious calls, messages or communications transported through their equipment and network. These tracing facilities are to be provided to authorized officers of Government of India including Police, Customs, Excise, Intelligence Department officers etc.
9. ISPs must provide necessary facilities to the Government to counteract espionage, subversive acts, sabotage or any other unlawful activity.

According to **clause 34** of this license:

1. Government can monitor telecommunication traffic in the ISP network. The ISP has to pay for the necessary hardware and software for this monitoring.
2. ISPs must maintain a log of all users connected and the service they are using (mail, telnet, http etc.). I
3. ISPs must also log every outward login or telnet through their computers. These logs, as well as copies of all the packets originating from the Customer Premises Equipment of the ISP, must be available in real time to the Telecom Authority. ISPs must ensure privacy of communication on their network.
4. ISPs must ensure that unauthorized interception of messages does not take place on their networks.
5. The Government can takeover the service, equipment and networks of ISPs in case of emergency, war etc.
6. The complete and updated list of the ISP’s subscribers must be available in a password protected portion of the ISP’s website. This is for the use of authorized Intelligence Agencies.
7. In case of dedicated line customers, the ISP must maintain logs in the following format:

Customer name	**IP Address allotted**	**Bandwidth provided**	**Address of Installation**	**Date of Installation / Commissioning**	**Contact person with Phone / email**
Bhilai Institute of Technology	221.134.89.235	4 Mbps 1:1 Leased Port	BIT,Bhilai House, Durg	12/4/2003	D. P. Mishra, 9229594625/dpmishra@bitdurg.org

8. The Chief Officer-In-Charge of technical network operations and the Chief Security Officer of the ISP should be a resident Indian citizen.
9. ISP must ensure that the information transacted by the subscribers is secure and protected.

10. The ISP officials dealing with the lawful interception of messages must be resident Indian citizens.
11. The majority Directors on the Board of the ISP must be Indian citizens.
12. Ministry of Home Affairs will regularly do security vetting in case foreigners are holding the positions of the Chairman, Managing Director, Chief Executive Officer (CEO) and/or Chief Financial Officer (CFO) of the ISP.
13. ISPs are required to physically monitor, on a monthly basis, those customers who have a high UDP traffic value. UDP (user datagram protocol) is generally used for transmitting voice, streaming video, IP TV, voice over IP and online games.

The Cyber Regulations Appellate Tribunal (Chapter-10)– This tribunal basically provides an option for an appeal against the order made by the Adjudicating officer. This chapter explains the requirement, establishment, composition, procedures, and powers of Cyber Appellate Tribunal. Also covers issues relating to legal representation, limitation, jurisdiction of civil courts, appeal to high court.

ESTABLISHMENT OF CYBER APPELLATE TRIBUNAL

- The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.
- The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

Composition of Cyber Appellate Tribunal.

A Cyber Appellate Tribunal shall consist of one person only (hereinafter referred to as the Residing Officer of the Cyber Appellate Tribunal) to be appointed, by notification, by the Central Government

Procedure and Powers of the Cyber Appellate Tribunal

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 Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:

- Summoning and enforcing the attendance of any person and examining him on oath;
- Requiring the discovery and production of documents or other electronic records;
- Receiving evidence on affidavits;
- Issuing commissions for the examination of witnesses or documents;
- Reviewing its decisions;
- Dismissing an application for default or deciding it ex pane;
- Any other matter which may be prescribed.

Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

Penalties and Adjudication (Chapter-12) – All criminal activities arising out of the usage of computers and computer networks not only invite imprisonment, but also invite penalties ranging up to whopping one crore. Sections in this chapter explain the activities that invite penalties. Also explained

in this chapter are the roles and responsibilities of the Adjudicating officer, who is nominated to investigate such activities.

Penalty for Damage to Computer, Computer System, etc.

If any person without permission of the owner or any other person who is in charge 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;
- 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 there under;
- Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.
Explanation.- For the purposes of this section:

- "Computer contaminant" means any set of computer instructions that are designed-
- To modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
- By any means to usurp the normal operation of the computer, computer system, or computer network;
- "Computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
- "Computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, daia or instruction is executed or some other event takes place in that computer resource;
- "Damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

Penalty for Failure to Furnish Information Return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to:

- Furnish any document, return or report to the Controller or ?he Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
- File any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

- Maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Residuary Penalty

Whoever contravenes any rules or regulations made under this Act, for .the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

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 there under 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 or award such compensation as he thinks fit in accordance with the provisions of that section.
- 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 oh the Cyber Appellate Tribunal under sub-section (2) of section 58
- 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.

Factors to be taken into Account by the Adjudicating Officer

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely:

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

QUESTIONS:

1. Write a note on the overview of IT ACT-2000 by specifying different chapters, Sections and major sections dealing with crime
2. Give the details of laws amended by IT ACT 2000 with reasons
3. Write a note on the amendments and limitations of IT ACT-2000
4. What is Digital signature? How its created and verified explain with suitable block diagram
5. What is cryptography? Explain its types along with examples
6. Explain the working of RSA algorithm
7. Justify why digital signatures are prepared with private key of subscriber
8. Write a note on e-governance and role of IT ACT associated with it
9. Write a note on following (a) Legal Recognition of e-records and (b) legal recognition of digital signature by giving details of sections responsible
10. How e-records are authenticated, explain the criteria specified for authentication of e-records under section-3
11. Explain section –19 of IT ACT (Legal recognition of CA)
12. Write a note on cyber crimes and offences
13. Explain the liabilities or responsibilities of Network Service Provider (NSP)
14. What is Cyber Regulation Appellate tribunal
15. Write a note on penalties and Adjudication