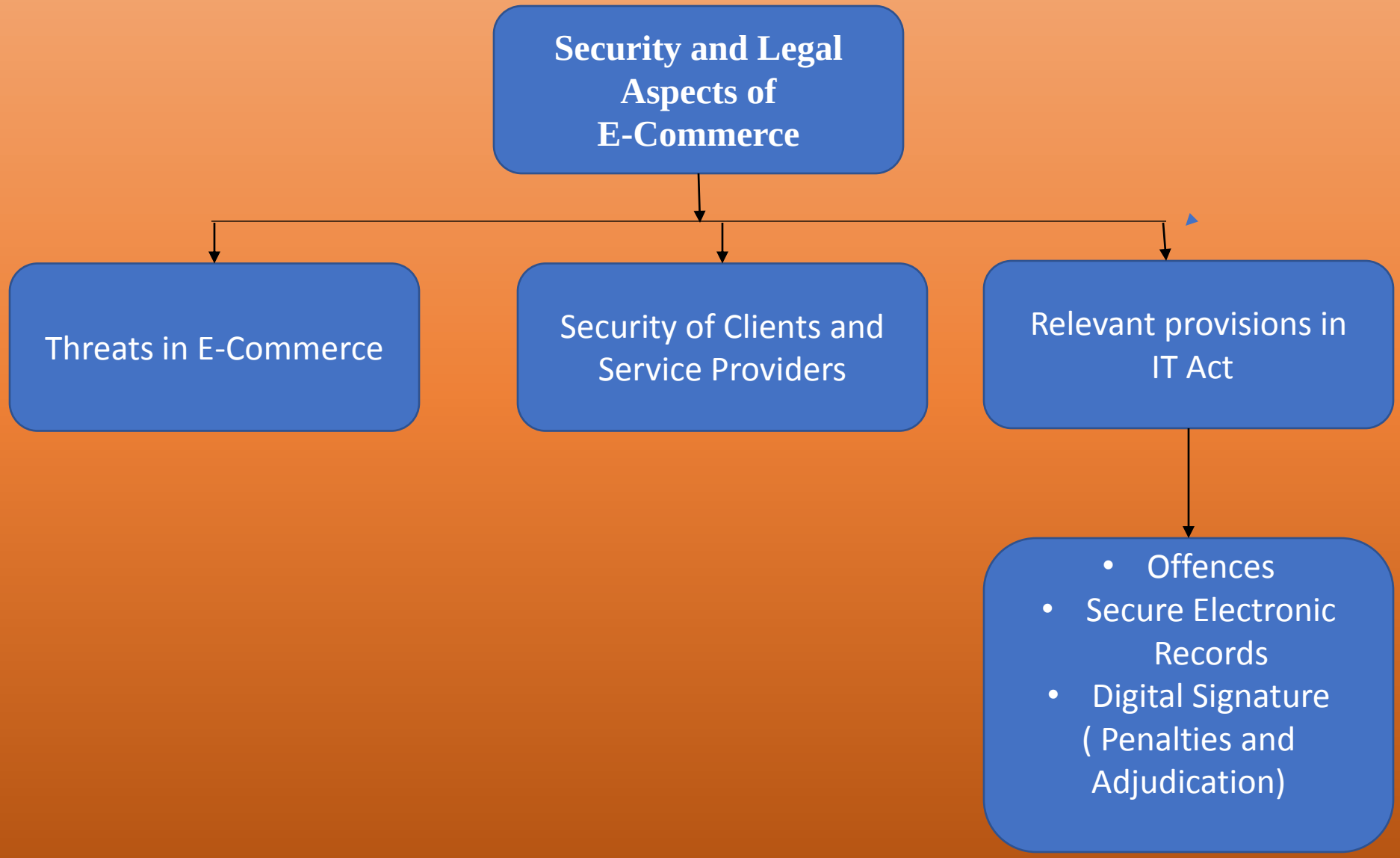
Unit - 5

Security and Legal Aspects of E-Commerce


Security and Legal Aspects of E-Commerce
Threats in E-Commerce
Security of Clients and Service Providers
Relevant provisions in IT Act
Offences
Secure Electronic Records
Digital Signature (Penalties and Adjudication)

Objectives of the IT 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“
- To facilitate electronic filing of documents with Government agencies and E-Payments
- To amend the Indian Penal Code, Indian Evidence Act,1972, the Banker’s Books Evidence Act 1891,Reserve Bank of India Act ,1934
- Aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means.

Objectives

- **Legal Recognition for E-Commerce**
  - Digital Signatures and Regulatory Regime
  - Electronic Documents in place of paper documents

- **E-Governance**
  - Electronic Filing of Documents

- **Amend certain Acts**

- **Define Civil wrongs, Offences, punishments**
  - Investigation, Adjudication
  - Appellate Regime

Security in E-Commerce

Introduction :-

E-Commerce security refers to the principles which guide safe electronic transactions, allowing the buying and selling of goods and services through the Internet, but with protocols in place to provide safety for those involved.

Definition :-

Ecommerce security is a set of protocols that safely guide ecommerce transactions. Stringent security requirements must be in place to protect companies from threats like credit card fraud, or they risk jeopardizing revenue and customer trust, due to the inability to guarantee safe credit card processing.

Threats in E-Commerce

- A threat is anything that can disrupt the operations, functioning, integrity, or availability of a network system.
- A threat is an object, person , or other entity that represents a constant danger to an asset.
- Management must be informed of the various kinds of threats facing the organization.
- By examining each threat category management effectively protects information through policy, education, training and technology.

Type of Threats in E-Commerce

- Secrecy threats
- Wiretapping and integrity threats
- Cyber vandalism
- Spoofing denial of service threats
- Threats from internal employees

Secrecy Threats

- Secrecy is a technical issue that requires sophisticated physical and logical mechanism and focuses on the prevention of unauthorised disclosure of information.
- The privacy of information on internet is threatened by snipper programs. A snipper program provides the means to tap into internet and record information that passes through a particular computer while travelling from source to destination.
- Unauthorised individuals steal personal information (eg., credit card number, name, address, etc.) by recording information packets;
- Snipper programs read, descrypt, and record email transmissions.

Wiretapping and Integrity Threats

- This threat occurs when a message stream of information (e.g., banking transaction) is altered by an unauthorised person.

- Attackers attempt to read stored files, message packets passing by on the network. Other processes , memory, etc.

Cyber Vandalism

- Electronically defacing an existing Web site's page by inserting different content material (which may include offensive pornographic material).
- It is also an example of an integrity violation of the web site contents. Such a violation could cause damage to e-commerce operations through denial of service or loss of trust in the web site.
- Cyber-Vandalism is intentionally disrupting, defacing, or even destroying a site

Spoofing

- Misrepresenting oneself by using fake email addresses or masquerading as someone else.

- Pretending to mimic someone or presenting a fake web site to spoof visitors (e.g., a hacker substitutes their web site address in place of the real one by one by taking advantage of backdoors).

- This type of action can have direct consequences for buyers and sellers using e-commerce sites to transact business

Denial of Service Threats

- Flooding a Web site with useless traffic to inundate and overwhelm the network.
- Distributed Denial of Service attack uses numerous computers to attack the target network from numerous launch points.
- The denial of service attacks may cause a network to shut down, making it impossible for users to access the site. The longer the site is shut down , the more damage is done to a site’s reputation.

Threats from Internal Employees

- Employees with access to sensitive information.
- Sloppy internal security procedures.
- Able to roam throughout an organization’s system without leaving a trace.
- In case of e-commerce sites, the largest disruptions to service, destruction of sites, and diversion of customer credit data and personal information come from trusted insider employees.

Security of Clients and Service Provider

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.

6 dimensions of e-commerce security

1. Integrity: prevention against unauthorized data modification
2. Nonrepudiation: prevention against any one party from reneging on an agreement after the fact
3. Authenticity: authentication of data source
4. Confidentiality: protection against unauthorized data disclosure
5. Privacy: provision of data control and disclosure
6. Availability: prevention against data delays or removal

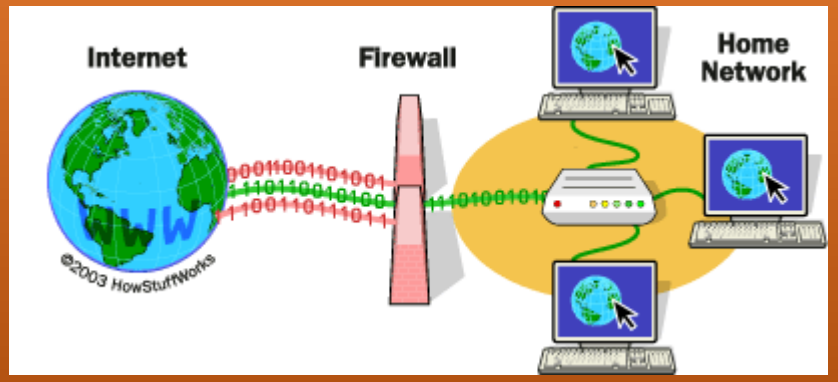
The tools which can be used to protect information and systems against compromise, intrusion and misuse are:

- Firewalls
- Encryption
- Message authentication
- Site blocking
- Operating system controls
- Anti-virus software
- Scanners
- Active monitors
- Behaviour blockers
- Integrity checkers

Firewalls

- A firewall is a software or a hardware combination that is installed in a network to control the packet traffic that moves through it. Companies will place a firewall at the internet entry point of their networks as it provides a defense between a network and the internet.

- All traffic from the inside to outside and from outside to inside the network must pass through it.
- Only authorized traffic, as defined by the local security policy, is allowed to pass through it.
- The firewall itself is immune to penetration.

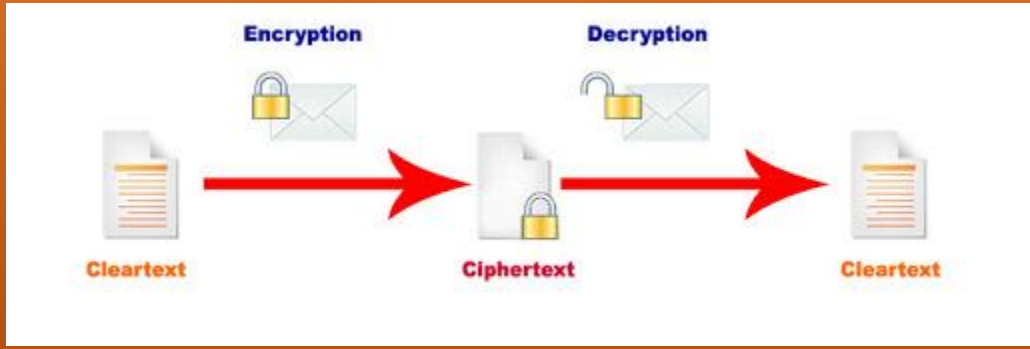


Encryption

- The process of transforming plain text or data into cipher text that cannot be read by anyone outside of the sender and the receiver.
- The purpose of encryption is

  (a) to secure stored information and

  (b) to secure information transmission.
- Cipher text is text that has been encrypted and thus cannot be read by anyone besides the sender and the receiver



Message Authentication

- Protect against active attacks
  - falsification of data
  - eavesdropping
- Message is authentic if it genuine and comes from the alleged source.
- ‘authentication allows received to verify that message is authentic
  - Message has not altered
  - Message is from authentic source
  - Message timeline

Site Blocking

- Site blocking is a software based approach that prohibits access to certain websites that are deemed inappropriate by management.
- It is a process by which a firewall or www proxy prevents users from accessing some network resources.
- For example, sites that contain explicit objectionable material can be blocked by management to prevent employees from accessing these sites from company’s internet servers.

Operating System Controls

- The computer operating systems have a built-in user-name and password requirement.
- This feature of operating system provides a level of authentication.
- If the user is listed in the accesses list for the requested access, the access is allowed, otherwise a protection violation occurs, and the user job is denied access to the file.

Anti-Virus Software

- A virus is a form of software that attaches itself to another program that can cause damage to a host system. A worm is a kind of virus that reproduces itself on computers that it infects. Both of these annoyances moves rapidly through the internet. Antivirus software can detect viruses and worms and can delete them or isolate them on the host computer so they cannot run (ex: Norton, Symantec, McAfee).

Scanners

- The scanners checks or scans the operating system and other application software installed on the hard drives. While scanning, it checks the bit patterns in all software against the bit patterns contained in the virus definition of the scanner. If they are found similar, they are labelled as virus.

Active Monitors

- Active monitors are used to watch what is happening on a system. This is the real time or on-access portion of your virus scanner. If you only use the on-demand scanner you will only detect files once they have been infected.

- It blocks a virus to access the specific portions to which only the operating system has the authorized access.

Behavior Blockers

- A behavior blocker is a type of program that prevents certain actions from being taken. A behavior blocker may prevent a program from writing to the registry, the boot sector, or files. Sometimes behavior blocking technologies are built into programs that have other capabilities as well.

- Blockers can potentially detect a virus at an early stage. Most hardware-based antivirus mechanisms are based on the concept

Integrity Checkers

- Integrity checking products work by reading your entire disk and recording integrity data that acts as a signature for the files and system sectors. An integrity check program with built-in intelligence is the only solution that can handle **all** the threats to your data as well as viruses. Integrity checkers also provide the only reliable way to discover what damage a virus has done.

- **Integrity checking** is the process of comparing the current state of stored data and/or programs to a previously recorded state in order to detect any changes (and so it sometimes called change detection).

Digital Signature and Electronic Signature

- An electronic and Digital Signatures
- Authenticates the identity of the sender of a message, or the signer of a document,
- Or ensures that the contents of a message are intact.

- Digital Signatures features:
- Are easily transportable,
- Cannot be imitated by someone else,
- And can be automatically time-stamped

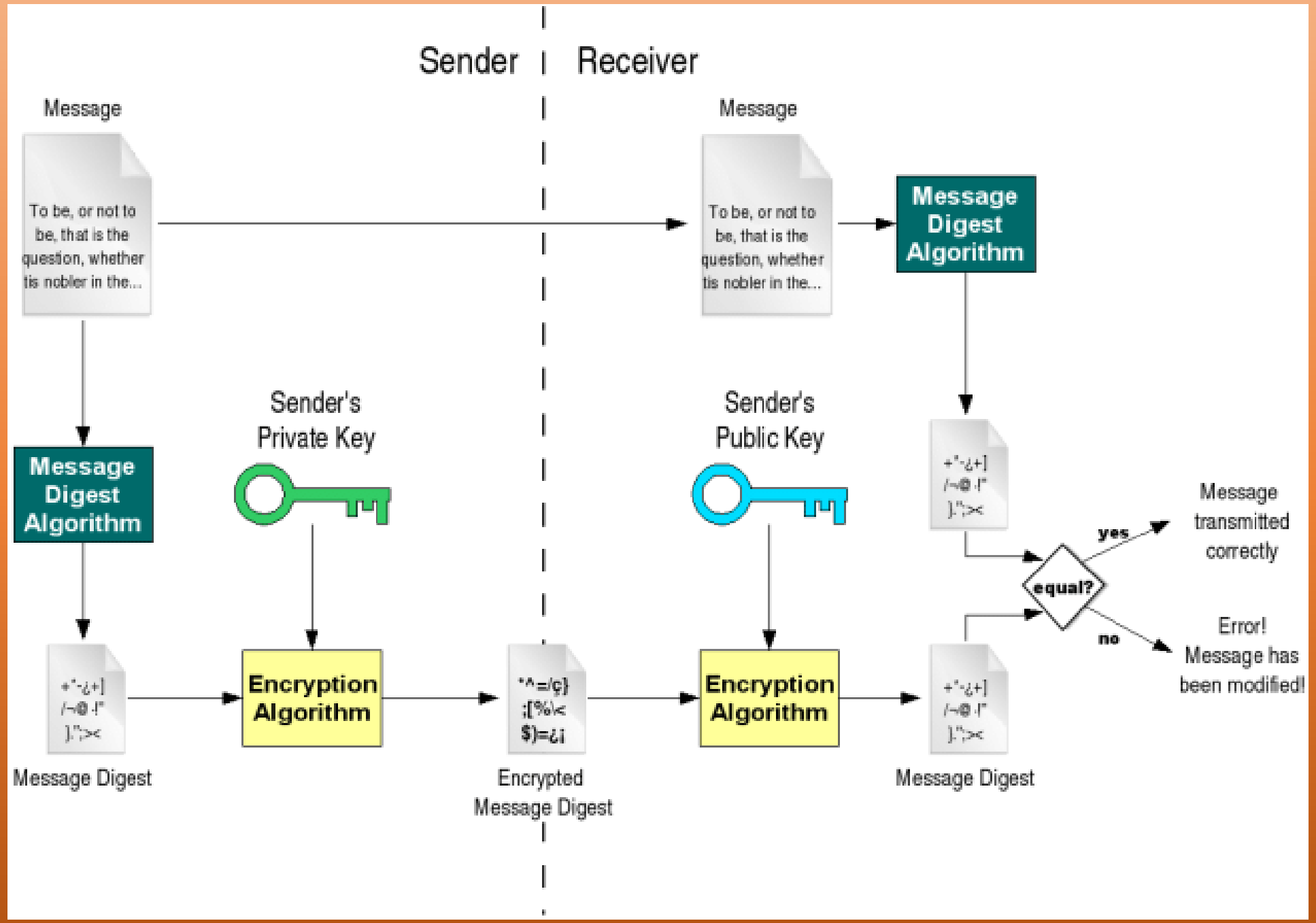
- The ability to ensure that the original signed message arrived means that :

the sender can not easily repudiate it later.

Digital signature – how?

Bind the message originator with the exact contents of the message

–A hash function is used to transform messages into a 128-bit digest (message digest).
–The sender’s private key is used to encrypt the message digest (digital signature)
–The message + signature are sent to the receiver
–The recipient uses the hash function to recalculate the message digest
–The sender’s public key is used to decrypt the message digest
–Check to see if the recalculated message digest = decrypted message digest


Sender
Receiver
Message
To be, or not to be, that is the question, whether tis nobler in the...
Message
To be, or not to be, that is the question, whether tis nobler in the...
Message Digest Algorithm
Message Digest Algorithm
Sender's Private Key
Sender's Public Key
+˚-¿+|
/¬@·!"
].";><
Encryption Algorithm
*^=/ç}
;[%\<
$)=¿i
Encryption Algorithm
+˚-¿+|
/¬@·!"
].";><
+˚-¿+|
/¬@·!"
].";><
equal?
yes
no
Message transmitted correctly
Error! Message has been modified!
Message Digest
Encrypted Message Digest
Message Digest

AUTHENTICATION OF ELECTRONIC RECORDS

The Act provides that the authentication of the electronic record can be effected by the use of asymmetric crypto system and **hash** function which envelop and transform the initial electronic record into another electronic record.

A "hash function" is an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known 'as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

- To derive or reconstruct the original electronic record from the hash result produced by the algorithm;
- That two different electronic records can produce the same hash result using the algorithm.

The record can be accessed by the use of public key of the subscriber. The private key and the public key are unique to the subscriber and constitute a functioning key pair.

SECTION 3A - AUTHENTICATION OF ELECTRONIC RECORDS BY USE OF ELECTRONIC SIGNATURE.

- A subscriber can authenticate any electronic record by such an electronic signature or an electronic authentication technique which is considered reliable and may be specified in the schedules. In order for the electronic signature to be reliable
- The signature creation data or authentication data are, within the context they are used, linked to the signatory, or as the case may be, the authenticator and to no other person;
- The signature creation data or authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and to no other person;
- Any alteration to the electronic signature made after affixing such signature is detectable.
- Any alteration to the information made after its authentication by electronic signature is detectable.
- It fulfills other prescribed conditions.

Legal Recognition of Digital Signatures

- Acceptance of contract expressed by electronic means
- e-Commerce and Electronic Data interchange
- e-Governance
- Electronic filing of documents
- Retention of documents in electronic form
- Uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records or documents
- Publication of official gazette in the electronic form
- Interception of any message transmitted in the electronic or encrypted form

SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURES

- **SECTION 14 - SECURE ELECTRONIC RECORD**

  Where any security procedure is applied to an electronic record, at a specific point of time, then from such point onwards up to the time of verification, the record is deemed to be a secure electronic record.

- **SECTION 15 - SECURE ELECTRONIC SIGNATURE**

  An electronic signature is unique to the subscriber. Once the signature is affixed to an electronic record it can be used to identify the subscriber. It is presumed to be under the exclusive control of the subscriber. The signature signifies the time when it is affixed to an electronic record and the manner in which the signature was created. If any one tries to alter such a signed electronic record, then the signature gets invalidated. An electronic signature will be deemed to be secure if it can be proved that, it was under the exclusive control of the signatory at the time of affixing and the signature data (private key) was stored and affixed in the specified manner.

Civil Offences Under IT Act, 2000

Section	Offence	Punishment
43	Damage to Computer, Computer system etc	Compensation to the tune of Rs.1 crore to the affected person
43A	Compensation for failure to protect data	Not exceeding five crores rupees, to the person so affected
44(a)	Furnish any document, return or report to the controller or the certifying authority	Penalty not excedding one lakh and fifty thousand rupees for each such failure
44(b)	For failing to file any return or furnish any information or other doument within the prescribed time	Penalty not excedding five thousand rupees for every day during such failure continues
44(c)	For not maintaining books of account or records	Penalty not excedding ten thousand rupees for every day during such failure continues
45	Offences for which no penalty is separately provided	Compensation not exceeding twenty five thousand rupees to the affected person or a penalty not exceeding twenty five thousand rupees

The various offences and corresponding punishments are summarized and tabulated below with detailed explanation in the following paragraphs.

Section	Contents	Imprisonment Up to	Fine Up to
65	Tampering with computer source code documents	3 years or/and	2,00,000
66	Hacking with computer system dishonestly or fraudulently	3 years or/and	5,00,000
66B	receiving Stolen computer resource	3 years or/and	1,00,000
66C	Identity Theft - fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person	3 years and	1,00,000
66D	cheating by Personation by using computer resource	3 years and	1,00,000
66E	Violation of Privacy	3 years or/and	2,00,000

Section	Contents	Imprisonment Up to	Fine Up to
66F	Whoever,- A. with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by – 1. Denial of Access 2. Attempting to Penetrate computer resource 3. Computer containment B. knowingly or intentionally penetrates and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations, or likely to cause injury to the interests of the sovereignty and integrity of India	Imprisonment for Life	
67	Publish or transmit Obscene material - 1st time Subsequent Obscene in elec. Form	3 years and 5 years and	5,00,000 10,00,000
67A	Publishing or transmitting material containing Sexually Explicit Act - 1st time Subsequent	5 years and 7 years and	10,00,000 10,00,000

Section	Contents	Imprisonment Up to	Fine Up to
67B	Publishing or transmitting material containing Children in Sexually Explicit Act - 1st time	5 years and	10,00,000
	Subsequent	7 years and	10,00,000
67C	Contravention of Retention or preservation of information by intermediaries	3 years and	Not Defined
68	Controller's directions to certifying Authorities or any employees failure to comply knowingly or intentionally	2 years or/and	1,00,000
69	Failure to comply with directions for Intercepting, monitoring or decryption of any info transmitted through any computer system/network	7 Years and	Not Defined
69A	Failure to comply with directions for Blocking for Public Access of any information through any computer resource	7 Years and	Not Defined
69B	Failure to comply with directions to Monitor and Collect Traffic Data	3 Years and	Not Defined
70	Protected system. Any unauthorised access to such system	10 years and	Not Defined
70B (7)	Failure to provide information called for by the *I.C.E.R.T or comply with directions	I year or	1,00,000

Section	Contents	Imprisonment Up to	Fine Up to
71	Penalty for Misrepresentation or suppressing any material fact	2 years or/and	1,00,000
72	Penalty for breach of confidentiality and privacy of el. records, books, info., etc without consent of person to whom they belong.	2 years or/and	1,00,000
72A	Punishment for Disclosure of information in breach of lawful contract	3 years or/and	5,00,000
73	Penalty for publishing False Digital Signature Certificate	2 years or/and	1,00,000
74	Fraudulent Publication	2 years or/and	1,00,000
75	Act also to apply for offences or contravention committed outside India if the act or conduct constituting the offence involves a computer, computer system or computer network located in India		
76	Confiscation of any computer, computer system, floppies, CDs, tape drives or other accessories related thereto in contravention of any provisions of the Act, Rules, Regulations or Orders made.		
77	Penalty and Confiscation shall not interfere with other punishments provided under any law.		
78	Power to investigate offences by police officer not below rank of Dy. Superintendent of Police.		