**FUNDAMENTAL OF E-COMMERCE**

**UNIT-5**

**BBA- N (606)**

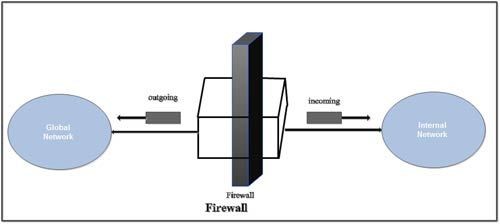
**FIREWALLS AND DATABASE RECOVERY**

A firewall is a device installed between the internet network of an organization and the rest of Internet. When a computer is connected to Internet, it can create many problems for corporate companies. Most companies put a large amount of confidential information online. Such information should not be disclosed to the unauthorized persons. Second problem is that the virus, worms and other digital pests can breach the security and can destroy the valuable data.

The main purpose of a firewall is to separate a secure area from a less secure area and to control communications between the two. Firewall also controlling inbound and outbound communications on anything from a single machine to an entire network.

On the Other Hand Software firewalls, also sometimes called personal firewalls, are designed to run on a single computer. These are most commonly used on home or small office computers that have broadband access, which tend to be left on all the time.

A software firewall prevents unwanted access to the computer over a network connection by identifying and preventing communication over risky ports. Computers communicate over many different recognized ports, and the firewall will tend to permit these without prompting or alerting the user.



**A firewall can serve the following functions:**

1. Limit Internet access to e-mail only, so that no other types of information can pass between the intranet and the Internet

2. Control who can telnet into your intranet (a method of logging in remotely

3. Limit what other kinds of traffic can pass between your intranet and the Internet.

A firewall can be simple or complex, depending on how specifically you want to control your Internet traffic. A simple firewall might require only that you configure the software in the router that connects your intranet to your ISP. A more complex firewall might be a computer running UNIX and specialized software.

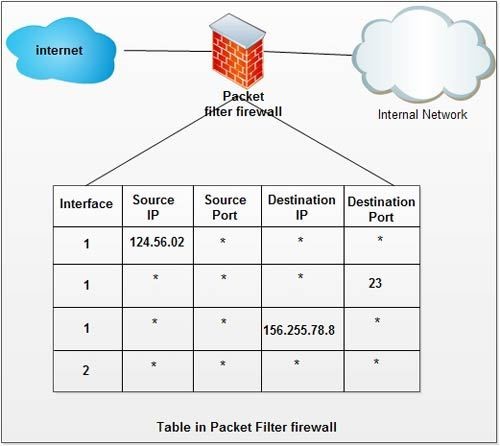
**Firewall systems fall into two categories:**

* Network-level
* Application-level

### ****Network-Level Firewalls****

It can be used as packet filter. These firewalls examine only the headers of each packet of information passing to or from the Internet. The firewall accepts or rejects packets based on the packet’s sender, receiver, and port. For example, the firewall might allow e-mail and Web packets to and from any computer on the intranet, but allow telnet (remote login) packets to and from only selected computers.

Packet filter firewall maintains a filtering table that decides which packets are to be forwarded or discarded. A packet filter firewall filters at the network or transport layer.



As shown in fig. the packets are filtered according to following specifications:

1. Incoming packets from network 124.56.0.2 are block (\* means any).
2. Incoming packets destined for any internal TELNET server (port 23) are blocked.
3. Incoming packets for internal host 156.255.7.8.8 are blocked.
4. Outgoing packets destined for an HTTP server (port 80) are blocked i.e. employees of organization are not allowed to browse the internet and cannot send any HTTP request.

### ****Application-Level Firewalls****

These firewalls handle packets for each Internet service separately, usually by running a program called a proxy server, which accepts e-mail, Web, chat, newsgroup, and other packets from computers on the intranet, strips off the information that identifies the source of the packet, and passes it along to the Internet.

When the replies return, the proxy server passes the replies back to the computer that sent the original message. A proxy server can also log all the packets that pass by, so that you have a record of who has access to your intranet from the Internet, and vice versa.

### ****Database Recovery:****

* **Crash Recovery**

DBMS is a highly complex system with hundreds of transactions being executed every second. The durability and robustness of a DBMS depends on its complex architecture and its underlying hardware and system software. If it fails or crashes amid transactions, it is expected that the system would follow some sort of algorithm or techniques to recover lost data.

* **Failure Classification**

To see where the problem has occurred, we generalize a failure into various categories, as follows −

* **Transaction failure**

A transaction has to abort when it fails to execute or when it reaches a point from where it can’t go any further. This is called transaction failure where only a few transactions or processes are hurt.

Reasons for a transaction failure could be:

* **Logical errors:** Where a transaction cannot complete because it has some code error or any internal error condition.
* **System errors:** Where the database system itself terminates an active transaction because the DBMS is not able to execute it, or it has to stop because of some system condition. For example, in case of deadlock or resource unavailability, the system aborts an active transaction.

#### System Crash

There are problems − external to the system − that may cause the system to stop abruptly and cause the system to crash. For example, interruptions in power supply may cause the failure of underlying hardware or software failure.

Examples may include operating system errors.

**Disk Failure**

In early days of technology evolution, it was a common problem where hard-disk drives or storage drives used to fail frequently.

Disk failures include formation of bad sectors, unreachability to the disk, disk head crash or any other failure, which destroys all or a part of disk storage.

**Storage Structure**

We have already described the storage system. In brief, the storage structure can be divided into two categories −

* **Volatile storage**− As the name suggests, a volatile storage cannot survive system crashes. Volatile storage devices are placed very close to the CPU; normally they are embedded onto the chipset itself. For example, main memory and cache memory are examples of volatile storage. They are fast but can store only a small amount of information.
* **Non-volatile storage**− These memories are made to survive system crashes. They are huge in data storage capacity, but slower in accessibility. Examples may include hard-disks, magnetic tapes, flash memory, and non-volatile (battery backed up) RAM.

**Recovery and Atomicity**

When a system crashes, it may have several transactions being executed and various files opened for them to modify the data items. Transactions are made of various operations, which are atomic in nature. But according to ACID properties of DBMS, atomicity of transactions as a whole must be maintained, that is, either all the operations are executed or none.

When a DBMS recovers from a crash, it should maintain the following −

* It should check the states of all the transactions, which were being executed.
* A transaction may be in the middle of some operation; the DBMS must ensure the atomicity of the transaction in this case.
* It should check whether the transaction can be completed now or it needs to be rolled back.
* No transactions would be allowed to leave the DBMS in an inconsistent state.

There are two types of techniques, which can help a DBMS in recovering as well as maintaining the atomicity of a transaction −

* Maintaining the logs of each transaction, and writing them onto some stable storage before actually modifying the database.
* Maintaining shadow paging, where the changes are done on a volatile memory, and later, the actual database is updated.

**Log-based Recovery**

Log is a sequence of records, which maintains the records of actions performed by a transaction. It is important that the logs are written prior to the actual modification and stored on a stable storage media, which is failsafe.

Log-based recovery works as follows:

* The log file is kept on a stable storage media.
* When a transaction enters the system and starts execution, it writes a log about it.

<Tn, Start>

* When the transaction modifies an item X, it write logs as follows −

<Tn, X, V1, V2>

It reads Tn has changed the value of X, from V1 to V2.

* When the transaction finishes, it logs −

<Tn, commit>

**The database can be modified using two approaches:**

* **Deferred database modification:** All logs are written on to the stable storage and the database is updated when a transaction commits.
* **Immediate database modification:** Each log follows an actual database modification. That is, the database is modified immediately after every operation.

**Recovery with Concurrent Transactions**

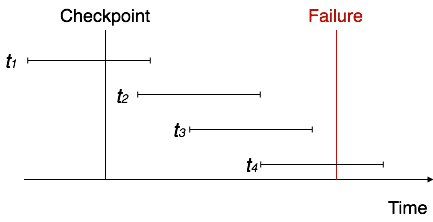
When more than one transaction are being executed in parallel, the logs are interleaved. At the time of recovery, it would become hard for the recovery system to backtrack all logs, and then start recovering. To ease this situation, most modern DBMS use the concept of ‘checkpoints’.

#### Checkpoint

Keeping and maintaining logs in real time and in real environment may fill out all the memory space available in the system. As time passes, the log file may grow too big to be handled at all. Checkpoint is a mechanism where all the previous logs are removed from the system and stored permanently in a storage disk. Checkpoint declares a point before which the DBMS was in consistent state, and all the transactions were committed.

#### Recovery

When a system with concurrent transactions crashes and recovers, it behaves in the following manner:



* The recovery system reads the logs backwards from the end to the last checkpoint.
* It maintains two lists, an undo-list and a redo-list.
* If the recovery system sees a log with <Tn, Start> and <Tn, Commit> or just <Tn, Commit>, it puts the transaction in the redo-list.
* If the recovery system sees a log with <Tn, Start> but no commit or abort log found, it puts the transaction in undo-list.

All the transactions in the undo-list are then undone and their logs are removed. All the transactions in the redo-list and their previous logs are removed and then redone before saving their logs.

# Security issues of e-commerce: E-locking

An electronic lock (or electric lock) is a locking device which operates by means of electric current. Electric locks are sometimes stand-alone with an electronic control assembly mounted directly to the lock. Electric locks may be connected to an access control system, the advantages of which include: key control, where keys can be added and removed without re-keying the lock cylinder; fine access control, where time and place are factors; and transaction logging, where activity is recorded. Electronic locks can also be remotely monitored and controlled, both to lock and to unlock.

**Authentication methods**

A feature of electronic locks is that the locks can deactivated or opened by authentication, without the use of a traditional physical key:

**Numerical codes, passwords, and passphrases**

Perhaps the most common form of electronic lock uses a keypad to enter a numerical code or password for authentication. Some feature an audible response to each press. Combination lengths are usually between four and six digits long.

**Security tokens**

Another means of authenticating users is to require them to scan or “swipe” a security token such as a smart card or similar, or to interact a token with the lock. For example, some locks can access stored credentials on a personal digital assistant (PDA) or smartphone, by using infrared, Bluetooth, or NFC data transfer methods.

**Biometrics**

As biometrics become more and more prominent as a recognized means of positive identification, their use in security systems increases. Some electronic locks take advantage of technologies such as fingerprint scanning, retinal scanning, iris scanning and voice print identification to authenticate users.

**RFID**

Radio-frequency identification (RFID) is the use of an object (typically referred to as an “RFID tag”) applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader. This technology is also used in some modern electronic locks.

# Basics of Encryption and Decryption

### ****ENCRYPTION****

In computing, encryption is the method by which plaintext or any other type of data is converted from a readable form to an encoded version that can only be decoded by another entity if they have access to a decryption key. Encryption is one of the most important methods for providing data security, especially for end-to-end protection of data transmitted across networks.

Encryption is widely used on the internet to protect user information being sent between a browser and a server, including passwords, payment information and other personal information that should be considered private. Organizations and individuals also commonly use encryption to protect sensitive data stored on computers, servers and mobile devices like phones or tablets.

### ****Benefits of Encryption****

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the internet or any other computer network. A number of organizations and standards bodies either recommend or require sensitive data to be encrypted in order to prevent unauthorized third parties or threat actors from accessing the data. For example, the Payment Card Industry Data Security Standard requires merchants to encrypt customers’ payment card data when it is both stored at rest and transmitted across public networks.

Modern encryption algorithms also play a vital role in the security assurance of IT systems and communications as they can provide not only confidentiality, but also the following key elements of security:-

* **Authentication:** The origin of a message can be verified.
* **Integrity:** Proof that the contents of a message have not been changed since it was sent.
* **Non-repudiation:** The sender of a message cannot deny sending the message.

### ****Types of Encryption****

**(1) Symmetric key / Private key**

In symmetric-key schemes, the encryption and decryption keys are the same. Communicating parties must have the same key in order to achieve secure communication.

**(2) Public key**

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key that enables messages to be read, Public-key encryption was first described in a secret document in 1973;, before, then all encryption schemes were symmetric-key (also called private-key).

### ****DECRYPTION****

The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

One of the reasons for implementing an encryption-decryption system is privacy. As information travels over the Internet, it is necessary to scrutinise the access from unauthorized organizations or individuals. Due to this, the data is encrypted to reduce data loss and theft. Few common items that are encrypted include text files, images, e-mail messages, user data and directories. The recipient of decryption receives a prompt or window in which a password can be entered to access the encrypted data. For decryption, the system extracts and converts the garbled data and transforms it into words and images that are easily understandable not only by a reader but also by a system. Decryption can be done manually or automatically. It may also be performed with a set of keys or passwords.

There are many methods of conventional cryptography, one of the most important and popular method is Hill cipher Encryption and Decryption, which generates the random Matrix and is essentially the power of security. Decryption requires inverse of the matrix in Hill cipher. Hence while decryption one problem arises that the Inverse of the matrix does not always exist. If the matrix is not invertible then the encrypted content cannot be decrypted. This drawback is completely eliminated in the modified Hill cipher algorithm. Also this method requires the cracker to find the inverse of many square matrices which is not computationally easy. So the modified Hill-Cipher method is both easy to implement and difficult to crack.

# The Information Technology Act, 2000- Definition/Intro

### Salient Features of I.T Act

The salient features of the I.T Act are as follows:

* 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.
* It 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.
* It 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.

### Scheme of I.T Act

The following points define the scheme of the I.T. Act:

* The I.T. Act contains **13 chapters**and **90 sections**.
* The last four sections namely sections 91 to 94 in the I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers’ Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.
* It commences with Preliminary aspect in Chapter 1, which deals with the short, title, extent, commencement and application of the Act in Section 1. Section 2 provides Definition.
* Chapter 2 deals with the authentication of electronic records, digital signatures, electronic signatures, etc.
* Chapter 11 deals with offences and penalties. A series of offences have been provided along with punishment in this part of The Act.
* Thereafter the provisions about due diligence, role of intermediaries and some miscellaneous provisions are been stated.
* The Act is embedded with two schedules. The First Schedule deals with Documents or Transactions to which the Act shall not apply. The Second Schedule deals with electronic signature or electronic authentication technique and procedure. The Third and Fourth Schedule are omitted.

### Application of the I.T Act

As per the sub clause (4) of Section 1, nothing in this Act shall apply to documents or transactions specified in First Schedule. Following are the documents or transactions to which the Act shall not apply −

* **Negotiable Instrument**(Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
* A **power-of-attorney**as defined in section 1A of the Powers-of-Attorney Act, 1882;
* A **trust**as defined in section 3 of the Indian Trusts Act, 1882;
* A **will**as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition;
* Any **contract**for the sale or conveyance of immovable property or any interest in such property;
* Any such class of documents or transactions as may be notified by the Central Government.

### 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.

### Intermediary Liability

Intermediary, dealing with any specific electronic records, is a person who on behalf of another person accepts, stores or transmits that record or provides any service with respect to that record.

According to the above mentioned definition, it includes the following:

* Telecom service providers
* Network service providers
* Internet service providers
* Web-hosting service providers
* Search engines
* Online payment sites
* Online auction sites
* Online market places and cyber cafes

### 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.

# Cryptography, Public key and Private key Cryptography

### ****CRYPTOGRAPHY****

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.

Cryptography, or cryptology, is the practice and study of hiding information. It is sometimes called code, but this is not really a correct name. It is the science used to try to keep information secret and safe. Modern cryptography is a mix of mathematics, computer science, and electrical engineering. Cryptography is used in ATM (bank) cards, computer passwords, and shopping on the internet.

Different types of cryptography can be easier or harder to use and can hide the secret message better or worse. Ciphers use a “key” which is a secret that hides the secret messages. The cryptographic method needn’t be secret. Various people can use the same method but different keys, so they cannot read each other’s messages. Since the Caesar cipher has only as many keys as the number of letters in the alphabet, it is easily cracked by trying all the keys. Ciphers that allow billions of keys are cracked by more complex methods.

**Modern cryptography concerns itself with the following four objectives:-**

**(1) Confidentiality:-**The information cannot be understood by anyone for whom it was unintended.

**(2) Integrity:-** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

**(3) Non-repudiation:-** The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

**(4) Authentication:-** The sender and receiver can confirm each other?s identity and the origin/destination of the information.

**TYPES OF CRYPTOGRAPHY**

**(1) Public Key Cryptography**

Public key cryptography, or asymmetrical cryptography, is any cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner.

This accomplishes two functions: authentication, where the public key verifies a holder of the paired private key sent the message, and encryption, where only the paired private key holder can decrypt the message encrypted with the public key.

In a public key encryption system, any person can encrypt a message using the receiver’s public key. That encrypted message can only be decrypted with the receiver’s private key. To be practical, the generation of a public and private key -pair must be computationally economical. The strength of a public key cryptography system relies on the computational effort (work factor in cryptography) required to find the private key from its paired public key. If so, effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

**(2) Private key cryptography**

In cryptography, a private key (secret key) is a variable that is used with an algorithm to encrypt and decrypt code. Quality encryption always follows a fundamental rule: the algorithm doesn’t need to be kept secret, but the key does. Private keys play important roles in both symmetric and asymmetric cryptography.

Most cryptographic processes use symmetric encryption to encrypt data transmissions but use asymmetric encryption to encrypt and exchange the secret key. Symmetric encryption, also known as private key encryption, uses the same private key for both encryption and decryption. The risk in this system is that if either party loses the key or the key is intercepted, the system is broken and messages cannot be exchanged securely.