5.1 INTRODUCTION (Security thread)

Security threats to a system can be classified as :

(1) Physical threats (2) Accidental error

(3) Unauthorized access (4) Malicious misuse

The malicious misuse is any form of tampering or alteration of the computer system including generation of illegal codes to alter the standard codes of the system. We will be discussing such type of threats in detail in this chapter.

- An *attack* is an act that takes advantage of a vulnerability to compromise a controlled system.
- It is accomplished by a *threat agent* that damages or steals an organization's information or physical asset.
- *Vulnerability* is an identified weakness in a controlled system, whose controls are not present or are no longer effective.

- Attack is said to have taken place when a specific act or action comes into play and may cause a potential loss.

5.2 MALICIOUS SOFTWARE

- Computer software is termed "*malicious*" (meaning bad intention) when it has been written with an intention to harm, disrupt or circumvent computer systems and network functions.
- The malicious software attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
- Malicious software is used for two types of attacks :
  (i) Software or code that causes access violations. Here the code deletes, steals, alters or executes unauthorized files.
  (ii) Here the code enables denial of service attack where the genuine user is prevented from using the system.
- Malicious software can be divided into two categories :
  (i) *Parasitic* : These need a host program like application program, utility or system program. Such type of malware cannot exist independently. For example, viruses, logic bombs and backdoors.
  (ii) *Independent* : These are self-contained program that can be scheduled and run by the operating system. Examples are worms and bot programs.
- The most dangerous malicious software attack is the polymorphic or multivector worm. These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

Attack Replication Vectors

Following are the various types of replication vectors associated with malicious software which are made use of in attacks :

(1) *IP scan and Attack* : The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers.

(2) *Web browsing* : If the infected system has *write* access to any Web pages, it makes all Web content files (.html, .asp, .cgi and others) infectious, so that users who browse to those pages become infected.

(3) *Virus* : Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.

(4) *Unprotected shares* : Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.

(5) *Mass Mail* : By sending e-mail infections to addresses found in the address book, the infected machine infects many users, whose mail -reading programs also automatically run the program and infect other systems.

ple Network Management Protocol (SNMP) : By using the widely known
non passwords that were employed in early versions of this protocol, the
ng program can gain control of the device. Most vendors have closed these
erabilities with software upgrades.

5.3 VIRUSES

- Computer virus is a software program designed to infect and damage a computer system, network or other programs.
- Through its instructional code, the virus can make copies of itself. In this way it can spread from one system to another. The various methods by which a virus can get into a system are through :
  (i) infected floppy disks.
  (ii) an e-mail attachment infected with virus.
  (iii) downloading software already infected with the virus.
- Virus can erase data on our computers, encrypt files, delete directory structures, prohibit us from using our own computer, send files stored on our computer to contacts in our address book without our knowledge and so on.
- Symptoms are virus infection are :
  (i) Launch process of an application or a program gets slow.
  (ii) System gets to shutdown or restart mode automatically.
  (iii) Files either appear or disappear.
  (iv) Size of the installed program gets changed automatically.
  (v) Interface of applications or programs might get change.
  (vi) Access to drivers is restricted.
- A few methods of protecting against virus attack are :
  (i) Install anti-virus software and update it regularly.
  (ii) Regularly backup systems after they have been scanned for virus and are considered clean from virus infection.
  (iii) E-mail attachments should not be opened directly. Preferably we should use a document viewer to read received documents.

5.3-1 TYPES OF VIRUSES

Different types of virus can be classified as :

(1) *Polymorphic virus* : It is a virus that changes its characteristics with each infection. Hence it is more difficult to detect. Examples of this type of virus are Stimulate, Cascade, Involuntary, Virus 101 etc.

(2) *Boot sector virus* : these virus infect a hard-drive's master boot record. The virus is then loaded into memory whenever the system starts or is rebooted. Examples are Stone, Disk Killer, Form and Michelangelo.

nts are

...itic virus : A parasitic virus attaches itself to a file in order to ... generally keeps most of the file intact and either adds itself to the start or ...e file. COM and EXE files are easiest to infect as they are simply loaded ...y into memory and execution always starts at the first instruction.

(4) ***Stealth virus*** : This virus hides its track after infecting the computer. Once the computer has been infected, the virus can make modifications to allow the computer to appear that it has not lost any memory and/or that the file size has not changed. Examples are Joshi, whale, Frodo etc.

(5) ***Multipartite virus*** : These virus are a combination of a boot sector virus and a file virus. It has the ability to infect in multiple ways. It provides harm to a system in such a way that it infects boot sector and executable files. Hence virus eradication must deal with all the possible sites of infection.

5.4 WORMS

- A worm is a malicious program that replicates itself constantly, without requiring another program to provide a safe environment for replication.
- Worm usually perform malicious actions such as using up the computer's resources and possibly shutting the system down.
- Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.
- Worms use parts of an operating system that are automatic and usually invisible to the user. They commonly get noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.
- Once the worm has infected a computer, it can redistribute itself to all e-mail addresses found on the infected system.
- Furthermore, a worm can deposit copies of itself onto all Web servers that the infected systems can reach, so that users who subsequently visit those sites become infected.
- Examples are : MS-Blaster, MyDoom, Netsky which are multifaceted attack worms.

Differences between Computer Virus and Worms

(1) A computer worm can run itself whereas a virus needs a host program to run. The virus code runs as part of the host program.

(2) A worm is a self-replicating program. It doesn't alter files like virus but resides in active memory and duplicates itself.

(3) A computer worm can spread without a host program.

Protecting against Computer Worms

- Worms mainly spread by exploiting vulnerabilities in operating systems or by tricking users to assist them.
- Users should not open unexpected e-mail and should not run attached files or programs or visit websites with such e-mail links.

unable to spread.

anti-virus and anti-spyware software are also helpful against worms. However, it must be kept up to date with new pattern files.

TYPES OF COMPUTER WORMS

Various types of computer worms are :

(1) ***E-mail worms*** **:** This type of worm is spread through infected e-mail messages. Any form of attachment or link in an e-mail may contain a link to an infected website. Clicking of attachment/link in the e-mail starts activation of the worm.

Known methods to spread are :

- MS Outlook services
- Direct connection to SMTP servers using their own SMTP API
- Windows MAPI functions

This type of worm is known to harvest an infected computer for e-mail addresses from different sources.

- Windows Address Book database [WAB]
- MS Outlook address book
- Files with appropriate extensions will be scanned for e-mail like strings

(2) ***Instant messaging worms*** **:** The spreading used is via instant messaging applications by sending links to infected websites to everyone on the local contact list. The only difference between these and e-mail worms are the way chosen to send the links.

(3) ***Internet worms*** **:** Internet worms will scan all available network resources using local operating system services and/or scan the Internet for vulnerable machines. Attempt will be made to connect to these machines and gain full access to them. Another way is that the worms scan the Internet for machines still open for exploitation, *i.e.,* not patched.

(4) ***IRC worms*** **:** Chat channels are the main target and the same infection/spreading method is used as above—sending infected files or links to infected websites. Infected file sending is less effective as the recipient needs to confirm receipt, save the file and open it before infection will take place.

(5) ***File-sharing networks worms*** **:** File-sharing Networks worms copies itself into a shared folder, most likely located on the local machine. The worm will place a copy of itself in a shared folder under a harmless name. Now the worm is ready for download via the P2P network and spreading of the infected file will continue.

(6) ***Payloads*** **:** A "payload" is code designed to do more than spread the worm—it might delete files on a host system, encrypt files in a cryptoviral extortion attack, or send documents via e-mail. Many worms have been created which are only designed to spread, and do not attempt to alter the systems they pass through. However, the network traffic and other unintended effects can often cause major disruption.

N HORSES

jan horse is a software program that hide their true nature and reveal their esigned unwanted or harmful behaviour only when activated.

Their name is based on the famous battle for the city of Troy in ancient Greece. Enemy soldiers left a hollow wooden horse filled with soldiers at the gate of the city. Innocent people of Troy (called Trojans) brought the horse into the city thinking it was a gift. At night enemy soldiers came out of the horse opened the city gate to bring in more soldiers and the city was defeated and destroyed.

- Trojan is a file or e-mail attachment which is disguised as a friendly or legitimate file. When executed, the file corrupts data and can even install a backdoor which hackers can utilize to access the network.
- Fig (1) shows a Trojan horse attack.

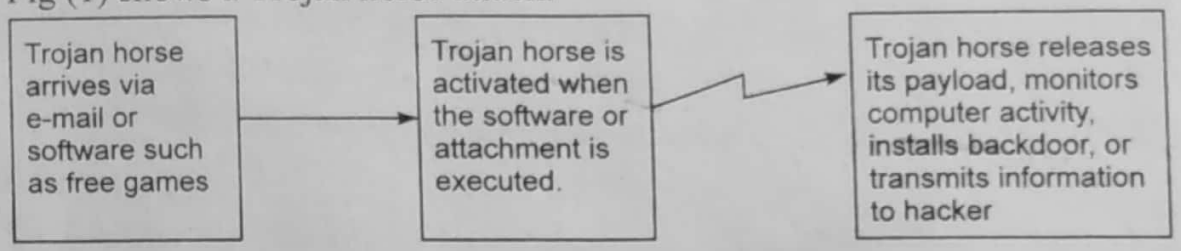

Fig. (1) Trojan horse attack

- Trojan horse programs are introduced into the system by initially planting them in software repositories that many people can access such as on personal computer network server. Unsuspecting users copy and run them. If a Trojan performs a useful function and causes no immediate or obvious damage, a user may continue to spread it by sharing the program with other friends and co-workers.
- Trojan horses fit into one of the following three models :
  (i) continuing to perform the function of the original program and additionally performing a separate malicious activity.
  (ii) Continuing to perform the function of the original program but modifying the function to perform malicious activity or to disguise other malicious activity.
  (iii) Performing a malicious function that completely replaces the function of the original program.
- Types of Trojans
  - Data Sending Trojans
  - Proxy Trojans
  - FTP Trojans
  - Security software disabler Trojans
  - Denial-of-Service (DoS) attack Trojans

Difference between Trojan horse and Virus or Worms

- Trojan horses disguise themselves as friendly programs. Viruses and worms are much more abvious in their actions.
- Trojan horses do not replicate like worms and viruses.

Logic bombs are codes embedded in some legitimate program that are executed when a pre-defined event occurs.

- Examples of conditions that can be used as triggers for a logic bomb are the presence or absence of certain files, a particular day of the week or date or a particular user running the application.
- These bombs display a message to the user and occur at a time when either the user is accessing the Internet or making use of a word processor application.
- Once triggered, a bomb may alter or delete data or entire files, cause a machine halt, or do some other damage.

The logic bomb initiation is a four-step process as under :

(1) Attacker implants the logic bomb.

(2) Victim reports the installation.

(3) Attacker sends the attack message.

(4) Victim does as the logic bomb dictates.

Mail Bombing

- Another form of e-mail attack that is also a denial of service (DOS) called a *mail bomb.*
- Attacker routes large quantities of e-mail messages to the target.
- The messages are usually large and constructed from meaningless data in an effort to consume additional system and network resources.
- The target of the attack receives unmanageably large volumes of unsolicited e-mail.
- By sending large e-mails, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.
- The target e-mail address is buried under thousands or even millions of unwanted e-mails such that the e-mail system can not accept any more messages.

5.7 TRAPDOORS

- A *trapdoor* or a *backdoor* is a secret means of access to a computer program that bypasses security mechanisms.
- Sometimes these entries are left by system designers or maintenance staff for trouble shooting or other purposes. These are referred to as maintenance hook.
- A trap door is hard to detect, because often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system. The trapdoor is code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by an unlikely sequence of events.

...ner installed as an administrative tool or a means of attack, a trap door is a ...curity risk when unscrupulous programmers use them to gain unauthorized access.

- Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a backdoor.
- Such an attack is usually used as either an access or modification attack. A Virus or worm has a payload that installs a backdoor or trapdoor component in a system, which allows the attacker to access the system at will with special privileges.
- Some of the tools that are used to create backdoor attacks are Back Orifice and Net Bus.
- It is difficult to implement operating system controls for backdoors. Security measures must focus on the program development and software update activities.

5.8 SPOOFING ATTACK

- *Spoofing* means providing false identify information in order to gain unauthorized access to other's computer system.
- In spoofing attack, one person or program successfully pretends as another by falsifying data. In this way they gain an illegitimate advantage. In other words, we can say that spoofing is an attempt by someone or something to pretend as someone else.

Types of Spoofing

(1) *IP spoofing* : It refers to connection hijacking through a fake IP address. It is a technique used to gain unauthorized access to computers, wherein the intruder sends messages to a computer that has an IP address that indicates that the messages are coming from a trusted host.

Fig. (2) shows the occurence of a spoofing attack.

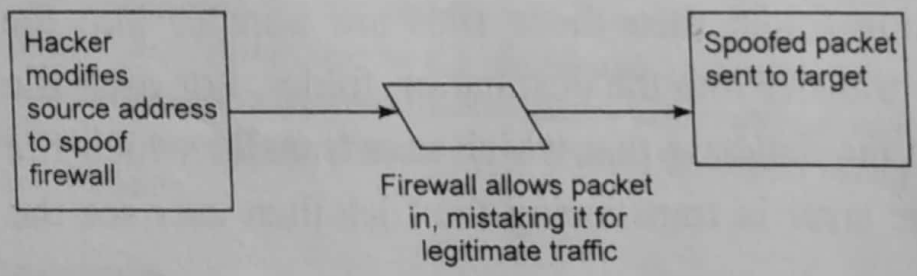

Fig. (2) IP spoofing

(2) *Man-in-the-middle attack* :

- Also called as *TCP hijacking attack.*
- An attacker monitors packets from the network, modifies them, and inserts them back into the network.
- This type of attack uses IP spoofing.

TCP hijacking session, the spoofing involves the interception of an cryption key exchange.

- Company A attempts to establish an encrypted session with company B.
- Hacker intercepts transmission and poses as company B. Hacker exchanges his own keys with company A. Hacker then establishes a session with company B, posing as company A.
- Company B sends all messages to the hacker who receives, decrypts, copies and forwards modified or copies to company A.

(3) *URL spoofing and phishing* : Another kind of spoofing is "web page spoofing", also known as *phishing*. In this attack, a legitimate web page such as a bank's site is reproduced in "look and feel" on another server under control of the attacker. The intent is to fool the users into thinking that they are connected to a trusted site, for instance to harvest user names and passwords.

This attack is often performed with the aid of URL spoofing, which exploits web browser bugs in order to display incorrect URLs in the browsers location bar; or with DNS cache poisoning in order to direct the user away from the legitimate site and to the fake one. Once the user puts in his password, the attack-code reports a password error, then redirects the user back to the legitimate site.

(4) *Referer spoofing* : Some websites, allow access to their materials only from certain approved (login-) pages. This is enforced by checking the referer header of the HTTP request. However, this referer header can be changed (known as "Referer spoofing" or "Ref-tar spoofing"), allowing users to gain unauthorized access to the materials.

(5) *Poisoning of file-sharing networks* : "Spoofing" can also refer to copyright holders placing distorted or unlistenable versions of works on file-sharing networks, to discourage downloading from these sources.

(6) *Caller ID spoofing* : There are now technologies (especially associated with VoIP) that allow callers to lie about their identity, and present false names and numbers, which could of course be used as a tool to defraud or harass. Because there are services and gateways that interconnect VoIP with other public phone networks, these false Caller IDs can be transmitted to any phone, which makes the whole Caller ID information now next to useless. Due to the distributed geographic nature of the Internet, VoIP calls can be generated in a different country to the receiver, which means that it is very difficult to have a legal framework to control those who would use fake Caller IDs as part of a scam.

5.9 E-MAIL VIRUSES

When the e-mail consisted of text messages only it was a very safe communication medium. However, the advance features of modern e-mail come at a price. E-mail programs that support attached files, HTML messages and embedded scripts can be used to send viruses and other malicious software.

...ng user
...id and
...t their

...used for spreading e-mail virus is through e-mail attachments. ...e file is opened that is attached to a mail message, the program runs and ...infected on the machine. In some cases,the address book is used to mail ..."itself" to everyone on the address book. These infected messages appear to ...riginated from a person who does not even know that they were sent. Viruses that ...k this way include Melissa virus, Klez etc.

Viruses can be embedded in the mail message itself. This is not possible in a plain text message. However, when we use HTML mail containing pictures or sound, such HTML message can contain programs that execute viruses. This is the reason why many mailing lists block HTML mail.

Protection against E-mail Virus Attack

Following are some basic steps which should be taken to protect against e-mail virus attack :

(1) Install anti-virus software and keep it up-to-date. Note that firewalls are not as effective as anti-virus software.

(2) E-mail attachments should not be opened directly.

(3) A document viewer should be used to read received documents.

5.10 MACRO VIRUSES

Many applications allow us to create a script of commands that the application can run. This is done to simplify complicated procedures. Typically it is used to automate repetitive tasks and thereby save keystrokes. The script written for this purpose is known as a "*macro*" as they are small programs. A user might define a sequence of keystrokes in a macro and set it up so that the macro is involved when a function key or special short combinations of keys is input. Hackers often create their own macros to destroy computer or data.

Macro virus is embedded in automatically executing macro-code common in word processors, spread sheets and database applications. When we open a word processing or spreadsheet document, the macro virus is activated and it infects the normal template (Normal .dot)—a general purpose file that stores default document formatting setting. Every document we open refers to the normal template and hence gets infected with the macro virus. Since this virus attaches itself to documents, the infection can spread if such documents are opened on other computers.

Macro viruses are very dangerous because of following reasons :

(1) A macro virus is platform independent. Many macro viruses infect Microsoft Word documents or other Microsoft Office documents. Any hardware platform and operating system that supports these applications can be infected.

(2) Macro viruses infect documents and not executable portions of code. Most of the information introduced into a computer system is in the form of a document rather than a program.

(3) Macro viruses are easily spread. A very common method is by e-mail.

...ical file system access controls are of limited use in preventing their spread.
...les of macro virus are Word Concept, Nuclear and DMV.

DENIAL OF SERVICES (DoS) ATTACK

- Attacker sends a large number of connection or information requests to a target.
- The target system cannot handle so many requests that are made along with other legitimate requests for service.
- This may result in a system crash, or merely an inability to perform ordinary functions.
- Examples of DoS attacks are Ping of Death and Teardrop attacks.
- The hacker sends a request to the server to connect to it. When the server responds with an acknowledgment and tries to establish a session, it can not find the system that made the request. This is because all requests have false return addresses. The server waits for some time before closing the connection. In the meantime a new batch of forged requests arrive. This causes the server to slow down or eventually crash.

The common method of blocking a "denial-of-service" attack is to set up a filter or "sniffer" on a network before a stream of information reaches a site's Web servers. The filter can look for attacks by noticing patterns or identifiers contained in the information. If a pattern comes in frequently, the filter can be instructed the block messages containing that pattern. In this way Web servers are protected from having their lines tied up.

Distributed Denial-of-Service (DDoS) Attack

DDoS is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time. DDoS attacks involve breaking into hundreds or thousands of computers all over the Internet. Then the attacker installs DDoS software on them, allowing them to control all these burgled machines to launch coordinated attacks on victim sites. These attacks typically exhaust bandwidth, router processing capacity or network stack resources, breaking network connectivity to the victims. A hacker begins a DDoS attack by exploiting a vulnerability in one computer system and making it the DDoS "master". From this master system the intruder identifies and communicates with other system that can be compromised. The intruder loads cracking tools available on the Internet on multiple compromised systems. With a single command, the intruder instructs the controlled machines to launch one of many flood attacks against a specified target. The inundation of packets to the target causes a denial of service.

5.12 E-COMMERCE

- Electronic commerce, commonly known as *e-commerce*, refers to the buying and selling of products or services over electronic systems such as the Internet and other computer networks.

...ludes the entire online process of developing, marketing/selling, ...ng, servicing and paying for products and services.

...e, electronic commerce or e-commerce is a term for any type of business, ... commercial transaction that involves the transfer of information across the internet. It covers a range of different types of businesses, from consumer based retail sites, through auction or music sites, to business exchanges, trading goods and services between corporations.

- E-commerce allows consumers to electronically exchange goods and services with no barriers of time or distance.
- The amount of trade conducted electronically has grown extraordinarily with the use of Internet.
- The use of e-commerce has increased considerably due to innovations in electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange, inventory management systems, and automated data collection systems.
- Mostly e-commerce involves the transportation of physical items in some way. However, e-commerce also includes business for virtual items such as access to premium content on a website.
- Online retailers are sometimes known as *e-tailers* and online retail is sometimes known as *e-tail.*
- Electronic commerce is generally considered to be the sales aspect of e-business. It also consists of the exchange of data to facilitate the financing and payment aspects of the business transactions.

pes of e-commerce

The various types of e-commerce models are :

(1) *Business to consumer* : As the name suggests, it is the model involving ...raction of businesses and consumers. Business-to-consumer (B2C, sometimes also ...led Business-to-Customer) describes activities of businesses serving end consumers ...h products and/or services. A B2C business is one that provides products or services ...ectly to the consumer. Consumers directly interact with the products on supplier's ...bsite.

An example of a B2C transaction would be a person buying a pair of shoes from a ...iler. However, the sale of the shoe from the shoemaker to the e-tailer would be ...sidered a (B2B) transaction.

(2) *Business-to-business* : On the Internet, B2B (business-to-business), also ...wn as e-biz, is the exchange of products, services, or information between ...inesses rather than between businesses and consumers. The buyers and sellers are ...h business entities and do not involve an individual consumer. Business-to-business ...cribes commerce transactions between businesses, such as between a manufacturer ... a wholesaler, or between a wholesaler and a retailer.

For example, an automobile manufacturer makes several B2B transactions such as ...ing tires, glass for windscreens, and rubber hoses for its vehicles.

umer to Consumer – (C2C)

ctronic commerce involves the electronically-facilitated transactions consumers through some third party. Individuals sell products or services y to other individuals using a common platform. A common example is the ine auction, in which a consumer posts an item for sale and other consumers bid to purchase it. The third party generally charges a flat fee or commission for providing a common platform. The sites are only intermediaries, just there to match consumers. They do not have to check quality of the products being offered. Example of C2C e-commerce is e-Bay, snapdeal.com etc.

(4) ***M-commerce*** : It refers to the use of mobile devices for conducting the transactions. The mobile device holders can contact each other and can conduct the business. Even the web design and development companies optimize the websites so that they can be easily viewed on mobile devices.

Advantages of E-commerce

E-commerce has changed and defined a new type of relationship between seller and customers. The advantages of e-commerce are :

(i) Lower transaction cost.
(ii) Online business operates 24 × 7 hours.
(iii) Increases the volume of purchase and sales.
(iv) Veriety in modes of shopping.
(v) Improved relations with customers.
(vi) Business conducted while sitting at home.

5.13 ELECTRONIC PAYMENT SYSTEM

Electronic payments are the central part of e-commerce activities as it deals with the strategies for the payment of goods and services by online customers. Electronic payments also refer to the activity of account settlement where the prompt settlement of payments is crucial. If the debit and credit to the bank account, customer and the company are not settled immediately or suffers due to conventional processing delays, then the entire business chain may be interrupted. Payment and settlement of the business account are the bottleneck in all e-commerce activities. Conventional instruments for payments such as demand draft, credit notes, and cheques are not suited to e-commerce. The electronic version of this instrument also may not work well particularly when small payments are to be made. The supplier as well as the customer would like to settle the payment online when the amount to be paid is small. Conventional instruments are too slow to be processed and the overheads in processing such instruments may be high.

Electronic payment is a financial exchange that takes place online between buyers and sellers. The content of this exchange is usually some form of digital financial instrument (such as encrypted credit card numbers, electronic cheques or digital cash) that is backed by a bank or an intermediary, or by a legal tender.

Various instruments which may used to make payment on the Internet are Credit/Debit cards, Smart Cards, Electronic Cash, Electronic Wallet etc. Important issues related to the electronic payment system are :

(i) Methods, form and characteristic of payment instrument such as credit/debit cards.

(i) How to minimize the financial risk such as leakage of information, mistakes and frauds.

(ii) Devising methods for the completion of electronic payment cycle.

The various factors that have led the financial institutions to make use of electronic payments are :

(1) *Decreasing technology cost* : The cost of the technology used in the networks is decreasing day by day, which is evident from the fact that computers are now very cheap and Internet is becoming almost free everywhere in the world.

(2) *Reduced operational and processing cost* : Due to reduced technology cost, the processing cost of various commerce activities has become less. In electronic transactions we save both paper and time.

(3) *Increasing online commerce* : Various innovative technologies have encouraged the use of electronic payments. They are :

(a) *Affecting the consumers* : Credit cards, Debit Cards, ATMs (Automated Teller Machines), stored value cards, E-Banking.

(b) *Enabling online commerce* : Digital Cash, E-Cash, Smart cards (or Electronic Purse) and encrypted Credit cards.

Some commonly used protocols for secured transaction are :

(1) Secure Electronic Payment Protocol (SEPP)

(2) Secure Electronic Transaction Protocol (SET)

SEPP has been developed by Master Card and Netscape. It has been implemented in the Netscape web browsers. Secure Electronic Transaction Protocol it a new e-commerce industry standard. Many companies are implementing SET protocol and is has many features in common with SEPP. SET is also one of the popular protocols for safe electronic transaction. It was developed by Microsoft and VISA. SET uses the cryptographic standard to secure the authentication and verification is done using digital signatures.

Electronic payment system involves a three way communication between customer, company and the bank. The electronic payment process has been shown in fig. (3).

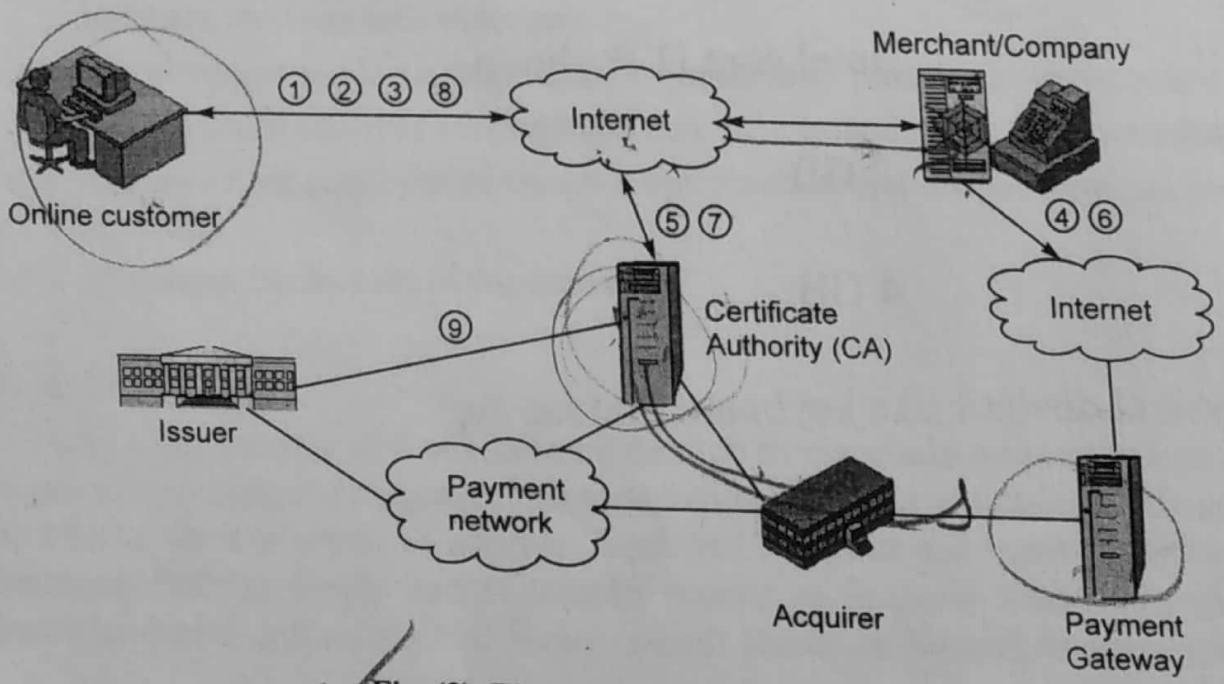

Fig. (3) Electronic payment system

rence to the figure, note that :

- The customer is a person who wants to buy the product or services from a company. He does it by visiting the web site of the company. The customer is also a holder of a credit card and intends to pay for the purchased product and services through his credit card.
- The merchant/company's web site displays and sells the items such as goods and services. It also accepts the payment from the customer against the purchased items and services.
- An issuer is a bank that offers credit card association branded payment cards directly to customers. They are association between card issuing banks. The well known credit card associations are Visa, Master card, American express etc.
- An acquirer is the bank that processes credit/debit card payments for products or services for a merchant or company.
- Certificate authority represents the agent or broker who creates and distributes the digital certificate to customers and other financial institutions. The agent works on behalf of the credit card issuer bank.

The transaction process involves the following steps which have been marked in the figure :

(1) The customer sends an initial message to the company web site (merchant).
(2) Company responds by sending the invoice message, enabling the customer to validate goods and services of the company.
(3) The customer then prepares the purchase order and sends the credit card details. The credit card details are encrypted so that it can only be decrypted by the bank.
(4) The merchant sends to the payment-processing organization (via the payment gateway or acquirer) a request for authorization.
(5) Authorization is handled by existing processes using existing networks. The merchant receives authorization.
(6) The merchant sends a capture request (to actually commit the transaction).
(7) The merchant receives confirmation that the transaction has been accepted.
(8) The merchant sends the cardholder confirmation that the payment has been accepted.
(9) The issuer banks bills to the customer.

5.14 E-CASH

E-cash is the transfer of funds initiated through an electronic terminal, telephonic instrument or computer or magnetic tape so as to order, instruct or authorize a financial institution to debit or credit an account. It utilizes computer and telecommunication components both to supply and to transfer money or financial assets. Transfer is information-based and intangible. Hence e-cash stands in contrast to conventional

payment modes that rely on physical delivery of cash or checks. it can be changed electronically. The other terms used for e-cash are *electronic money*, *ency, digital cash, digital currency* and *cyber currency*.

- The primary function of e-cash is to facilitate transaction on the Internet.
- The reality of e-cash is only slightly more complicated, and these complications make the transaction both secure and private.
- E-cash truly globalize the economy, since the user can download money into his cyber wallet in any currency desired.
- When a user wants e-cash offline all that is necessary is smart card technology.
- It is similar to debit/credit card, but e-cash allows individuals to conduct transaction with each other.
- It is similar to personal cheque, but it is feasible for very small transaction.

E-cash can be represented by two models :

(1) ***Online form*** : It allows for the completion of all types of Internet transactions.

(2) ***Offline form*** : It is a digitally encoded card that can be used for most of the transactions which can be carried out through cash money.

E-cash is used for the following three broad categories of payments :

(1) *Banking and financial payments* :

- Large-scale or wholesale payments (*e.g.*, : Bank-to-Bank transfer)
- Small-scale or retail payments (*e.g.*, : automated teller machines and cash-dispensers)
- Home banking (*e.g.*, : bill payment)

(2) *Retailing payments* :

- Credit cards (*e.g.*, : VISA or Master cards)
- Private label credit/debit cards
- Change cards

(3) *On-line electronic commerce payments* :

- Token- based payment system
  - Electronic cash (*e.g.* : Digicash)
  - Electronic checks (*e.g.* : Netcheque)
  - Smart cards or debit cards
- Credit card-based payment system
  - Encrypted credit cards (*e.g.* : www form-based encryption)\
  - Third-party authorization numbers

5.14-1 CREDIT CARDS

Credit cards are small plastic cards issued to users as a system of payment. They work on the *post-paid* mechanism where the holder buys goods and services based on

promise to pay for these goods and services later on. The merchant or gets their money from the credit card organization in real time.

Credit cards are payment instrument which have now become very popular. Credit are issued by a financial institution which allows us to make purchases up to a certain limit on credit. Most of the credit card companies recognize the organization or shop etc. from where we may purchase the item. Payment of these items is made by the credit card company on our behalf. The credit card companies regularly send the bill to the customer for the shopping they have done. In e-commerce, use of credit card is very common. If consumers want to purchase a product or service, they simply send their credit card details to the service provider involved and the credit card organization will handle this payment like any other transaction.

Process in Purchasing through Credit Card

When the customer wishes to purchase items from a web site or a shop he places the purchase order electronically and sends encrypted credit card number. This information will be sent to the customer bank through the credit card processor. After checking the authenticity of the credit card, the banks allows the company to go ahead with the purchase. The bank will issue an electronic token to the company. The customer bank will realize the payment through monthly or fortnightly bill sent to the customer.

Advantages of Credit Card

The various advantages offered by using credit cards are :

(1) ***Safe and secured money*** **:** Credit card offers safety and security as compared to cash money. There is no loss even when we loose or somebody steals our credit card. At the same time it has the same buying power as cash money.

(2) ***Purchase power and base of purchase*** **:** Credit cards can make it easier to buy things. If we don't like to carry large amounts of cash or if a company doesn't want to handle cash (for example most airlines, hotels, and car rental agencies), putting purchases on a credit card can make buying things easier.

(3) ***Protection of purchases*** **:** Credit cards may also offer additional protection if something we have bought is lost, damaged, or stolen. Both our credit card statement (and the credit card company) can vouch for the fact that we have made a purchase if the original receipt is lost or stolen. In addition, some credit card companies offer insurance on large purchases.

(4) ***Building a rcedit line*** **:** Having a good credit history is often important, not only when applying for credit cards, but also when applying for things such as loans, rental applications, or even some jobs. Having a credit card and using it wisely (making payments on time and in full each month) will help us build a good credit history.

(5) ***Emergencies*** **:** Credit cards can also be useful in times of emergency. While we should avoid spending outside our budget sometimes emergencies (such as our car breaking down or flood or fire) may lead to a large unexpected but necessary purchase.

(6) ***Credit card benefits*** **:** In addition to the benefits listed above, some credit cards offer additional benefits, such as discounts from particular stores or companies,

...surance.) While most of these benefits are meant to encourage us to spend ...money through credit card, the benefits are real and can be helpful as long as we ...d within our limits.

...isadvantages of credit cards

The disadvantages of credit cards are :

(1) ***Blowing our budget*** : The biggest disadvantage of credit cards is that they encourage people to spend money more than they have. Most credit cards do not require us to pay off our balance each month. While this may seem like 'free money' at the time, we will have to pay it off — and the longer we wait, the more money we will owe since credit card companies charge interest each month on the money we have borrowed.

(2) ***High interest rates and increased debt*** : Credit card companies charge an enormous amount of interest on each balance that we don't pay off at the end of each month.

(3) ***Credit card fraud*** : Like cash, sometimes credit cards can be stolen. They may be physically stolen (if we lose your wallet) or someone may steal our credit card number (from a receipt, over the phone, or from a Web site) and use our card to rack up debts. However with the security features available now-a-days it has become a rare phenomenon.

5.14-2 DEBIT CARDS

A *debit card* (also known as a *bank card* or *check card*) is a plastic card that provides an alternative payment method to cash when making purchases. Functionally, it can be called an electronic check, as the funds are withdrawn directly from either the bank account or from the remaining balance on the card. Debit cards may also allow for instant withdrawal of cash, acting as the ATM card for withdrawing cash. The difference between a credit card and a debit card is that we may not be having the money when we make a purchase through a credit card. The money is given to the merchant for which we are required to pay interest or service charges later on at a convenient time. In case of debit card we can only spend the amount of money which we have in our account. The funds are transferred immediately from the bearer's bank account.

There are three ways in which the debit card transactions are processed :

(1) Online debit, for example, PIN debit

(2) Offline debit, for example, Signature debit

(3) E-purse card system in which value is stored in the card chip, for example, smart card based debit cards.

Advantages of Debit Cards

Advantages of debit cards are :

(1) A consumer who is not credit worthy and may find it difficult or impossible to obtain a credit card can more easily obtain a debit card, allowing him to make

debit, which includes the use of a credit card, but not online debit card transactions.

For most transactions, a check card can be used to avoid check writing altogether. Check cards debit funds from the user's account on the spot. This finalizes the transaction at the time of purchase, and bypassing the requirement to pay a credit card bill at a later date, or to write an insecure check containing the account holder's personal information.

(3) Like credit cards, debit cards are accepted by merchants with less identification and scrutiny than personal checks. This makes transactions quicker and less intrusive. Unlike personal checks, payment via a debit card can not be later dishonored.

(4) Unlike a credit card, which charges higher fees and interest rates when a cash advance is obtained, a debit card may be used to obtain cash from an ATM or a PIN-based transaction at no extra charge, other than a foreign ATM fee.

Disadvantages of Debit Cards

The disadvantages associated with debit cards are :

(1) Use of a debit card is not usually limited to the existing funds in the account to which it is linked. Most banks allow a certain threshold over the available bank balance which can cause overdraft fees if the users transaction does not reflect available balance.

(2) Many banks are now charging over-limit fees or non-sufficient funds fees based upon pre-authorizations, and even refused transactions by the merchant (some of which may be not known until later date by account holder).

(3) Many merchants mistakenly believe that amounts owed can be "taken" from a customer's account after a debit card (or number) has been presented, without agreement as to date, payee name, amount and currency, thus causing penalty fees for overdrafts, over-the-limit, amounts not available causing further rejections or overdrafts, and rejected transactions by some banks.

(4) In some countries debit cards offer lower levels of security protection than credit cards.

(5) In many places, laws protect the consumer from fraud much less than with a credit card. While the holder of a credit card is legally responsible for only a minimal amount of a fraudulent transaction made with a credit card, which is often waived by the bank. The consumer also has a shorter time (usually just two days) to report such fraud to the bank in order to be eligible for such a waiver with a debit card, whereas with a credit card, this time may be up to 60 days. A thief who obtains or clones a debit card along with its PIN may be able to clean out the consumer's bank account and the consumer will have no recourse.

come from two greek word "Kryptos" meaning Hidden and graphic mean "writing".

Cryptography

The original purpose of cryptography was to hide something that had been written. Cryptography is used to hide the meaning of information in any form such as data stored on a disc or a message in transit through a communication network. Cryptography can be applied to anything that can be digitally coded such as : Software, graphics, voice or video. Fig. (4) shows a cryptographic system.

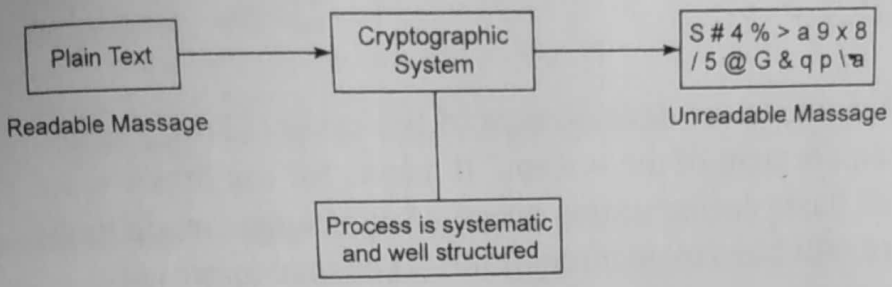

Fig. (4) Cryptographic system

Following are the four objectives of cryptography :

(1) ***Confidentiality*** : Ensure data is read only by authorized parties,

(2) ***Data integrity*** : Ensure data wasn't altered between sender and recipient,

(3) ***Authentication*** : Ensure data originated from a particular party.

(4) ***Non-repudiation*** : Prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

Need for Cryptography

- Cryptography is probably the most important aspect of communications security and is becoming increasingly important as a building block for information system security.
- It helps in providing accountability, fairness, accuracy and confidentiality.
- It can prevent fraud in e-commerce and assure the validity of financial transactions.

Terms Associated with Cryptography

Before we proceed further, there are certain terms which we need to understand.

- *Encryption* is the process of converting an original message into a form that is unreadable to unauthorized individuals *i.e.*, to anyone without the tools to convert the encrypted message back to its original format.
- *Cipher* is transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components.
- *Ciphertext* or *Cryptogram* is the unintelligible encrypted or encoded message resulting from an encryption.
- *Decryption* is the process of converting the ciphertext into a message that conveys readily understood meaning.

decryption, i.e., it
decryption.

- *Key* or *Cryptovariable*
ciphertext from plain
- *Cryptoanalysis* is t
plaintext) from an en
the algorithms and k
used to break a ciphe
accepted as authentic
creating secret codes
secret codes.

Characteristics of Cryptog

Cryptographic systems a

(1) *The type of operatio*

encryption algorithms are ba
element in the plaintext (bit
element, and *transposition*,
fundamental requirement is
reversible). Most systems in

(2) *The number of keys*

system is referred to as symm
If the sender and receiver us
two-key, or public-key encry

(3) *The way in which th*

input one block of element a
stream cipher processes th
element at a time, as it goes

Threats to Cryptographic

The various threats to a

(1) *Brute force attack*
on a piece of cip
obtained.

(2) Password hacking

(3) Packet sniffing

(4) Modification of th

Requirements for Secure

There are two requirem

(1) We need a strong
algorithm to be s
access to one or m

decryption, i.e., it is the data either before encryption or after successful decryption.

- *Key* or *Cryptovariable* is the information used alongwith an algorithm to create ciphertext from plaintext.
- *Cryptoanalysis* is the process of obtaining the original message (called plaintext) from an encrypted message (called the ciphertext) without knowing the algorithms and keys used to perform the encryption. It is a set of methods used to break a cipher system and/or forge coded signals so that they will be accepted as authentic. Hence, whereas cryptography is the science and art of creating secret codes, cryptoanalysis is the science and art of breaking these secret codes.

Characteristics of Cryptographic Systems

Cryptographic systems are characterized along three independent dimensions :

(1) *The type of operations used for transforming plaintext to ciphertext* : All encryption algorithms are based on two general principles: *substitution*, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and *transposition*, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, all operations are reversible). Most systems involve multiple stages of substitutions and transpositions.

(2) *The number of keys used* : If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

(3) *The way in which the plaintext is processed* : *A block cipher* processes the input one block of element at a time, producing an output block for each input block. *A stream cipher* processes the input elements continuously, producing output one element at a time, as it goes along.

Threats to Cryptographic Systems

The various threats to a cryptographic system are :

(1) *Brute force attack* (breaking the key) : The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

(2) Password hacking

(3) Packet sniffing

(4) Modification of the original document

Requirements for Secure Cryptographic Systems

There are two requirements for secure use of cryptographic system:

(1) We need a strong encryption algorithm. At a minimum, we would like the algorithm to be such that an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext

The opponent should be unable to decrypt ciphertext or discover the key even if he is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

2) Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

Importance of keys in Cryptography

Keys are used in cryptography to encrypt the information. Only a person with the appropriate key can make it readable again. Thus, it means that without an appropriate key, one cannot access the message or decode it to a readable form. Key plays an important role in cryptography. Thus, the key is used for locking of the encrypted message which can only be unlocked/decrypted using the correct combination of the key (Private Key) or the same key which was used for locking/encrypting (Public key).

- ***Public key*** : Public key are those keys which are made available to anyone who needs it and is used to encrypt the data.
- ***Private key*** : Private key is safe and is not available to anyone except the creator and is used to decrypt the data encrypted by public key.

5.17-1 PUBLIC KEY CRYPTOGRAPHY

In traditional cryptography, the same key is used by the sender and the receiver of a message for encryption and decryption. This method is known as *symmetric cryptography*.

Public-key cryptography is also called asymmetric cryptography. It uses a secret private key that must be kept from unauthorized users and a public key that can be made public to anyone. Both the public key and the private key are mathematically linked. Data encrypted with the public key can be decrypted only by the private key, and data signed with the private key can only be verified with the public key. The public key can be published to anyone. Both keys are unique to the communication session.

An encryption algorithm performs mathematical operations on the plaintext. Substitutions and transformations are conducted on the plaintext to generate the ciphertext. Public key and private key are agreed upon. One selected key is used as public key and is used for encryption. The other is used as private key for decryption and is only known by the recipient. The ciphertext message is transmitted and received by the receiver. The decryption algorithm generates the plaintext from the ciphertext and the private key at the receiver's end.

Public-key cryptographic algorithms use a fixed buffer size. Private-key cryptographic algorithms use a variable length buffer. Public-key algorithms cannot be used to chain data together into streams like private-key algorithms can. With private-key algorithms only a small block size can be processed, typically 8 or 16 bytes.

The public key cryptography can be used not only for privacy (encryption) but also for authentication. It is used in digital signatures for authentication purposes.

Advantages of public key cryptography are :

(1) Each user has a pair of key—a public key and a private key. The private key is kept a secret, while the public key may be distributed.

(2) Messages are encrypted with recipient's public key and can only be decrypted with corresponding private key.

(3) No need to exchange the keys among the users.

(4) Public key cryptography prevents the sender of the information from claiming later that the information was never sent.

(5) It allows the recipient of the information to verify that it has not been modified in transit.

Comparison between Symmetric and Asymmetric Cryptography

Symmetric Cryptography	Asymmetric Cryptography
Strengths : (1) Much faster than asymmetric system. (2) Hard to break with a large key size.	**Strengths :** (1) Better key distribution than symmetric system. (2) Better scalability than symmetric system. (3) Can provide authentication and non repudiation.
Weakness : (1) Requires secure delivery mechanism. (2) Key management can become overwhelming. (3) Does not provide authenticity or non-repudiation	**Weakness :** (1) Works slowly as compared to symmetric key system. (2) Involves mathematical intensive tasks.

5.18 DIGITAL SIGNATURES

A digital signature is an electronic analogue of a written signature. The digital signature can be used to provide assurance that the claimed signatory signed the information. In addition, a digital signature may be used to detect whether or not the information was modified after it was signed (*i.e.*, direct integrity of signed data). These assurances may be obtained whether the data was received in a transmission or retrieved from storage. A properly implemented digital signature algorithm that meets the requirements of this standard can provide these services, for example, RSA, DSA, Rabin signature algorithm, Undeniable signatures etc.

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives the recipient a reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe that the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects. Properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message. Further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages may be anything representable as a bit string. Examples are electronic mail, contracts, or a message sent via some other cryptographic protocol.

A digital signature scheme typically consists of three algorithms :

(1) A *key generation algorithm* that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

(2) A *signing algorithm* that, given a message and a private key, produces a signature.

(3) A *signature verifying algorithm* that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required :

(1) A signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key.

(2) lt should be computationally impossible to generate a valid signature for a party who does not possess the private key.

Uses of Digital Signature

As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory.

Some common reasons for applying a digital signature to communications are :

(1) *Authentication* : Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.