ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

DIPLOMA IN CYBER SECURITY

DCS-03

Information Security

Block 1

INFORMATION SECURITY CONCEPTS AND CRYPTOGRAPHY

ଓଡ଼ିଶା ରାଜ୍ୟ ମୁକ୍ତ ବିଶ୍ୱବିଦ୍ୟାଳୟ, ସମ୍ବଲପୁର, ଓଡ଼ିଶା
Odisha State Open University, Sambalpur, Odisha
Established by an Act of Government of Odisha.

EXPERT COMMITTEE

Dr P.K.Behera (Chairman)
Reader in Computer Science
Utkal University
Bhubaneswar, Odisha

Dr. J.R.Mohanty (Member)
Professor and HOD
KIIT University
Bhubaneswar, Odisha

Sh Pabitrananda Pattnaik(Member)
Scientist –E,NIC
Bhubaneswar, Odisha

Sh Malaya Kumar Das (Member)
Scientist –E,NIC
Bhubaneswar, Odisha

Dr. Bhagirathi Nayak (Member)
Professor and Head(IT & System)
Sri Sri University
Bhubaneswar, Odisha

Dr.Manoranjan Pradhan (Member)
Professor and Head(IT & System)
G.I.T.A
Bhubaneswar, Odisha

Sri V.S.Sandilya (Convenor)
Academic Consultant (I.T)
Odisha State Open University,
Sambalpur, Odisha

DIPLOMA IN CYBER SECURITY

Course Writer
Chandrakant Mallick
Consultant (Academic)
School of Computer and Information Science
Odisha State Open University, Odisha

1st Edition - 2016 Printed at - Shree Mandir Publications, BBSR

UNIT-1

INFORMATION SECURITY CONCEPTS Unit Structure

1.0 INTRODUCTION

Computers are used by millions of people for many purposes like Banking, Shopping, Tax returns, Education, Military, Communication, Business, Research, Entertainment and many more. It necessitates protecting the assets of computer in all such applications. The assets of the computer mean the hardware and software including the information available in many forms. In the present day context information is the most valuable asset than any other in an organization. Information Security deals with all aspects of protecting information. In this unit we will discuss some fundamentals concepts of information security.

1.1 LEARNING OBJECTIVES

After studying this unit, you should be able to:

- Understand the concepts of security and its types.
- Understand what information security is and how it plays an important role today.
- Distinguish the meaning of computer security, information security and network security.
- Describe the key security requirements of confidentiality, integrity, and availability.
- Discuss the types of security threats and attacks.
- Understand the X.800 security architecture for OSI
- Summarize the key terms and critical concepts of information security.

1.2 INFORMATION SECURITY ISSUES

The information security within an organization has undergone two major changes in the last several decades.

The world before computers was much simpler in some ways-

- Signing, legalizing a paper would authenticate it.
- Photocopying was easily detected
- Erasing, inserting, modifying words on a paper document easily detectable

- Secure transmission of a document: seal it and use a reasonable mail carrier (hoping the mail train does not get robbed)
- One can recognize each other's face, voice, hand signature, etc.

In the world of computers the ability to copy and alter information has changed dramatically as-

- There is no difference between an "original" file and copies of it.
- Removing a word from a file or inserting others is undetectable
- Adding a signature to the end of a file/email: one can impersonate it –add it to other files as well, modify it, etc.
- Difficult to authenticate the person electronically communicating with you.

So, it needs automated tools for protecting files and other information stored on the computer.

1.3 BASIC TERMINOLOGIES AND DEFINITIONS

Cyber security or information technology security focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security.

So Information Security is a crucial issue in many applications. The basic terminologies similar to information security are discussed as follows.

Computer security is a collection of tools designed to protect the assets of the computer system; information and services they provide.

Computer Security (Definition)

The NIST *Computer Security Handbook* [NIST95] defines the term *computer security* as follows:

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of

information system resources (includes hardware, software, firmware, information/data, and telecommunications) is called ***Computer Security***.

The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.

Another major change that affected security is introduction of computer networks and distributed systems that facilitates carrying of data from one computer to the other. So it is even more essential to provide security to information for the systems that access information over public telephone networks or data networks or the Internet. The measure that is needed to protect data during their transmission is called **Network Security**.

Network security mechanisms need to protect the network and the network-accessible resources from unauthorized access by consistent and continuous monitoring and measurement of its effectiveness.

Now a day's virtually all business, government and academic institutions interconnect their data processing systems with collection of interconnected networks called Internet. The mechanism used to determine, prevent, detect and correct security violations that involve transmission of information is called **Internet Security**.

Similarly the mechanism to make sure that nosy people cannot read or secretly modify or disclose the information is called **Information Security**.

Information security, sometimes shortened to InfoSec, is the practice of defending **information** from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Information security (Definition)

Wikipedia *defines* ***Information security*** *(sometimes shortened to InfoSec), as the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction*.

It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Point-to-Make: Making a network or a communication system secure involves more than just keeping it free of programming errors as it involves often intelligent,

dedicated and well-funded adversaries.

Possible adversaries

An **adversary** is generally considered to be a person, group, or force that opposes and/or attacks.

- **A Student is interested** to have fun snooping on other people's email
- **A Cracker** tries to test out someone's security system, to steal data
- **A Businessman wants** to discover a competitor's strategic marketing plan
- **An Ex-employee wants** to get revenge for being fired.
- **An Accountant interested** to embezzle money from a company
- **A Stockbroker wants** to deny a promise made to a customer by email
- **A Convict** to steal credit card numbers for fraudulent actions.
- **A Spy wants** to learn an enemy's military or industrial secrets
- **A Terrorist wants** to use internet for attacks

1.4 INFORMATION SECURITY GOALS

The meaning of terminologies change over time and this is especially true in the rapidly changing technology industry. For example, we have information security, computer security, cyber security and IT security.

Not only have these names changed meaning over time, there isn't necessarily a clear consensus on the meanings and the degree to which they overlap or are interchangeable. In our context we will frequently refer information security in this course.

As per the definition above there are three measure goals of Information security that include Confidentiality, Integrity and availability.

Fig:Information Security goals

1. Confidentiality

It covers two related concepts to ensure:

Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Confidentiality or Secrecy requires that the information in a computer system only be accessible for reading by authorized parties.

This type of access includes:

- Printing
- Displaying
- Other forms of disclosure, including simply revealing the existing of an object

We need to protect our information from malicious actions that threat confidentiality of its information.

The principle of confidentiality specifies that only the sender and the intended receiver should be able to access the message.

Confidentiality gets compromised if an unauthorized person is able to access the message.

2. Integrity

Information has integrity when it is timely, accurate, complete, and consistent. However, computers are unable to provide or protect all of these qualities. The term Integrity covers two related concepts:

(i) Data integrity is a requirement that information and programs are changed only in a specified and authorized manner.

(ii) System integrity is a requirement that a system "performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system."

The definition of *integrity* has been, and continues to be, the subject of much debate among computer security experts.

In context of information security, we mean information has integrity it has not been altered i.e. if the content of the message does not change during transmission the the integrity are maintained.

If the content of the message changes during transmission then the integrity is lost.

The changes need to be done to the information only by the authorized user through authorized mechanisms.

- Integrity requires that the computer system asset can be modified only by authorized parties.
- Modification includes:
- Writing
- Changing
- Changing status
- Deleting and
- Creating

3. Availability

Availability requires that computer system assets are available to authorized parties.

Availability is arequirement intended to assure that systems work promptly and service is not denied to anauthorized user. The principle of availability states the resources should be available to authorized users all the times.**These three concepts form what is often referred to as the Confidentiality Integrity and Availability (CIA) Triad.**

The three concepts embody the fundamental security objectives for both data and for information as well as computing services. For example, the NIST standard FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*) lists confidentiality, integrity, and availability as the three security objectives for information and for information systems.

FIPS 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

A loss of confidentiality is the unauthorized disclosure of information.

Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

A loss of integrity is the unauthorized modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information.

A loss of availability is the disruption of access to or use of information or aninformation system.

Other Security principles

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Three of the most commonly mentioned are as follows:

Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and thateach input arriving at the system came from a trusted source.

Authentication mechanisms help to establish proof of identities. Authentication process ensures that the origin of an electronic message or a document is correctly identified.

Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after action, recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Non-Repudiation: The user sends a message to B and can't deny that she had sent that message. For example A could send a fund transfer request to the bank B over the Internet. After the bank performs the fund transfer as per A's instruction, A could claim that she never sent the fund transfer request. Thus A repudiates or denies her fund transfer instruction.

1.5 CHALLENGES OF INFORMATION SECURITY

Information security is both complex and challenging. Some of the reasons are as follows:

1. Security is not as simple as it might be understood by the novice users. The requirements seem to be straight forward; the major requirements for security services can be confidentiality, authentication, nonrepudiation, or integrity. But the mechanisms used to meet those requirements can be quite complex.

2. In developing a particular security mechanism or algorithm, one must

alwaysconsider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

3. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.

4. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement and in a logical sense (e.g., at what layer or layers of architecture such as TCP/IP should mechanisms be placed).

5. Security mechanisms typically involve more than a particular algorithm orprotocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transittime of a message from sender to receiver, then any protocol or networkthat introduces variable, unpredictable delays may render such time limits meaningless.

6. The attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

7. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.

8. Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment.

9. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

1.6 THE OSI SECURITY ARCHITECTURE

ITU-T Recommendation X.800, *Security Architecture for OSI*, defines a systematic approach of defining the requirements for security and characterizing

the approaches to satisfying those requirements. The OSI security architecture is useful to managers as a way of organizing the task of providing security. Furthermore, because this architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms.

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows.

Security attack: Any action that compromises the security of information owned by an organization.

Security mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.

Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

In the literature, the terms *threat* and *attack* are commonly used to mean more or less the same thing. In RFC 4949, *Internet Security Glossary, threats and attacks are defined as follows.*

Threat: A threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

Attack: An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

1.7 TYPES OF SECURITY ATTACKS

There are several types of security attacks but we can classify them based on the security goals they compromise. The following figure shows the categories of different types of security attacks.

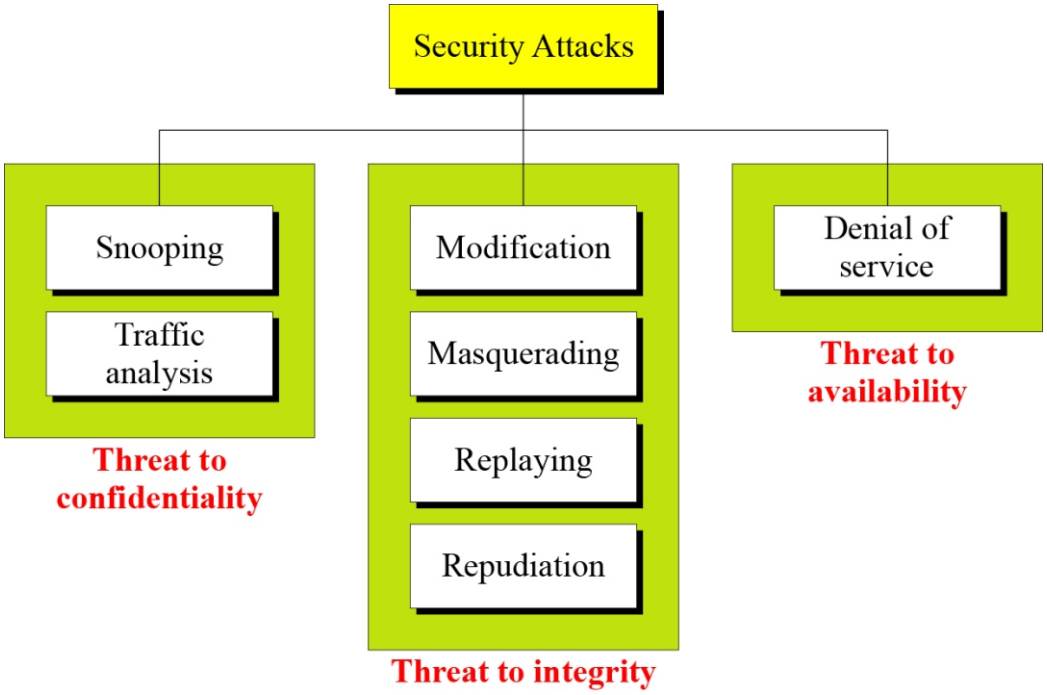

Fig: Taxonomy of attacks with relation to security goals

1.7.1 Attacks on Confidentiality

***Snooping* refers to unauthorized access to or interception of data.**

Traffic analysis refers to obtaining some other type of information by monitoring online traffic.

1.7.2 Attacks on Integrity

Modification means that the attacker intercepts the message and changes it.

Masquerading *or spoofing* happens when the attacker impersonates somebody else.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

1.7.3 Attacks on Availability

Denial of Service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system**.**

1.8 CLASSIFICATIONS OF SECURITY ATTACKS

According to both X.800 and RFC 4949, security attacks are classified as passive *attacks* and *active attacks.*

Fig: Categories of attacks

1.8.1 Passive Attacks

A passive attack attempts to learn or make use of information from the system but does not affect system resources. A passive attack is difficult to detect and isolate. These do not involve any modification to the contents. So the approach should be to prevent a passive attack rather than detection and corrective actions on it. Passive attacks are of two types:

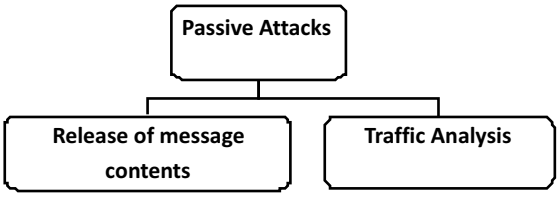

Fig: Classifications of Passive attacks

i) Release of message contents

The release of message contents means the message content may be disclosed somehow during transit. A third party may passively capture the message content without the knowledge of the sender and the receiver. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

ii) Traffic Analysis refers to obtaining some other type of information by monitoring online traffic. Suppose that wehad a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messagesbeing exchanged. This information might be useful in guessing the nature of the communication that was taking place.

1.8.2 Active Attacks:

An active attack attempts to alter system resources or affect their operation. These

attacks involve some modifications of original message in some manner or creation of false messages.

It is hard to prevent the active attacks. It is rather easier to detect and recover from them.

1.8.2.1 Types of active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:

Masquerade, replay, modification of messages, and denial of service.

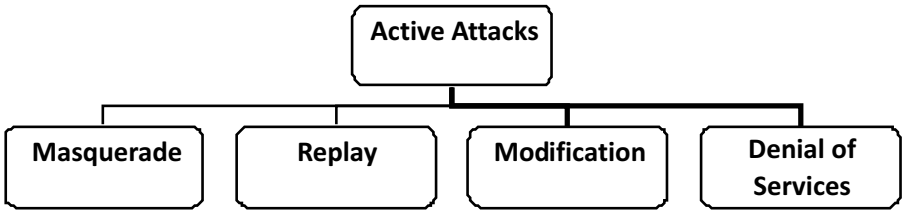

Fig: Classifications of active attacks

A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of theother forms of active attack. For example, authentication sequences can be capturedand replayed after a valid authentication sequence has taken place, thus enabling anauthorized entity with few privileges to obtain extra privileges by impersonating anentity that has those privileges.

Replay involves the passive capture of a data unit and its subsequent retransmissionto produce an unauthorized effect.

Modification of messages simply means that some portion of a legitimatemessage is altered, or that messages are delayed or reordered, to produce anunauthorized effect.

The **denial of service** prevents or inhibits the normal use or management ofcommunications facilities. This attack may have a specific target; forexample, an entity may suppress all messages directed to a particular destination (e.g., the securityaudit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

1.8.3 Passive versus Active Attacks

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success.On the other hand, it is quite difficult to prevent active attacks absolutely

because of the wide variety of potential physical, software, and network vulnerabilities.Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

Different types of attacks that threaten the security goals are explained in the following table.

Table: Passive versus Active Attacks

Attacks	Active/Passive	Threatening
Snooping Traffic Analysis	Passive	Confidentiality
Masquerading, Replay, Modification, Repudiation	Active	Integrity
Denial of Services	Active	Availability

1.9 SELF-ASSESSMENT QUESTIONS-

1Answer the following questions in brief.

1. What are the three goals of Information Security?

……

……

……

2. Identify different categories of active attacks

……

……

……

3. Identify different categories of passive attacks.

……

……

……

4. What is the difference between passive and active attacks?

……

……

……

5. Name the security attacks on confidentiality.

……

……

……

6. Name the security attacks on integrity

……

……

……

7. Name the security attacks on availability.

……

……

……

1.10 SECURITY SERVICES AND MECHANISMS

ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms is used to provide a service.

1.10.1 Security Services

Security ServicesX.800 divides these services into five categories and fourteen specific services

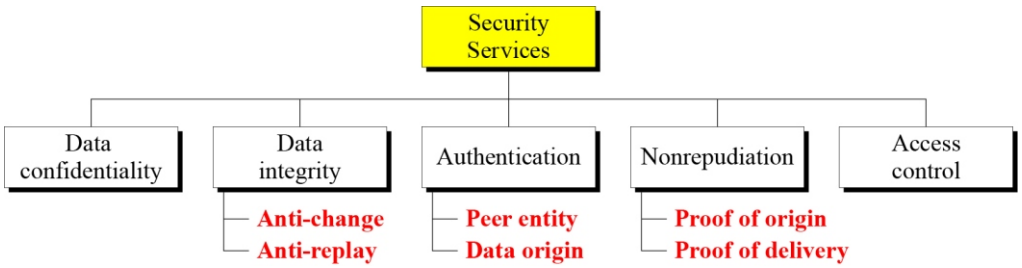

Fig: Categories of Security Services

Authentication

The authentication service is concerned with assuring that a communication isauthentic. In the case of a single message, such as a warning or alarm signal, thefunction of the authentication service is to assure the recipient that the messageis from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the servicemust assure that the connection is not interfered with in such a way that a thirdparty can masquerade as one of the two legitimate parties for the purposes ofunauthorized transmission or reception.Two specific authentication services are defined in X.800.

Peer entity authentication: Provides for the corroboration of the identityof a peer entity in an association. Two entities are considered peers if theyimplement to same protocol in different systems; for example two TCP modulesin two communicating systems. Peer entity authentication is provided foruse at the establishment of, or at times during the data transfer phase of, aconnection. It attempts to provide confidence that an entity is not performingeither a masquerade or an unauthorized replay of a previous connection.

Data origin authentication: Provides for the corroboration of the source of adata unit. It does not provide protection against the duplication or modificationof data units. This type of service supports applications like electronic mail, where there are no prior interactions between the communicating entities.

Access Control

In the context of network security, access control is the ability to limit and controlthe access to host systems and applications via communications links. To achievethis, each entity trying to gain access must first be identified, or authenticated, sothat access rights can be tailored to the individual.

Data Confidentiality

Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between twousers over a period of time. For example, when a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message.

These refinements are less useful than the broad approach and may even be

morecomplex and expensive to implement.The other aspect of confidentiality is the protection of traffic flow from analysis.This requires that an attacker not be able to observe the source and destination, frequency,length, or other characteristics of the traffic on a communications facility.

Data Integrity As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforwardapproach is total stream protection.

A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered underthis service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any largercontext, generally provides protection against message modification only.

We can make a distinction between service with and without recovery.Because the integrity service relates to active attacks, we are concerned with detection rather than prevention. If a violation of integrity is detected, then the servicemay simply report this violation, and some other portion of software or human intervention is required to recover from the violation. Alternatively, there are mechanisms available to recover from the loss of integrity of data, as we will reviewsubsequently. The incorporation of automated recovery mechanisms is, in general, the more attractive alternative.

Non-repudiation

Nonrepudiation prevents either sender or receiver from denying a transmitted message.Thus, when a message is sent; the receiver can prove that the alleged sender infact sent the message. Similarly, when a message is received, the sender can provethat the alleged receiver in fact received the message.

Availability Services

Both X.800 and RFC 4949 define availability to be the property of a system or asystem resource being accessible and usable upon demand by an authorized systementity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users requestthem). A variety of attacks can result in the loss of or reduction in availability. Someof these attacks are amenable to automated countermeasures, such as authenticationand encryption, whereas others require some sort of physical

action to preventor recover from loss of availability of elements of a distributed system.

1.10.2 Security Mechanisms

As defined in X.800, thesecurity mechanisms aredivided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service. X.800 distinguishes between reversible encipherment mechanisms and irreversible encipherment mechanisms. A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted. Irreversible encipherment mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.

1.10.3 Specific Security Mechanisms

Some specific security mechanism may be incorporated into the appropriate protocollayer in order to provide some of the OSI securityservices.

Encipherment

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or moreencryption keys.

Digital Signature

Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unitto prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

Access Control

A variety of mechanisms that enforce access rights to resources.

Data Integrity

A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange

A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding

The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control

Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization

The use of a trusted third party is to assure certain properties of a data exchange.

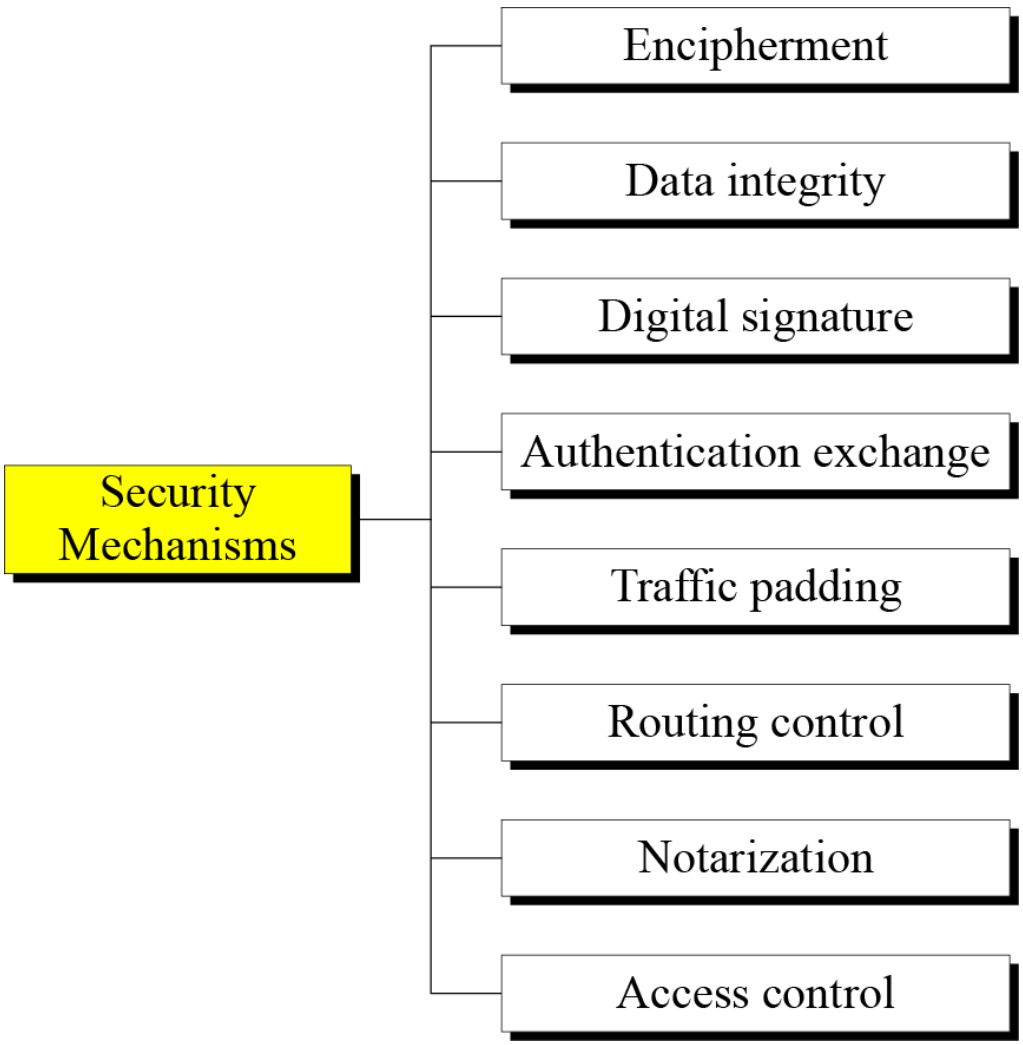

Fig: Security Mechanisms

1.10.4 Pervasive Security Mechanisms

Mechanisms those are not specific to any particularOSI security service or protocol layer.

Trusted Functionality

That which is perceived to be correct with respectto some criteria (e.g., as established by a security policy).

Security Label

The marking bound to a resource (which may be a data unit) that names or designates the security attributesof that resource.

Event Detection

It means the detection of security-relevant events.

Security Audit Trail

Data collected and potentially used to facilitate asecurity audit, which is an independent review andexamination of system records and activities.

Security Recovery

Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

1.11 RELATION BETWEEN SECURITY SERVICES AND MECHANISMS

The relationship between security services and mechanisms are summarized in the table below:

Table: Relationship between Security Services and Mechanisms

Security Services	Security Mechanisms
Data confidentiality	Encipherment and routing control
Data Integrity	Encipherment, Digital Signature, Data integrity
Authentication	Encipherment, Digital Signature, Authentication Exchanges
Nonrepudiation	Digital Signature, Data integrity and notarization
Access Control	Access control mechanism

1.12 SELF-ASSESSMENT QUESTIONS-2

1. What are the key challenges of Information Security?

……

……

……

2. What are Passive Attacks**?** Why are they difficult to detect? Name some passive attacks.

……

……

……

3. List and briefly define categories of security services.

……

……

……

1.13 KEY TERMS AND CONCEPTS

- **Computer Security** is concerned with protecting the assets of the computer system; information and services they provide.
- **Network Security** is the measures to protect data during their transmission.
- **Internet Security** is the measures to protect data during their transmission over a collection of interconnected networks called Internet.
- **Information Security** is about to prevent attacks or failing that to detect attacks on information based schemes/systems.
- **Security attack** means any action that compromises the security of information owned by an organization.
- **Security mechanism** is a mechanism that is designed to detect, prevent or recover from a security attack.
- **Security service** means a service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

1.14 ANSWER TO SELF-ASSESSMENT QUESTIONS-1

1. The three security goals are *confidentiality*, *integrity*, and *availability*.
   Confidentiality means protecting confidential information.
   Integrity means that changes to the information need to be done only by authorized entities.
   Availability means that information needs to be available to authorized entities.
2. Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.
3. Passive attack attempts to learn or make use of information from the system but does not affect system resources. A passive attack is difficult to detect and isolate. Passive attacks are of two types: Release of message contents and Traffic Analysis.
4. *Passive attacks* are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent *active attacks* absolutely because of the wide variety of potential physical, software,

and network vulnerabilities. Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.

5. The attacks on confidentiality include the following:

- *Snooping* refers to unauthorized access to or interception of data.
- *Traffic analysis* refers to obtaining some other type of information by monitoring online traffic.

6. The attacks on Integrity *include the following*

- *Modification* means that the attacker intercepts the message and changes it.
- *Masquerading or spoofing* happens when the attacker impersonates somebody else.
- *Replaying* means the attacker obtains a copy of a message sent by a user and later tries to replay it.
- *Repudiation* means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

7. The attacks on availability include the following.

- Denial of Service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

1.15 ANSWER TO SELF-ASSESSMENT QUESTIONS-2

1: Information security is both complex and challenging. Some of the reasons are as follows:

(i) The major requirements for security services can be confidentiality, authentication, nonrepudiation, or integrity. But the mechanisms used to meet those requirements can be quite complex.

(ii) In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features.

(iii) Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed.

(iv) Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense (e.g., at what layer or layers of an architecture such as TCP/IP

[Transmission Control Protocol/Internet Protocol] should mechanisms be placed).

(v) Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information.

(vi) The attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

(vii) There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.

(viii) Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment.

(ix) Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

(x) Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

1. Passive attacks are in the nature of eavesdropping on, or monitoring of, transmission, the goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of massage contents and traffic analysis. The release of message contents is easily understood.

A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

A second type of passive attack, traffic analysis, is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message.

The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these message .the opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged .This information might be useful in guessing the nature of the communication that was taking place . Passive attacks are very difficult to detect

because they do not involve any alteration of the data.

Typically, the message traffic is not sent and received in an apparently normal fashion and the sender nor receiver is aware that a third party has read the message or observed the traffic pattern.

However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

2. There are five security services: *data confidentiality*, *data integrity*, *authentication*, *on-repudiation*, and *access control*.

- *Data confidentiality* is to protect data from disclosure attack.
- *Data integrity* is to protect data from modification, insertion, deletion, and replaying.
- *Authentication* means to identify and authenticate the party at the other end of the line.
- *Nonrepudiation* protects against repudiation by either the sender or the receiver of the data.
- *Access control* provides protection against unauthorized access to data.

1.16 REFERENCES AND SUGGESTED READINGS

1. William Stallings, "Cryptography and Network Security-Principles and Practices", Prentice-Hall of India.
2. Charles P.Pfleeger, Shari Lawrence Pfleeger, even Shah, "Security in Computing", Pearson Education
3. Bernad Menezes, "Network Security & Cryptography", CENGAGE Learning.

Atul Kahate, "Cryptography and Network Security", TMH Publishing Company Limited

UNIT-2

INTRODUCTION TO CRYPTOGRAPHY

Unit Structure

2.0 INTRODUCTION

Cryptography, which comes from the Greek words *kryptos*, meaning "hidden," and *graphein*, meaning "to write," is the process of making and using codes to secure the transmission of information. Cryptanalysis is the process of obtaining the original message (called the plaintext) from an encrypted message (called the ciphertext) without knowing the algorithms and keys used to perform the encryption.

The science of encryption and decryption is known as cryptology. Cryptology encompasses both cryptography and cryptanalysis.

Encryption is the process of converting an original message into a form that is unreadable to unauthorized individuals-that is; to anyone without the tools to convert the encrypted message back to its original format.

Decryption is the process of converting the cipher text into a message that conveys readily understood meaning.

In order to understand cryptography and its uses, you must be familiar with a number of key terms that are used in cryptography.

In this unit, we will discuss the basic cryptography concepts and its related terminologies used in the area of Cryptography.

2.1 LEARNING OBJECTIVES

After studying this unit, you should be able to:

- Understand the basic terms used in cryptography.
- Understand the principles of cryptography and cryptanalysis.
- Describe different types of cryptanalytic attacks.
- Different types of cryptography
- Discuss the network security model
- Explain different classical encryption techniques.

2.2 BASIC TERMINOLOGIES

Cryptography

The art or science encompassing the principles and methods of transforming an

intelligible message into one that is unintelligible, and then retransforming that message back to its original form is called cryptography.

Plaintext: The original intelligible message.

Ciphertext: The transformed message.

Cipher: An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods

Key: Some critical information used by the cipher, known only to the sender& receiver

Encipher (encode): The process of converting plaintext to cipher text using a cipher and a key.

Decipher (decode): the process of converting cipher text back into plaintext using a cipher and a key.

Cryptanalysis: The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. It is also called code breaking.

Cryptology: It includes both cryptography and cryptanalysis

Code: An algorithm for transforming an intelligible message into an unintelligible one using a code-book.

2.3 CRYPTOGRAPHIC SYSTEMS

Cryptographic systems are generally classified along three independent dimensions:

(i) Type of operations used for transforming plain text to cipher text

All the encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged.

(ii) The number of keys used

If the sender and receiver uses same key then it is said to be symmetric key (or) single key (or) conventional encryption. If the sender and receiver use different keys then it is said to be public key encryption.

(iii) The way in which the plain text is processed

A **block cipher** processes the input and block of elements at a time, producing output block for each input block.

A **stream cipher** processes the input elements continuously, producing output element one at a time, as it goes along.

2.4 CRYPTANALYSIS

The process of attempting to discover the plaintext or the key or both is known as cryptanalysis. The strategy used by the cryptanalyst depends on the nature of the encryption scheme and the information available to the cryptanalyst.

A **cryptanalyst** can do any or all of six different things:

1. Attempt to break a single message
2. Attempt to recognize patterns in encrypted messages, to be able to break subsequent ones by applying a straightforward decryption algorithm
3. Attempt to infer some meaning without even breaking the encryption, such as noticing an unusual frequency of communication or determining something by whether the communication was short or long
4. Attempt to deduce the key, in order to break subsequent messages easily
5. Attempt to find weaknesses in the implementation or environment of use of encryption
6. Attempt to find general weaknesses in an encryption algorithm, without necessarily having intercepted any messages

2.4.1 Types of Cryptanalytic Attacks

There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

- **Cipher text only** – A copy of cipher text alone is known to the cryptanalyst.
- **Known plaintext** – The cryptanalyst has a copy of the cipher text and the corresponding plaintext.
- **Chosen plaintext** – The cryptanalysts gains temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.
- **Chosen cipher text** – The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key.

2.4.2 Brute-force attack

The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained. On an average, half of all possible keys must be tried to achieve success. If either type of attack succeeds in deducing the key, the effect is catastrophic: All future and past messages encrypted with that key are compromised.

2.5 STEGANOGRAPHY

A plaintext message may be hidden in any one of the two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text. A simple form of steganography, but one that is time consuming to construct is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message. Let us consider the following examples.

(I) The sequence of first letters of each word of the overall message spells out the real (Hidden) message.

(ii) Subset of the words of the overall message is used to convey the hidden message. Various other techniques have been used historically, some of them are:

Character marking – selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light.

Invisible ink – a number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

Pin punctures – small pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light.

Type written correction ribbon – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Drawbacks of Steganography

It requires a lot of overhead to hide a relatively few bits of information. Once the system is discovered, it becomes virtually worthless.

2.6 NETWORK SECURITY MODEL

A model for network security is shown in the following figure. A message is to be transferred from one party to another across some sort of Internet service. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of

communication protocols (e.g., TCP/IP) by the two principals. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

One is a security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the other is the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Otherwise a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

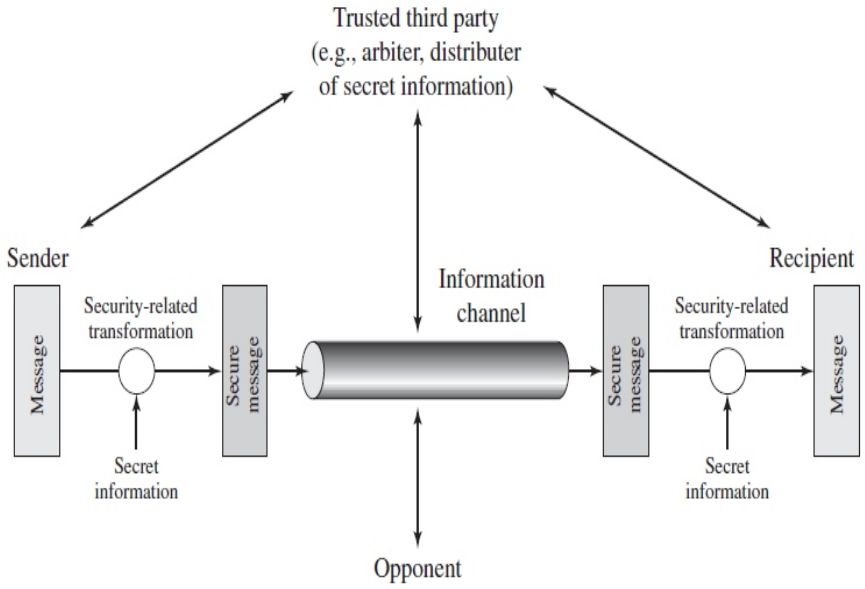

Fig: Network Security Model

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

2.7 TYPES OF CRYPTOGRAPHY

Based on the security models different cryptographic algorithms have been developed to prevent and defend attacks. Based on the type of algorithms cryptographic systems are categories in to two categories**.**

1. Symmetric key Cryptography

In symmetric key Cryptography, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are the same.

2. Public key Cryptography

In public key cryptography, encryption key is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.

2.8 SYMMETRIC KEY CRYPTOGRAPHY

A symmetric encryption scheme has five ingredients:

Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.

Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.

The exact substitutions and transformations performed by the algorithm depend on the key.

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

There are two requirements for secure use of conventional encryption:

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 or figure out the key. This requirement is usually stated in a stronger form: The opponent should be unable to decrypt ciphertext or discover the key even if he or she 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.

We assume that it is impractical to decrypt a message on the basis of the ciphertext plus knowledge of the encryption/decryption algorithm. In other words, we do not need to keep the algorithm secret; we need to keep only the key secret.

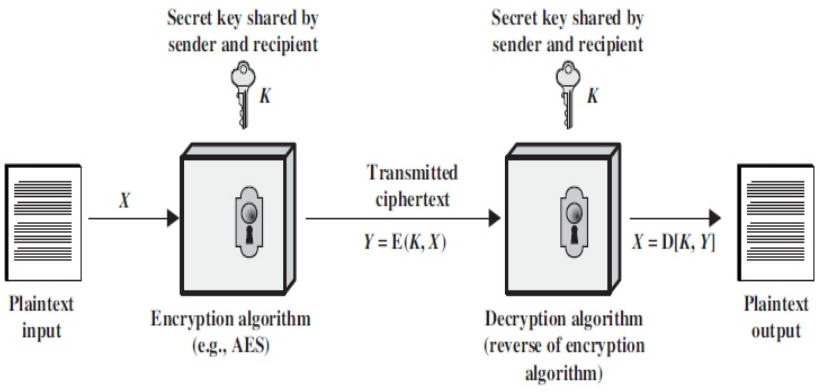

Fig.: Symmetric key Cryptography

This feature of symmetric encryption is what makes it feasible for widespread use. The fact that the algorithm need not be kept secret means that manufacturers can and have developed low-cost chip implementations of data encryption algorithms. These chips are widely available and incorporated into a number of products. With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key.

Let us take a closer look at the essential elements of a symmetric encryption scheme, using the following figure.

A source produces a message in plaintext, $X = [X_1, X_2... X_M]$. The M elements of X are letters in some finite alphabet. Traditionally, the alphabet usually consisted of the 26 capital letters. Now days, the binary alphabet {0, 1} is typically used. For encryption, a key of the form $K = [K_1, K_2... K_J]$ is generated. If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it to both source and destination.

With the message X and the encryption key K as input, the encryption algorithm forms the cipher text $Y = [Y_1, Y_2... Y_N]$. We can write this as

$$Y = E (K, X)$$

This notation indicates that Y is produced by using encryption algorithm E as a function of the plaintext X, with the specific function determined by the value of the key K.

The intended receiver, in possession of the key, is able to invert the transformation:

X = D (K, Y).

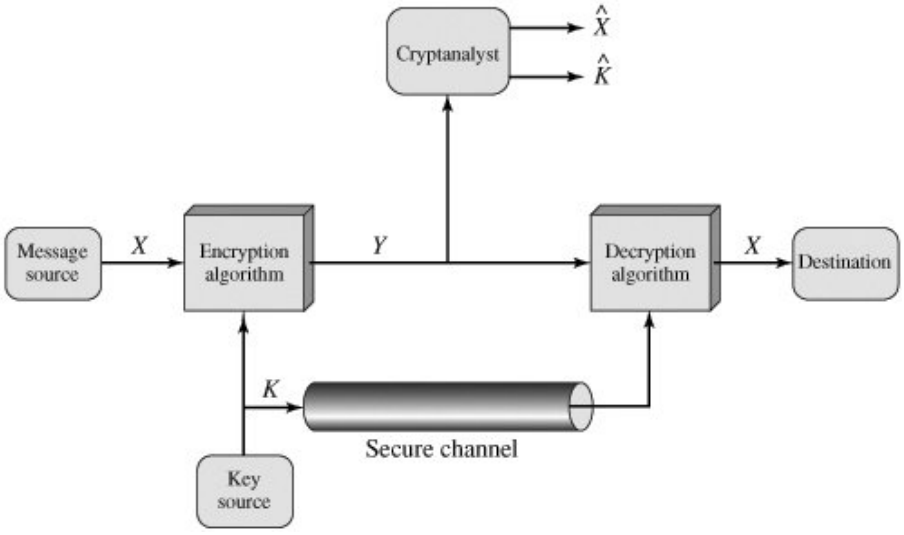

Fig.: Essential elements of a symmetric encryption

An opponent, observing Y but not having access to K or X, may attempt to recover X or K or both X and K. It is assumed that the opponent knows the encryption (E) and decryption (D) algorithms. If the opponent is interested in only this particular message, then the focus of the effort is to recover X by generating a plaintext estimate

2.8.1 Unconditionally secure vs. computationally secure Encryption

Unconditionally secure Encryption:

An encryption scheme is **unconditionally secure** if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. That is, no matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext, simply because the required information is not there. There is no encryption algorithm that is unconditionally secure. Therefore, all that the users of an encryption algorithm can strive for is an algorithm that meets one or both of the following criteria:

- The cost of breaking the cipher exceeds the value of the encrypted information.
- The time required to break the cipher exceeds the useful lifetime of the information.

Computationally secure Encryption

An encryption scheme is said to be **computationally secure** if either of the foregoing two criteria are met. The rub is that it is very difficult to estimate the amount of effort required to cryptanalyze ciphertext successfully.

1.8.2 Block Cipher Vs. Stream Cipher

Now we will discuss the method in which the plain text is converted into cipher text. In some methods, plain text is treated as numerous units or blocks and then it is converted into cipher text. But in some methods, plain text is divided into bits and these bits individually are given as input to the method which converts each single bit to the cipher text.

Therefore, there are two cipher methods (Block Cipher and Stream Cipher) in which plain text is given as input in order to convert them to their corresponding cipher text using any of these ciphering techniquees.

Block Cipher

Block Cipher, as the name suggests, takes input (i.e. plain text) and divides the plain text into number of units or blocks. After receiving input, plain text as a unit or block is encrypted with the key and converts it to a cipher text**.**

Advantages of Block Cipher:

- It is faster than stream cipher.
- If any block contains any transmission error then it will not have effect on other blocks.
- It is not sufficient in hardware but may be used to connect keyboard to CPU (central process unit)
- Block ciphers can be easier to implement in software, because there is no bit manipulation like in stream cipher which is time consuming process and treats data in computer-sized blocks
- Block Cipher is more suitable in trading applications.
- Short blocks at the end of a message can also be added with blank or zero status.

Disadvantages of Block Cipher:

- If two same unit or blocks of plaintext is there, then the cipher produces same cipher text for units or blocks.
- It is easy to insert or delete units/blocks.
- Block encryption may be more susceptible to cryptanalysis attack as compared to stream cipher as block cipher provides strong hints to attacker because two same units produce same cipher text.
- Block encryption is more susceptible to replay as compare to stream encryption.

Stream Cipher

Stream Cipher takes input (i.e. plain text) and divide this plain text into number of bits (combination of such bits is plain text). After receiving single bit which represents as a part of plain text is encrypted with the key and converts it to a cipher text.

Advantages of Stream Cipher:

- Stream cipher is suitable for hardware implementation as only encryption and decryption data one bit at a time.
- Stream cipher is less susceptible to cryptanalysis than block cipher as block cipher provides strong hints to attacker because two same units produce same cipher text.
- Stream cipher is less vulnerable to insertion or deletion of units.
- This cipher can be more easily analyzed mathematically.
- It is more suitable for military applications.

Disadvantage of Stream Cipher:

- If during transmission, any bit is lost or become erroneous, then it is difficult to

re-arrange and collect all the converted cipher text which in return may result in re-transmission of the entire plain text.

- It is slower than block but can be configured to make faster by implemented in special purpose hardware capable of encryption several million bits for second.
- It is not suitable for the software.

2.9 CLASSICAL ENCRYPTION TECHNIQUES

The two basic building blocks of Classical encryption techniques are substitution and transposition.

2.9.1 Substitution Techniques

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols to obtain the cipher text.

If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Caesar Cipher

The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. Let us consider the following example.

Plaintext: meet me after the toga party

Cipher: PHHW PH DIWHU WKH WRJD SDUWB

Note*:* The alphabet is wrapped around, so the letter following Z is A.

We can define the transformation by listing all possibilities, as follows:

Plaintext: a b c d e f g h i j k l m n o p q r s t u v w x y z

Ciphertext: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Let us assign a numerical equivalent to each letter:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows. For each plaintext letter: p, substitute the cipher text letter: C

$$C = E(3, p) = (p + 3) \bmod 26$$

Encryption:

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

$$C = E(k, p) = (p + k) \bmod 26$$

Where, k takes on a value in the range 1 to 25.

Decryption:

The decryption algorithm for the Caesar Cipher is simply

$$p = D(k, C) = (C - k) \bmod 26$$

Limitations of the Caesar Cipher

If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys.

- ***Note:*** Three important characteristics of this problem enabled us to use a brute force

Cryptanalysis of Caesar Cipher:

1. The encryption and decryption algorithms are known.
2. There are only 25 keys to try.
3. The language of the plaintext is known and easily recognizable.**2.9.1.1 Monoalphabetic Ciphers**

A **monoalphabetic cipher** uses a fixed substitution over the entire message. It is an improvement over Caesar Cipher. It eliminates the limitations of Caesar Cipher.

The Caesar cipher is far from secure with only 25 possible keys, in which a simple brute force cryptanalysis is possible.

A dramatic increase in the key space can be achieved by allowing an arbitrary substitution. Before proceeding, we define the term *permutation*.

A **permutation** of a finite set of elements is an ordered sequence of all the elements of S, with each element appearing exactly once.

For example, if ,S={a,b,c}, there are six permutations of S:

abc, acb, bac, bca, cab, cba

In general, there are n! permutations of a set of n elements, because the first element can be chosen in one of *n* ways, the second in (n-1)ways, the third in (n-2)ways, and so on.

Recall the assignment for the Caesar cipher:

Plain: a b c d e f g h i j k l m n o p q r s t u v w x y z

Cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

If, instead, the "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4×10^{26} keys.

Play fair Cipher

The best-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams. The Playfair algorithm is based on the use of a 5 × 5 matrix of letters constructed using a keyword.

Example: Let us consider the example solved by Lord Peter Wimsey in Dorothy Sayers's *Have His Carcase:*

M	*O*	*N*	*A*	*R*
C	*H*	*Y*	*B*	*D*
E	*F*	*G*	*I/J*	*K*
L	*P*	*Q*	*S*	*T*
U	*V*	*W*	*X*	*Z*

In this case, the keyword is *monarchy*. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter. Plaintext is encrypted two letters at a time, according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs become BP and ea becomes IM (or JM, as the encipherer wishes).

The Playfair cipher is a great advance over simple monoalphabetic ciphers.

For one thing, whereas there are only 26 letters, there are 26 × 26 = 676 digrams, so that identification of individual digrams is more difficult. Furthermore, the relative frequencies of individual letters exhibit a much greater range than that of digrams,

making frequency analysis much more difficult. For these reasons, the Play air cipher was for a long time considered unbreakable. It was used as the standard field system by the British Army in World War I and still enjoyed considerable use by the U.S. Army and other Allied forces during World War II.

Limitations of Playfair Cipher:

Despite this level of confidence in its security, the Play air cipher is relatively easy to break, because it still leaves much of the structure of the plaintext language intact. A few hundred letters of ciphertext are generally sufficient.

2.9.1.2 Polyalphabetic Ciphers

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is polyalphabetic cipher. All the techniques have the following features in common. A set of related monoalphabetic substitution rules are used A key determines which particular rule is chosen for a given transformation.

Vigenere Cipher:

In this scheme, the set of related monoalphabetic substitution rules consisting of 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g., Caesar cipher with a shift of 3 is denoted by the key value 'd‟ (since a=0, b=1, c=2 and so on).

To aid in understanding the scheme, a matrix known as vigenere tableau is constructed each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top. Refer the following Vigenere tableau.

The process of Encryption is simple: Given a key letter X and a plaintext letter y, the cipher text is at the intersection of the row labelled x and the column labelled y; in this case, the cipher text is V.

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

Table: Vigenere tableau

	PLAIN TEXT															
KEY LETTERS		a	b	c	d	e	f	g	h	i	j	k	…	x	y	z
	a	A	B	C	D	E	F	G	H	I	J	K	…	X	Y	Z
	b	B	C	D	E	F	G	H	I	J	K	L	…	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	…	Z	A	B
	d	D	E	F	G	H	I	J	K	L	M	N	…	A	B	C
	e	E	F	G	H	I	J	K	L	M	N	O	…	B	C	D
	f	F	G	H	I	J	K	L	M	N	O	P	…	C	D	E
	g	G	H	I	J	K	L	M	N	O	P	Q	…	D	E	F
	:	:	:	:	:	:	:	:	:	:	:	:	…	:	:	:
	x	X	Y	Z	A	B	C	D	E	F	G	H	…			W
	y	Y	Z	A	B	C	D	E	F	G	H	I	…			X
	z	Z	A	B	C	D	E	F	G	H	I	J	…			Y

Example: Let us consider the following.

Key = d e c e p t i v e d e c e p t i v e d e c e p t i v e

PT = w e a r e d i s c o v e r e d s a v e y o u r s e l f

CT = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.

Advantages of Vigenere Cipher

- There are multiple cipher text letters for each plaintext letter, so it is almost secured.

Disadvantages of Vigenere Cipher

- The key is periodically repeated
- Data can be detected from the key length

One Time Pad Cipher

It is an unbreakable cryptosystem. It represents the message as a sequence of 0s and 1s.This can be accomplished by writing all numbers in binary, for example, or

by using ASCII. The key is a random sequence of 0's and 1's of same length as the message. Once a key is used, it is discarded and never used again. The system can be expressed as follows:

$C_i = P_i \oplus K_i$

C_i - i^{th} binary digit of cipher text

P_i - i^{th} binary digit of plaintext

K_i - i^{th} binary digit of key

Exclusive OR operation

Thus the cipher text is generated by performing the bitwise XOR of the plaintext and the key.

Decryption uses the same key. Because of the properties of XOR, decryption simply involves the same bitwise operation:

$P_i = C_i \oplus K_i$

e.g., plaintext = 0 0 1 0 1 0 0 1

Key = 1 0 1 0 1 1 0 0

Ciphertext = 1 0 0 0 0 1 0 1

Advantage:

- Encryption method is completely unbreakable for a ciphertext only attack.

Disadvantages:

- It requires a very long key which is expensive to produce and expensive to transmit.
- Once a key is used, it is dangerous to reuse it for a second message; any knowledge on the first message would give knowledge of the second.

2.9.2 Transposition Techniques

All the techniques examined so far involve the substitution of a cipher text symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Rail fence techniques:

Rail fence is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Plaintext = meet at the school house

To encipher this message with a rail fence of depth 2, we write the message as follows:

m e a t e c o l o s

e t t h s h o h u e

The encrypted message is MEATECOLOSETTHSHOHUE

Row Transposition Cipher

A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.

e.g., plaintext = meet at the school house

Key = 4 3 1 2 5 6 7

Plain Text = m e e t a t t
h e s c h o o
l h o u s e

The cipher text is: esotcueehmhlahstoeto

Strength of Row Transposition Cipher

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.

2.10 SELFASSESSMENT QUESTIONS

1. Define cryptanalysis .List the types of cryptanalytic attacks.

……

……

……

……

2. Differentiate symmetric and asymmetric key Cryptography.

……

……

……

……

3. Differentiate unconditionally secured and computationally secured algorithm.

……

……

……

……

4. Specify the components of secret key cryptography.

……

……

……

……

5. Compare Substitution and Transposition techniques.

……

……

……

……

6. Differentiate between Block cipher and Stream Cipher.

……

……

……

……

1.11 KEY TERMS & CONCEPTS

- **Cryptology** is the study of cryptography and cryptanalysis. Cryptology encompasses both cryptography and cryptanalysis.
- **Cryptography** is the study of principles and methods of transforming a message into an unintelligible form and then retransforming that message back to its original form.
- **Cryptanalysis** is the process of attempting to discover the plaintext or the key or both without knowledge of the key. It is also called code breaking
- **Steganography** is a technique to conceal the existence of the message.
- **Transposition** cipher is an encryption technique which is achieved by performing some sort of permutation on the plaintext letters.
- A **block** cipher processes the input one block of elements 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.

2.12 ANSWER TO SELFASSESSMENT QUESTIONS

1. Cryptanalysis is a process of attempting to discover the key or plaintext or both. The types of cryptanalytic attacks are:

(i) Cipher text only

(ii) Known plaintext

(iii) Chosen plaintext

(iv) Chosen cipher text

(v) Chosen text

2. Difference between symmetric and asymmetric key cryptography are as follows:

Symmetric Cryptography uses single key to encrypt and decrypt data whereas Asymmetric Cryptography uses public key to encrypt the data and private key to decrypt it.

Symmetric key cryptography is much faster than asymmetric key encryption.

Symmetric key cryptography does not require a lot of computer resources when compared to public key encryption which uses up more computer resources.

In Symmetric Cryptography, secret key exchange is a problem. But in asymmetric cryptography, there is no such key exchange problem.

In Symmetric Cryptography, origin and authenticity of message cannot be guaranteed whereas Asymmetric Cryptography provides method for message authentication, detection of tampering, non-repudiation.

Symmetric Cryptography prevents widespread message security compromise but in Asymmetric Cryptography, widespread security compromise is possible.

• Examples of Symmetric Cryptography include DES, AES and examples of Asymmetric Cryptography are RSA, ECC.

2. An Encryption algorithm is unconditionally secured means:

(i) If the cipher text generated by the encryption scheme doesn't contain enough information to determine corresponding plaintext.

An Encryption Algorithm is computationally secured means:

(i) The cost of breaking the cipher exceeds the value of enough information.

(ii) Time required to break the cipher exceed the useful lifetime of information.

4. The five components of secret key cryptography are:

(i) Plaintext

(ii) Encryption algorithm

(iii) Secret key

(iv) Cipher text

(v) Decryption algorithm

5. The two encryption techniques are different in the following ways.

Substitution	Transposition
• A substitution techniques is one in which the letters of plaintext are replaced by other letter or by number or symbols. • Example: Caesar cipher.	• It means, different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. • Example: DES, AES

6. Following are the advantages and disadvantages of Block and Stream Cipher.

Advantages of Block Cipher:

- It is faster than stream cipher.
- If any block contains any transmission error then it will not have effect on other blocks.
- It is not sufficient in hardware but may be used to connect keyboard to CPU (central process unit)
- Block ciphers can be easier to implement in software, because there is no bit manipulation like in stream cipher which is time consuming process and treats data in computer-sized blocks
- Block Cipher is more suitable in trading applications.
- Short blocks at the end of a message can also be added with blank or zero status.

Disadvantages of Block Cipher:

- If two same unit or blocks of plaintext is there, then the cipher produces same cipher text for units or blocks.
- It is easy to insert or delete units/blocks.
- Block encryption may be more susceptible to cryptanalysis attack as compared to stream cipher as block cipher provides strong hints to attacker because two same units produce same cipher text.
- Block encryption is more susceptible to replay as compare to stream encryption.

Advantages of Stream Cipher

- Stream cipher is suitable for hardware implementation as only encryption and decryption data one bit at a time.
- Stream cipher is less susceptible to cryptanalysis than block cipher as block cipher provides strong hints to attacker because two same units produce same cipher text.
- Stream cipher is less vulnerable to insertion or deletion of units.

- This cipher can be more easily analyzed mathematically.
- It is more suitable for military applications.
- It is less useful for attackers as same plain text is encrypted but in single individual bits and not in units.

Disadvantage of Stream Cipher:

- If during transmission, any bit is lost or become erroneous, then it is difficult to re-arrange and collect all the converted cipher text which in return may result in re-transmission of the entire plain text.
- It is slower than block but can be configured to make faster by implemented in special purpose hardware capable of encryption several million bits for second.
- It is not suitable for the software.

2.13 REFERENCES AND SUGGESTED READINGS

1. William Stallings, "Cryptography and Network Security-Principles and Practices", Prentice-Hall of India.
2. Charles P.Pfleeger, Shari Lawrence Pfleeger, even Shah, "Security in Computing", Pearson Education
3. Bernad Menezes, "Network Security & Cryptography", CENGAGE Learning.
4. Atul Kahate, "Cryptography and Network Security", TMH Publishing Company Limited.

UNIT-3

CRYTOGRAPHIC ALGORITHMS

3.0 INTRODUCTION

We have discussed in the previous unit that cryptography is an important means of protecting information from attackers.

Cryptography is the science of transforming information into a secure form so that it can be transmitted or stored and unauthorized persons cannot access it. Whereas Cryptography scrambles a message so that it cannot be viewed, steganography hides the existence of data. What appears to be a harmless image can contain hidden data, usually some types of messages, embedded within the image. In this unit we will discuss about different algorithms designed for encryption and decryption in both symmetric and asymmetric encryption algorithms.

3.1 LEARNING OBJECTIVES

- After going through this unit, you will be able to understand:
- What is different cryptographic algorithm?
- What is Hashing, Message Digest?
- What is the difference between Symmetric and Asymmetric key Cryptographic algorithm?
- How Cryptography is used in secure applications?

3.2 CRYTOGRAPHIC ALGORITHMS.

There are three categories of cryptographic algorithms. These are known as hash algorithms, symmetric encryption algorithms, and asymmetric encryption algorithms.

3.2.1 Hash Algorithm

The most basic type of cryptographic algorithm is a hash algorithm. Hashing is a process for creating a unique digital fingerprint for a set of data. This fingerprint, called a hash (sometimes called a one-way hash or digest) represents the contents. Although hashing is considered a cryptographic algorithm, its purpose is not to create a ciphertext that can later be decrypted.

Hashing is primarily used for comparison purposes. A hash that is created from a set of data cannot be reversed. For example, if 12,345 is multiplied by 143, the result is 1,765,335. If the number 1,765,335 was given to a user, and the user was asked to

determine the two original numbers to create1, 765, 335, it would be virtually impossible to work backward and derive the original numbers. This is because there are too many mathematical possibilities.

Hashing is similar in that is used to create a value, yet it is not possible to work —backward to determine the original set of data. A practical example of hash algorithm is used with some automated teller machine (ATM) cards. A bank customer has a personal identification number (PIN) of 93542. This number is hashed and the result is permanently stored on a magnetic stripe on the back of the ATM card. When visiting an ATM, the customer is asked to insert the card and then enter the PIN on a keypad. ATM takes the PIN entered and hashes it with the same algorithm used to create the hash stored on the card. If the two values match, then the user can access the ATM. Hashing with ATMs is shown below in the figure.

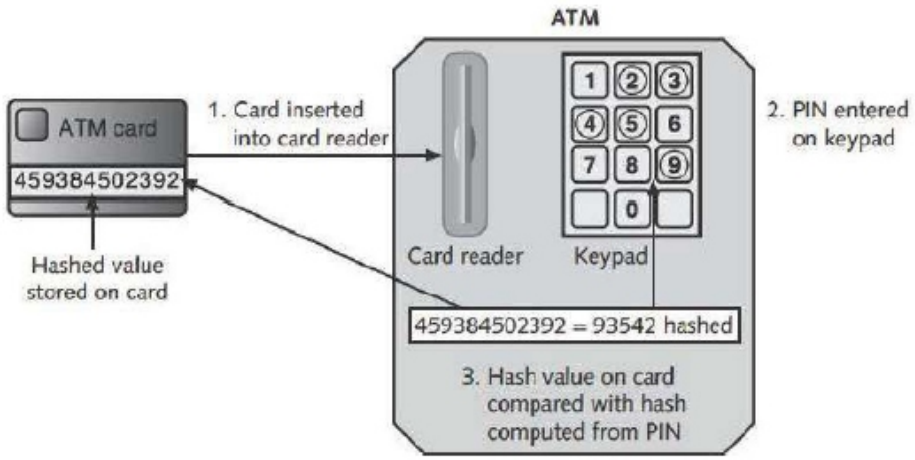

Fig: Hashing at an ATM

Hashing algorithm is considered secure if it has these characteristics:

Fixed size: A hash of a short set of data should produce the same size as a hash of a long set of data. For example, a hash

i. of the single letter a is 86be7afa339d0fc7cfc785e72f578d33, while a hash of 1 million occurrences of the letter a is 4a7f5723f954eba1216c9d8f6320431f,, the same length.

ii. Unique: Two different sets of data cannot produce the same hash, which is known as a collision. Changing a single letter in one data set should produce an entirely different hash. For example, a hash of Today is Sunday is8b9872b8ea83df7152ec0737d46bb951 while the hash of Today is Sunday (changing the initial S to s) is 4ad5951de752ff7f579a86bfafc2c.

iii. Original: It should be impossible to produce a data set that has a desired or

predefined hash.

iv. Secure: The resulting hash cannot be reversed in order to determine the original plaintext

Hashing is used to determine the integrity of a message or contents of a file. In this case, the hash serves as a check to verify that the original contents have not been changed. For example, when an e-mail message is created, a hash can also be created based on the message contents. The message and the hash are transmitted to the recipient, or the hash is posted where the reader can retrieve it. Upon receiving the message, the same hash is generated again on the message. If the original hash is the same as the new hash, then the message has not been altered. However, if an attacker performs a man-in-middle attack to intercept and change the message, the hash values will not match. Using hashing for protecting against man-in-the-middle attacks as shown in figure below.

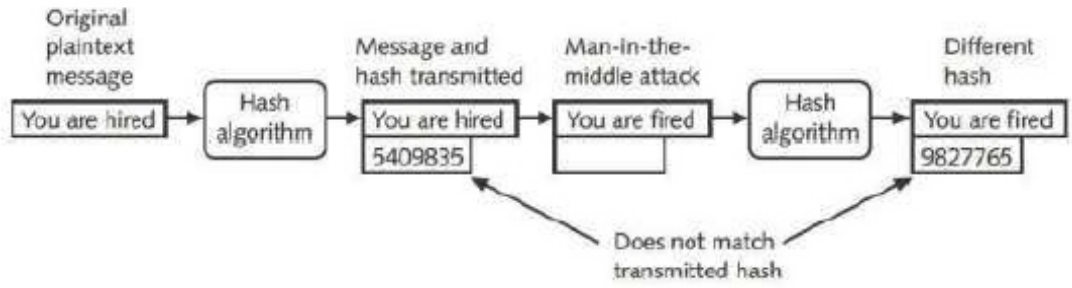

Fig: Man-in-the-middle attack defeated by Hashing

A variation that provides improved security is the Hashed Message Authentication Code (HMAC). HMAC begins with a shared secret key that is in the possession of both the sender and receiver. The sender creates a hash and then encrypts that hash with the key before transmitting it with original data. The receiver uses their key to decrypt the hash and then creates their own hash of the data, comparing the two values. HMAC is widely used by Internet security protocols to verify the integrity of transmitted data during secure communications. Hash values are often posted on download sites in order to verify the integrity of files that can be downloaded. Hashing can be used to verify the integrity of data. The protections provided by hashing are given in the below table.

Table: Information protections by hashing cryptography

Characteristic	Protection?
Confidentiality	No
Integrity	Yes
Availability	No
Authenticity	No
Non repudiation	N

The Most common hash algorithms are Message Digest, Secure hash Algorithm. Whirlpool, RIPEMD, and Password hashes.

3.2.2 Message Digest (MD)

One common hash algorithm is the Message Digest (MD) algorithm, which has three versions. Message Digest 2 (MD2) takes plaintext of any length and creates hash 128 bits long. MD2 begins by dividing the message into 128 bit sections. If the message is less than 128 bit, data known as padding is added. For example, if a 10-byte message is abcdefghij, MD2 would pad the message to make it abcdefghij666666 to create a length of 16 bytes (128 bits). The padding is always the number of bytes that must be added to create a length of16 bytes; in this example, 6 is he padding because 6 more bytes had to be added to the 10 original bytes. After padding, a 16-byte checksum is appended to the message. Then the entire string is proces128 bit hash. MD2 was developed in 1989 and was optimized to run on Intel-based computers that processed 8 bit at a time. MD2 is considered too slow today and is rarely used.

3.2.3 Message Digest 4

(MD4) was developed in 1990 for computers that processed 32 bits at a time. Like MD2, MD4 takes plaintext and creates a hash of128 bits. The plaintext message itself is padded to a length of 512 bits instead of 128 bits. The plaintext message itself is padded to a length of 512 bits instead of 128 bits as with MD2. Flaws in the MD4 hash algorithm have prevented this MD from being widely accepted.

3.2.4 Message Digest 5 (MD5)

A revision of MD4, was created the following year and designed to address MD4's weaknesses.

Like MD4, the length of a message is padded to 512 bits. The hash algorithm then uses four variables of 32 bits each in a round-robin fashion to create a value that is compressed to generate the hash. Weaknesses have been revealed in the compression function that could lead to collisions, so some security experts recommend that a more secure hash algorithm be used instead.

Note: The TCP/IP protocol Simple Network Management Protocol (SNMP) version 3 default protocol is MD5.

3.2.5 Secure Hash algorithm (SHA)

A more secure hash than MD is the Secure Hash algorithm (SHA). Like MD, the SHA is a family of hashes. The first version was SHA-0, yet due to a flaw it was withdraw shortly after it was first released. It successor, SHA-1, is patterned after

MD4 and MD5, but creates a hash that is 160 bit in length instead of 128 bits. SHA pads messages of fewer than 512 bits with zeros and an integer that describes the original length of the message. The padded message is then run through the SHA algorithm to produce the hash.

Note: SHA-1 was developed in 1993 by the U.S. National Security Agency (NSA) and the National Institute of Standards and Technology (NIST). The other hashes are known as SHA-2,

SHA-2 actually is composed of four variations, known as SHA-224, SHA-256, SHA-384 and SHA-512 (the number following SHA indicates the length in bits of the hash that is generated). SHA-2 is considered to be *secure hash. Yet, there have been no weaknesses identified with it.*

Note: In 2007, an open competition for new SHA-3 hash was announced. Of the 51 entries that were accepted to Round 1 of the competition, only 14 were selected for Round 2 (one of the entries rejected was a new MD6). In late 2010, five finalists were announced for the final round 3, with the new standard expected to appear by 2012.

3.2.6 Whirlpool

Whirlpool is a relatively recent cryptographic hash function that has received international recognition and adoption by standards organizations, including the International Organization for Standardization (ISO). Named after the first galaxy recognized to have a spiral structure, it creates a hash of 512 bits. Whirlpool is being implemented in several new commercial cryptography applications.

TIP: According to creators, Whirlpool will not be patented and can be freely used for any purpose.

3.2.7 RACE Integrity Primitives Evaluation Message Digest (RIPEMD)

Another hash was developed by the Research and Development and Advanced Communications technologies (RACE) organization, which is affiliated with the European Union (EU). RIPEMD stands for RACE Integrity Primitives Evaluation Message Digest, which was designed after MD4.The primary design feature of REPEMD is two different and independent parallel chains of computation, the results of which are then combined at the end of the process. RIPEMD has several versions and all based on the length of the hash created. RIPEMD-128 is a replacement for the original RIPEMD and is faster than RIPEMD-160. RIPEMD-256 and RIPEMD-320 reduce the risk of collisions, yet do not provide any higher levels of security.

3.3 PASSWORD HASHES

Another use for hashes is in strong password. When a password for an account is created, the password is hashed and stored. When a user enters her password to log in, that password is likewise hashed and compared with the stored hashed version; if the two hashes match, then the user is authorized. Microsoft Windows operating systems hash password in two ways. The first is known as the LM (LAN Manager) hash. The LM hash is in not actually a hash, because a hash is a mathematical function used to fingerprint the data. The LM hash instead uses a cryptography one-way function (OWF): instead of encrypting the password with another key, the password itself is the key. The LM has is considered a very weak function for storing password. First, the LM hash is not case sensitive, meaning that there is no difference between uppercase (A) and lowercase

(a). This significantly reduces the character set that an attacker must use. Second, the LM has splits all password into two7- character parts. If the original password is fewer the 14 characters, it simply pads the parts; if it is longer, the extra characters are dropped. This means that an attacker attempting to break an LM hash must only break two 7-character passwords from a limited character set. To address the security issues in the LM hash, Microsoft introduced the NTLM (New Technology LAN Manager) hash. Unlike the LM hash, the NTLM has does not limit stored password to two 7-character parts. In addition, it is case sensitive and has larger character set of 65,535 characters. The original version of NTLM uses a weak cryptographic function and does not support more recent cryptographic methods; Microsoft recommends that it should not be used. The current version is NTLMv2 and uses HMAC with MD5. It is considered a much stronger hashing algorithm.

The salt, along with the number of "rounds" (iterations) used with the salt, is stored along with the "salted" password hash.

3.4 SYMMETRIC CRYPTOGRAPHIC ALGORITHMS

The original cryptographic algorithms for encrypting and decrypting documents are symmetric

Cryptographic algorithms. These include the Data Encryption Standard, Triple Data Encryption Standard, Advanced Encryption Standard, and several other algorithms.

3.4.1 Understanding Symmetric Algorithms

Symmetric cryptographic algorithms use the same shared single key to encrypt and decrypt a document. Unlike hashing in which the hash is not intended to be decrypted, symmetric algorithms are designed to encrypt and decrypt the cipher text; a document encrypted with a symmetric cryptographic algorithm by Bob will be decrypted when received by Alice. It is therefore essential that the key be kept confidential, because if an attacker obtained the key, he could read all the encrypted documents. For this reason, symmetric encryption is also called Private Key cryptography. Symmetric encryption is illustrated in Figure below where identical keys are used to encrypt and decrypt a document.

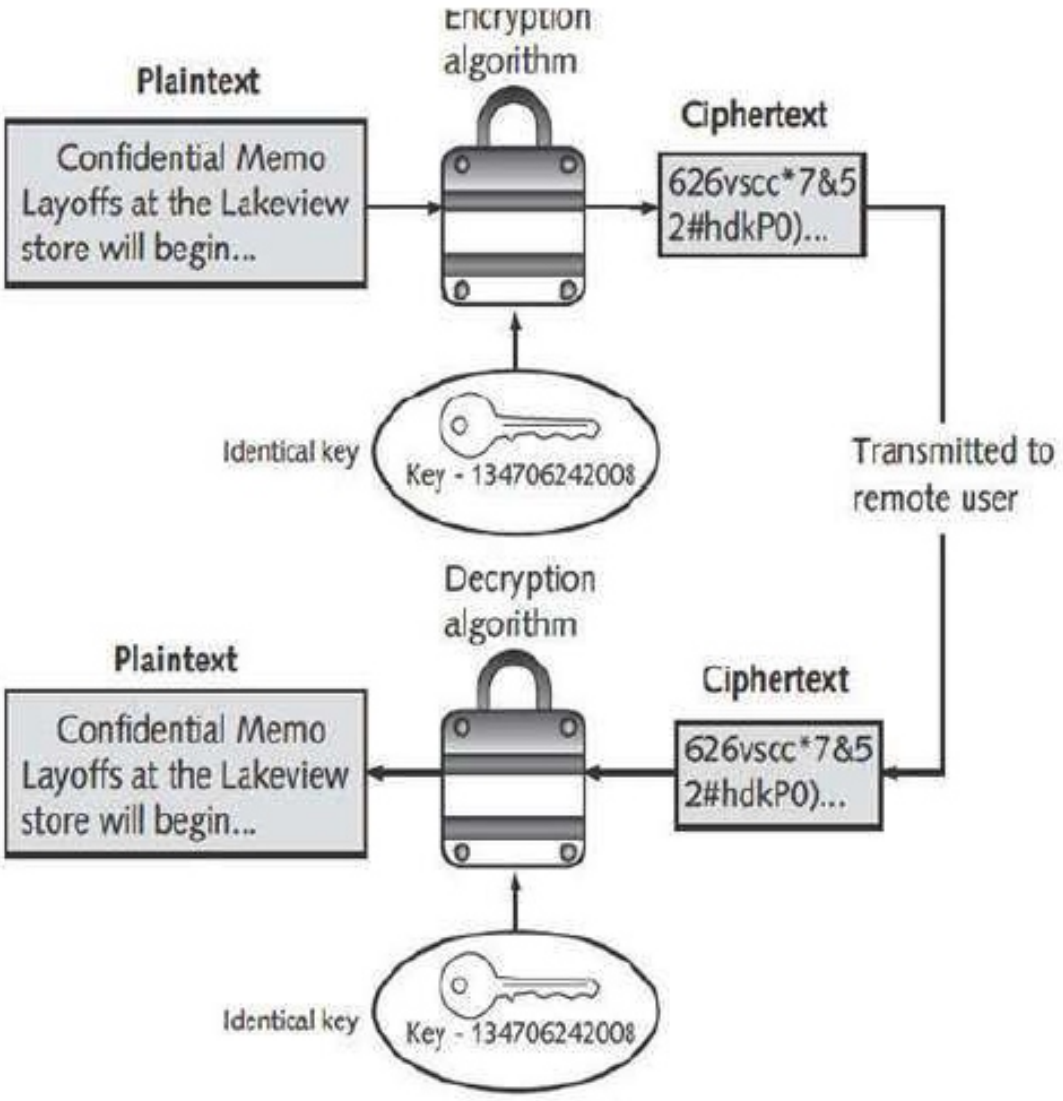

Fig: Symmetric (Private Key) Cryptography

Symmetric algorithms, like other types of cryptographic algorithms, can be classified into two categories based on the amount of data that is processed at a time.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z — Plaintext letters
Z Y X W V U T S R Q P O N M L K J I H G F E D C B A — Substitution letters

The first category is known as a stream cipher. A stream cipher takes one character and replaces it with one character, as shown in figure

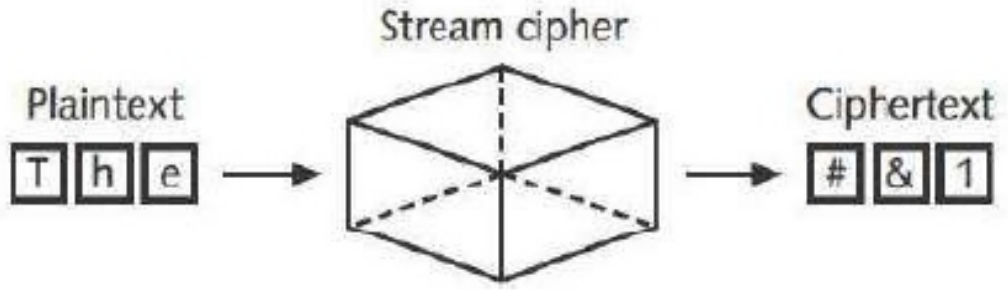

Fig: Stream Cipher

Note: The Wireless Wired Equivalent Privacy (WEP) protocol is a stream cipher.

The simplest type of stream cipher is a substitution cipher. Substitution ciphers simply substitute one letter or character for another as shown in below given figure. Sometimes known as mono alphabetic substitution cipher, stream cipher can be easy to break. A homo alphabetic substitution cipher maps a single plaintext character to multiple cipher text characters

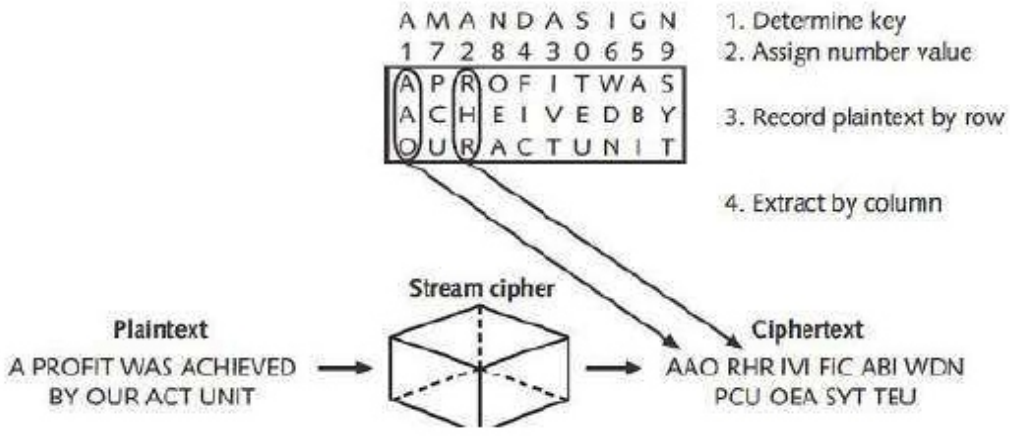

Fig: Transposition Cipher

With most symmetric ciphers, the final step is to combine the cipher stream with the plaintext to create the ciphertext which is shown in figure below.

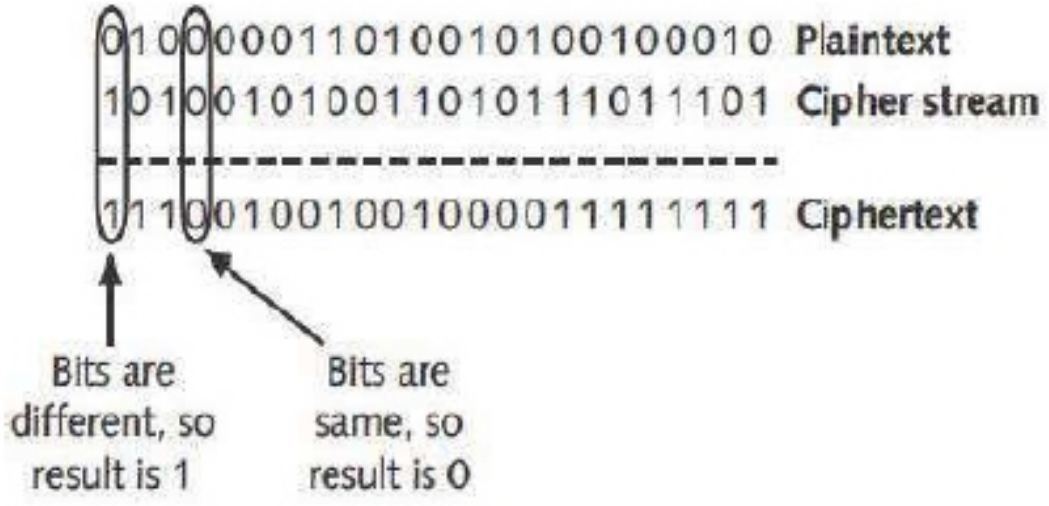

Fig: Combine Cipher

The process of accomplished through the exclusive OR (XOR) binary logic operations because all encryption occurs in binary. XOR is used to combine two streams of bits into one with a modified addition process. If two corresponding bits to be added are the same, the result is 0; if the bits are different, the result is a 1. Instead of combining the cipher stream with the plain text, a variation is to create a truly random key (called a pad) to be combined with the plain text. This is known as a one-time pad (OTP). If the pad is a random string of numbers that is kept secret and not reused, then an OTP can be considered secure. OTPs are rarely used and are more theoretical than practical.

3.4.2 Block Cipher

The second category of algorithms is known as a block cipher. Whereas a stream cipher works on one character at a time, a block cipher manipulates an entire block of plaintext at one time.

The plaintext message is divided into separate block of 8 to 16 bytes, and then each block is encrypted independently. For additional security, the blocks can be randomized. Stream and block ciphers each have advantages and disadvantages. A stream cipher is fast when the plaintext is short, but can consume much more processing power if plaintext itself. Because of this consistency, an attacker can examine streams and may be able to determine the key. Block ciphers are considered

more secure because the output is more random. When using a block cipher, the cipher is reset to its original state after each block is processed. This results in the ciphertext being more difficult to break. Symmetric cryptography can provide strong protection

against attacks as long the key is kept secure. The protections provided by symmetric cryptography are summarized in below given table.

Table: Information protections by symmetric cryptography

Characteristic	Protection?
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Authenticity	No
Nonrepudiation	No

3.4.3 Data Encryption System (DES)

One of the first widely popular symmetric cryptography algorithms was the Data Encryption system (DES). The predecessor of DES was a product originally designed in the early 1970s by

IBM called Lucifer that had a key length of 128 bits. The key was later shortened to 56 bits and renamed DES. The U.S. government officially adopted DES as the standard for encrypting non classified information. DES effectively catapulted the study of cryptography into the public arena. Until the deployment of DES, cryptography was studied almost exclusively by military personnel. The popularity of DES helped move cryptography implementation and research to academic and commercial organizations. DES is block cipher. It divides plaintext into 64-bit blocks and then executes the algorithm 16 times. There are four modes of DES encryption.

Although DES was once widely implemented, its 56-bit key is no longer considered secure and has been broken several times. It is not recommended for use.

3.4.4 Triple Data Encryption Standard (3DES)

Triple Data Encryption Standard (3DES) is designed to replace DES. As its name implies. 3DES uses three of encryption instead of just one. The ciphertext of one round becomes the entire input for the second iteration. 3DES employs a total of 48 iterations in its encryption (3 iterations times' 16 rounds). The most secure version of 3DES use different keys for each round, as shown in figure below. In some versions of 3DES, only two keys are used, but the first key is repeated for the round of encryption. The version of 3DES that uses three keys is estimated to be 2 to the power of 56 times stronger than DES.

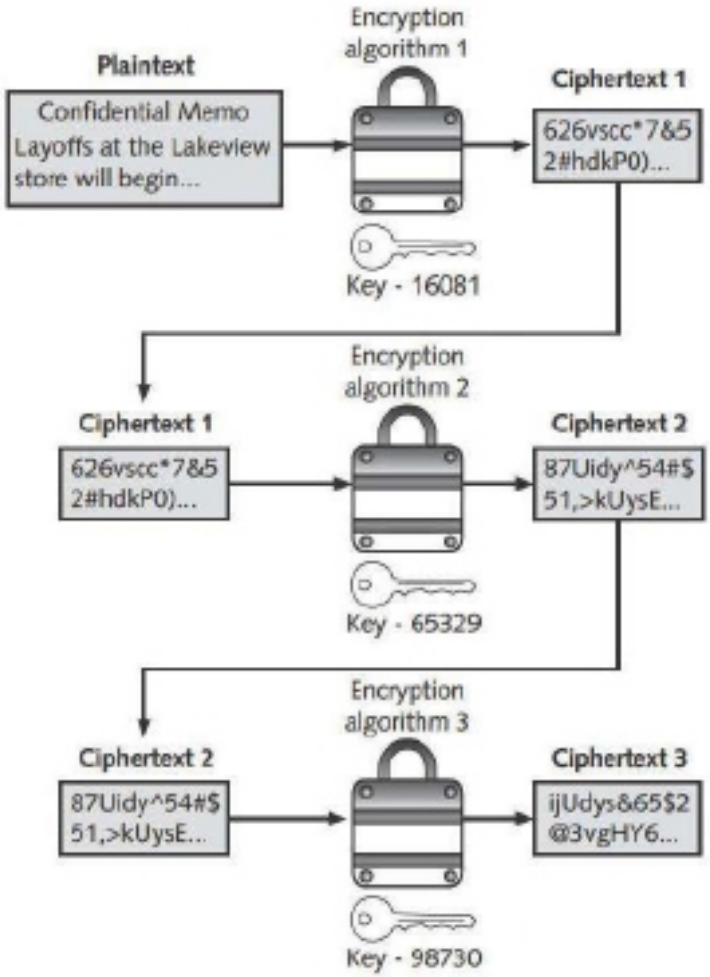

Fig: 3DES

Although 3DES address several of the key weakness of DES, it is no longer considered the most secure symmetric cryptographic algorithm. By design, 3DES performs better in hardware than as software.

3.4.5 Advance Encryption Standard (AES)

The Advance Encryption Standard (AES) is a symmetric cipher that was approved by the NIST in late 2000 as a replacement for DES. The process began with the NIST publishing requirements for a new symmetric algorithm and requesting proposals. After a lengthy process that required the cooperation of the U.S. Government, industry, and higher education, five finalists were chosen, with the ultimate winner being an algorithm known as AES. AES is now the official standard for encryption by the U.S. Government.

AES performs three steps on every block (128 bits) of plaintext. Within Step-2, multiple rounds are performed depending on the key size: a 128-bit key performs 9 rounds; a192-bit key performs 11 rounds, and a 256-bit key, known as AES-256, uses 13 rounds. Within each round, bytes are substituted and rearranged, and then special multiplication is performed based on the new arrangement. AES is designed to be secure well into the future. To date, no attacks have been successful against AES.

3.4.6 Other Algorithms

Several other symmetric cryptographic algorithms are also used. Rivest Cipher (RC) is a family of cipher algorithms designed by Ron Rivest. He developed six ciphers, ranging from RC1 to

Rc6 (but did not release RC1 and RC3). RC2 is block cipher that process a block of 64 bits. RC4 is a stream cipher that accepts keys up to 128 on wireless LANs. RC5 is a block cipher that can accept blocks and keys of different lengths. RC6 has three key sizes 128, 192, and 256 bits) and performs 20 rounds on each block. The International Data Encryption Algorithm (IDEA) algorithm dates back to the early 1990s and used in European nations. It is a block cipher that processes 64 bits with a 128-bite key with 8 rounds. Although considered to be secure, a weak key of all zeros has been identified for this algorithm. The algorithm Blowfish is block cipher that operates on 64-bit block and can have a key length from 32 to 448 bits. Blowfish was designed to run efficiently on 32-bit computers. To date, no significant weaknesses have been identified. A later derivation of Blowfish known as Twofishis also considered being a strong algorithm, although it has not been used as widely as Blowfish.

3.5 ASYMMETRIC CRYPTOGRAPHIC ALGORITHMS

If Bob wants to send an encrypted message to Alice using symmetric encryption, he must be sure that she has the key to decrypt the message. Yet how should Bob get the key to Alice? He cannot send it electronically through the Internet, because that would make it vulnerable to be intercepted by attackers. Nor can he encrypt the key and send it. Because Alice would not have a way to decrypt the encrypted key. These illustrate the primary weakness of symmetric encryption algorithms; distributing and maintaining a secure single key among multiple users often scattered geographically poses significant challenges. A completely different approach from symmetric cryptography is asymmetric cryptographic algorithms, also known as public key cryptography. Asymmetric encryption uses two keys instead of only one. These keys are mathematically related and are known as the public key and the private key. The public key is known to everyone and can be freely distributed, while the private key is known only to the individual to whom it belongs. When Bob wants to send a secure message to Alice, he uses Alice' public key to encrypt the message. Alice then uses her private key to decrypt it. Asymmetric cryptography is illustrated in figure below.

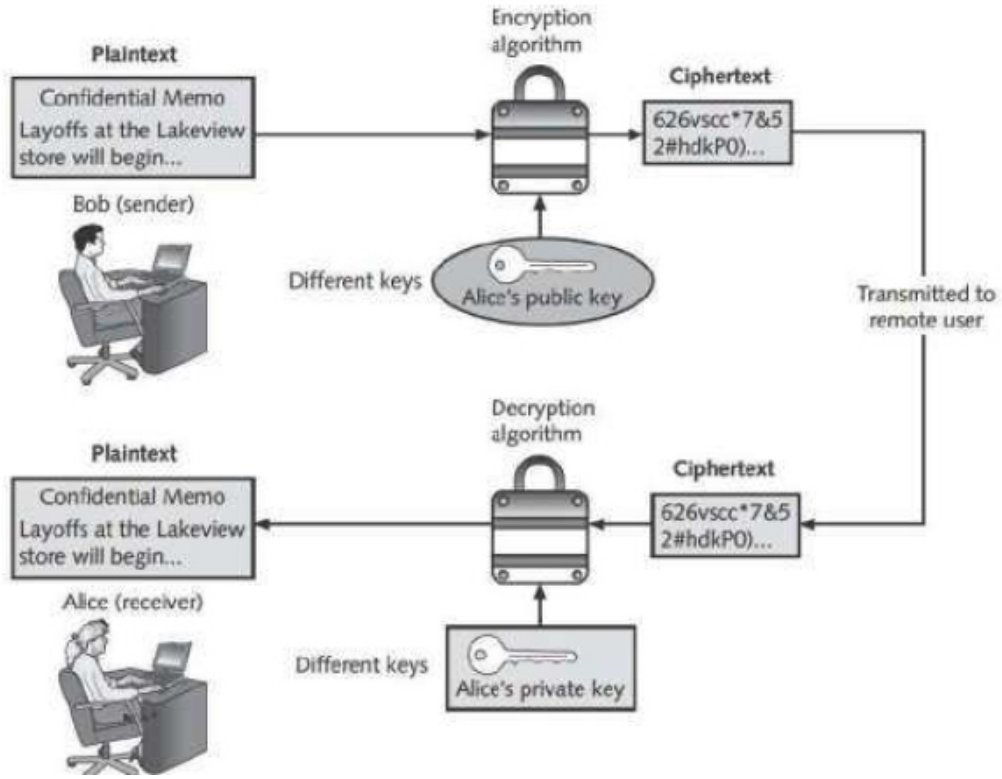

Fig: Asymmetric (Public key) cryptography

Asymmetric encryption was developed by Whitfield Diffie and Martin Hellman of the Massachusetts Institute of Technology (MIT) in 1975.

There are several important principles regarding asymmetric cryptography:

Key Pairs: Unlike symmetric cryptography that uses only one key, asymmetric cryptography requires a pair of keys.

Public Key: Public keys by their nature are designed to be ―public and do not need to be protected. They can be freely given to anyone or even posted on the Internet.

Private Key: The Private Key should be kept confidential and never shared. Both directions. Asymmetric cryptography keys can work in both directions.

A document encrypted with a public key can be decrypted with the corresponding private key.

In the same way, a document encrypted with a private key can be decrypted with its public key. Asymmetric cryptography can also be used to provide proofs, suppose that Alice receives an encrypted document that says it came from Bob. Alice can be sure that the encrypted message was not viewed or altered by someone else while being transmitted, yet how can she know for certain that Bob was actually the sender? Because Alice's public key is widely available, anyone could use it to encrypt the document. Another individual could have created a fictitious document, encrypted it with Alice's public key, and then sent it to Alice while pre tending to be Bob. While Alice's key can verify that no one read or changed the document in transport, it cannot verify the sender.

Proof can be provided with asymmetric cryptography by creating a digital signature, which is an electronic verification of the sender. A handwritten signature on paper document servers as proof that the signer has read and agreed to the document. A digital signature is much the same, although it can provide additional benefits.

A digital signature can do the following:

- Verify the sender. A digital signature serves to confirm the identity of the person from whom the electronic message originated.
- Prevent the sender from disowning the message. The signer cannot later attempt to disown it by claiming the signature was forged.
- Prove the integrity of the message. A digital signature can also prove that the message has not been altered since it was signed.

The basis for a digital signature rests on the ability of asymmetric keys to work in

both directions (a public key can encrypt a document that can be decrypted with a private key, and the Private Key can encrypt a document that can be decrypted by the public key). The steps for Bob to send a digitally signed message to Alice are illustrated in figure below.

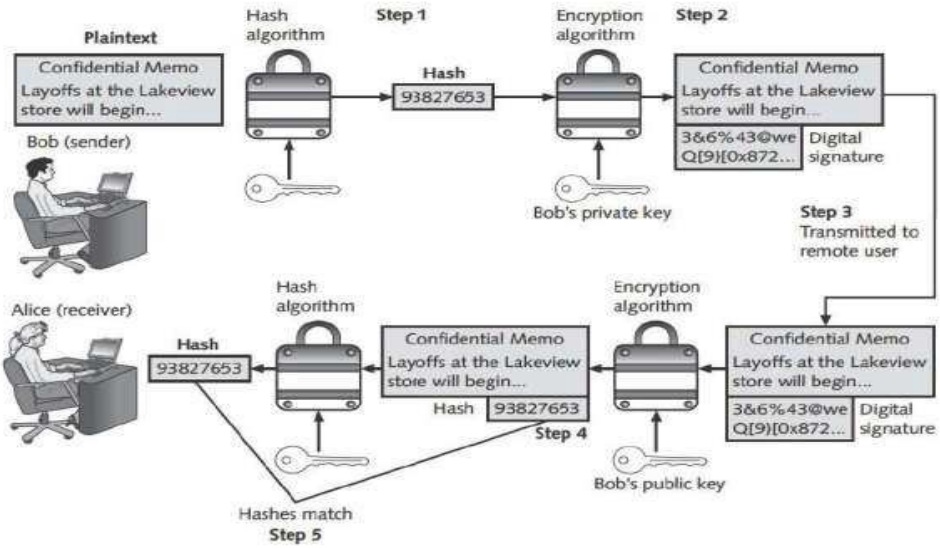

Fig: Digital Signature

1. After creating a memo, Bob generates a hash on it.
2. Bob then encrypts the hash with his private key. This encrypted hash is the digital signature for the memo.
3. Bob sends both the memo and the digital signature to Alice.
4. When Alice receives them, she decrypts the digital signature using Bob's public key, revealing the hash. If she cannot decrypt the digital signature, then she knows that it did not come from Bob (because only Bob's public key is able to decrypt the hash generated with his private key).
5. Alice then hashes the memo with the same hash algorithm Bob used and compares the result to the hash she received from Bob. If they are equal, Alice can be confident that the message has not changed since he signed it. Yet if the hashes
6. are not equal, the message has changed since it was signed.

Action	Whose key to use	Which key to use	Explanation
Bob wants to send Alice an encrypted message	Alice's key	Public key	When an encrypted message is to be sent, the recipient's key is used and not the sender's keys
Alice wants to read an encrypted message sent by Bob	Alice's key	Private key	An encrypted message can only be read by using the recipient's private key
Bob wants to send a copy to himself of the encrypted message that he sent to Alice	Bob's key	Public key to encrypt Private key to decrypt	An encrypted message can only be read by the recipient's private key; Bob would need to encrypt it with his own public key and then use his private key to decrypt it
Bob receives an encrypted reply message from Alice	Bob's key	Private key	The recipient's private key is used to decrypt received messages
Bob wants Susan to read Alice's reply message that he received	Susan's key	Public key	The message should be encrypted with Susan's key for her to decrypt and read it with her private key
Bob wants to send Alice a message with a digital signature	Bob's key	Private key	Bob's private key is used to encrypt the hash
Alice wants to see Bob's digital signature	Bob's key	Public key	Because Bob's public and private keys work in both directions, Alice can use his public key to decrypt the hash

Fig: Asymmetric Cryptography Practices

3.6 RSA ALGORITHM

The asymmetric algorithm RSA was published in 1977 and patented by MIT in 1983. The RSA Algorithm is the most common asymmetric cryptography algorithm and is the basis for several products. RSA stands for last names of its three developers, Ron Rivest, Adi Shamir and Leonard Adleman.

The RSA algorithm multiples two large prime numbers (a prime number is a number divisible only by itself and 1), p and q, to compute their product (n=pq)). Next a number e is chosen that is less than n and a prime factor to (p-1)(q-1). Another number d is determined, so that (ed-1) is divisible by (p-1) (q-1). The values of e and d are the public and private exponents. The public key is the pair (n.e), while the private key is (n,d). The numbers p and q can be discarded. An illustration of the RSA algorithm using very small number is as follows:

i. Select two prime numbers, p and q (in this example), p=7 and q=19).

ii. multiply p and q together to create n (7*19=133)

iii. Calculate m as p-1* q-1([7-1] * [19-1] or 6 * 18 = 108)

iv. Find a number *e* so that it and m have no common positive divisor other than 1(5)

v. Find a number d so that d=1+n*m)/e ([1+3*108]/5 or 325/5 = 65

For this example, the public key n is 133 and e is 5, while for the private key, n is133 and d is 65.

Note: RSA is slower than other algorithms; DES is approximately 100 times faster than RSA in software and between 1,000 and 10,000 times as fast in hardware.

3.6.1 Elliptic curve Cryptography (ECC)

Elliptic curve Cryptography (ECC) was first proposed in the mid-1980s. Instead of using large prime numbers as with RSA, elliptic curve cryptography uses sloping curves. An elliptic curve is a function drawn on an X-Y axis as a gently curved line. By adding the values of two points on the curve, a third point on the curve can be derived. With ECC, users share one elliptic curve and one point on the curve. One user chooses a secret random number and computes a public key based on a point on the curve, the other user does the same. They can now exchange messages because the shared public keys can generate a private key on an elliptic curve.

a) ECC is considered an alternative for prime numbers-based asymmetric cryptography for mobile and wireless devices. Because mobile devices are limited in terms of computing power due to their smaller size, ECC offers security that is comparable to other asymmetric cryptography, but with smaller key sizes. This can result in faster computations and lower power consumption.

b) Another asymmetric algorithm known as the Diffie-Heliman algorithm does not encrypt and decrypt text. Rather, the strength of Diffie-Hellman is that it allows two users to share a secret key securely over a public network. Once the key has been shared, then both parties can use it to encrypt and decrypt messages using symmetric cryptography.

3.7 USING CRYPTOGRAPHY

Cryptography should be used to secure any and all data that needs to be protected. This includes individual files or databases that are stored on standard desktop computer servers, removable media or mobile devices. Cryptography can be

applied through either software or hardware.

3.7.1 Encryption through Software

Encryption can be implemented through cryptographic software running on a system. This can be applied to individual files by using the software to encrypt and decrypt each file. The encryption can also be performed on a larger scale through using the file system or by encrypting the entire disk drive.

3.7.2 File and File System Cryptography

Encryption software can be used to encrypt or decrypt files one by one. However, this can be a cumbersome process. Instead, protecting groups of files, such as all files in a specific folder, can take advantage of the operating system's file system.

A file system is a method used by operating system to store, retrieve and organize files. Protecting individual files or multiple files through file system cryptography can be performed using software such as pretty Good Privacy and Microsoft Windows Encrypting File System.

3.7.3 Pretty Good Privacy (PGP/GPG)

One of the most widely used asymmetric cryptography systems for files and e-mail messages on windows systems is a commercial product called Pretty Good Privacy (PGP). A similar program known as GNU Privacy Guard (GPG) is an open source product. GP windows, UNIX and Linux Operating systems. Messages encrypted by PGP can generally be decrypted by GPG and vice versa. G versions run on windows, UNIX and Linux Operating systems. Messages encrypted by PGP can generally be decrypted by GPG and vice versa.

a) PGP and GPG use both asymmetric and symmetric cryptography. PGP/GPG generates a random symmetric key and uses it to encrypt the message. The symmetric key is then encrypted using the receiver's public key and sent along with the message. When the recipient receives a message, PGP/GPG first decrypts the symmetric key with the recipient's private key. The decrypted symmetric key is then used to decrypt the rest of the message.

b) PGP uses symmetric cryptography because it is faster than asymmetric cryptography.

c) PGP uses RSA for protecting digital signatures and 3DES or IDEA for symmetric encryption. GPG is unable to use IDEA because IDEA is patented. Instead, GPG uses one of several open-source algorithms.

3.8 SELFASSESSMENT QUESTIONS

1. What are the principle elements of a public key cryptosystem?

……
……
……
……

2. What is a hash function?

……
……
……
……

3. What are the requirements of the hash function?

……
……
……
……

4. What are the properties a digital signature should have?

……
……
……
……

5. What requirements should a digital signature scheme should satisfy?

……
……
……
……

6. Discuss about Data Encryption Standard (DES)

……
……
……
……

7. Explain RSA with the help of an example?

……

……

……

……

……

3.9 KEY TERMS & CONCEPTS

A Cryptographic Hash Function takes a message of arbitrary length and creates a message digest of fixed length.

Message Digest (MD) is a series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message.

Secure Hash algorithm (SHA) is a family of hashes. It is a more secured hash than MD.

Whirlpool is an iterated cryptographic hash function, based on the Miyaguchi-Preneel scheme that uses a symmetric-key block cipher in place of the compression function**.**

Data Encryption Standard (DES) is a block cipher. It divides plaintext into 64-bit blocks and then executes the algorithm 16 times for encryption.

Advance Encryption Standard (AES) is a symmetric cipher that was approved by the NIST. AES is now the official standard for encryption by the U.S. Government. AES performs three steps on every block (128 bits) of plaintext at a time.

RSA stands for last names of its three developers, Ron Rivest, Adi Shamir and Leonard Adelman, was published in 1977 and patented by MIT in 1983. The RSA Algorithm is the most common asymmetric cryptography algorithm.

3.10 ANSWER TO SELFASSESSMENT QUESTIONS

1. The principle elements of a cryptosystem are:

(i) Plain text

(ii) Encryption algorithm

(iii) Public and private key

(iv) Cipher text

(v) Decryption algorithm

2. Hash function accept a variable size message M as input and produces a fixed size hash code H(M) called as message digest as output. It is the variation on the message authentication code.

3. The hash function should satisfy the following requirements.

(i) H can be applied to a block of data of any size.

(ii) H produces a fixed length output.

(iii) H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical

4. The properties of digital signature include the following:

(i) It must verify the author and the data and time of signature.

(ii) It must authenticate the contents at the time of signature.

(iii) It must be verifiable by third parties to resolve disputes.

5. The requirements of a digital signature include the following:

(i) The signature must be bit pattern that depends on the message being signed.

(ii) The signature must use some information unique to the sender, to prevent both forgery and denial.

(iii) It must be relatively easy to produce the digital signature.

(iv) It must be relatively easy to recognize and verify the digital signature.

(v) It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.

(vi) It must be practical to retain a copy of the digital signature in storage.

6. The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in 1977. DES has been the most widely used symmetric-key block cipher since its publication.

DES takes 64 bit plain text converts it into 64 bit cipher text with the help of 64 bit key which later reduced to 56 bit key as every 8th bit of 64 bit is discarded to form a key of 54 bit. As DES is a block cipher, it takes plain text as block of 64 bit.

7. RSA is an asymmetric block cipher. It was developed by Ron Rivest, Adiv Shamir and Leonard Adleman in 1977.

RSA with an example:

Let us choose two large prime numbers p=61 and q= 53

- Multiply p and q together to get n =61*53=3233
- Choose the encryption key e, such that e and (p - 1) x (q - 1) are relatively prime.
- (p-1) =(61-1)=60
- (q-1) =(53-1)=52
- (p - 1) × (q - 1) =60*52=3120
- Choosing a relatively prime number between 1<e<3120 which is not a multiple of 3120. We can choose e=17
- Compute decryption key d such that d = 17 mod (3120) = 2753
- Construct public key as (17, 3233) and construct cipher text,
  c = 6517 mod (3233) =2790
- Construct private key as (2753, 3233) and construct plain text,
  p =27902753 mod (3233) =65

3.11 REFERENCES AND FURTHER READINGS

1. William Stallings, "Cryptography and Network Security-Principles and Practices", Prentice-Hall of India.
2. Information System Security (CEGCS-04), Study Materials of Uttarakhand Open University, Haldwani, for Certificate in e e-Governance and Cyber Security.
3. Charles P.Pfleeger, Shari Lawrence Pfleeger, even Shah, "Security in Computing", Pearson Education
4. Bernad Menezes, "Network Security & Cryptography", CENGAGE Learning.
5. Atul Kahate, "Cryptography and Network Security", TMH Publishing Company Limited.

Comments