

# CRYPTOGRAPHY

CSC316

For BSc CSIT Fifth Semester

By : Narendra Bohara

Text Book

1. W. Stallings, *Cryptography and Network Security*, Pearson Education.

## References:

1. William Stallings, *Network Security, Principles and Practice*.
2. Matt Bishop, *Computer Security, Art and Science*.
3. Mark Stamp, *Information Security: Principles and Practices*.
4. Bruce Schneier, *Applied Cryptography*.
5. Douglas. R. Stinson. *Cryptography: Theory and Practice*.
6. B. A. Forouzan, *Cryptography & Network Security*, Tata Mc Graw Hill.

# COURSE OVERVIEW

## Cryptography

**Course Title:** Cryptography

**Course No:** CSC316

**Nature of the Course:** Theory + Lab

**Semester:** V

**Full Marks:** 60 + 20 + 20

**Pass Marks:** 24 + 8 + 8

**Credit Hrs:** 3

**Course Description:** The course introduces the underlying principles and design of cryptosystems. The course covers the basic concepts of cryptography including: traditional ciphers, block ciphers, stream ciphers, public and private key cryptosystems. The course also includes the theory of hash functions, authentication systems, network security protocols and malicious logic.

**Course Objectives:** The objectives of this course are to familiarize the students with cryptography and its applications. The students will be able to develop basic understanding of cryptographic mechanisms.

# EVALUATION SYSTEM

- **INTERNAL EVALUATION : 20 Marks**
  - Attendance
  - Assignment
  - MID-TERM
  - Presentation and others
- **PRACTICAL : 20 Marks**
  - Report
  - Practical –Work
  - Viva
- **BOARD EXAMINATION : 60 Marks**

# UNIT I: INTRODUCTION AND CLASSICAL CIPHERS

## Contents:

- ❑ **Security: Computer Security, Information Security, Network Security, CIA Triad, Cryptography, Cryptosystem, Cryptanalysis, Security Threats and Attacks, Security Services, Security Mechanisms .**

- ❑ **Classical Cryptosystems:**

**Substitution Techniques: Ceasar, Monoalphabetic, Playfair, Hill, Polyalphabetic ciphers, One-time pad Transposition Techniques: Rail Fence Cipher.**

- ❑ **Modern Ciphers: Block vs. Stream Ciphers, Symmetric vs. Asymmetric Ciphers**

# WHAT IS COMPUTER SECURITY?

- ❑ 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).
- This definition introduces three key objectives that are at the heart of computer security:
  - Confidentiality
  - Integrity
  - Availability

# CONFIDENTIALITY

**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.

# **Integrity** covers two related concepts.

**Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.

**System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

**Availability:** Assures that systems work promptly and service is not denied to authorized users.

# CIA TRIAD

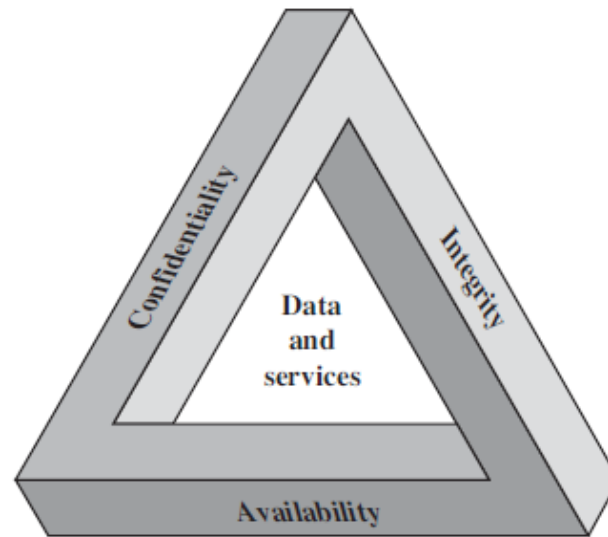


Figure 1.1 The Security Requirements Triad



# CIA

The three concepts embody the fundamental security objectives for both data and for information and 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.

**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 an information system.

SOME IN THE SECURITY FIELD FEEL THAT ADDITIONAL CONCEPTS ARE NEEDED TO PRESENT A COMPLETE PICTURE. TWO 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 that each input arriving at the system came from a trusted source.

**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

# EXAMPLES

## □ **CONFIDENTIALITY**

□ Student grade information is an asset whose confidentiality is considered to be highly important by students. In the United States, the release of such information is regulated by the Family Educational Rights and Privacy Act (FERPA). Grade information should only be available to students, their parents, and employees that require the information to do their job.

□ **INTEGRITY** In a hospital patient's allergy information stored in a database. The doctor should be able to trust that the information is correct and current. Now suppose that an employee (e.g., a nurse) who is authorized to view and update this information deliberately falsifies the data to cause harm to the hospital. The database needs to be restored to a trusted basis quickly, and it should be possible to trace the error back to the person responsible. Patient allergy information is an example of an asset with a high requirement for integrity. Inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability.

# ***AVAILABILITY***

The more critical a component or service, the higher is the level of availability required.

Consider a system that provides authentication services for critical systems, applications, and devices. An interruption of service results in the inability for customers to access computing resources and staff to access the resources they need to perform critical tasks. The loss of the service translates into a large financial loss in lost employee productivity and potential customer loss.

public Web site for a university; the Web site provides information for current and prospective students and donors. Such a site is not a critical component of the university's information system, but its unavailability will cause some embarrassment.

# AVAILABILITY

<https://cdcsit.edu.np>

509

**Bandwidth Limit Exceeded**

# WHAT IS INFORMATION SECURITY?

- ❑ Information security (also known as InfoSec) ensures that both physical and digital data is protected from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction.
- ❑ Information security differs from cybersecurity in that InfoSec aims to keep data in any form secure, whereas cybersecurity protects only digital data.
- ❑ If your business is starting to develop a security program, information security is where you should first begin, as it is the foundation for data security.

# WHAT IS NETWORK SECURITY?

Network security, a subset of cybersecurity, aims to protect any data that is being sent through devices in your network to ensure that the information is not changed or intercepted.

The role of network security is to protect the organization's IT infrastructure from all types of cyber threats including:

Viruses, worms and Trojan horses

Hacker attacks

Denial of service attacks

Spyware and adware



# HOW TO MANAGE NETWORK SECURITY

Firewalls

Anti-virus software

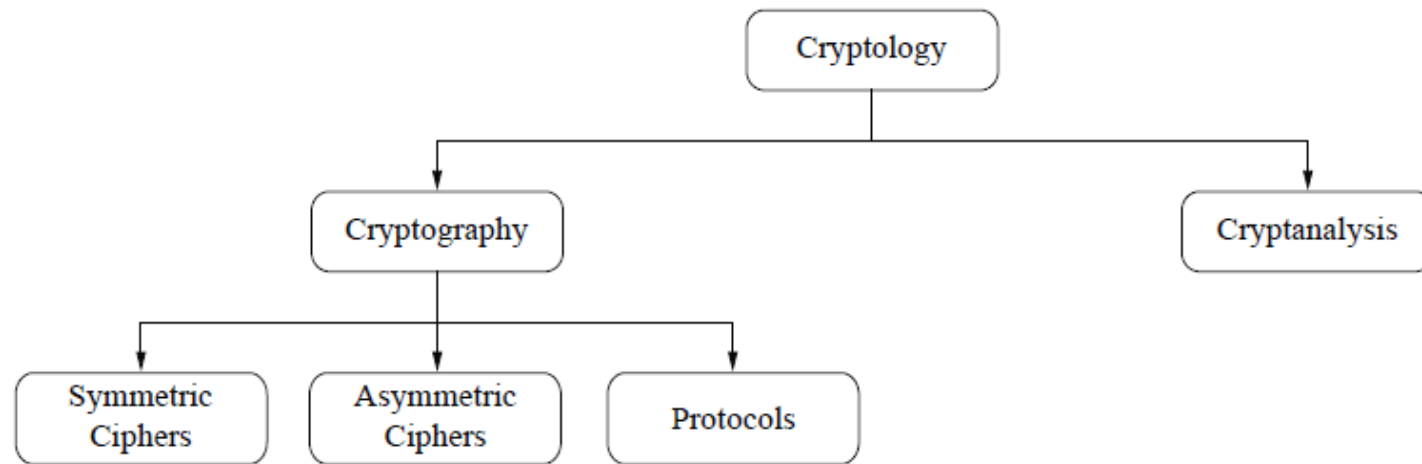
Intrusion detection and prevention systems (IDS/IPS)

Virtual private networks (VPN)



# OVERVIEW OF CRYPTOLOGY

CRYPTOLOGY SPLITS INTO TWO MAIN BRANCHES:



# CRYPTOGRAPHY

- ❑ The word 'cryptography' was coined by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing i.e. "secret writing"
- ❑ refer to the science and art of transforming messages to make them secure and immune to attacks.
- ❑ is the science of secret writing with the goal of hiding the meaning of message.

# CRYPTOGRAPHY

Cryptographic systems are characterized along three independent dimensions:

## 1. The type of operations used for transforming plaintext to ciphertext

All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. Most systems, referred to as *product systems*, involve multiple stages of substitutions and transpositions.

## 2. The number of keys used.

If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.

## 3. The way in which the plaintext is processed

A *block cipher* processes the input one block of 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.

# Cryptanalysis

---

- is the science and sometimes art of *breaking* cryptosystems.
- The process of attempting to discover the plaintext or key is known as cryptanalysis.

You might think that code breaking is for the intelligence community or perhaps organized crime, and should not be included in a serious classification of a scientific discipline. However, most cryptanalysis is done by respectable researchers in academia nowadays.

Cryptanalysis is of central importance for modern cryptosystems: without people who try to break our crypto methods, we will never know whether they are really secure or not.

**Because cryptanalysis is the only way to assure that a cryptosystem is secure, it is an integral part of cryptology.**

# CRYPTANALYSIS

- The strategy used by the cryptanalyst depends on the nature of the encryption scheme and the information available to the cryptanalyst.

# TYPES OF ATTACKS ON ENCRYPTED MESSAGES

| Type of Attack    | Known to Cryptanalyst   |
|-------------------|---|
| Ciphertext only   | <ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext to be decoded</li></ul>   |
| Known plaintext   | <ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext to be decoded</li><li>• One or more plaintext–ciphertext pairs formed with the secret key</li></ul>   |
| Chosen plaintext  | <ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext to be decoded</li><li>• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key</li></ul>  |
| Chosen ciphertext | <ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext to be decoded</li><li>• Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key</li></ul>  |
| Chosen text       | <ul style="list-style-type: none"><li>• Encryption algorithm</li><li>• Ciphertext to be decoded</li><li>• Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key</li><li>• Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key</li></ul> |

# BRUTE-FORCE ATTACK

The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

# STEGANOGRAPHY

- ❑ Steganography is similar but adds another dimension to Cryptography.
- ❑ In this method, people not only want to protect the secrecy of an information by concealing it, but they also want to make sure any unauthorized person gets no evidence that the information even exists. For example, **invisible watermarking**.
- ❑ In steganography, an unintended recipient or an intruder is unaware of the fact that observed data contains hidden information. In cryptography, an intruder is normally aware that data is being communicated, because they can see the coded/scrambled message.



# STEGANOGRAPHY

*Attack the Hill at GR  
3614*

Message to be hidden



Embedding data



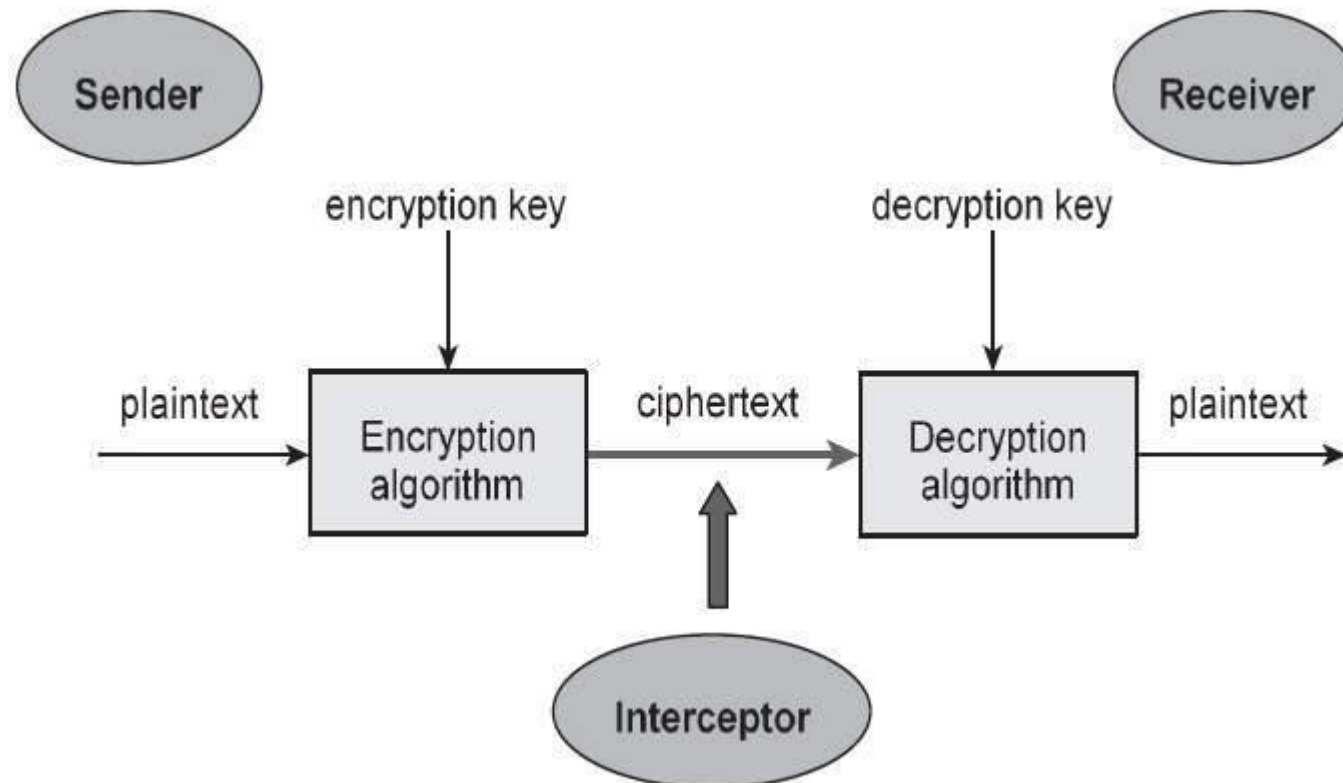
Carrier File



Carrier File with Hidden Message

# CRYPTOSYSTEM

□ A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is



❑ The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

## ❑ Components of a Cryptosystem

**Plaintext.** It is the data to be protected during transmission.

**Encryption Algorithm.** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.

**Ciphertext.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.

**Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.

**Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.

**Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a **key space**.

An **interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. He, however, must never know the decryption key.

# THE OSI SECURITY ARCHITECTURE

- ❑ To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.
- ❑ The International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) Recommendation X.800, *Security Architecture for OSI*, defines such a systematic approach.
- ❑ The OSI security architecture is useful to managers as a way of organizing the task of providing security.
- ❑ The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows:

# ASPECTS OF SECURITY

3 aspects of information security:

- **security attack**
- **security mechanism**
- **security service**

## **Note terms**

note terms

- *threat* – a potential for violation of security
- *attack* – an assault on system security, a deliberate attempt to evade security services

# SECURITY ATTACKS, MECHANISMS, AND SERVICES

**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.**

# SECURITY MECHANISMS

- ❑ A process that is designed to detect, prevent, or recover from a security attack.
- ❑ The mechanisms are divided into

## SPECIFIC SECURITY MECHANISMS

those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and

## PERVASIVE SECURITY MECHANISMS

those that are not specific to any particular protocol layer or security service.



# SPECIFIC SECURITY MECHANISMS

**Encipherment:** The use of mathematical algorithms to transform data into a form that is not readily intelligible.

**Digital Signature:** allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

**Access Control :**that enforce access rights to resources.

**Data Integrity:**to assure the integrity of a data unit or stream of data units.

**Authentication Exchange :**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:** Use of a trusted third party to assure certain properties of a data exchange.

# PERVASIVE SECURITY

**Trusted Functionality:** That which is perceived to be correct with respect to some criteria.

**Event Detection:** Detection of security-relevant events.

**Security Audit Trail:** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

# SECURITY ATTACKS

A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in terms of *passive attacks* and *active attacks*.

A passive attack attempts to learn or make use of information from the system but does not affect system resources.

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

# PASSIVE ATTACKS

## ❑ The release of message contents

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

## ❑ The traffic analysis

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 messages**. 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.

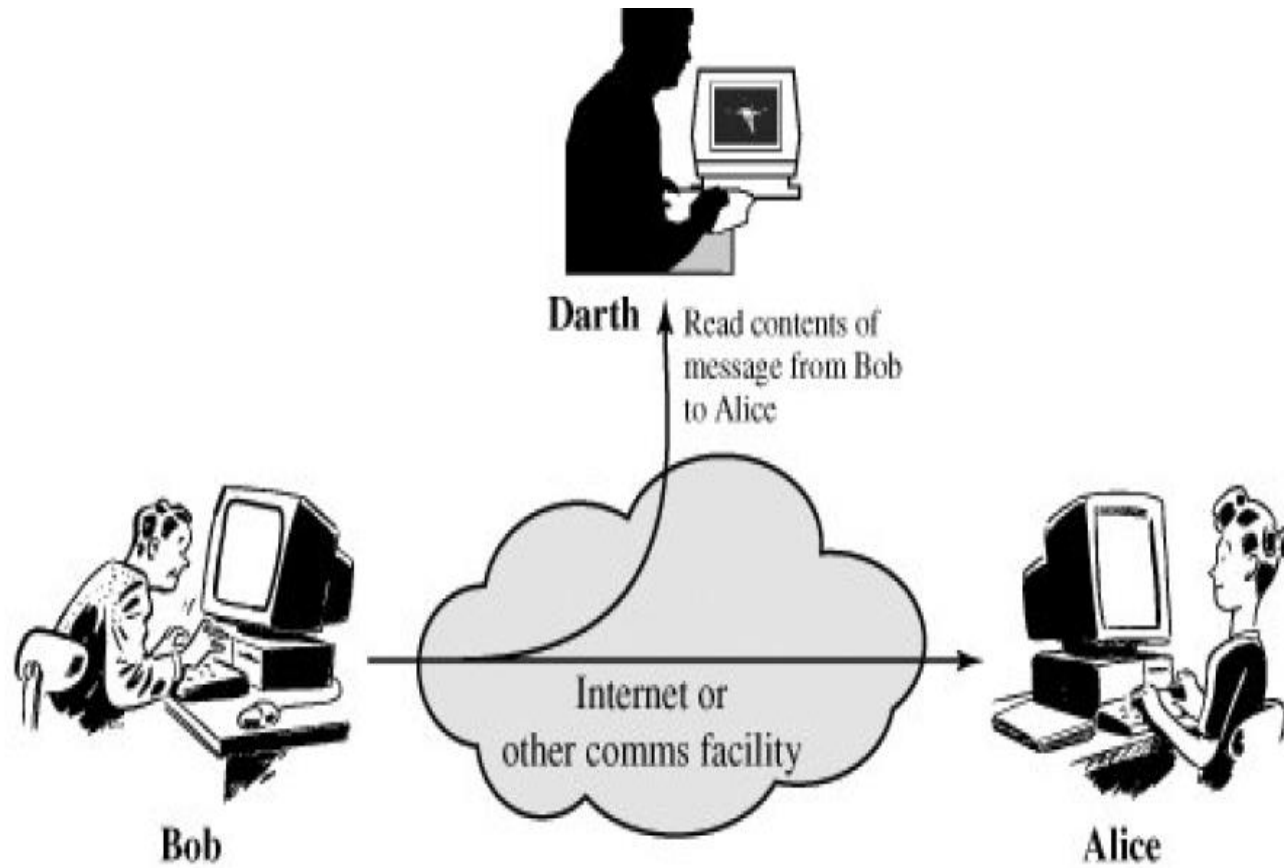
# PASSIVE ATTACK

Passive attacks are very difficult to detect because they do not involve any alteration of the data.

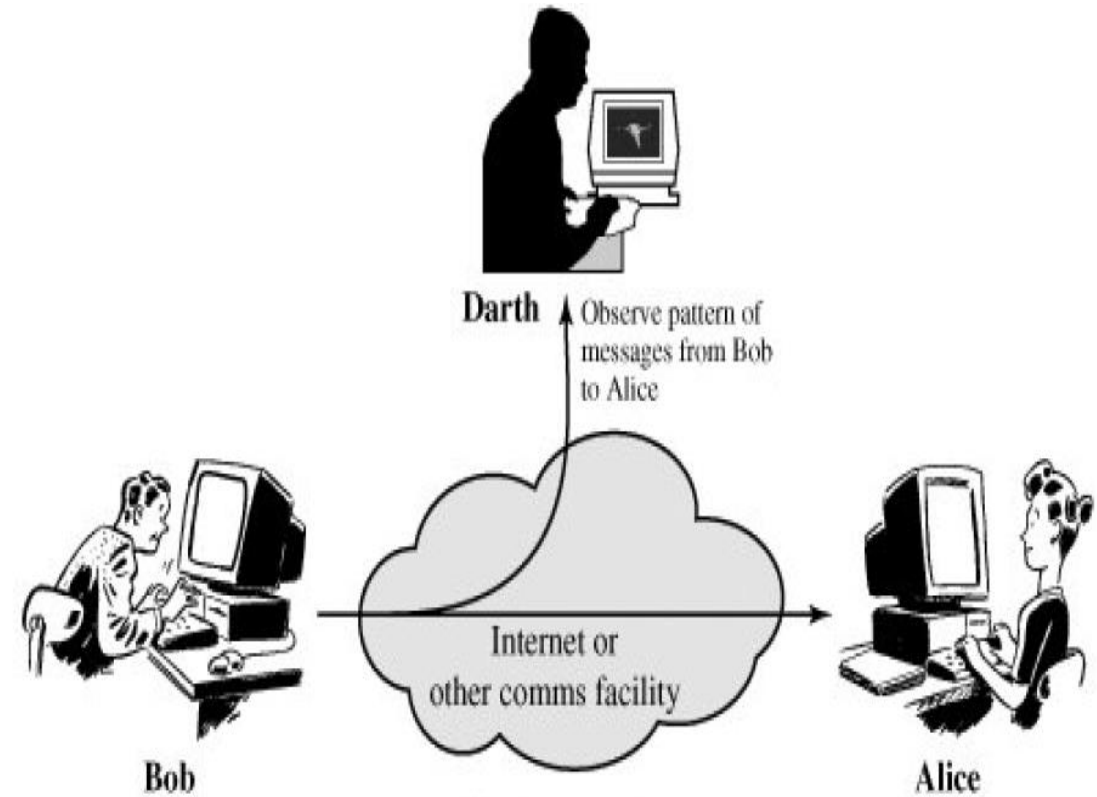
Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.

However, it is feasible to prevent the success of these attacks, usually by using encryption.

# PASSIVE ATTACK



(a) Release of message contents



(b) Traffic analysis

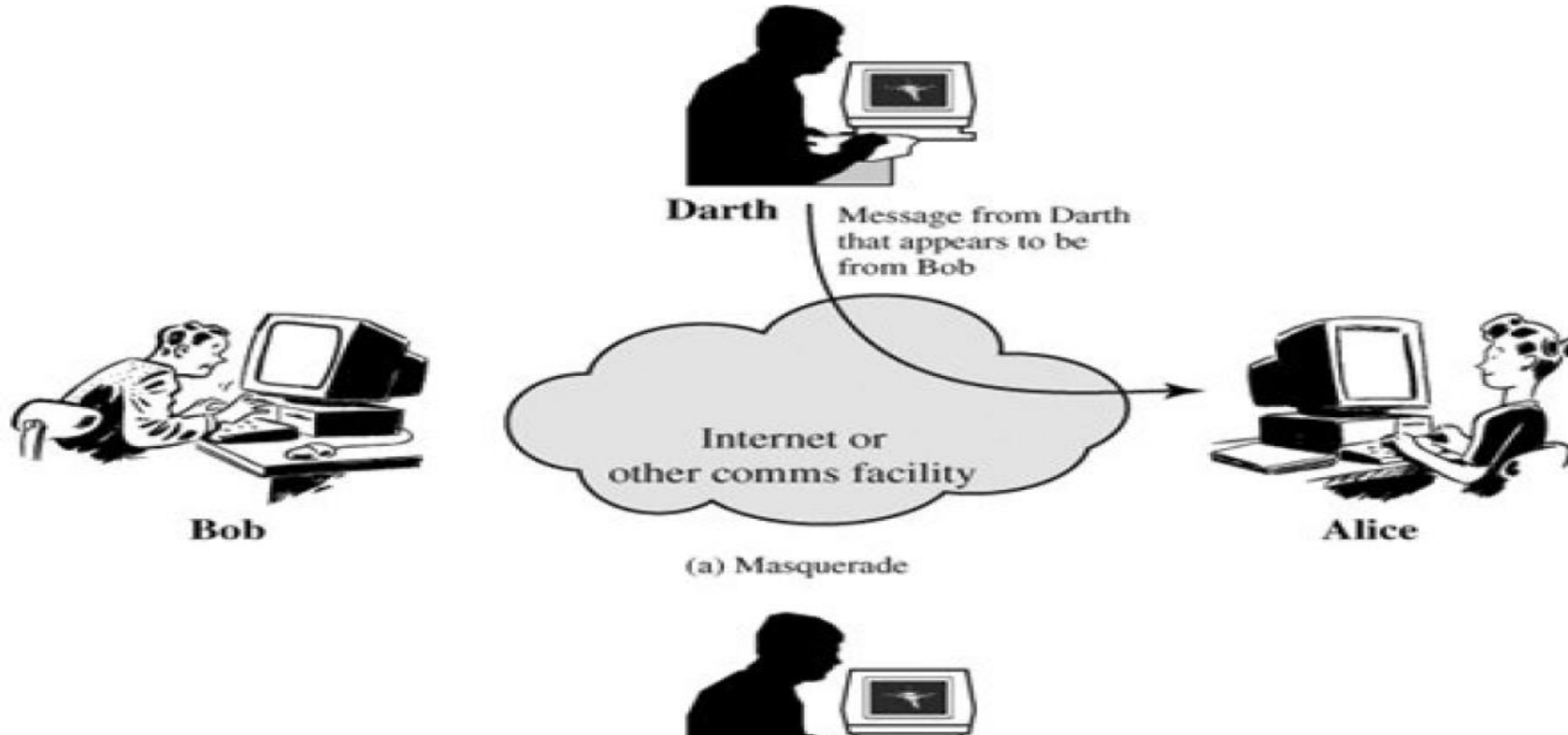
# ACTIVE ATTACK ATTACK

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.

# MASQUERADE

- A **masquerade** takes place when one entity pretends to be a different entity.





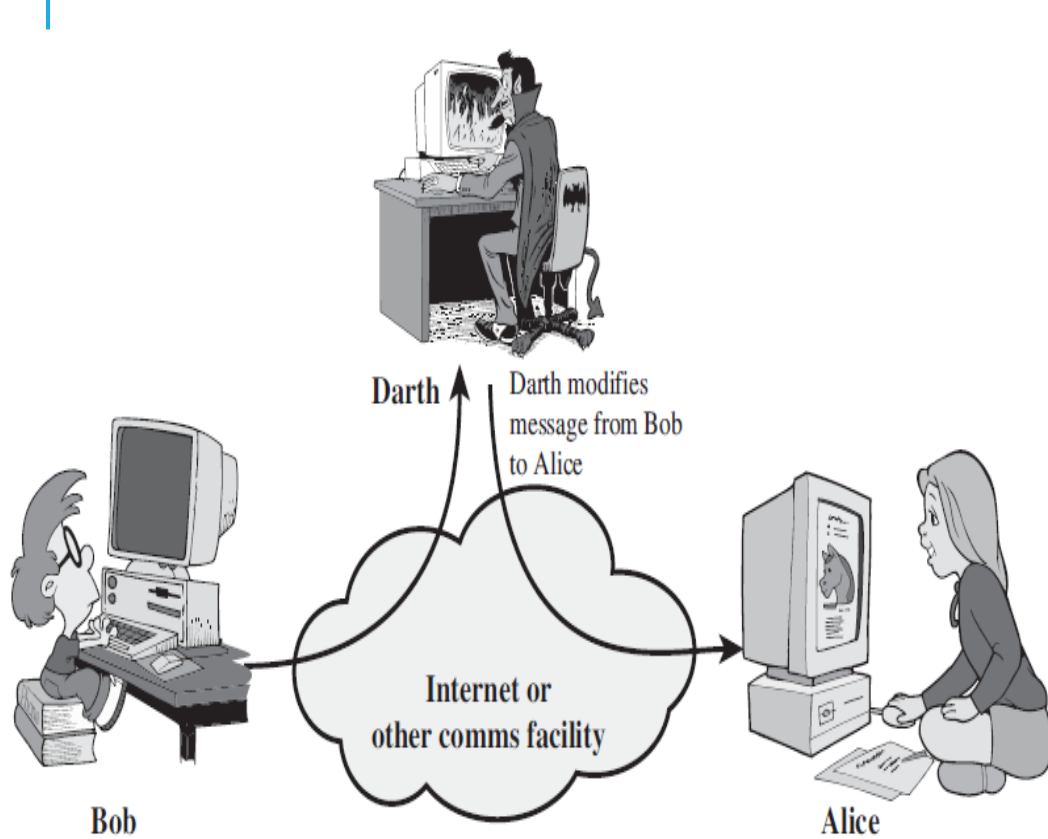
# ACTIVE ATTACK

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

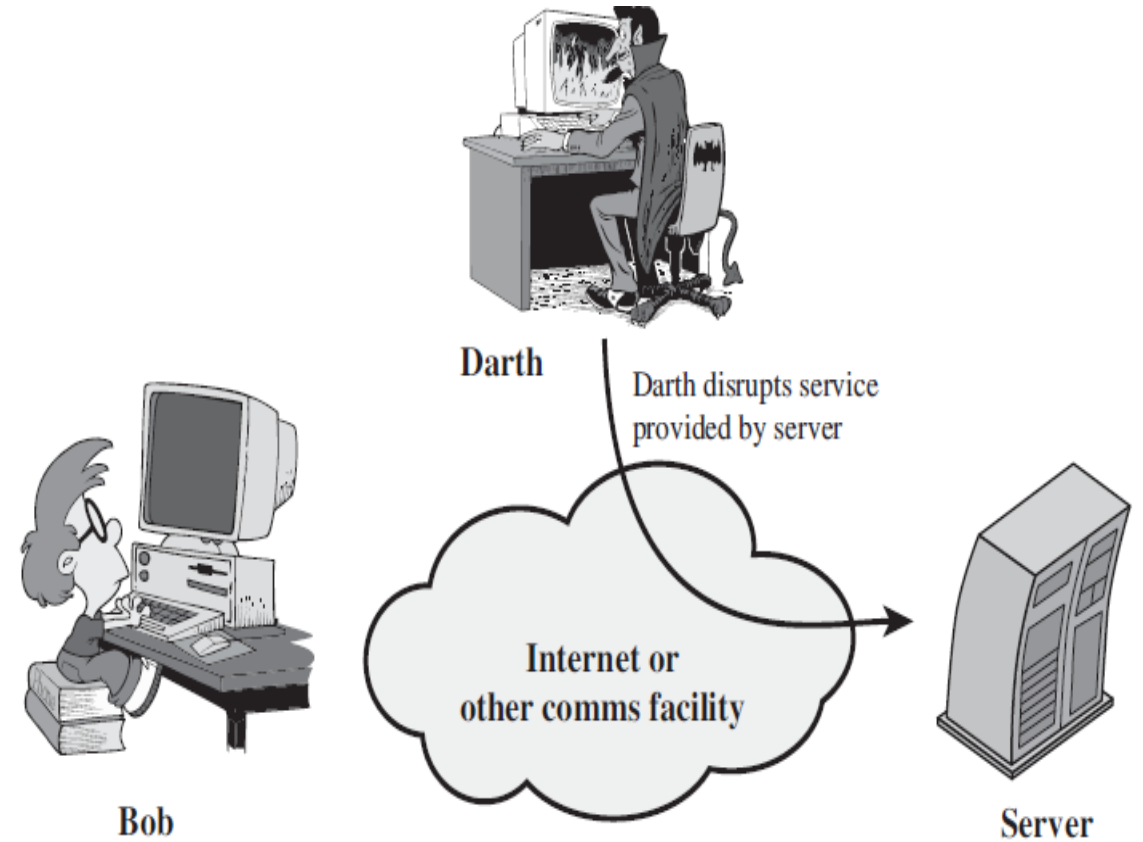
**Modification of messages** simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect . For example, a message meaning "Allow John Smith to read confidential file *accounts*" is modified to mean "Allow Fred Brown to read confidential file *accounts*."

The **denial of service** prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit 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.

# ACTIVE ATTACK



(c) Modification of messages



(d) Denial of service

# ACTIVE ATTACK

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.

# SECURITY SERVICES

□ X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. X.800 divides these services into five categories and fourteen specific services

1. Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender.

Authentication service has two variants –

**Message authentication/data-origin authentication:** identifies the originator of the message without any regard router or system that has sent the message. (the assurance that a given entity was the original source of the received data.) Message authentication simply authenticates one message; the process needs to be repeated for each new message.

**Entity(user) authentication** is assurance that data has been received from a specific entity, say a particular website (the assurance that a given entity is involved and currently active in a communication session.) An entity can be a person, a process, a client, or a server. The entity whose identity needs to be proved is called the claimant; the party that tries to prove the identity of the claimant is called the verifier.

# SECURITY SERVICES

## 2. Access Control

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

## 3. Non-repudiation

It is a security service that ensures that an entity cannot refuse the ownership of a previous commitment or an action. It is an assurance that the original creator of the data cannot deny the creation or transmission of the said data to a recipient or third party.

Non-repudiation is a property that is most desirable in situations where there are chances of a dispute over the exchange of data. For example, once an order is placed electronically, a purchaser cannot deny the purchase order, if non-repudiation service was enabled in this transaction.



## **Nonrepudiation, Origin**

Proof that the message was sent by the specified party.

## **Nonrepudiation, Destination**

Proof that the message was received by the specified party.

# SECURITY SERVICES

## 4. Confidentiality

- ❑ Confidentiality is the fundamental security service provided by cryptography.
- ❑ It is a security service that keeps the information from an unauthorized person. It is sometimes referred to as **privacy** or **secrecy**.
- ❑ Confidentiality can be achieved through numerous means starting from physical securing to the use of mathematical algorithms for data encryption.

# SERVICES..

## 5. Data Integrity

- ❑ It is security service that deals with identifying any alteration to the data. The data may get modified by an unauthorized entity intentionally or accidentally.
- ❑ Integrity service confirms that whether data is intact or not since it was last created, transmitted, or stored by an authorized user.
- ❑ Data integrity cannot prevent the alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized manner.

## 6. Availability



Requires that computer system assets be available to authorized parties when needed.



# CRYPTOGRAPHY PRIMITIVES

Cryptography primitives are nothing but the tools and techniques in Cryptography that can be selectively used to provide a set of desired security services :

- ☐ Encryption
- ☐ Hash functions
- ☐ Message Authentication codes (MAC)
- ☐ Digital Signatures

| Primitives Service <br> | Encryption | Hash Function | MAC       | Digital Signature |
|---|------------|---------------|-----------|-------------------|
| Confidentiality   | Yes        | No            | No        | No                |
| Integrity   | No         | Sometimes     | Yes       | Yes               |
| Authentication  | No         | No            | Yes       | Yes               |
| Non Reputation  | No         | No            | Sometimes | Yes               |

# CLASSICAL ENCRYPTION TECHNIQUES

## SUBSTITUTION AND TRANSPOSITION

### Substitution Techniques

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

**Caesar Cipher**

**Monoalphabetic Ciphers**

**Playfair Cipher**

**Hill Cipher**

# CAESAR CIPHER (OR) SHIFT CIPHER

- ❑ The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

e.g., Plain text : pay more money

Cipher text: SDB PRUH PRQHB

The alphabet is wrapped around, so that the letter following Z is A.

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 |

A numerical equivalent to each letter:

- Then the algorithm can be expressed as follows. For each plaintext letter  $p$ , substitute the ciphertext letter  $C$ :

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

- 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. The decryption algorithm is simply

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

# TASKS

Encrypt the plaintext “meet me after the toga party” using Ceaser Cipher.

## Security of Ceaser Cipher

Caesar Cipher is **not a secure** cryptosystem because there are only 26 possible keys to try out. An attacker can carry out an exhaustive key search with available limited computing resources.

# MONOALPHABETIC AND POLYALPHABETIC CIPHER

- ❑ Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process.
- ❑ For example, if 'A' is encrypted as 'D', for any number of occurrence in that plaintext, 'A' will always get encrypted to 'D'.
- ❑ Polyalphabetic Cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process.
- ❑ **playfair and Vigenere Cipher are polyalphabetic ciphers.**

# PLAYFAIR CIPHER

- ❑ In this scheme, pairs of letters are encrypted, instead of single letters as in the case of simple substitution cipher.
- ❑ In playfair cipher, initially a key table is created. The key table is a  $5 \times 5$  grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table as we need only 25 alphabets instead of 26. If the plaintext contains J, then it is replaced by I.
- ❑ The sender and the receiver decide on a particular key, say 'tutorials'.
- ❑ In a key table, the first characters (going left to right) in the table is the phrase, excluding the duplicate letters. The rest of the table will be filled with the remaining letters of the alphabet, in natural order. The key table works out to be –



# PLAYFAIR CONTD..

## Process of Playfair Cipher

First, a plaintext message is split into pairs of two letters (digraphs). If there is an odd number of letters, a X is added to the last letter.

| 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 |

1. Repeating plaintext letters that would fall in the same pair are separated with a filler letter such as „X“.
2. 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 following the last.
3. Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last.
4. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

# PLAYFAIR CONTD..

Plaintext = meet me at the school house

cipher text => CL KL CL RS PD IL HY AV MP FH XL IU

Task :

Encrypt the message 'hide money' with the key of 'tutorials'

# STRENGTH OF PLAYFAIR CIPHER

- ❑ Playfair cipher is a great advance over simple mono alphabetic ciphers.
- ❑ Since there are 26 letters,  $26 \times 26 = 676$  diagrams are possible, so identification of individual digram is more difficult.
- ❑ Frequency analysis is much more difficult.

# POLYALPHABETIC CIPHERS

- ❑ The 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 substitution cipher.

All these techniques have the following features in common:

1. A set of related monoalphabetic substitution rules is used.
2. A key determines which particular rule is chosen for a given transformation

# MODIFIED CEASER CIPHER

In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25.

Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext letter a. Thus, a Caesar cipher with a shift of 3 is

We can express the Vigenère cipher in the following manner. Assume a sequence of plaintext letters  $P = p_0, p_1, p_2, \dots, p_{n-1}$  and a key consisting of the sequence of letters  $K = k_0, k_1, k_2, \dots, k_{m-1}$ , where typically  $m < n$ . The sequence of ciphertext letters  $C = C_0, C_1, C_2, \dots, C_{n-1}$  is calculated as follows:

$$\begin{aligned} C &= C_0, C_1, C_2, \dots, C_{n-1} = E(K, P) = E[(k_0, k_1, k_2, \dots, k_{m-1}), (p_0, p_1, p_2, \dots, p_{n-1})] \\ &= (p_0 + k_0) \bmod 26, (p_1 + k_1) \bmod 26, \dots, (p_{m-1} + k_{m-1}) \bmod 26, \\ &\quad (p_m + k_0) \bmod 26, (p_{m+1} + k_1) \bmod 26, \dots, (p_{2m-1} + k_{m-1}) \bmod 26, \dots \end{aligned}$$

Thus, the first letter of the key is added to the first letter of the plaintext, mod 26, the second letters are added, and so on through the first  $m$  letters of the plaintext. For the next  $m$  letters of the plaintext, the key letters are repeated. This process continues until all of the plaintext sequence is encrypted. A general equation of the encryption process is

$$C_i = (p_i + k_{i \bmod m}) \bmod 26 \quad (2.3)$$

In essence, each plaintext character is encrypted with a different Caesar cipher, depending on the corresponding key character.

**Similarly, decryption is done as**

$$P_i = (C_i - K_{i \bmod m}) \bmod 26$$

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword. For example, if the keyword is *deceptive*, the message “we are discovered save yourself” is encrypted as

key: *deceptivedeceptivedeceptive*


plaintext: *wearediscoveredsaveyourself*

ciphertext: *ZICVTWQNGRZGVTWAVZHCQYGLMGJ*

EXPRESSED NUMERICALLY, WE HAVE THE FOLLOWING RESULT.

|            |    |   |   |    |    |    |    |    |   |    |    |   |    |    |
|------------|----|---|---|----|----|----|----|----|---|----|----|---|----|----|
| key        | 3  | 4 | 2 | 4  | 15 | 19 | 8  | 21 | 4 | 3  | 4  | 2 | 4  | 15 |
| plaintext  | 22 | 4 | 0 | 17 | 4  | 3  | 8  | 18 | 2 | 14 | 21 | 4 | 17 | 4  |
| ciphertext | 25 | 8 | 2 | 21 | 19 | 22 | 16 | 13 | 6 | 17 | 25 | 6 | 21 | 19 |

|            |    |    |    |    |   |    |    |    |    |    |    |    |   |
|------------|----|----|----|----|---|----|----|----|----|----|----|----|---|
| key        | 19 | 8  | 21 | 4  | 3 | 4  | 2  | 4  | 15 | 19 | 8  | 21 | 4 |
| plaintext  | 3  | 18 | 0  | 21 | 4 | 24 | 14 | 20 | 17 | 18 | 4  | 11 | 5 |
| ciphertext | 22 | 0  | 21 | 25 | 7 | 2  | 16 | 24 | 6  | 11 | 12 | 6  | 9 |



The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword. Thus, the letter frequency information is obscured.



# THE MODERN VIGENÈRE CIPHER AND TABLEU

The Vigenère cipher bares much resemblance to the *Modified Caesar cipher*, discussed above, but uses a key phrase instead of the numbers in the shift vector.

The encryption process for this cipher takes each individual letter of a plaintext message and combines it with a letter from the key, together these two letters act as coordinates for a position on the Vigenère square shown below:

|     |   | 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 |
| Key | a | 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 |
|     | b | 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 | A |
|     | c | C         | 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 |
|     | d | 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 |
|     | e | 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 | D |
|     | f | F         | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
|     | g | G         | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
|     | h | H         | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
|     | i | I         | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
|     | j | J         | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
|     | k | K         | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
|     | l | L         | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
|     | m | M         | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
|     | n | N         | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
|     | o | O         | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|     | p | P         | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|     | q | Q         | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
|     | r | R         | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
|     | s | S         | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
|     | t | T         | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
|     | u | U         | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
|     | v | V         | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
|     | w | W         | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
|     | x | X         | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
|     | y | Y         | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
|     | z | Z         | 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 |

By: Narendra Bohara


6

the key is a repeating keyword. For example, if the keyword is *deceptive*, the message "we are discovered save yourself" is encrypted as follows:

key:           *deceptivedeceptivedeceptive*

plaintext:   wearediscoveredsaveyourself

ciphertext:  ZICVTWQNGRZGVTWAVZHCQYGLMGJ



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

The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword. Thus, the letter frequency information is obscured. However, not all knowledge of the plaintext structure is lost.

# ***VERNAM CIPHER***

The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plaintext and has no statistical relationship to it. Such a system was introduced by an AT&T engineer named Gilbert Vernam in 1918.

His system works on binary data (bits) rather than letters. The system can be expressed as follows

$$c_i = p_i \oplus k_i$$

where

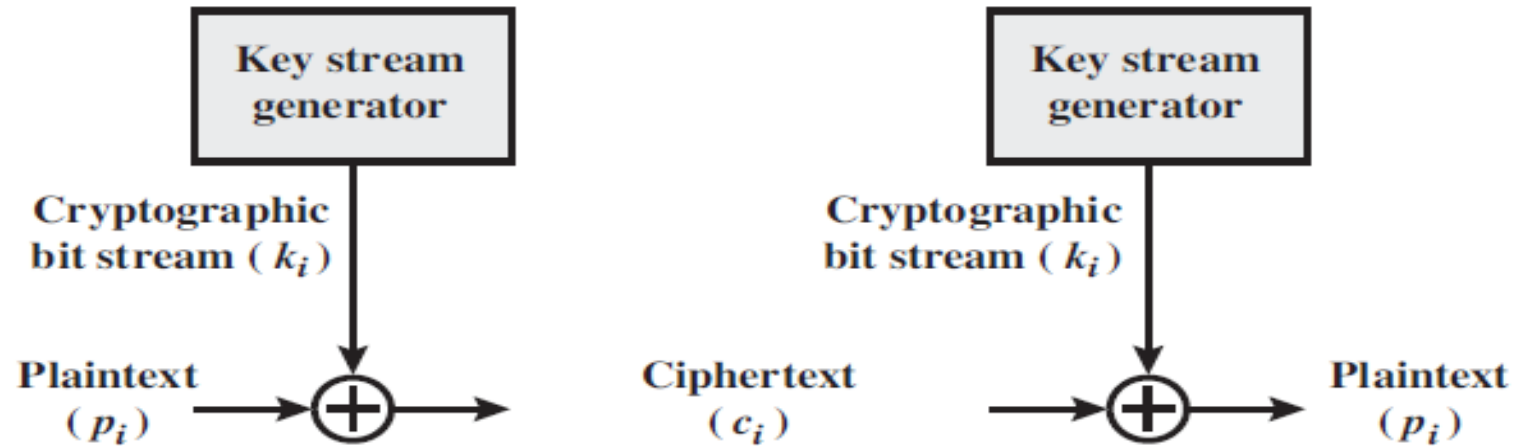
$p_i$  =  $i$ th binary digit of plaintext

$k_i$  =  $i$ th binary digit of key

$c_i$  =  $i$ th binary digit of ciphertext

$\oplus$  = exclusive-or (XOR) operation

# VERNAM CIPHER



**Figure 2.7** Vernam Cipher

Thus, the ciphertext is generated by performing the bitwise XOR of the plaintext and the key. Because of the properties of the XOR, decryption simply involves the same bitwise operation:

$$p_i = c_i \oplus k_i$$

# 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.
- ❑ 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:

$$C_i = P_i \oplus K_i$$


Where,  $C_i$  - ith binary digit of cipher text

$P_i$  - ith binary digit of plaintext

$K_i$  - ith binary digit of key

$\oplus$  - exclusive OR operation

- ❑ 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:


$$P_i = C_i \oplus K_i$$

Example

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.

# HILL CIPHER

- ❑ Another interesting multiletter cipher is the Hill cipher, developed by the mathematician Lester Hill in 1929.
- ❑ This encryption algorithm takes successive plaintext letters and substitutes for them  $m$  ciphertext letters.
- ❑ The substitution is determined by  $m$  linear equations in which each character is assigned a numerical value. For  $m=3$ , the system can be described as

**HERE  $\mathbf{C}$  AND  $\mathbf{P}$  ARE ROW VECTORS OF LENGTH 3 REPRESENTING THE PLAINTEXT AND CIPHERTEXT, AND  $\mathbf{K}$  IS A  $3 \times 3$  MATRIX REPRESENTING THE ENCRYPTION KEY. OPERATIONS ARE PERFORMED MOD 26.**

$$c_1 = (k_{11}P_1 + k_{12}P_2 + k_{13}P_3) \bmod 26$$

$$c_2 = (k_{21}P_1 + k_{22}P_2 + k_{23}P_3) \bmod 26$$

$$c_3 = (k_{31}P_1 + k_{32}P_2 + k_{33}P_3) \bmod 26$$

This This can be expressed in term of column vectors and matrices:

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$$

where  $\mathbf{C}$  and  $\mathbf{P}$  are column vectors of length 3, representing the plaintext and ciphertext, and  $\mathbf{K}$  is a  $3 \times 3$  matrix, representing the encryption key. Operations are performed mod 26.

or

$$\mathbf{C} = \mathbf{KP} \bmod 26$$

# CONSIDER THE PLAINTEXT "PAYMOREMONEY" AND USE THE ENCRYPTION KEY

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

The first three letters of the plaintext are represented by the vector

$$\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}. \text{ Then } \mathbf{K} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \text{LNS. Continuing in this fashion,}$$

the ciphertext for the entire plaintext is LNSHDLEWMTRW.

Decryption requires using the inverse of the matrix  $\mathbf{K}$ . The inverse  $\mathbf{K}^{-1}$  of a matrix  $\mathbf{K}$  is defined by the

equation  $\mathbf{K} \mathbf{K}^{-1} = \mathbf{K}^{-1} \mathbf{K} = \mathbf{I}$ , where  $\mathbf{I}$  is the matrix that is all zeros except for ones along the main diagonal from upper left to lower right. The inverse of a matrix does not always exist, but when it does, it satisfies the preceding equation.

In this case, the inverse is:

$$\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

This is demonstrated as follows:

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

# IN GENERAL,

$$\mathbf{C} = E(\mathbf{K}, \mathbf{P}) = \mathbf{K}\mathbf{P} \bmod 26$$

$$\mathbf{P} = D(\mathbf{K}, \mathbf{P}) = \mathbf{K}^{-1}\mathbf{C} \bmod 26 = \mathbf{K}^{-1}\mathbf{K}\mathbf{P} = \mathbf{P}$$

# EXAMPLE

For example, consider the plaintext “paymoremoney” and use the encryption key

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

The first three letters of the plaintext are represented by the vector . Then . Continuing in this fashion, the ciphertext for the entire plaintext is RRLMWBKASPDH.



# TRANSPOSITION TECHNIQUES

□ It is another type of cipher where the order of the alphabets in the plaintext is rearranged to create the ciphertext. The actual plaintext alphabets are not replaced.

**Example Rail fence**

# RAIL FENCE(ZIG-ZAG CIPHER)

- is the 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.
- The key of the rail fence is the number of rails , i.e., the depth of the diagonal

# EXAMPLE 1

**Key:** rail fence of depth 2

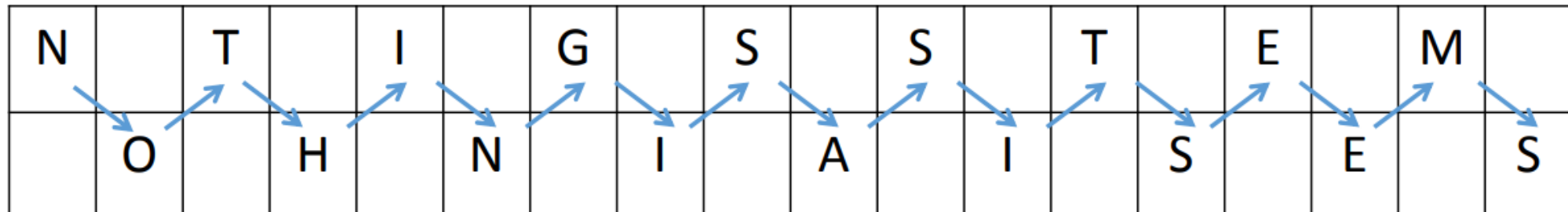
**Plaintext:** NOTHING IS AS IT SEEMS

**Encrypt:** First writing NOTHING IS AS IT SEEMS on two lines in a zig-zag pattern (or rail fence).

**The ciphertext** is produced by transcribing the first row followed by the second row.

## EXAMPLE...

WE ENCIPHER **NOTHING IS AS IT SEEMS** BY FIRST WRITING IT ON TWO LINES IN A ZIG-ZAG PATTERN (OR RAIL FENCE). THE CIPHERTEXT IS PRODUCED BY TRANSCRIBING THE FIRST ROW FOLLOWED BY THE SECOND ROW



Ciphertext: NTIGS STEMO HNIAI SES

# RAIL FENCE CONTD.. EXAMPLE 2

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

# DECRYPTION

To decrypt, we write half the letters on one line, half on the second. (Note that if there are an odd number of letters, we include the “middle” letter on the top line.)

**Example 3:** Decipher MKHSE LWYAE ATSOL.

Solution :

Since there are 15 letters, we write 8 on the top line and 7 on the bottom line so that

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M |   | K |   | H |   | S |   | E |   | L |   | W |   | Y |
|   | A |   | E |   | A |   | T |   | S |   | O |   | L |   |

Plaintext: **MAKE HASTE SLOWLY.**

## EXAMPLE 4 WITH DEPTH 3

For example, if the message is “GeeksforGeeks” and the number of rails = 3 then cipher is prepared as:

The diagram illustrates the preparation of a 3-rail cipher for the message "GeeksforGeeks". The message is written in a zigzag pattern across three rows (rails). Red arrows indicate the path of the zigzag, starting from the top-left cell and moving diagonally down to the middle row, then diagonally up to the top row, and repeating this pattern. The letters are placed in the cells as follows:

|   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| G |   |   |   | S |   |   |   | G |   |   |   | S |
|   | E |   | K |   | F |   | R |   | E |   | K |   |
|   |   | E |   |   |   | O |   |   |   | E |   |   |

## EXAMPLE 5

For the plaintext **"defend the east wall"** with a key size or the size of the row is 3, Encryption process is as follows,

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D |   |   |   | N |   |   |   | E |   |   |   | T |   |   |   | L |   |   |
|   | E |   | E |   | D |   | H |   | E |   | S |   | W |   | L |   | X |   |
|   |   | F |   |   |   | T |   |   |   | A |   |   |   | A |   |   |   | X |

That at the end of the message we have inserted two "X"s. These are called nulls and act as placeholders. We do this to make the text fit into the rail so that there is the same number of letters on the top row as well as on the bottom row. Otherwise, it is not necessary, it makes the decryption process a bit easier if the text has this format.

And the cipher text became: **"dnetleedheswlxftaax"**.



# RAIL FENCE CIPHER DECRYPTION

- ❑ The number of columns in rail fence cipher remains equal to the length of plain-text.
- ❑ The key remains the same as in encryption to the number of rails.
- ❑ Hence, the Rail Fence matrix can be constructed likely. Once we have got the matrix we can find-out the places where plain texts should be placed using the same way as we do in the encryption method of moving diagonally up and down alternatively to form text.
- ❑ Then, we fill the cipher-text accordingly to row-wise. After filling the text, we traverse the matrix in the zig-zag form to get the original text or the plain text.

# RAIL FENCE CIPHER DECRYPTION: EXAMPLE

For the ciphertext "**TEKOOHRACIRMNREATANFTETYTGHH**", it will be encrypted with a key size of 4.

We start by placing the "**T**" in the first square. You then dash the diagonal down places until you get back to the top line, and place the "**E**" here. Continuing to fill the rows you get the pattern below,

|   |   |   |   |   |  |   |  |   |   |   |  |   |  |   |   |   |  |   |  |   |   |   |   |   |   |   |  |
|---|---|---|---|---|--|---|--|---|---|---|--|---|--|---|---|---|--|---|--|---|---|---|---|---|---|---|--|
| T |   |   |   |   |  | E |  |   |   |   |  | K |  |   |   |   |  | O |  |   |   |   |   | O |   |   |  |
|   | - |   |   |   |  | - |  | - |   |   |  | - |  | - |   |   |  | - |  | - |   |   | - |   | - |   |  |
|   |   | - |   | - |  |   |  | - |   | - |  |   |  | - |   | - |  |   |  | - |   | - |   |   |   | - |  |
|   |   |   | - |   |  |   |  |   | - |   |  |   |  |   | - |   |  |   |  |   | - |   |   |   |   | - |  |

As we have a key size of 4 and the length of the message is 28 so we make like this and continues this till all the text does not fit into it.

|   |   |   |   |   |   |  |   |   |   |   |   |  |   |   |   |   |   |  |   |   |   |   |   |  |   |   |
|---|---|---|---|---|---|--|---|---|---|---|---|--|---|---|---|---|---|--|---|---|---|---|---|--|---|---|
| T |   |   |   |   | E |  |   |   |   |   | K |  |   |   |   |   | O |  |   |   |   |   | O |  |   |   |
|   | H |   |   |   | R |  | A |   |   |   | C |  | I |   |   |   | R |  | M |   |   |   | N |  | R |   |
|   |   | - |   | - |   |  |   | - |   | - |   |  |   | - |   | - |   |  |   | - |   | - |   |  |   | - |
|   |   |   | - |   |   |  |   |   | - |   |   |  |   |   | - |   |   |  |   |   | - |   |   |  |   | - |

Second stage in decryption process,

|   |   |   |   |   |   |  |   |   |   |   |  |   |   |   |   |  |   |   |   |   |  |   |   |
|---|---|---|---|---|---|--|---|---|---|---|--|---|---|---|---|--|---|---|---|---|--|---|---|
| T |   |   |   |   | E |  |   |   |   | K |  |   |   |   | O |  |   |   |   | O |  |   |   |
|   | H |   |   |   | R |  | A |   |   | C |  | I |   |   | R |  | M |   |   | N |  | R |   |
|   |   | E |   | A |   |  | T |   | A |   |  | N |   | F |   |  | T |   | E |   |  | T |   |
|   |   |   | - |   |   |  |   | - |   |   |  |   | - |   |   |  |   | - |   |   |  |   | - |

Third stage in decryption process,

|   |   |   |   |   |   |  |   |   |   |   |  |   |   |   |   |  |   |   |   |   |  |   |   |
|---|---|---|---|---|---|--|---|---|---|---|--|---|---|---|---|--|---|---|---|---|--|---|---|
| T |   |   |   |   | E |  |   |   |   | K |  |   |   |   | O |  |   |   |   | O |  |   |   |
|   | H |   |   |   | R |  | A |   |   | C |  | I |   |   | R |  | M |   |   | N |  | R |   |
|   |   | E |   | A |   |  | T |   | A |   |  | N |   | F |   |  | T |   | E |   |  | T |   |
|   |   |   | Y |   |   |  |   | T |   |   |  |   | G |   |   |  |   | H |   |   |  |   | H |



Forth and the final stage in decryption process,

Now, we read them as diagonally from top to bottom then bottom to top and we get the plain text or the original text i.e. **"THEY ARE ATTACKING FROM THE NORTH"**.

# BLOCK CIPHERS

- ❑ Block ciphers encipher and decipher multiple bits at once, rather than one bit at a time.
- ❑ For this reason, software implementations of block ciphers run faster than software implementations of stream ciphers.
- ❑ Errors in transmitting one block generally do not affect other blocks, but as each block is enciphered independently, using the same key, identical plaintext blocks produce identical ciphertext blocks.
- ❑ This allows the analyst to search for data by determining what the encipherment of a specific plaintext block is.
- ❑ For example, if the word INCOME is enciphered as one block, all occurrences of the word produce the same ciphertext

# EXAMPLE

Consider a banking database with two records:

MEMBER: HOLLY INCOME \$100,000

MEMBER: HEIDI INCOME \$100,000

Suppose the encipherment of this data under a block cipher is

**ABCQZRME GHQMRSIB CTXUVYSS RMGRPFQN**

**ABCQZRME ORMPABRZ CTXUVYSS RMGRPFQN**

If an attacker determines who these records refer to, and that CTXUVYSS is the

encipherment of the INCOME keyword, he will know that Holly and Heidi have the

# COMPARISION OF STREAM AND BLOCK CIPHERS

| BASIS FOR COMPARISON                  | Block   | Stream   |
|---------------------------------------|---|--|
| Basic                                 | Converts the plain text by taking its block at a time.    | Converts the text by taking one byte of the plain text at a time |
| Complexity<br>Data Buffering required | Simple design<br>More space required                      | Complex comparatively<br>None of limited                         |
| No of bits used                       | 64 Bits or more   | 8 Bits   |
| Confusion and Diffusion               | Uses both confusion and diffusion                         | Relies on confusion only   |
| Algorithm modes used                  | ECB (Electronic Code Book)<br>CBC (Cipher Block Chaining) | CFB (Cipher Feedback)<br>OFB (Output Feedback)                   |



| Reversibility  | Reversing encrypted text is hard. | It uses XOR for the encryption which can be easily reversed to the plain text. |
|----------------|-----------------------------------|--|
| Implementation | Feistel Cipher                    | Vernam Cipher  |
|                |                                   |  |

# ADVANTAGES OF STREAM CIPHER OVER BLOCK CIPHER

- ❑ Stream ciphers are typically faster than block ciphers and work well for large or small chunks of data.
- ❑ Stream Ciphers does not require large memory because they only work on small bits at a time unlike block ciphers that require a relatively large memory because they work on a large chunk of data.
- ❑ Stream cipher bytes are individually encrypted with no connection to other chunks of data whereas block ciphers encrypt a whole block at a time.
- ❑ Stream ciphers are usually best for cases where the amount of data is either unknown or continuous such as network streams while block ciphers are more useful when the amount or length of data is known such as file, data fields or response protocol.

# EXAMPLES

Block Ciphers: AES, DES, 3DES, Blowfish, Twofish etc

Stream Cipher: RC4 (Rivest Cipher 4 or ARCFOUR or ARC4)

# SYMMETRIC (PRIVATE-KEY) CRYPTOGRAPHY

- traditional **private/secret/single key** cryptography uses **one key**
- shared by both sender and receiver
- if this key is disclosed communications are compromised
- also is **symmetric**, parties are equal

# SYMMETRIC ENCRYPTION MODEL

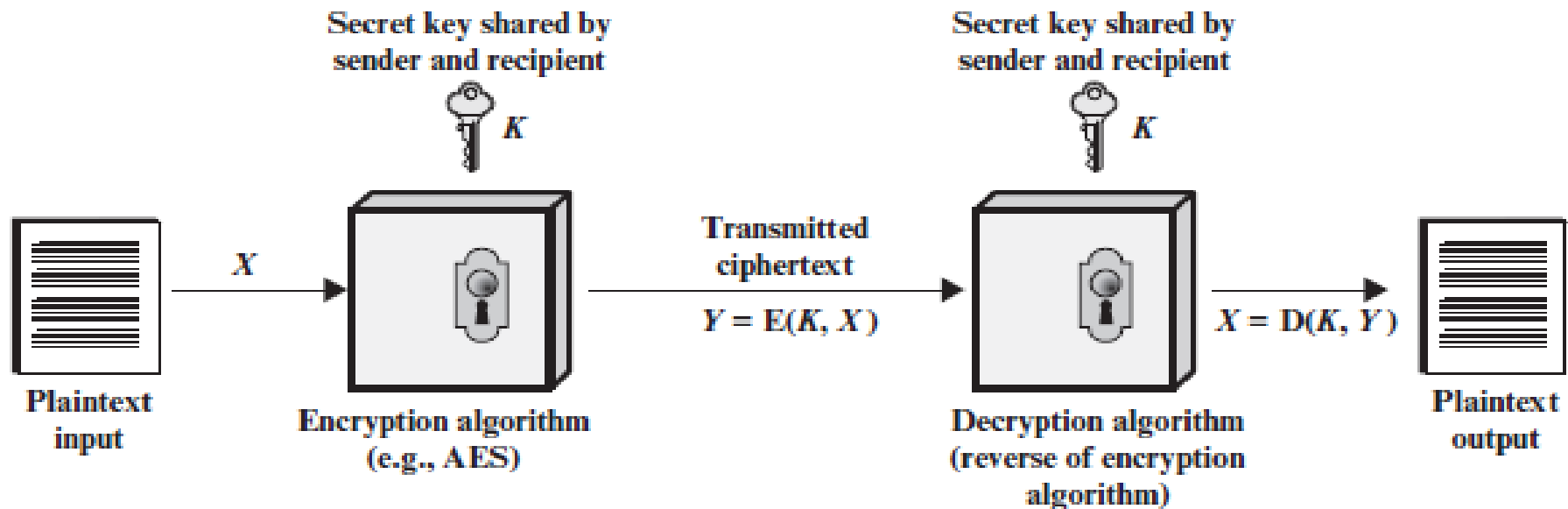


Figure 3.1 Simplified Model of Symmetric Encryption

# 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.

# PUBLIC-KEY CRYPTOGRAPHY

- ❑ uses two keys – a public & a private key.
- ❑ complements rather than replaces private key cryptography (efficiency reasons).

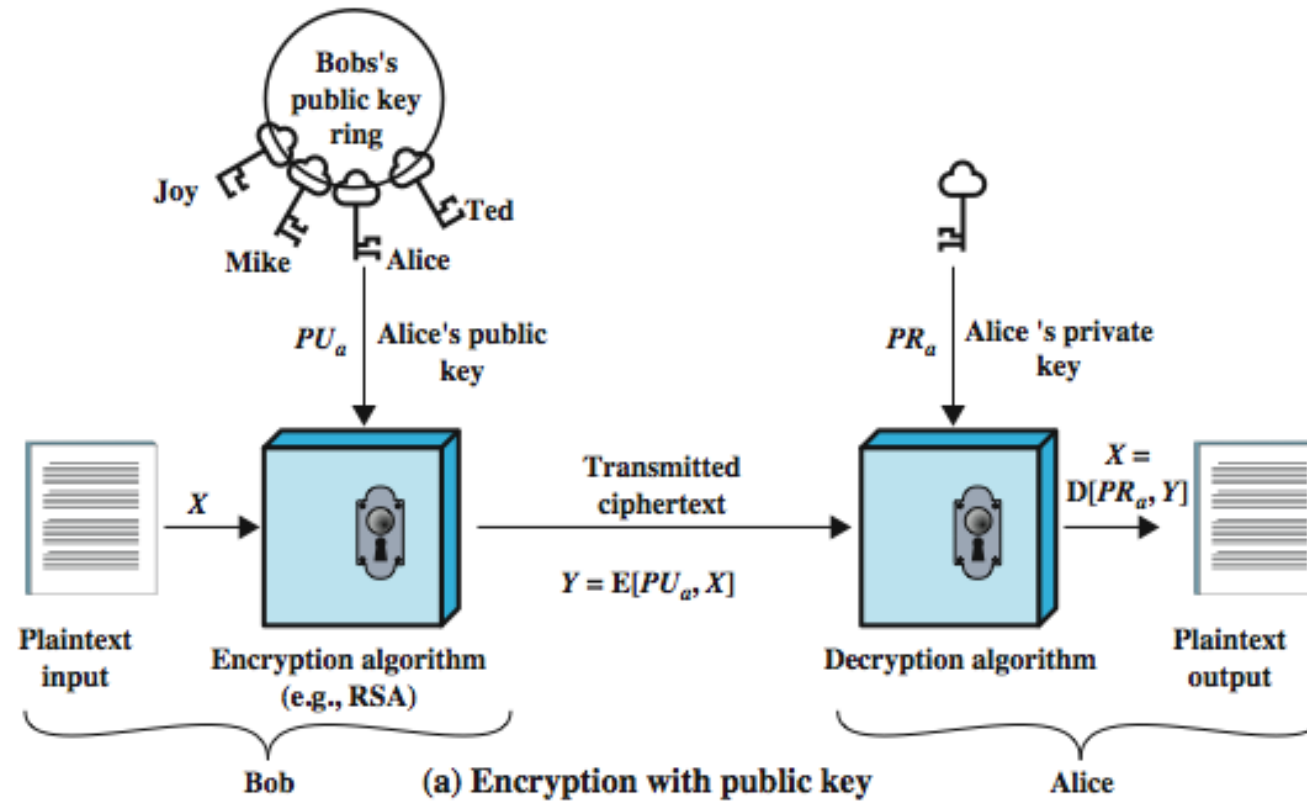
# WHY PUBLIC-KEY CRYPTOGRAPHY?

developed to address two key issues: –

- ❑ key distribution – how to have secure communications in general without having to trust a KDC with your key .
- ❑ digital signatures – how to verify a message comes intact from the claimed sender.



- ❑ public-key/two-key/asymmetric cryptography involves the use of two keys: – a public-key, which may be known by anybody, and can be used to encrypt messages, and verify signatures – a related private-key, known only to the recipient, used to decrypt messages, and sign (create) signatures.
- ❑ infeasible to determine private key from public (requires solving a hard problem).
- ❑ is asymmetric because – those who encrypt messages or verify signatures cannot decrypt messages or create signatures



# SYMMETRIC VS PUBLIC-KEY

| Conventional Encryption   | Public-Key Encryption   |
|---|---|
| <p><i>Needed to Work:</i></p> <ol style="list-style-type: none"><li>1. The same algorithm with the same key is used for encryption and decryption.</li><li>2. The sender and receiver must share the algorithm and the key.</li></ol> <p><i>Needed for Security:</i></p> <ol style="list-style-type: none"><li>1. The key must be kept secret.</li><li>2. It must be impossible or at least impractical to decipher a message if no other information is available.</li><li>3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.</li></ol> | <p><i>Needed to Work:</i></p> <ol style="list-style-type: none"><li>1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.</li><li>2. The sender and receiver must each have one of the matched pair of keys (not the same one).</li></ol> <p><i>Needed for Security:</i></p> <ol style="list-style-type: none"><li>1. One of the two keys must be kept secret.</li><li>2. It must be impossible or at least impractical to decipher a message if no other information is available.</li><li>3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.</li></ol> |

# PUBLIC-KEY APPLICATIONS

can classify uses into 3 categories:

- **encryption/decryption** (provide secrecy)
- **digital signatures** (provide authentication)
- **key exchange** (of session keys)

some algorithms are suitable for all uses, others are specific to one

| Algorithm      | Encryption/Decryption | Digital Signature | Key Exchange |
|----------------|-----------------------|-------------------|--------------|
| RSA            | Yes                   | Yes               | Yes          |
| Elliptic Curve | Yes                   | Yes               | Yes          |
| Diffie-Hellman | No                    | No                | Yes          |
| DSS            | No                    | Yes               | No           |

# PUBLIC-KEY REQUIREMENTS

Public-Key algorithms rely on two keys where:

- it is computationally infeasible to find decryption key knowing only algorithm & encryption key
- it is computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known
- either of the two related keys can be used for encryption, with the other used for decryption (for some algorithms)

these are formidable requirements which only a few algorithms have satisfied

# PUBLIC-KEY REQUIREMENTS

need a trapdoor one-way function

one-way function has

- $Y = f(X)$  easy
- $X = f^{-1}(Y)$  infeasible

a trap-door one-way function has

- $Y = f_k(X)$  easy, if  $k$  and  $X$  are known
- $X = f_k^{-1}(Y)$  easy, if  $k$  and  $Y$  are known
- $X = f_k^{-1}(Y)$  infeasible, if  $Y$  known but  $k$  not known

a practical public-key scheme depends on a suitable trap-door one-way function

# SECURITY OF PUBLIC KEY SCHEMES

- like private key schemes brute force **exhaustive search** attack is always theoretically possible.
- but keys used are too large ( $>512$  bits)
- security relies on a **large enough** difference in difficulty between **easy** (en/decrypt) and **hard** (cryptanalyse) problems
- more generally the **hard** problem is known, but is made hard enough to be impractical to break
- requires the use of **very large numbers**
- hence is **slow** compared to private key schemes