UNIT:1

Computer Security concepts, security services, and Active vs. Passive attacks, Security mechanisms, OSI Security Architecture, A Model for Network security, Classical Encryption Techniques, Substitution ciphers, Transposition ciphers.

Computer Security-generic name for the collection of tools designed to protect data and to thwart hackers

Network Security- measures to protect data during their transmission. This area covers the use of cryptographic algorithms in network protocols and network applications.

Cryptographic algorithms: This is the study of techniques for ensuring the secrecy and/or authenticity of information

SECURITY GOALS:

CONFEDENTIALITY:

- hiding information from an authorized access
- information while exchange should remain secret

DATA INTEGRITY:

- preventing information from un authorized modification
- need techniques to ensure the integrity of the data
  - preventing the modification
  - detect any modification made

AVAILABILITY:

- should be easily available to authorized users
- data must be available to authorized users

cryptographic algorithms are used to achieve the above goals

THE OSI SECURITY ARCHITECTURE

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

• **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 thedata 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 ATTACKS

Generic types of attacks

- Passive attacks
- Active attacks

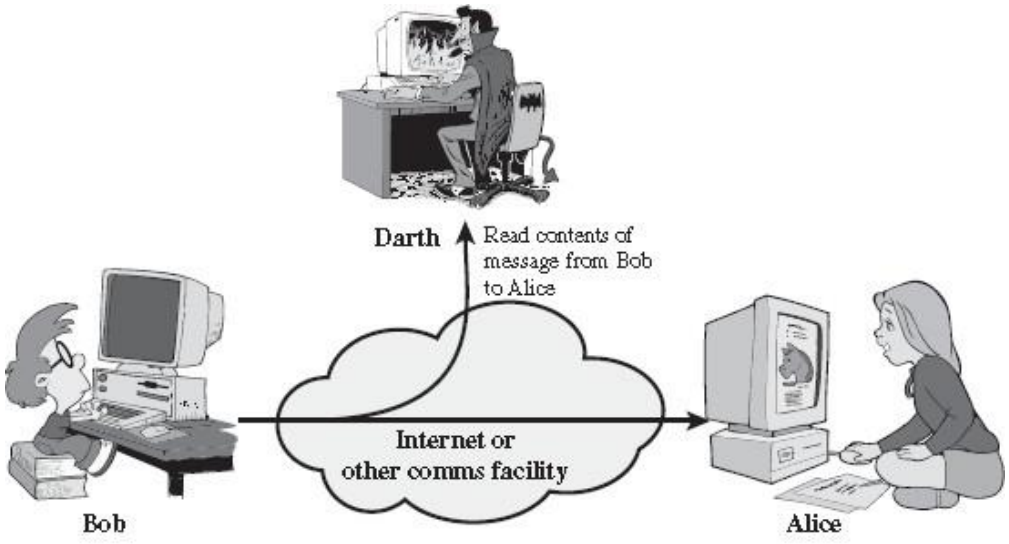
. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

Passive Attacks

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

1) Release of message contents:

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.

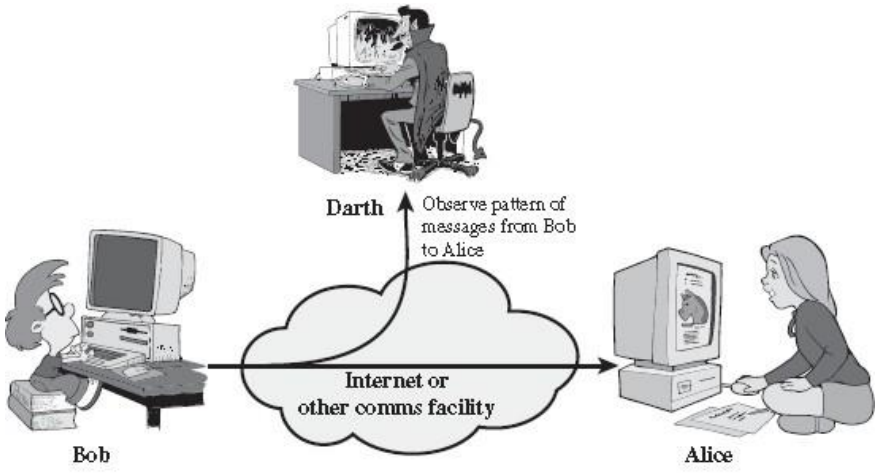


(a) Release of message contents

2) Traffic analysis:

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



(b) Traffic analysis

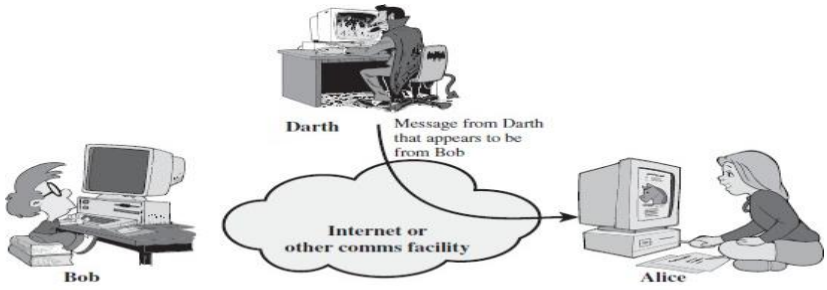
Active attack: An active attack attempts to alter system resources or affect their operation. Active attacks involve some modification of the data stream or the creation of a false stream. Active attacks can be subdivided into four categories:

- masquerade,
- replay,
- modification of messages, and
- Denial of service.

Masquerade:

A **masquerade** takes place when one entity pretends to be a different entity (Figure:). A masquerade attack usually includes one of the other forms of active attack.

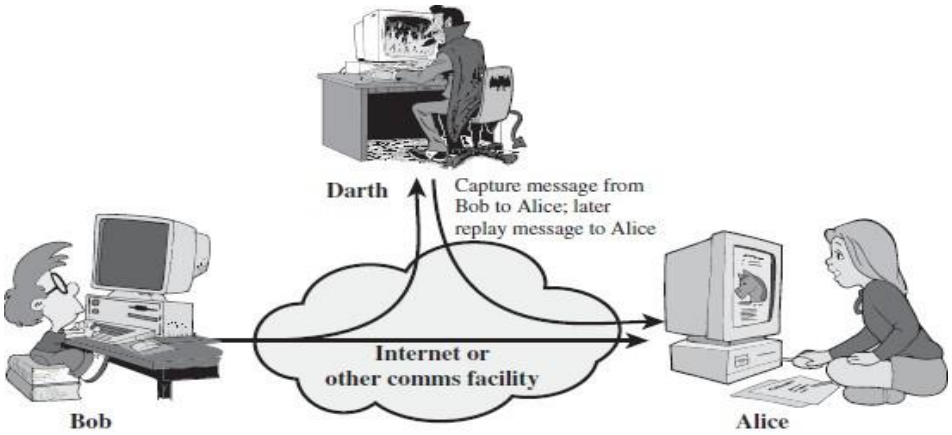
For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.



(a) Masquerade

Replay :

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

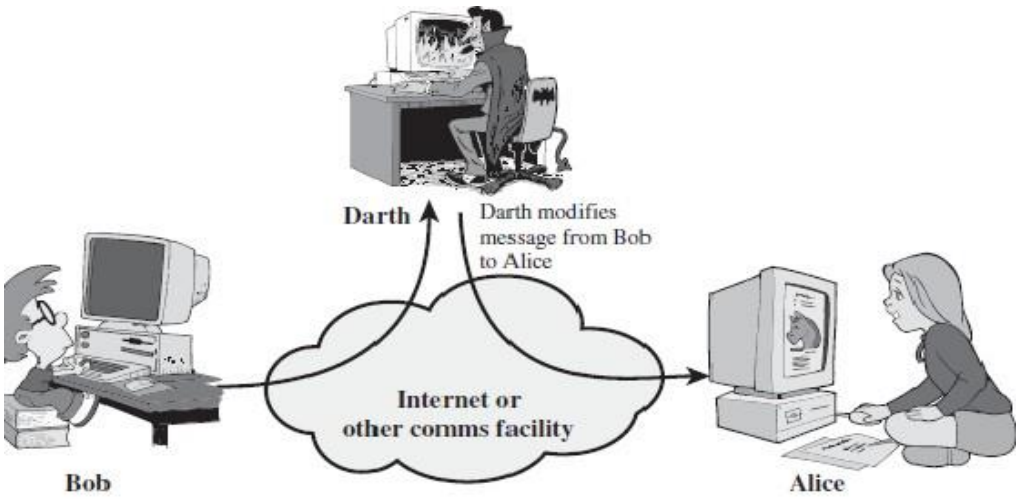


(b) Replay

Modification of messages:

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 (Figure: c).

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



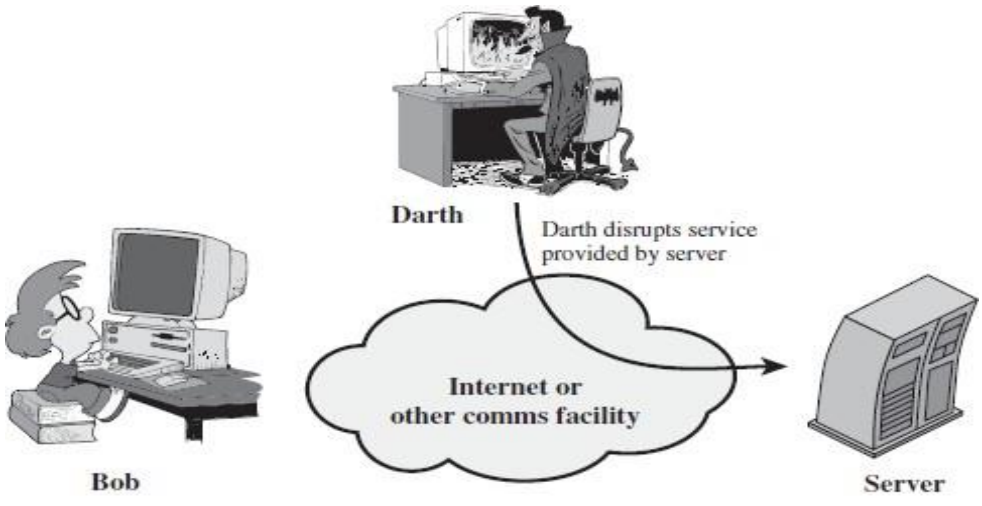
(c) Modification of messages

Denial of service:

The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure d). 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



(d) Denial of service

1.7 SECURITY SERVICES

The classification of security services are as follows:

CONFIDENTIALITY: Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. Confidentiality is the protection of transmitted data from passive attacks. 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.

Connection Confidentiality

The protection of all user data on a connection.

Connectionless Confidentiality

The protection of all user data in a single data block

Selective-Field Confidentiality

The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality

The protection of the information that might be derived from observation of traffic flows.

AUTHENTICATION: The authentication service is concerned with assuring that a communication is Authentic. The assurance that the communicating entity is the one that it claims to be.

Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Peer Entity Authentication

Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication

In a connectionless transfer, provides assurance that the source of received data is as claimed.

INTEGRITY: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.

NON REPUDIATION: Requires that neither the sender nor the receiver of a message be able to deny the transmission. when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message

ACCESS CONTROL: Requires that access to information resources may be controlled by the target system . 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

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

SECURITY MECHANISMS

One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are

1 ENCIPHERMENT

2 DIGITAL SIGNATURE

3 ACCESS CONTROL

ENCIPHERMENT: It refers to the process of applying mathematical algorithms for converting data into a form that is not intelligible. This depends on algorithm used and encryption keys.

DIGITAL SIGNATURE: The appended data or a cryptographic transformation applied to any data unit allowing to prove the source and integrity of the data unit and protect against forgery.

ACCESS CONTROL: A variety of techniques used for enforcing access permissions to the system 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 once a breach of security is suspected.

NOTARIZATION: The use of a trusted third party to assure certain properties of a data exchange

GENERAL TERMS:

An original message is known as the **plaintext**, while the coded message is called the **ciphertext**. The process of converting from plaintext to ciphertext is known as **enciphering** or **encryption**; restoring the plaintext from the ciphertext is **deciphering** or **decryption**. The many

Schemes used for encryption constitute the area of study known as **cryptography**. Such a scheme is known as a **cryptographic system** or a **cipher**. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of **cryptanalysis**. Cryptanalysis is what the layperson calls "breaking the code." The areas of cryptography and cryptanalysis together are called **cryptology**.

SYMMETRIC CIPHER MODEL:

Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption. Symmetric encryption, also referred to as conventional encryption or single-key encryption.

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.

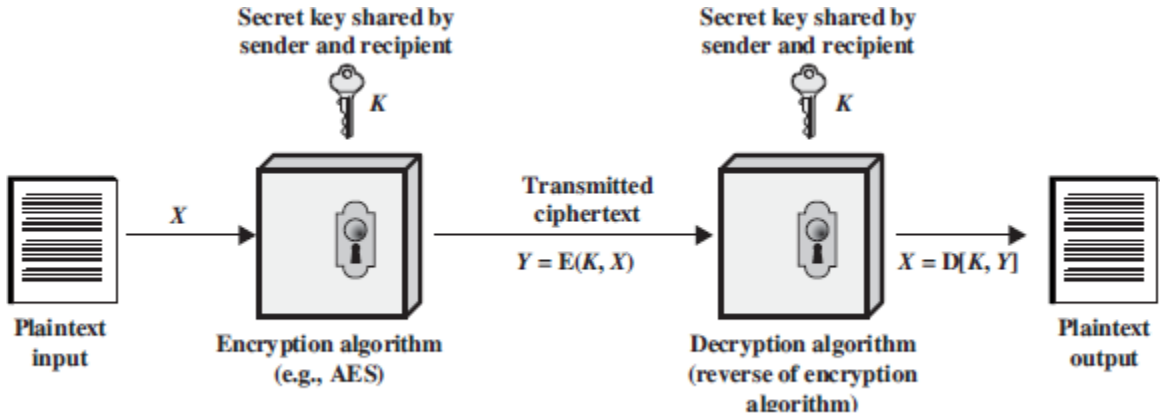
• **Secret key:** The secret key is also input to the encryption algorithm.The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.The exact substitutions and transformations performed by 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. • **Decryption algorithm:** This is essentially the encryption algorithm run inreverse. It takes the ciphertext and the secret key and produces the originalplaintext.

There are two requirements for secure use of conventional encryption:

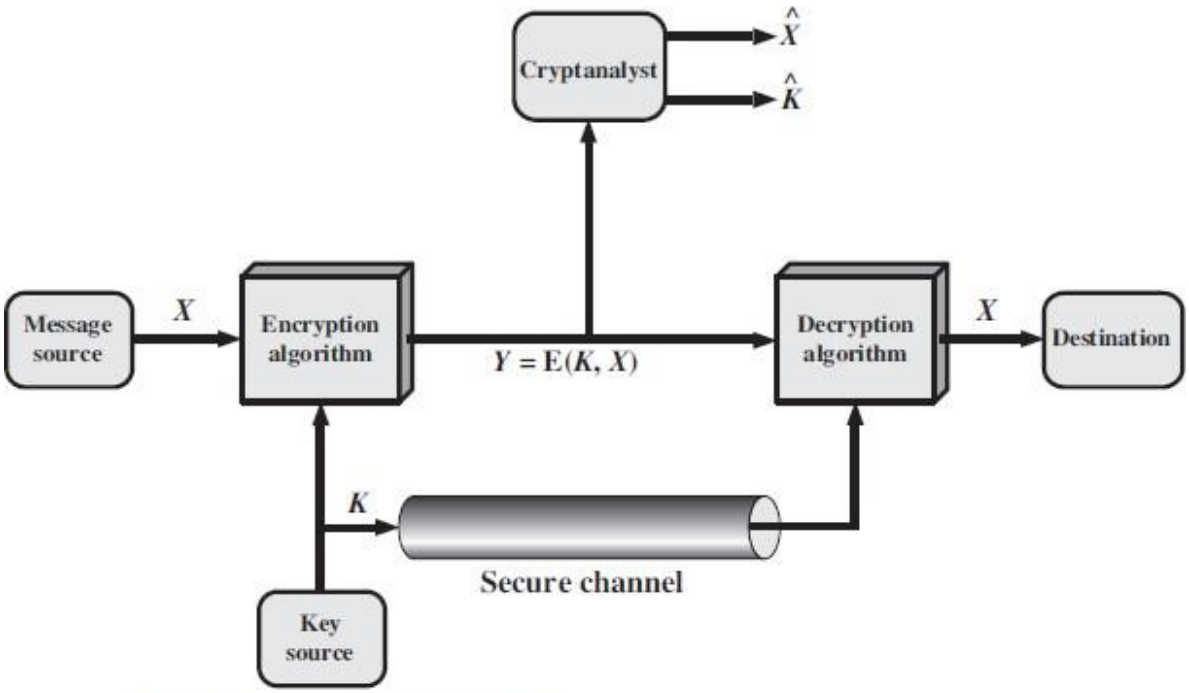
1. We need a strong encryption algorithm. At a minimum, we would like thealgorithm to be such that an opponent who knows the algorithm and hasaccess to one or more ciphertexts would be unable to decipher the ciphertextor figure out the key.

2.Sender and receiver must have obtained copies of the secret key in a securefashion and must keep the key secure.



Simplified Model of Symmetric Encryption

Let us take a closer look at the essential elements of a symmetric encryption scheme, using below Figure. A source produces a message in plaintext, . The elements of are letters in some finite alphabet. Traditionally, the alphabet usually consisted of the 26 capital letters. Nowadays,the binary alphabet {0, 1} is typically used. For encryption, a key of the form 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 toboth source and destination



Model of Symmetric Cryptosystem

With the message and the encryption key as input, the encryption algorithm forms the ciphertext .We can write this as This notation indicates that is produced by using encryption algorithm E as a function of the plaintext , with the specific function determined by the value of the key .

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

X=D(K,Y)

Cryptographic systems are characterized along three independent dimensions:

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

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.

SUBSTITUTION TECHNIQUES

1) Caesar cipher (or) shift cipher

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

plain: meet me after the toga party

cipher: PHHW PH DIWHU WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that letter following „z‟ is „a‟.

Then the algorithm can be expressed as follows. For each plaintext letter , substitute

The cipher text letter

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

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) mod 26

Drawbacks

- There are only 25 keys totry.
- The language of the plaintext is known and easily recognizable

2) Monoalphabetic Ciphers:

With only 25 possible keys, the Caesar cipher is far from secure. 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 , 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 3! permutations of a set of elements, because the first element can be chosen in one of n ways, the second in ways, the third in 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 $4 * 10^{26}$ possible keys.

Such an approach is referred to as a **monoalphabetic substitution cipher**, because a single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.

3) Playfair Cipher

The best-known multiple-letter encryption cipher is the Play fair, which treats digrams in the plaintext as single units and translates these units into cipher text digram's. The Play fair algorithm

is based on the use of a 5*5 matrix of letters constructed using a keyword.

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 itsown row and the column occupied by the other plaintext letter. Thus, hsbecomes BP and ea becomes IM (or JM, as the encipherer wishes).

example

Plaintext = meet me at the school house

Splitting two letters as a unit => me et me at thesch oxolho us ex

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

Strength of playfair cipher

Playfair cipher is a great advance over simple mono alphabetic ciphers. Since there are 26 letters, 26x26 = 676 diagrams are possible, so identification of individual diagram is more difficult.

4) Polyalphabetic ciphers

a)Vigenere cipher:

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

Strength of Vigenere cipher

- There are multiple cipher text letters for each plaintext letter.
- Letter frequency information is obscured.

b) Vernam cipher The ultimate defense against such a cryptanalysis is to choose a keyword that is as long as the plain text and has no statistical relationship to it. Such a system was introduced by an AT&T engineer named GilbertVernamin1918.His system works on binarydata (bits) rather than letters. Then system can be expressed succinctly as follows

$$c_i = p_i \oplus k_i$$

where

p_i= ith binarydigitofplaintext

k_i =ithbinary digit ofkey

c_i =ithbinary digit ofciphertext

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

Vernam Cipher

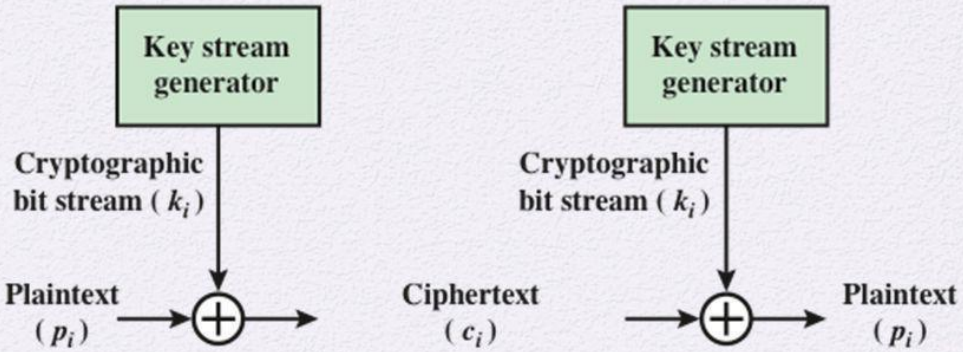


Figure 2.7 Vernam Cipher

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:

$$p_i = c_i \oplus k_i$$

Example :

1001001 1000110	plaintext
1010110 0110001	key
0011111 1110110	ciphertext

Decryption:

0011111 1110110	ciphertext
1010110 0110001	key
1001001 1000110	plaintext

c)One Time Pad:

It is an unbreakable cryptosystem. The key is of same length as the message. Once a key is used, it is discarded and never used again.

An example should illustrate our point. Suppose that we are using a Vigenère scheme with 27 characters in which the twenty-seventh character is the space character, but with a one-time key that is as long as the message. Consider the ciphertext

ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

We now show two different decryptions using two different keys:

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key: PXLMVMSYDOFUYRVZWCTNLEBNECVGDUPAHFZZLMNYIH

plaintext: MR MUSTARD WITH THE CANDLESTICK IN THE HALL

ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS

key: MFUGPMIYDGAXGOUFHKLLLMHSQDQOGTEWBQFGYOVUHWT

plaintext: MISS SCARLET WITH THE KNIFE IN THE LIBRARY

Suppose that a cryptanalyst had managed to find these two keys.Twopausible plaintexts are produced. How is the cryptanalyst to decide which is the correct decryption?

TRANSPOSITION TECHNIQUES:

a) Rail fence

Rail fenceis 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.

For example, to encipher the message “meet me after the toga party” with a rail fence of depth 2, we write the following:

m e m a t r h t g p r y

e t e f e t e o a a t

The encrypted message is

MEMATRHTGPRYETEFETEOAAT

b) Row Transposition Ciphers:

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.

For example,

Key: 4 3 1 2 5 6 7

Plaintext: a t t a c k p o

s t p o n e d

u n t i l t

w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.