USN □□□□□□□□□□

Internal Assesment Test 2 – April. 2018- **Scheme of evaluation and solution**

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Sub: | INFORMATION AND NETWORK SECURITY | | | | Sub Code: | 10IS835 | Branch: | ISE |
| Date: | 19 / 04 / 2018 | Duration: | 90 mins | Max Marks: 50 | Sem / Sec: | 8 (A,B) | | |

**1.** **Consider the following example as plain text "SACK GAUL SPARE NO ONE", Using Vernam Cipher method find the cipher text. ( Note: Consider the alphabet range from 1 to 26)** [10]

To examine the Vernam cipher and its use of modulo, consider the following example, which uses the familiar "SACK GAUL SPARE NO ONE" as plaintext.

In the first step of this encryption process, the letter "S" will be converted into the number 19 (because it is the 19th letter of the alphabet), and the same conversion will be applied to the rest of the letters of the plaintext message, as shown below.

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plain Text: | S | A | C | K | G | A | U | L | S | P | A | R | E | N | O | O | N | E |
| Plain Text Value(A) | 19 | 01 | 03 | 11 | 07 | 01 | 21 | 12 | 19 | 16 | 01 | 18 | 05 | 14 | 15 | 15 | 14 | 05 |
| One-Time Pad text: | F | P | Q | R | N | S | B | I | E | H | T | Z | L | A | C | D | G | J |
| OTP Value(B): | 06 | 16 | 17 | 18 | 14 | 19 | 02 | 09 | 05 | 08 | 20 | 26 | 12 | 01 | 03 | 04 | 07 | 10 |
| Sum of Plaintext : (A+B) | 25 | 17 | 20 | 29 | 21 | 20 | 23 | 21 | 24 | 24 | 21 | 44 | 17 | 15 | 18 | 19 | 21 | 15 |
| After Subtraction: | | | | 3 | | | | | | | | 18 | | | | | | |
| Ciphertext: | Y | Q | P | C | U | T | W | U | X | X | U | R | Q | O | R | S | U | O |

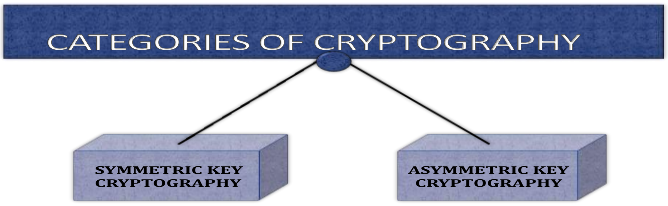
**2 (a)** **What is an cryptography? Discuss the symmetric and asymmetric encryption methods**. [6]

Cryptography: process of making and using codes to secure transmission of information.

Cryptography is the science of secret, or hidden writing.

It has two main Components:

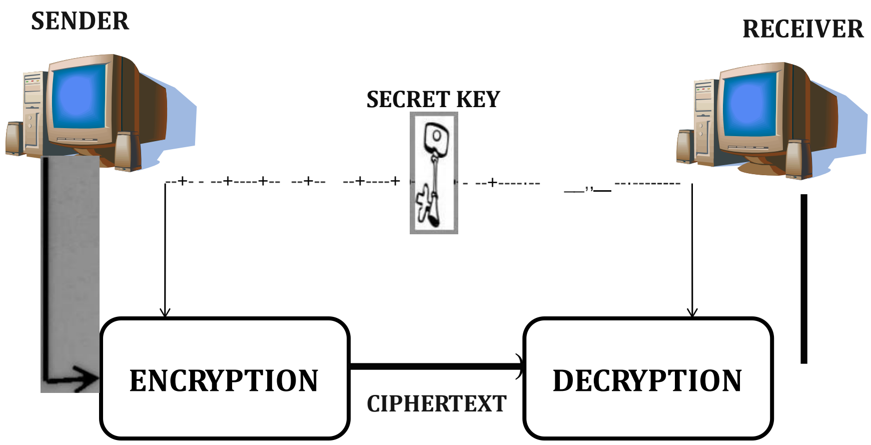
1. **Encryption**
   – Practice of hiding messages so that they can not be read by anyone other than the intended recipient
2. **Authentication & Integrity**
   – Ensuring that users of data/resources are the persons they claim to be and that a message has not been altered


CATEGORIES OF CRYPTOGRAPHY
SYMMETRIC KEY CRYPTOGRAPHY
ASYMMETRIC KEY CRYPTOGRAPHY

**SYMMETRIC KEY CRYPTOGRAPHY**

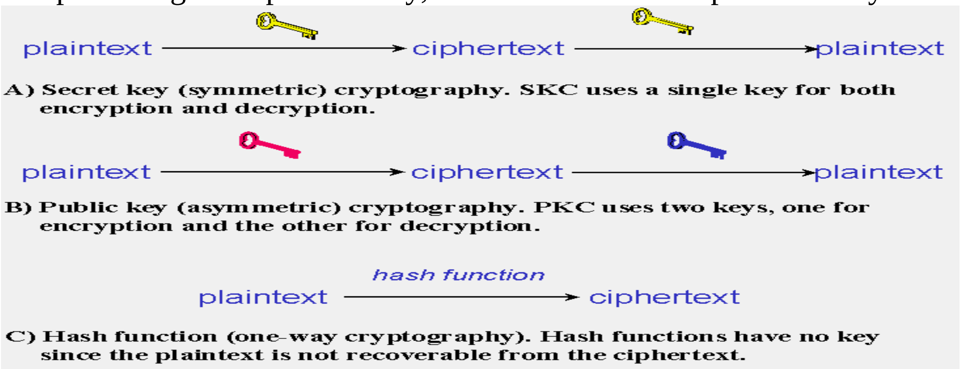
Also known as secret key. Sender & receiver uses same key & an encryption/decryption algorithm to encrypt/decrypt data. i.e. the key is shared. Common symmetric encryption algorithms include Blowfish, Data Encryption Standard (DES), This method works well if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers of people. In addition, there is also the problem of how you communicate the secret key securely.

SYMMETRIC KEY CRYPTOGRAPHY



# ASYMMETRIC KEY CRYPTOGRAPHY

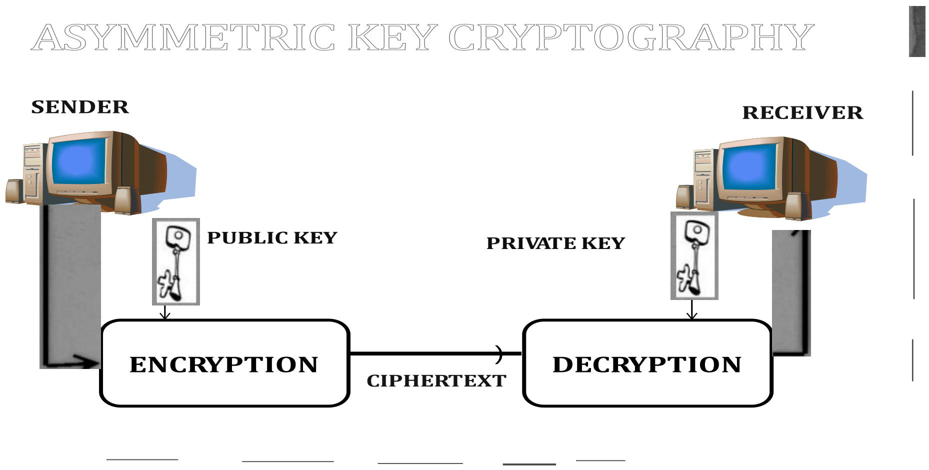
Also known as public key cryptography. Sender & receiver uses different keys for encryption & decryption namely PUBLIC & PRIVATE respectively.
Uses one key for encryption and another for decryption.uses a pair of keys for encryption and decryption The public key can be freely distributed without compromising the private key, which must be kept secret by its owner.



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

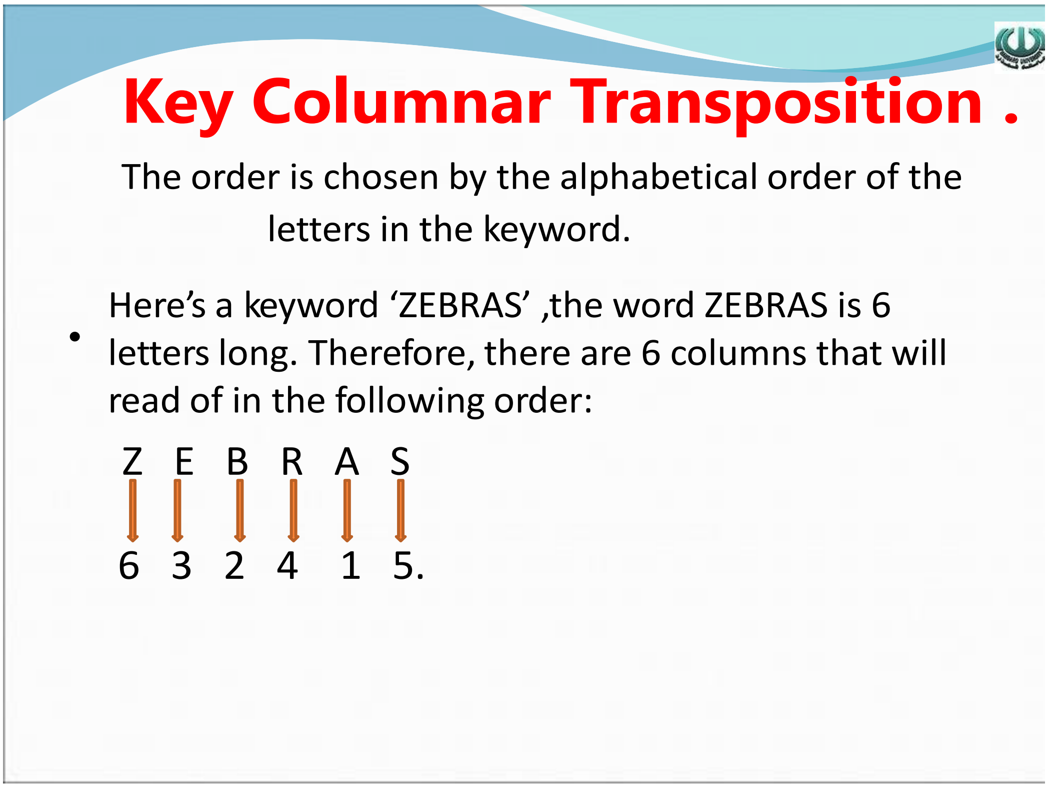
C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.



**(b) Explain the purpose of cryptography.** [4]

- Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C.
- It provides more efficient way of security by encrypting our data.
- It allows the sender and receiver to communicate more securely
- It is used in armies from older ages to modern ages. It allows the armies for exchanging information in the efficient and secured way.

**3 (a)** Suppose we have plain text Plain Text : 'Hamdard University Karachi'. Find cipher text using Key Columnar Transposition method. Consider key as "ZEBRAS".



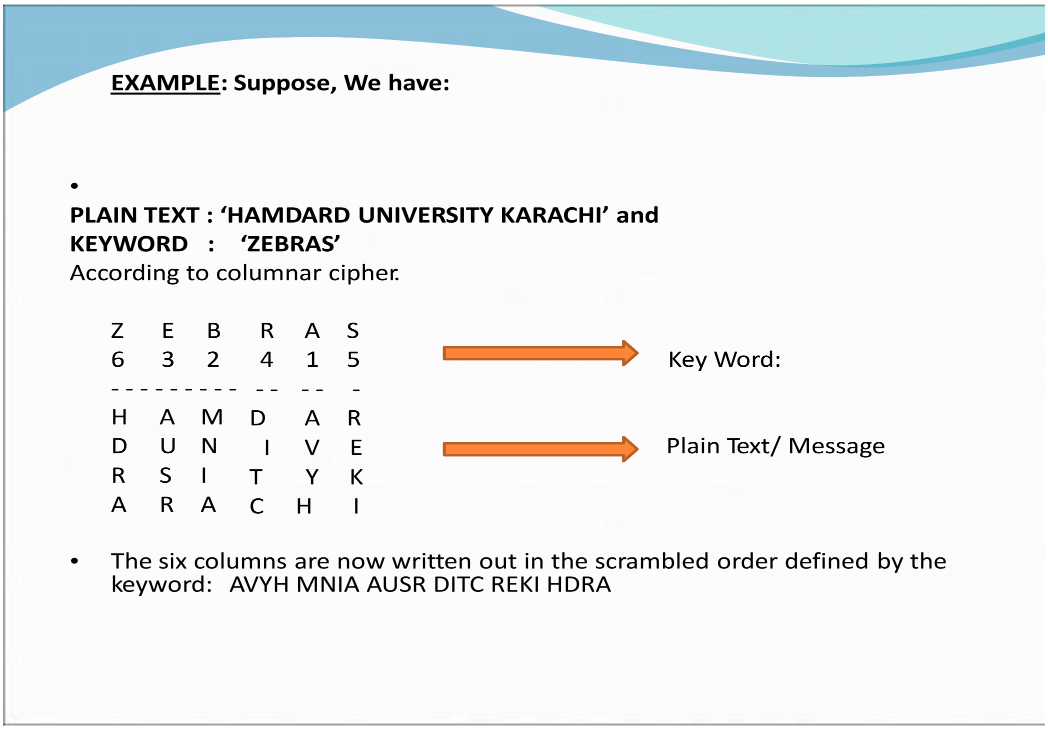
## Key Columnar Transposition .

The order is chosen by the alphabetical order of the letters in the keyword.

- Here's a keyword 'ZEBRAS' ,the word ZEBRAS is 6 letters long. Therefore, there are 6 columns that will read of in the following order:

Z E B R A S

6 3 2 4 1 5.



**EXAMPLE**: Suppose, We have:

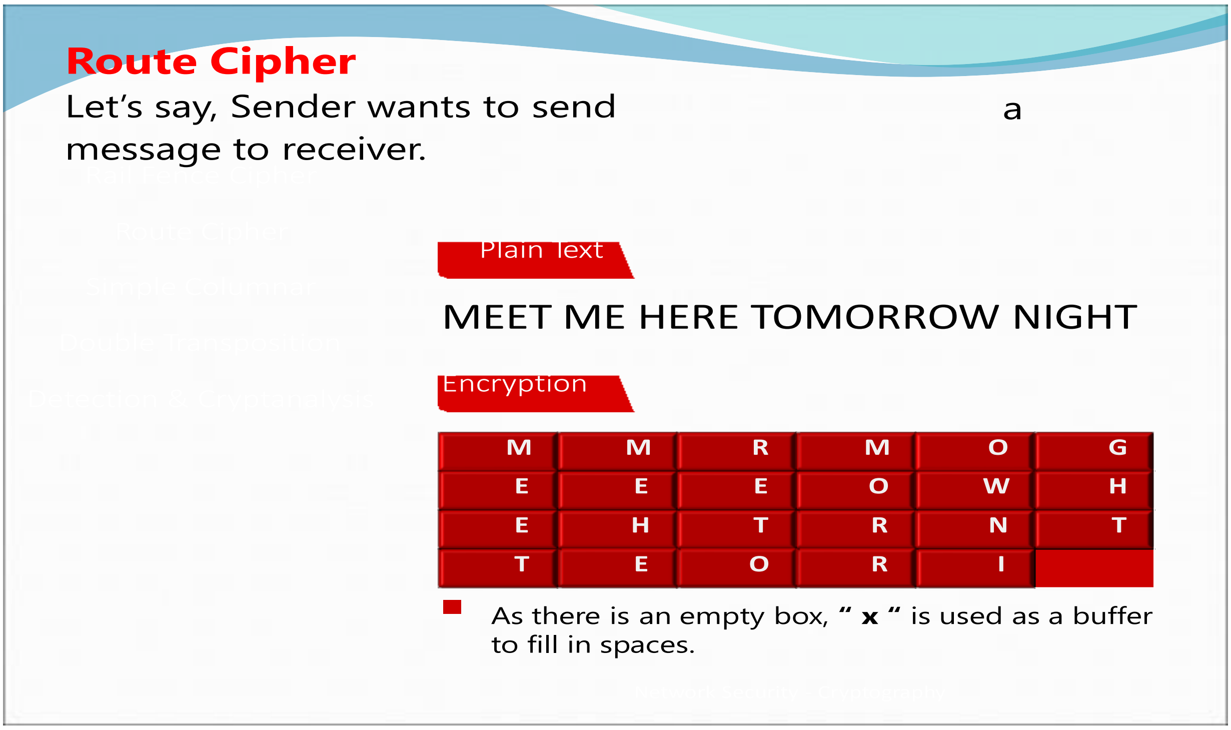
-

**PLAIN TEXT : 'HAMDARD UNIVERSITY KARACHI' and**
**KEYWORD : 'ZEBRAS'**
According to columnar cipher.

| | | | | | | |
|---|---|---|---|---|---|---|
| Z | E | B | R | A | S | |
| 6 | 3 | 2 | 4 | 1 | 5 | Key Word: |
| H | A | M | D | A | R | |
| D | U | N | I | V | E | Plain Text/ Message |
| R | S | I | T | Y | K | |
| A | R | A | C | H | I | |

- The six columns are now written out in the scrambled order defined by the keyword: AVYH MNIA AUSR DITC REKI HDRA

**(b)** Consider the plain text as " MEET ME HERE TOMORROW NIGHT" , find the cipher text using route cipher method.



## Route Cipher

Let's say, Sender wants to send a message to receiver.

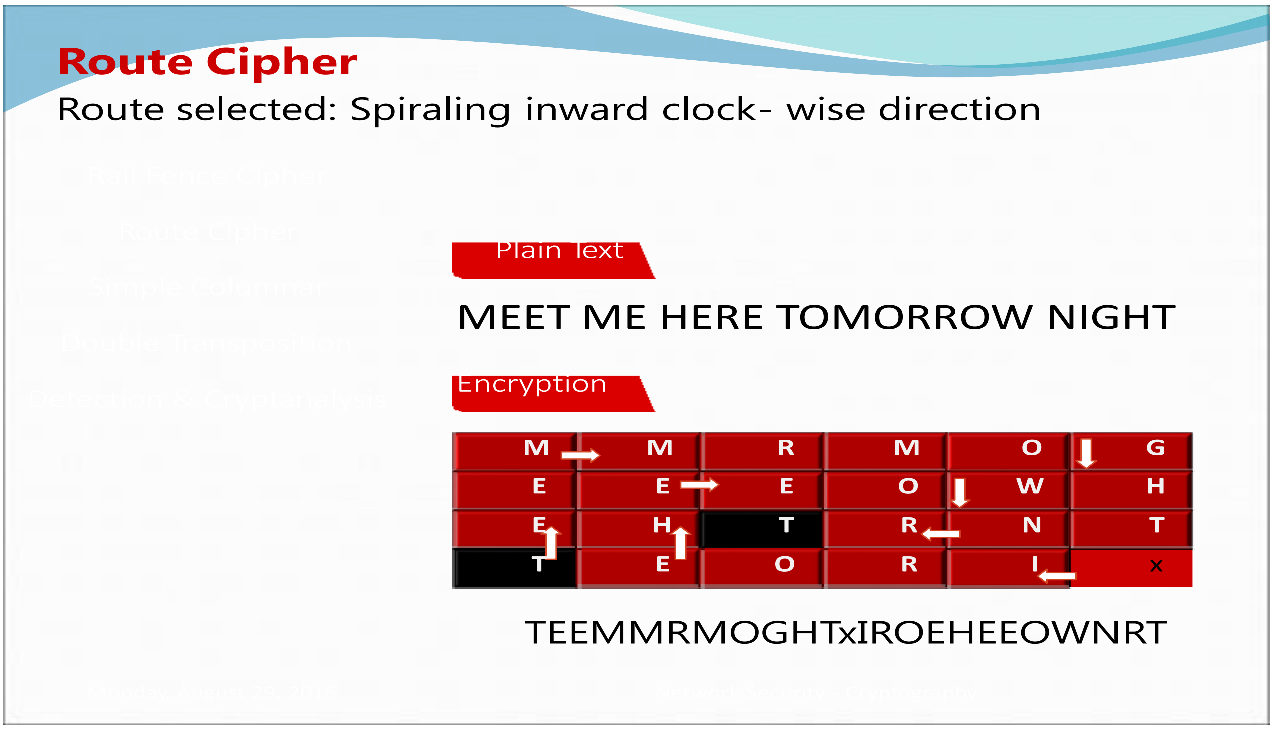
Plain Text

MEET ME HERE TOMORROW NIGHT

Encryption

| | | | | | |
|---|---|---|---|---|---|
| M | M | R | M | O | G |
| E | E | E | O | W | H |
| E | H | T | R | N | T |
| T | E | O | R | I | |

- As there is an empty box, " **x** " is used as a buffer to fill in spaces.



Route Cipher

Route selected: Spiraling inward clock- wise direction

Plain Text

MEET ME HERE TOMORROW NIGHT

Encryption

| | | | | | |
|---|---|---|---|---|---|
| M | M | R | M | O | G |
| E | E | E | O | W | H |
| E | H | T | R | N | T |
| T | E | O | R | I | x |

TEEMMRMOGHTxIROEHEEOWNRT

4. **Describe briefly the various security attacks and specific covered by X.800**

  - Enhance security of data processing systems and information transfers of an organization
  - Intended to counter security attacks
  - Often replicates functions normally associated with physical documents
    - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

- **Security *Service***
  - – A service intended to counter security attacks, typically by implementing one or more mechanisms.
- X.800:

“a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”

- RFC 2828:

“a processing or communication service provided by a system to give a specific kind of protection to system resources”

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication

**1. Authentication** The assurance that the communicating entity is the one it claims to be

- **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.

2. **Access Control**

  - The prevention of unauthorized use of a resource
    - who can have access to a resource,
    - under what conditions access can occur,
    - what those accessing the resource are allowed to do

**3. Data Confidentiality** The protection of data from unauthorized disclosure

- **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.
- **4. Data Integrity-** The assurance that data received are exactly as sent by an authorized entity (i.e., contains no modification, insertion, deletion or replay).
- **Connection Integrity with Recovery:** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
- **Connection Integrity without Recovery:** As above, but provides only detection without recovery.
- **Selective-Field Connection Integrity**: Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
- **Connectionless Integrity:** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
- **Selective-Field Connectionless Integrity:** Provides for the integrity of elected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

**5. Non-Repudiation -** Provides protection against denial by one of the entities involved in a communication of having participated in all/part of the communication.

- **Non repudiation, Origin**: Proof that the message was sent by the specified party.
- **Non repudiation, Destination:** Proof that the message was received by the specified party.

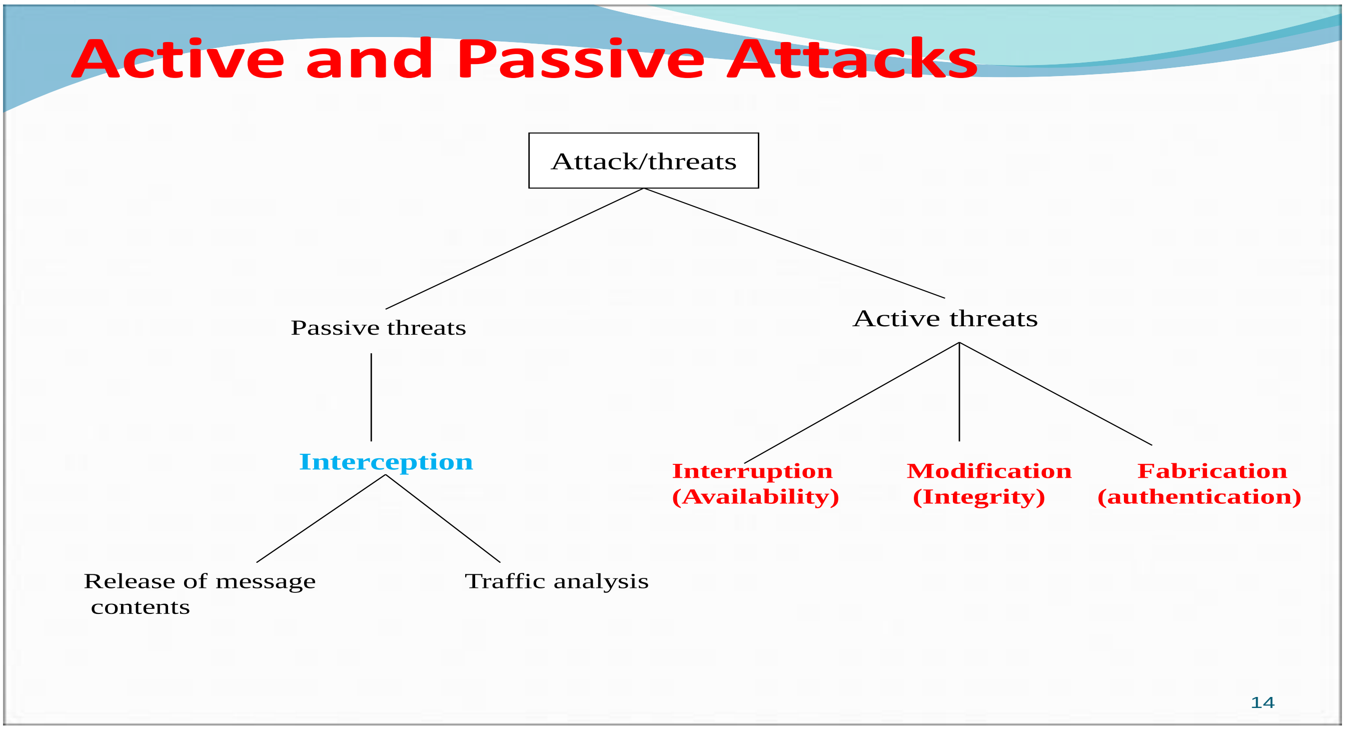
5 . **List differences between Kerberos version 4 and version 5.**

Comparison between Kerberos version 4 and version 5:

| | **Kerberos Version 4** | **Kerberos Version 5** |
|---|---|---|
| Chronology | Kerberos v4 was released prior to the version 5 in the late 1980’s. | The version 5 was published in 1993, years after the appearance of version 5. |
| Key salt algorithm | Uses the principal name partially. | Uses the entire principal name. |
| Encoding | Uses the “receiver-makes-right” encoding system. | Uses the ASN.1 coding system. |
| Ticket support | Satisfactory | Well extended. Facilitates forwarding, renewing and postdating tickets. |

| | | |
|---|---|---|
| Network addresses | Contains only a few IP addresses and other addresses for types of network protocols. | Contains multiple IP addresses and other addresses for types of network protocols. |
| Transitive cross-realm authentication support | No present support for the cause. | Reasonable support present for such authentication. |

6 . **Explain about passive and active attacks with example.**



Active and Passive Attacks

Attack/threats

Passive threats

Interception

Release of message contents

Traffic analysis

Active threats

Interruption (Availability)

Modification (Integrity)

Fabrication (authentication)

14

- **A *Passive attack*** can only observe communications or data. Example: Interception
- **An *Active attack*** can actively modify communications or data

• Often difficult to perform, but very powerful

– Mail forgery/modification

– TCP session hijacking /IP spoofing

Examples: Interruption, Modification ( also called active wiretapping), Fabrication

Types of Active Attacks: masquerade, replay, modification and denial of service.

**Passive Attack**

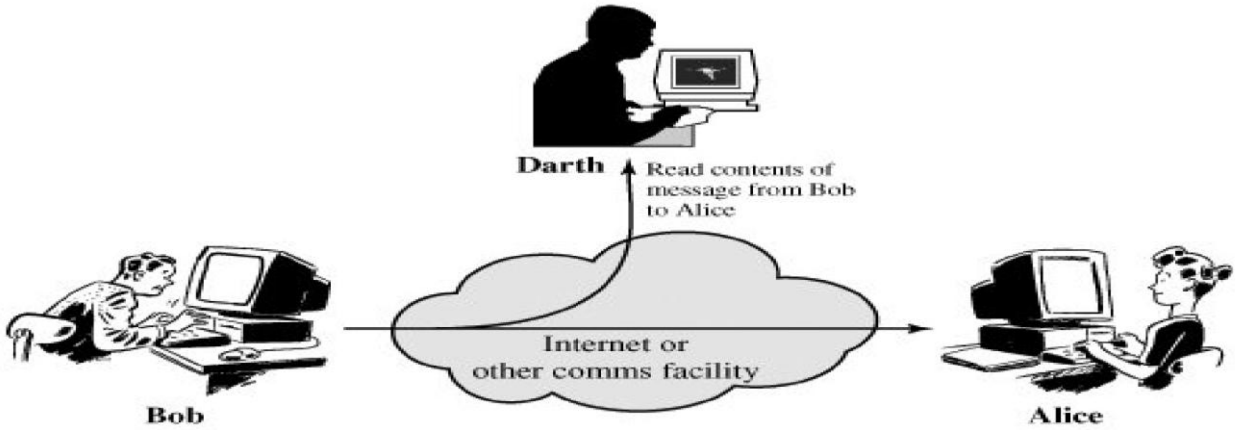
- Attempts to learn or make use of information from the system but does not affect system resources.
- Two types of passive attacks are:

1. Release of message contents
2. Traffic analysis.

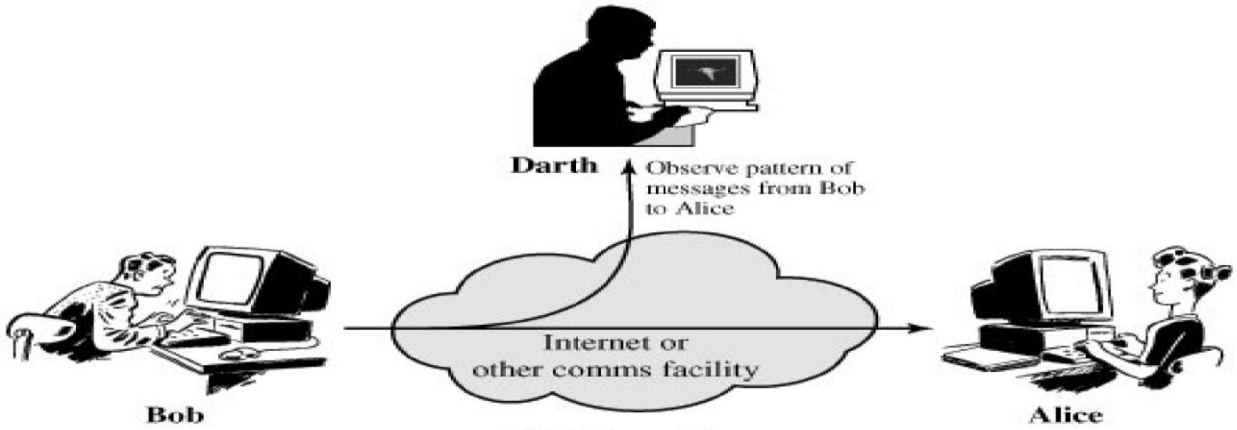
**Release of message contents:** A **telephone conversation**, an **e-mail message** and a **transferred file** may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

**Traffic analysis:** If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the **location** and identity of communication hosts and could observe the **frequency and length of messages** being exchanged. This information might be useful in guessing the nature of communication that was taking place.

- Passive attacks are very difficult to detect because they do not involve any alteration of data.
- However, it is feasible to prevent the success of these attacks.


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

(a) Release of message contents


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

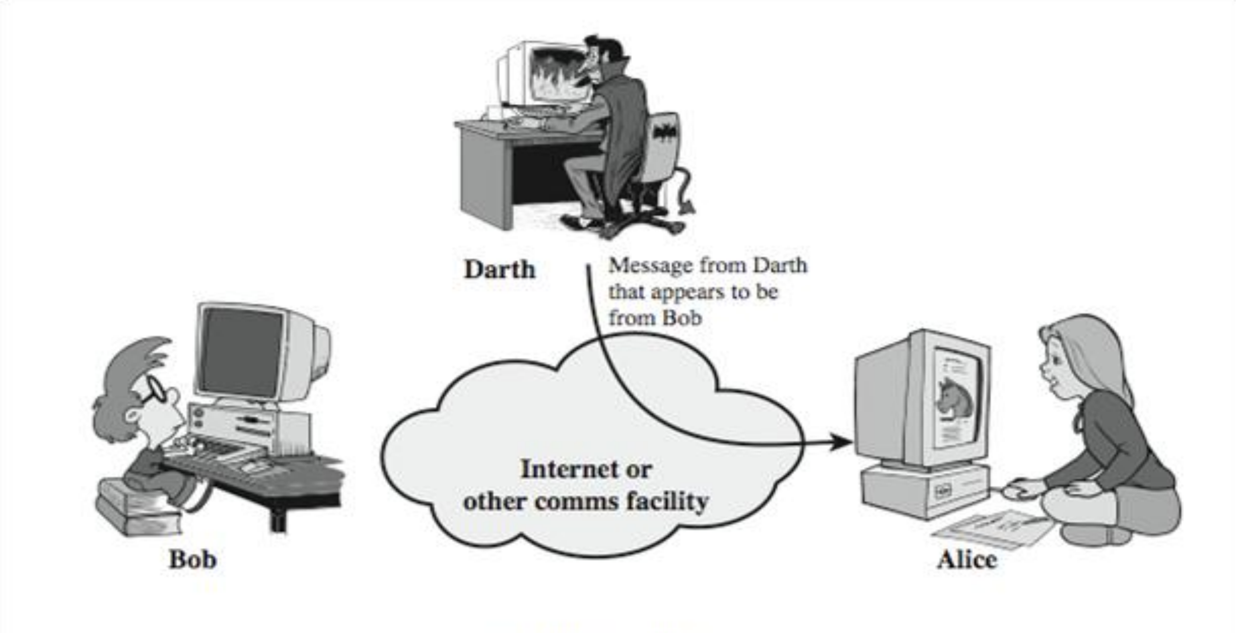
(b) Traffic analysis

**Active Attack**

- Modification of the data stream or the creation of a false stream
- Four types of active attacks
- Masquerade
- Replay
- Modification of messages
- Denial of service.

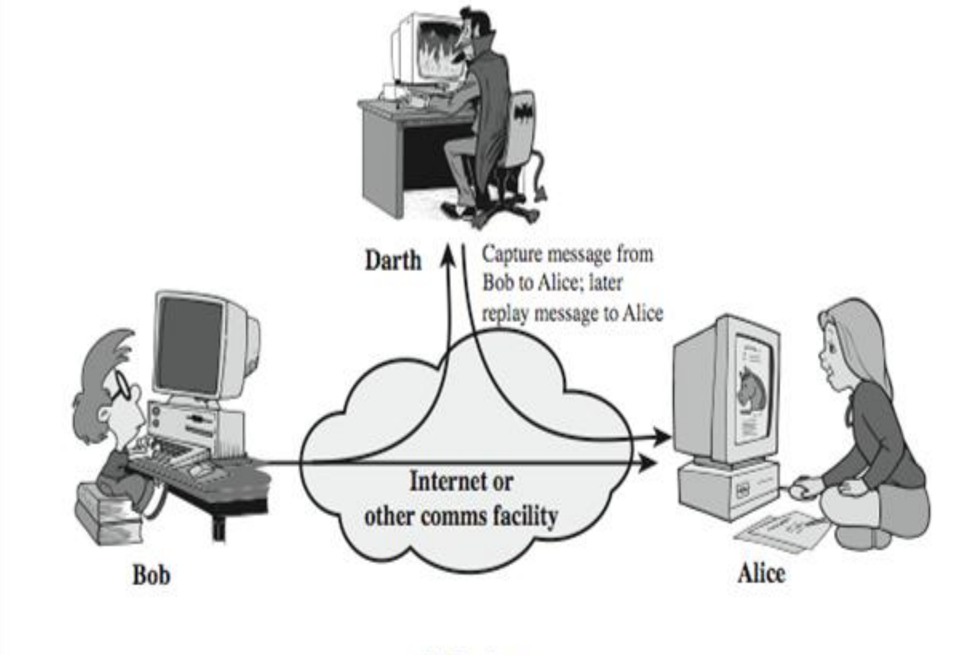
- These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:
- **Masquerade –** One entity pretends to be a different entity.

  Fabrication – attack on authenticity


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

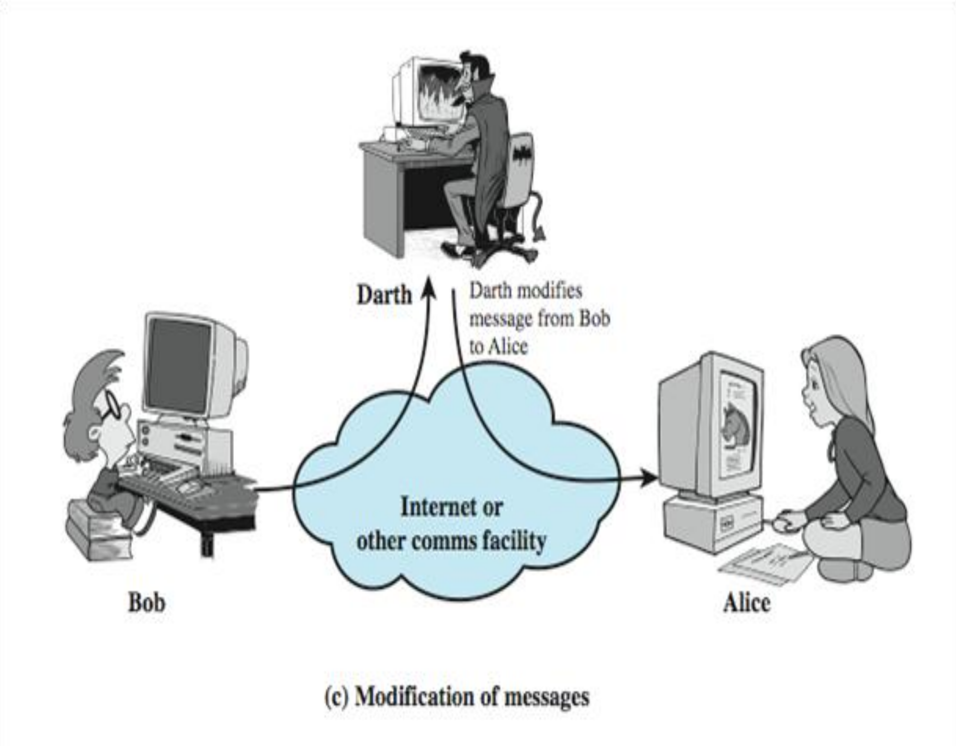
(a) Masquerade

- **Replay** – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.
- Fabrication – attack on authenticity


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

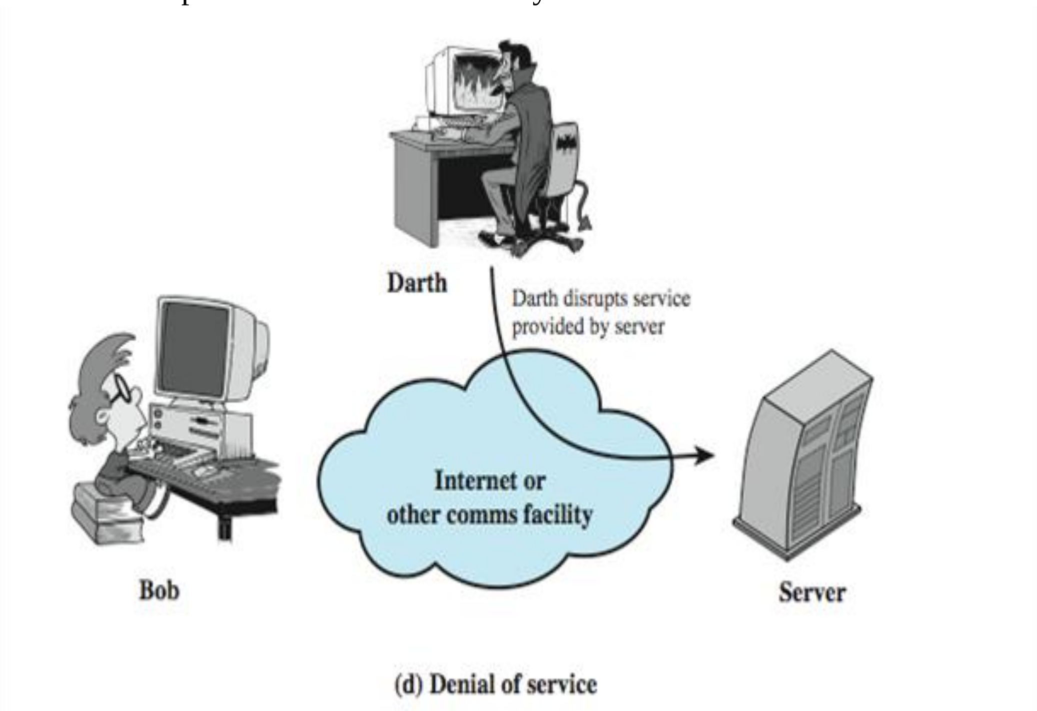
(b) Replay

- **Modification of messages** – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.
- Modification – attack on integrity


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

- **Denial of service** – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.
- Interruption – attack on availability


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

7. **Describe briefly the various specific security mechanism Covered by X.800**

- Feature designed to detect, prevent, or recover from a security attack
- No single mechanism that will support all services required
- **Security *Mechanism***
  - A process / device that is designed to detect, prevent or recover from a security attack.
  - However one particular element underlies many of the security mechanisms in use:

**cryptographic techniques**

- **Specific security mechanisms:**
  - Encipherment, Digital signatures, Access controls, Data integrity, Authentication exchange, Traffic padding, Routing control, Notarization

- **Pervasive security mechanisms:**
- Trusted functionality, Security labels, Event detection, Security audit trails, Security recovery

Incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

- **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 more encryption keys.
- **Digital Signature:** Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.
- **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 to assure certain properties of a data exchange.