University of Salahaddin - Erbil
College of Engineering
Department of Software Engineering

Data Security

Academic year 2021-2022
4th Year Material
Chapter One

Basic Principles in Data Security

Prepared By: Mr. **Zana Farhad Doghramachi, M.Tech(CSE)**
Zana.softeng@gmail.com

About me

- **M.Tech (CSE)** Master of Technology in Computer Science Engineering from IEC College of Engineering & Technology affiliated to Uttar Pradesh Technical University, India, December 2010.

- **B.Sc. (Software Engineering)** Bachelor in Software Engineering from Engineering College, Salahaddin University in Erbil, Iraq, July 2007.

- **Assistant Lecturer** at University of Salahaddin, College of Engineering, Software Engineering Department since December 2010.

Class Rules I

- Students are not allowed to attend class after 15 minutes from it's starting time.
- Students are allowed to leave class at any time during the lecture and they will not be signed as absent, however they will not allowed to return class, unless they have a reasonable excuse.
- Marks will NOT be awarded for attendance, but only for class participation.

Class Rules II

- Students are allowed to come to my office during office hours, which are specified in the time table.
- For further questions or feedback, you can contact me through the following Email: zana.softeng@gmail.com

About the Course

- Syllabus consist of nine chapters, two quiz and four lab works.
- We have two class a week for 2 hours, 2 hour theoretical and 2 hours practical, as it's mentioned in the time table.
- All lectures will be uploaded to the course webpage, which will be available soon.
- The course will be taught in Kurdish; yet students are allowed to ask question in English and Arabic.
- For further details, check Course book.

Introduction

- **Data Security**: Is the means of ensuring that data is kept safe from corruption and unauthorized access. Thus data security helps to ensure privacy. It also helps in protecting personal data. Data security is part of the larger practice of Information security.

- **Cryptology**: This is the study of techniques for ensuring the secrecy and/or authenticity of information. The two main branches of cryptology are ***cryptography***, which is the study of the design of such techniques; and ***cryptanalysis***, which deals with the defeating such techniques, to recover information, or forging information that will be accepted as authentic.

Basic Principles of IS I

- Three basic security concepts important to information are ***confidentiality***, ***integrity***, and ***availability***. Concepts relating to the people who use that information are authentication, authorization, and no repudiation.

Availability

- **Availability**: Requires that computer systems assets be available to authorized parties when needed.
- **Interruption**: An asset of the system is destroyed or becomes unavailable or unusable, This is an attack on availability.
- Information when become inaccessible, resulting in ***loss of availability***. This means that people who are authorized to get information cannot get what they need.

Confidentiality

- **Confidentiality**: Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. This type of access includes printing, displaying.

- **Interception**: An unauthorized party gains access to an asset. This is an attack on Confidentiality. The unauthorized party could be a person, a program, or a computer.

- Example, when information is read or copied by someone not authorized to do so, the result is known as ***loss of confidentiality***.

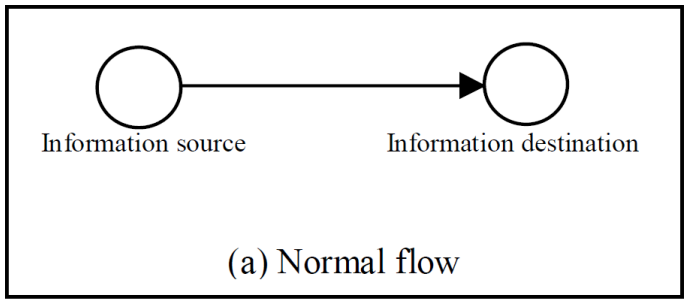
Integrity

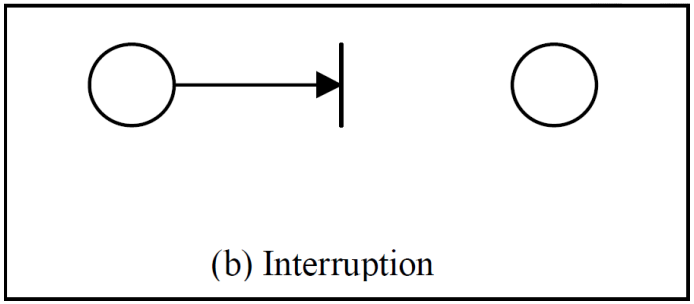
- **Integrity:** Ensures that only authorized parties are able to modify computer systems assets and transmitted information. Modification includes writing, changing, changing status, deleting, creating and delaying or replaying of transmitted messages.

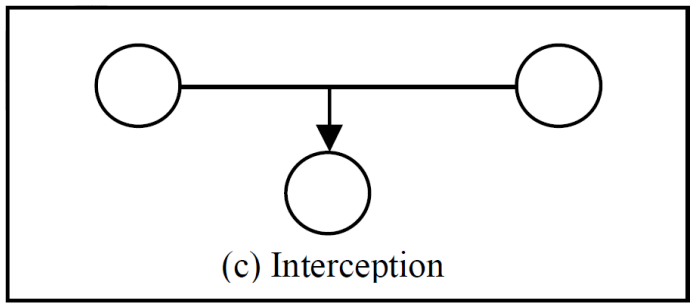
- **Modification**: An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity.

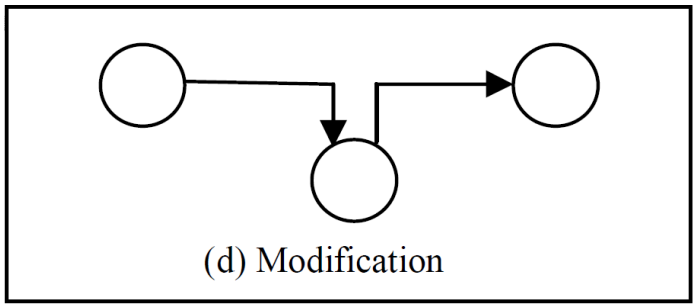
- When information is modified in unexpected ways, the result is known as ***loss of integrity***. This means that unauthorized changes are made to information.

Basic Principles of IS II









Key Points I

- The ***OSI*** (open systems interconnection) security architecture provides a systematic framework for defining ***security attacks, mechanisms,*** and ***services***.

- **Security attacks**: are classified as either passive attacks, which include unauthorized reading of a message of file and traffic analysis; and active attacks, such as modification of messages or files, and denial of service.

Key Points II

- **Security mechanism**: is any process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Examples of mechanisms are encryption algorithms, digital signatures, and authentication protocols.

- **Security services**: include authentication, access control, data confidentiality, data integrity, nonrepudiation, and availability.

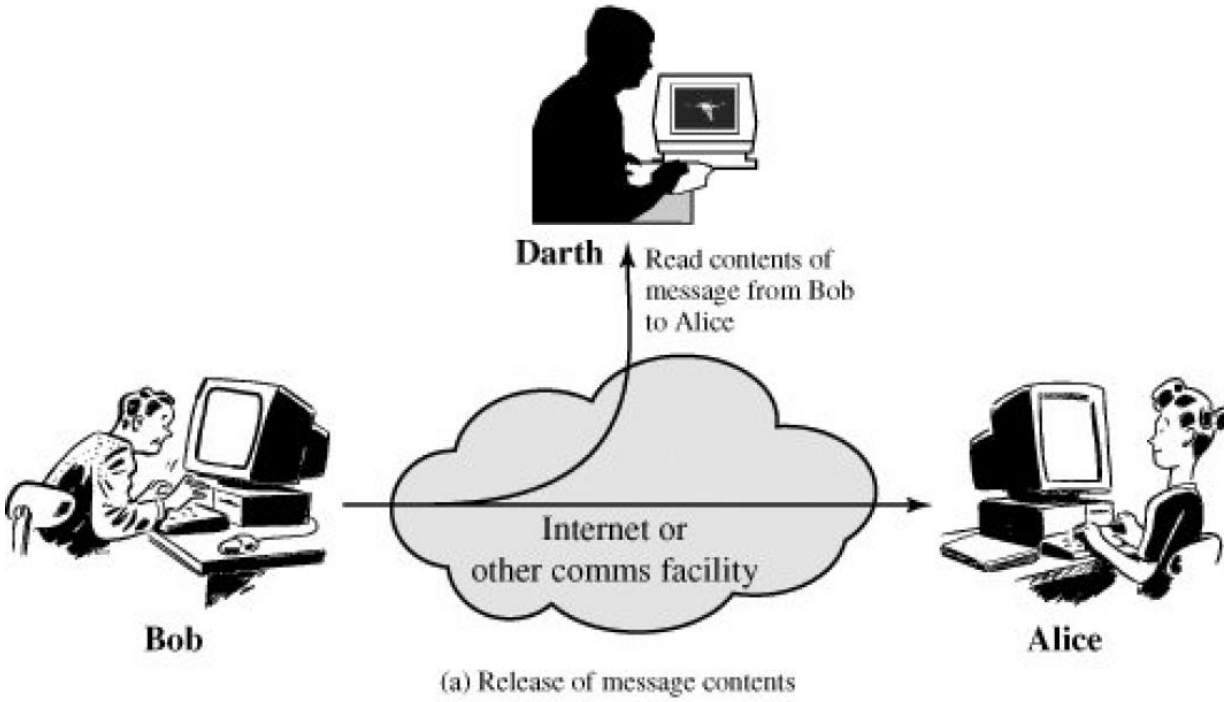
Passive attacks I

- 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 ***release of message contents*** and ***traffic analysis***.

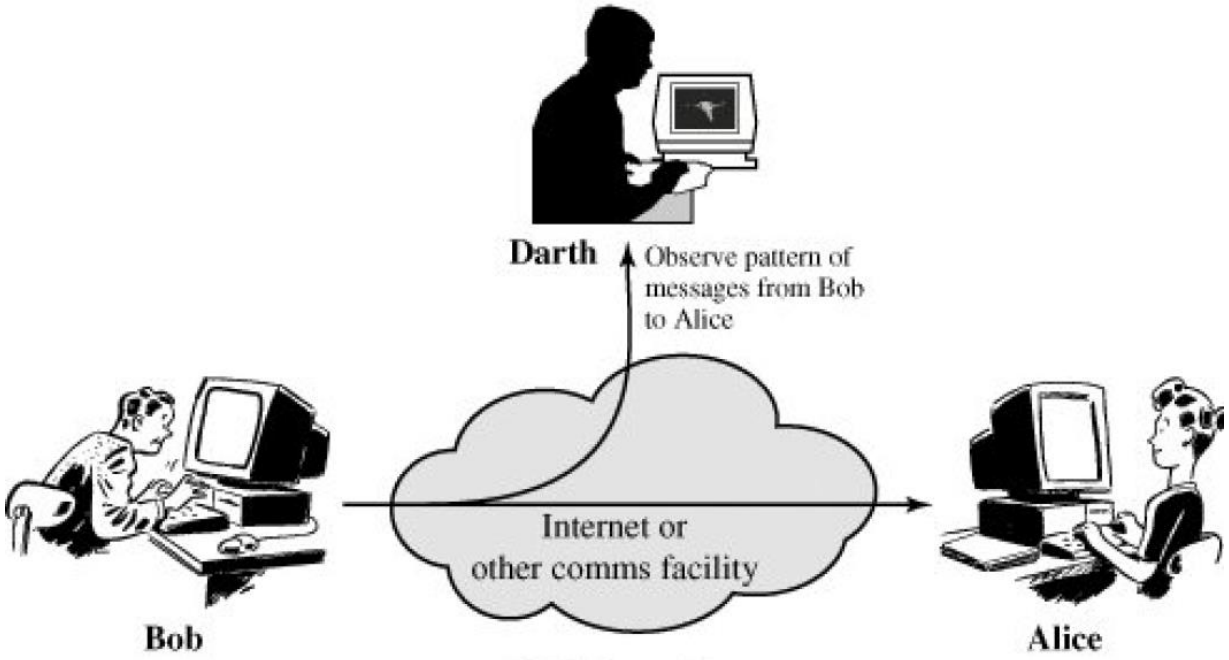
- The ***release of message contents*** is easily understood, A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

Passive attacks II

- Second type of passive attack, ***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.



(a) Release of message contents



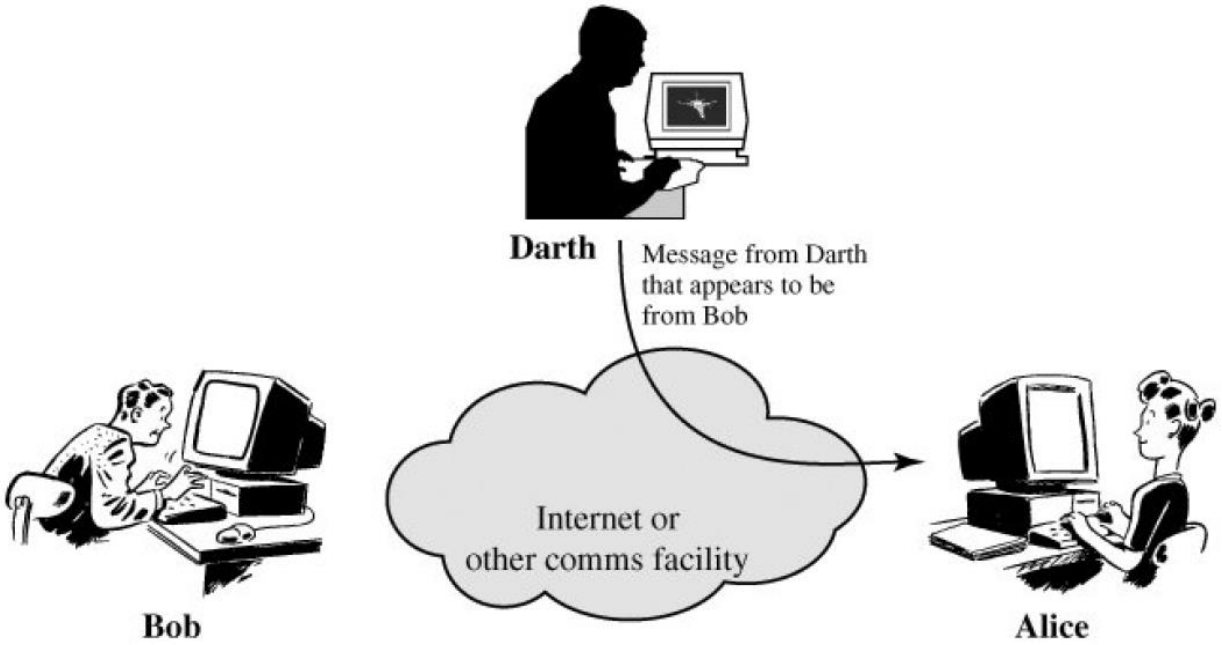
(b) Traffic analysis

Active attacks I

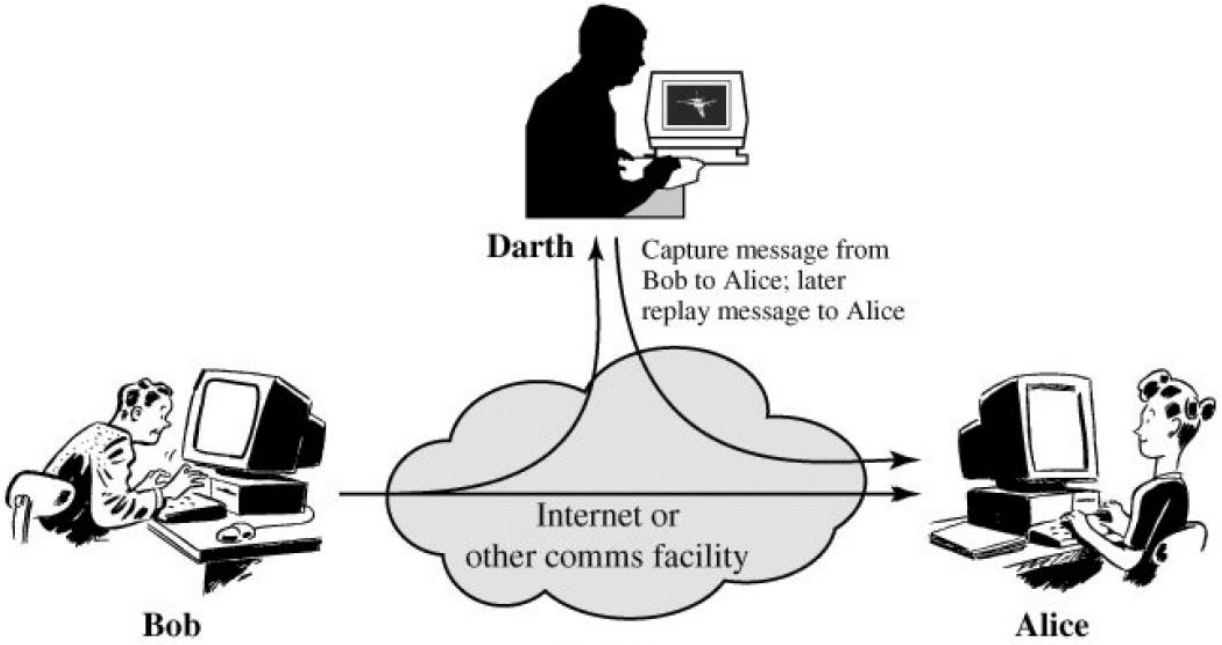
- Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: ***masquerade***, ***replay***, ***modification of messages***, and ***denial of service***.

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

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



(a) Masquerade

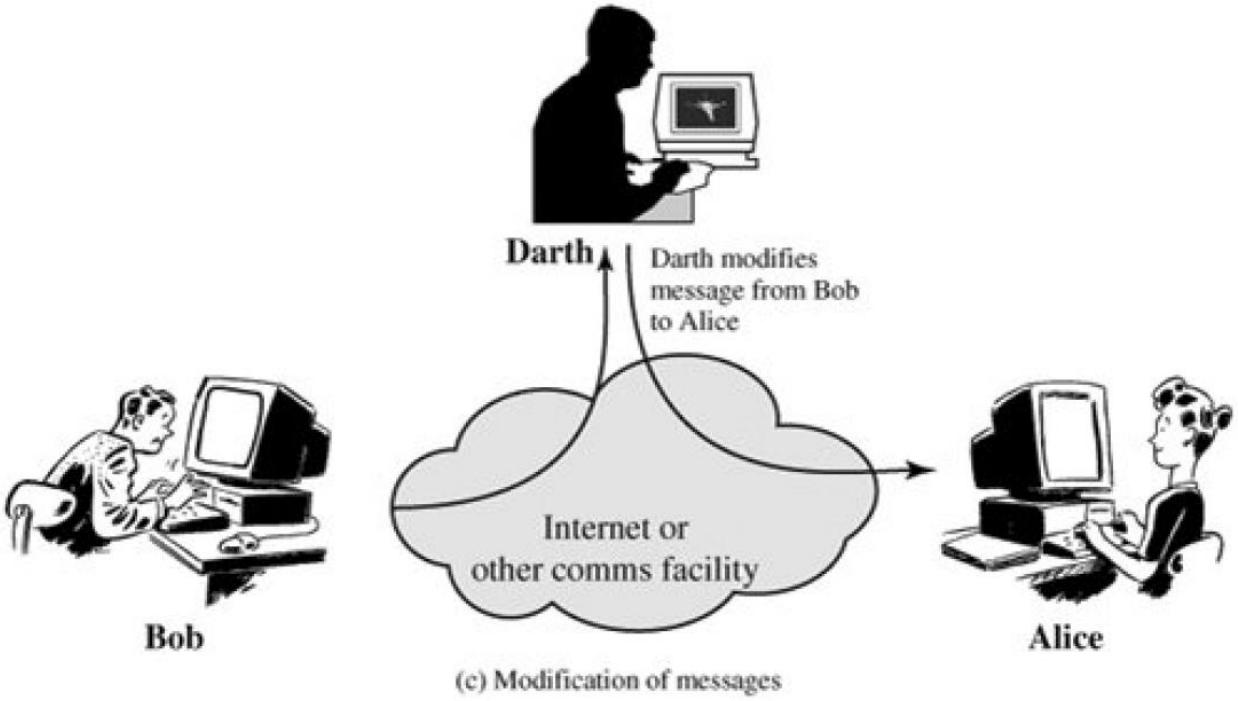


(b) Replay

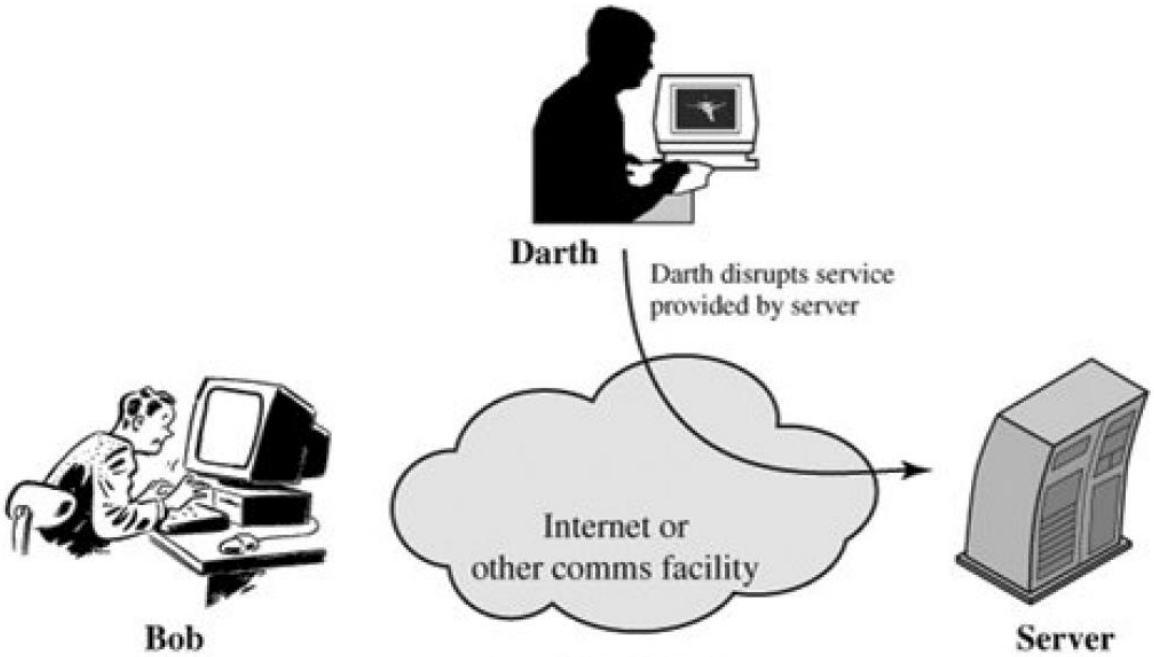
Active attacks II

- ***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 " let's meet today" is modified to mean " let's meet tomorrow”.

- The ***denial of service*** prevents or inhibits the normal use or management of communications facilities.



(c) Modification of messages



(d) Denial of service

Security Mechanisms

- Are implemented to protect data against security attacks. These mechanisms will be covered in the appropriate places in the next lectures and so we do not elaborate now.

- Examples of mechanisms are *encryption algorithms*, *digital signatures*, and *authentication protocols*.

Security Services I

- A service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

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

Security Services II

- **Access control:** is the ability to limit and control the access to host systems and application via communication links.

- **Authentication***:* is proving that a user is the person he or she claims to be. That proof may involve something the user knows (such as a password), something the user has (such as a “smartcard”), or something about the user that proves the person’s identity (such as a fingerprint).

Other terms in IS I

- **Authorization**: is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program.

- **Encryption**: The conversion of plaintext or data into unintelligible form by means of a reversible translation, based on a translation table or algorithm. Also called enciphering.

- **Decryption**: The translation of encrypted text or data (called ciphertext) into original text or data (called plaintext). Also called deciphering.

Other terms in IS II

- **Plaintext:** The input to an encryption function or the output of a decryption function.

- **Cipher**: An algorithm for encryption and decryption. A cipher replaces a piece of information (an element in plaintext) with another object, with the intent to conceal meaning. Typically, the replacement rule is governed by a secret key.

- **Ciphertext**: The output of an encryption algorithm; the encrypted form of a message or data.

Other terms in IS III

- **Asymmetric encryption**: A form of cryptosystem in which encryption and decryption are performed using two different keys, one of which is referred to as the public key and one of which is referred to as the private key. Also known as public key encryption.

- **Symmetric encryption**: A form of cryptosystem in which encryption and decryption are performed using the same key. Also known as conventional encryption.

Other terms in IS III

- **Public key**: One of the two keys used in an asymmetric encryption system. The public key is made public, to be used in conjunction with a corresponding private key.

- **Private key**: One of the two keys used in an asymmetric encryption system. For secure communication, the private key should only be known to its creator.

- **Session key**: A temporary encryption key used between two principals.

Homework

Q1: What are basic types of cryptanalysis attack?

Q2: What are common methods that can be used in ciphertext only attack?