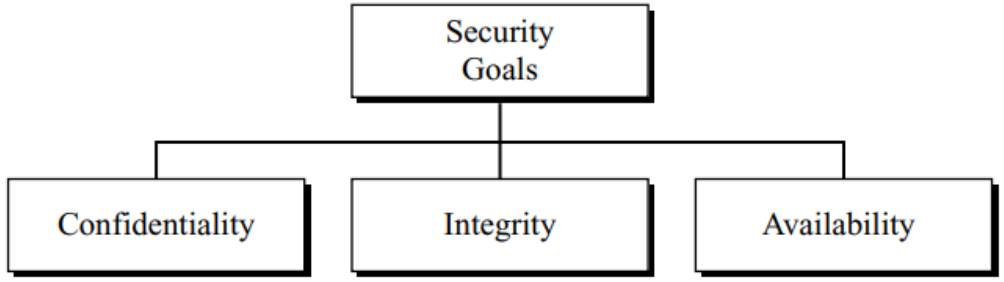
Cryptography and Network Security

Cryptography Overview and Terminologies

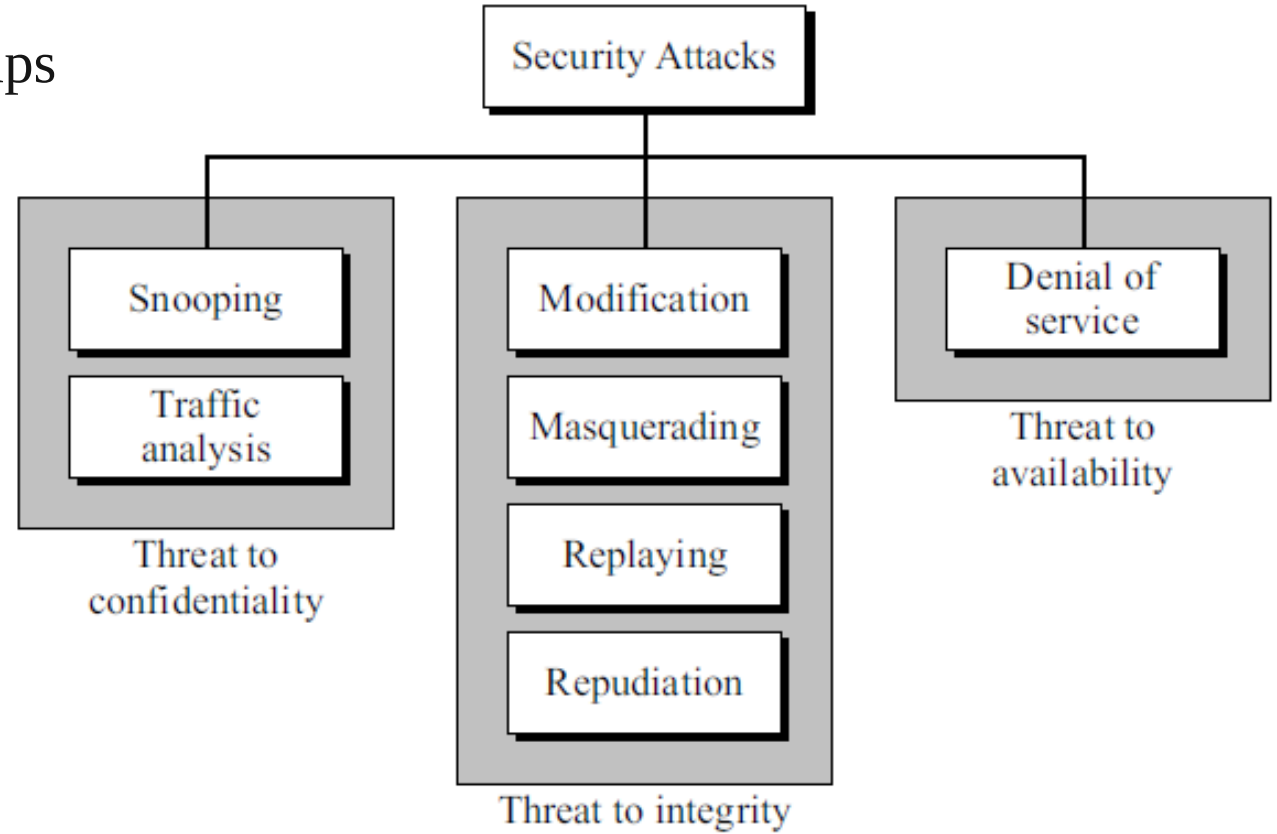
Security Goals

- Confidentiality:
  - Protect information against any malicious attacks
  - Conceal information during transmission too.
- Integrity:
  - Changes of information need to be done only by authorized entities.
- Availability:
  - Information needs to be available to authorized entities.



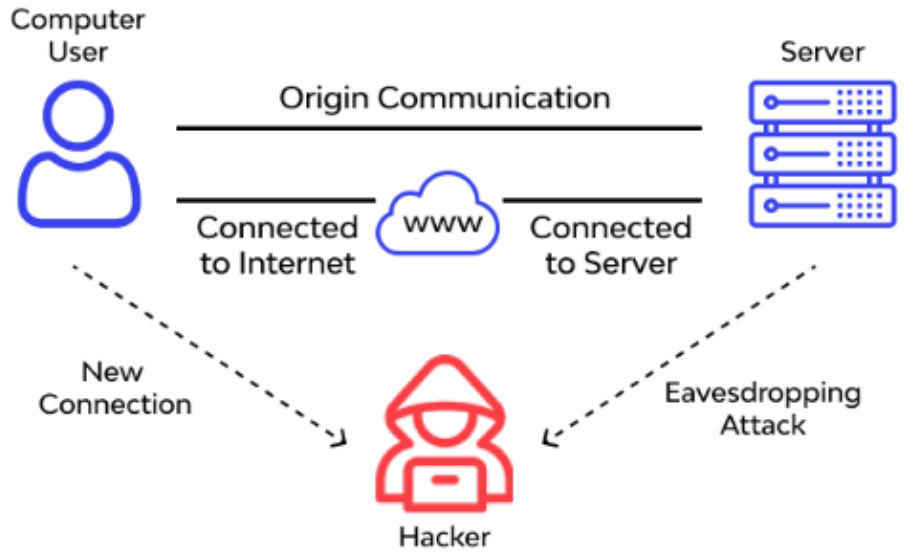
Security Attacks

- Our three goals of security – confidentiality, integrity, and availability – can be threatened by security attacks.
- All categories are divided |into three groups related to the security goals.



Attacks Threatening Confidentiality

- **Snooping** –
  - refers to unauthorized access to or interception of data.
  - An unauthorized entity may intercept the transmission of files using any program or utility that performs a monitoring function.
  - To prevent snooping, the data can be made nonintelligible to the intercepter by using encipherment techniques.



Attacks Threatening Confidentiality

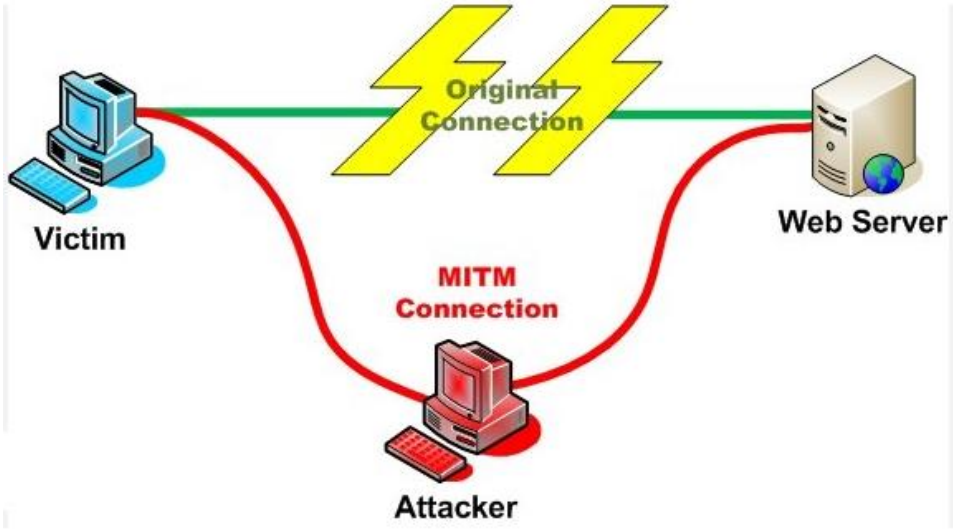
- **Traffic Analysis** –
  - Although encipherment of data may make it nonintelligible for the intercepter, he can obtain some other type information by monitoring online traffic.
  - For example, he can find the electronic address (such as the e-mail address) of the sender or the receiver.
  - He can collect pairs of requests and responses to help him guess the nature of transaction.

Attacks Threatening Integrity

- **Modification** –
  - After intercepting or accessing information, the attacker modifies the information to make it beneficial to himself.
  - For example, a customer sends a message to a bank to do some transaction. The attacker intercepts the message and changes the type of transaction to benefit himself.
  - Note that sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.

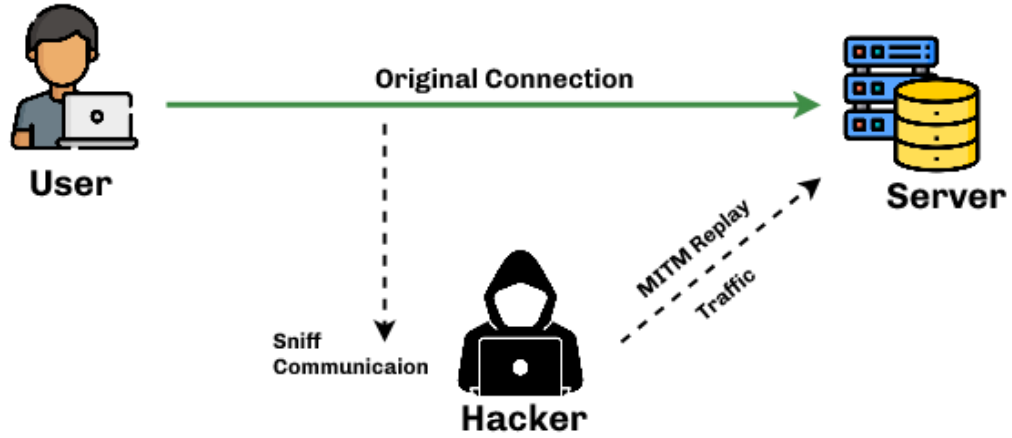
Attacks Threatening Integrity

- **Masquerading** –
  - Masquerading, or spoofing, happens when the attacker impersonates somebody else.
  - For example, an attacker might steal the bank card and PIN of a bank customer and pretend that he is that customer.
  - Sometimes the attacker pretends instead to be the receiver entity. For example, a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.



Attacks Threatening Integrity

- **Replaying** –
  - The attacker obtains a copy of a message sent by a user and later tries to replay it.
  - For example, a person sends a request to his bank to ask for payment to the attacker, who has done a job for him. The attacker intercepts the message and sends it again to receive another payment from the bank.



Attacks Threatening Integrity

- **Repudiation** –
  - This type of attack is different from others because it is performed by one of the two parties in the communication: the sender or the receiver.
  - The sender of the message might later deny that he has sent the message; the receiver of the message might later deny that he has received the message.
  - For example, denial by the sender would be a bank customer asking his bank to send some money to a third party but later denying that he has made such a request.
  - An example of denial by the receiver could occur when a person buys a product from a manufacturer and pays for it electronically, but the manufacturer later denies having received the payment and asks to be paid.

Attacks Threatening Availability

- **Denial of Service –**
  - Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.
  - The attacker can use several strategies to achieve this. He might send so many bogus requests to a server that the server crashes because of the heavy load.
  - The attacker might intercept and delete a server's response to a client, making the client to believe that the server is not responding.
  - The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system.

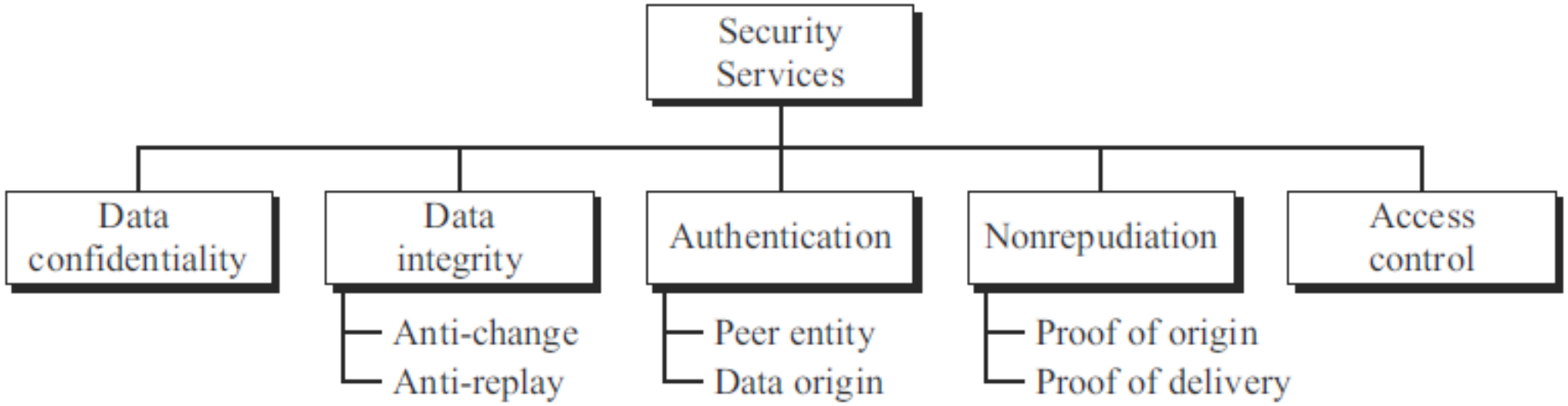
Passive Versus Active Attacks

- In a passive attack, the attacker's goal is just to obtain information.
- An active attack may change the data or harm the system.

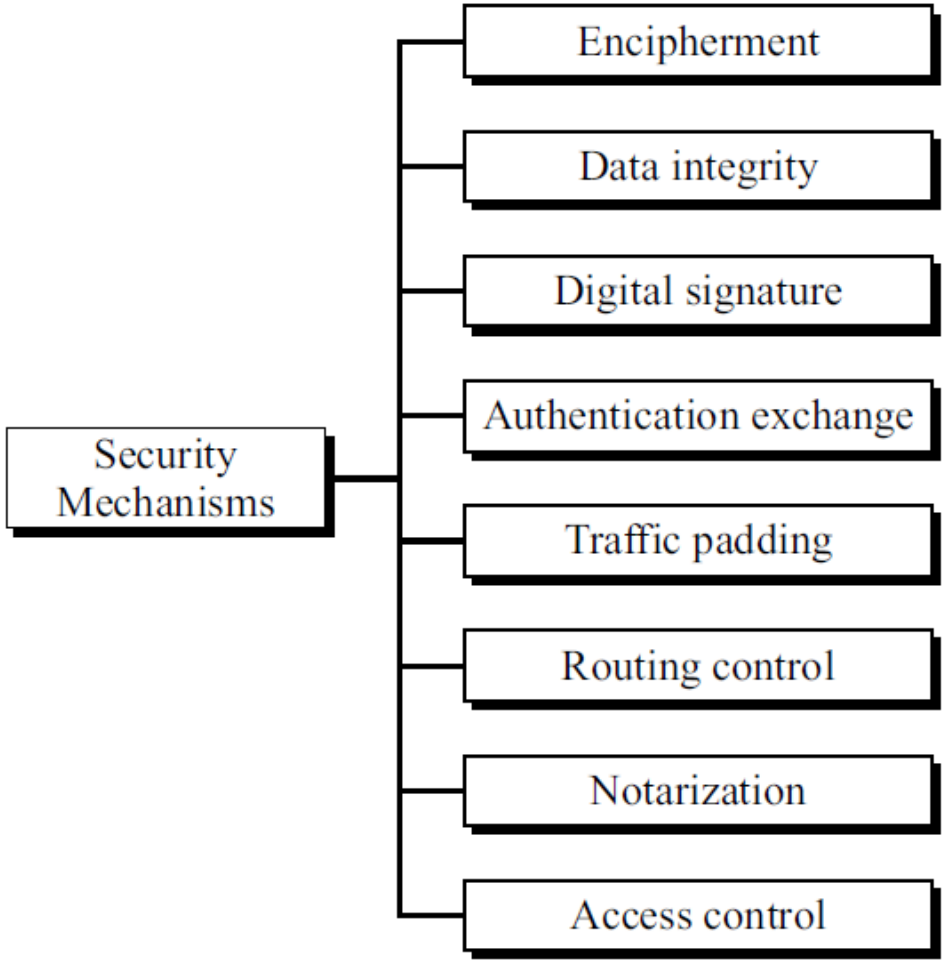
Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Security Services

- Five services have been designed to prevent the security attacks that we have mentioned.



Security Mechanisms



Security Mechanisms

- **Encipherment** – hiding or covering data, can provide confidentiality. Today two techniques – cryptography and steganography – are used for enciphering.
- **Data integrity** – appends to the data a short checkvalue. The receiver receives the data and the checkvalue. He creates a new checkvalue from the received data and compares the newly created checkvalue with the one received. If the two checkvalues are the same, the integrity of data has been preserved.
- **Digital signature** – the sender can electronically sign the data and the receiver can electronically verify the signature. The sender uses a private key and a public key. The receiver uses the sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.

Security Mechanisms

- **Authentication exchange** – two entities exchange some messages to prove their identity to each other. For example, one entity can prove that he knows a secret that only he is supposed to know.
- **Traffic padding** – inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.
- **Routing control** – selecting and continuously changing different available routes between the sender and the receiver.
- **Notarization** – selecting a third trusted party to control the communication between two entities. This can be done, for example, to prevent repudiation.
- **Access control** – uses methods to prove that a user has access right to the data or resources owned by a system. Examples of proofs are passwords and PINs.

Relation between security services and security mechanisms

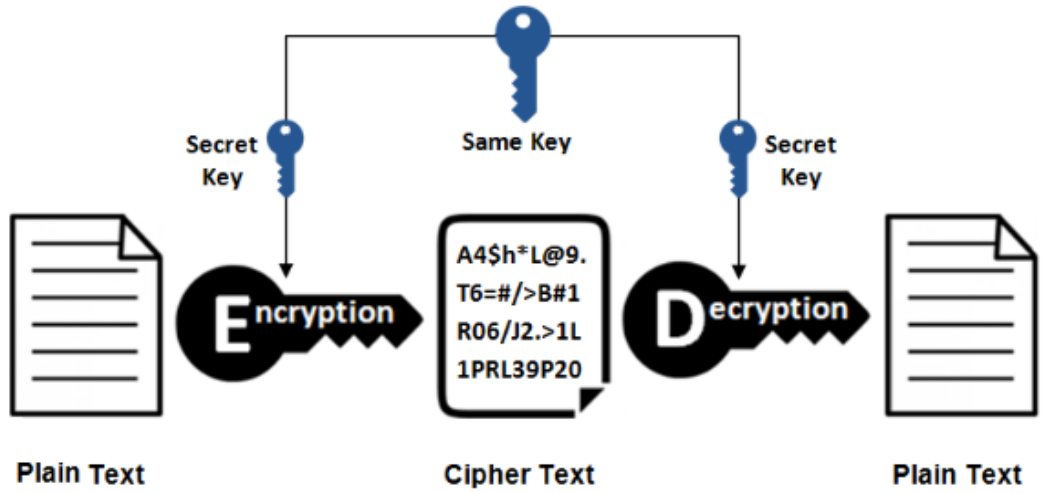
Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

TECHNIQUES: Cryptography

- Cryptography, a word with Greek origins, means “secret writing.”
- It is the science and art of transforming messages to make them secure and immune to attacks.
- In the past cryptography referred only to the encryption and decryption of messages using secret keys.
- At present it is defined as involving three distinct mechanisms: symmetric-key encipherment, asymmetric-key encipherment, and hashing.

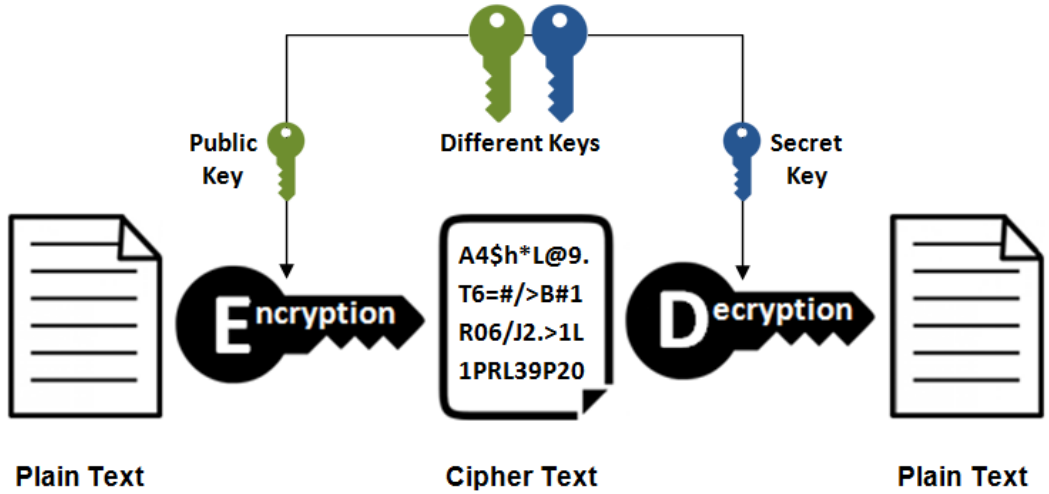
TECHNIQUES: Cryptography

- **Symmetric-Key Encipherment** –
  - Symmetric-key encipherment uses a single secret key for both encryption and decryption.
  - Encryption/decryption can be thought of as electronic locking.
  - In symmetric-key enciphering, a person puts the message in a box and locks the box using the shared secret key; another person unlocks the box with the same key and takes out the message.



TECHNIQUES: Cryptography

- **Asymmetric-Key Encipherment** –
  - We have the same situation as the symmetric-key encipherment, with a few exceptions.
  - First, there are two keys instead of one: one **public key** and one **private key**.
  - To send a secured message to person 2, person 1 first encrypts the message using person 2's public key. To decrypt the message, person 2 uses his own private key.



TECHNIQUES: Cryptography

- **Hashing** –
  - a fixed-length message digest is created out of a variable-length message.
  - The digest is normally much smaller than the message.
  - To be useful, both the message and the digest must be sent. Hashing is used to create checkvalues to provide data integrity.

TECHNIQUES: Steganography

- The word steganography, with origin in Greek, means “covered writing,”.
- Steganography means concealing the message itself by covering it with something else.
- Today, any form of data, such as text, image, audio, or video, can be digitized, and it is possible to insert secret binary information into the data during digitization process.

TECHNIQUES: Steganography

- **Text Cover –**
  - The cover of secret data can be text.
  - For example, we can use single space between words to represent the binary digit 0 and double space to represent binary digit 1.
  - The following short message hides the 8-bit binary representation of the letter A in ASCII code (01000001).

This book is mostly about cryptography, not steganography.

□ □□□ □ □ □ □□

0 1 0 0 0 0 1

TECHNIQUES: Steganography

- **Image Cover –**
  - Secret data can also be covered under a color image.
  - We have 2^8 different shades of each color.
  - In a method called LSB (least significant bit), the least significant bit of each byte is set to zero. This may make the image a little bit lighter in some areas, but this is not normally noticed.
  - We can hide a binary data in the image by keeping or changing the least significant bit.

```
01010011  10111100  01010101
01011110  10111100  01100101
01111110  01001010  00010101
```