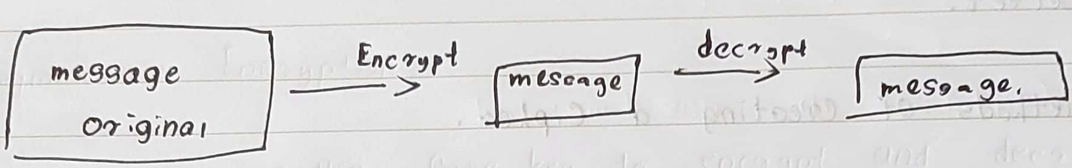
Date No

Cryptography (ICS) - Lec 01

- Cryptography meaning Converting am message to a Unrecdable format is Called Crypto graphy.

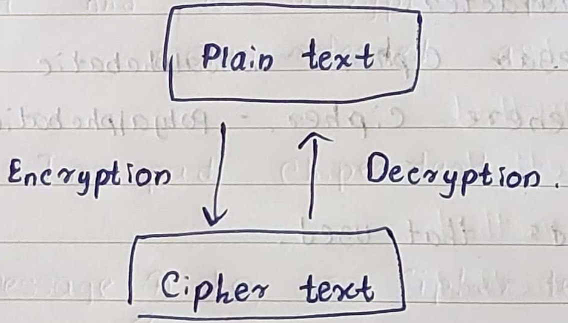


Services can be archeived by Cryptography.

- Authentication
- Integrity
- Confidentiality

original message - clear text , plain text

Encrypted message - Cipher text.



- We need encryption algorithem to Convert a plaint text to cipher text.
- We need decryption algorithem to Convert a ~~p~~ Cipher text to plain text.

Date No

- Combination of E.A and D.A is Called as Cipher.

each E.A and D.A has a key. Should keep it Secret.

Methods of creating a Cipher.

- Transposition
- Substitution.
- One-time pad. - later will learn

- Transposition cipher text.

  - no letteres are replaced. only rearrenged. (spell it backward).

  Eg : DES , 3DES

- Substitution cipher text.

  - Plane text characters are being replaced With another character.

  Eg : Caesar cipher - monoalphabatic
  Vigenere cipher. - polyalphobatic.

Variouse cipher methods that used.

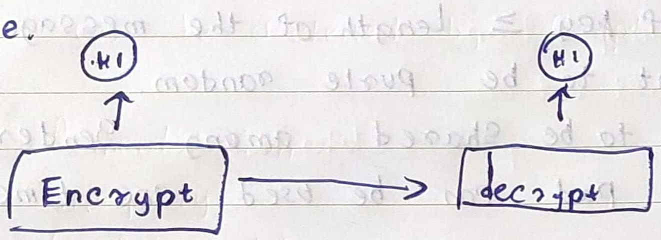
Scytale
Caesar Cipher
Vigenere cipher
Jefferson's encryption device

Encryption algorithms.

- Symmetric Encryption algorithms.
- Asymmetric Encryption algorithms.

◦ Symmetric Encryption.

◦ use same key to encrypt and decript the message.



◦ also known as shared key algorithms

◦ Asymmetric Encryption.

◦ here use a two different keys to Encrypt And to decrypt. (privat, public key)

◦ also referred as public key Cryptography.

◦ One-Time pad Chiper text.

message ⊕ key = Cipher tex
↑
XOR

Message → 1 1 1 0 0

key → 0 1 1 1 0 → encryption.

Cipher → 1 0 0 1 0

~~Enc~~ decryption

$$\left.\begin{array}{ll} \text{key} \to & 0\quad 1\quad 1\quad 1\quad 0 \\ \text{cipher} \to & \underline{1\quad 0\quad 0\quad 1\quad 0} \end{array}\right\} \text{decryption}$$

$$\begin{array}{ll} \text{Message} \to & 1\quad 1\quad 1\quad 0\quad 0 \end{array}$$

Conditions in one time pad

- length of key ≥ Length of the message.
- key want to be purle random.
- key has to be Shared among Sender and receiver.
- One key pad can be used one-time.

Cracking code (crypto analysis)

- guessing the meaning of the encrypted message without using a key Called Crypto analysis.

Methods used to Crypto analysis.

- Brute-force-method
- Ciphertext-Only method
- known-Plaintext method
- Chosen-plaintext method
- Chosen-ciphertext method
- Meet-in-Middle method.

Date No

- Brute-force method.
  - Attacker tries all possible methods untill find the Solution.

    Any mesrage is vulnerable to brute-force attack.