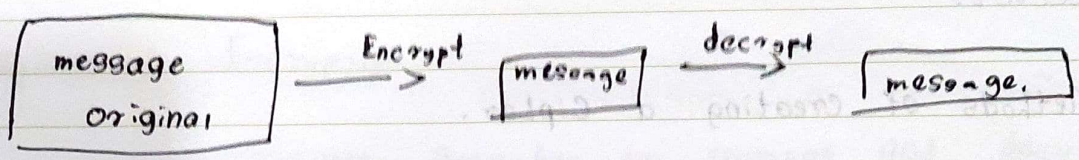
Cryptography (ICS) - Lec 01

- Cryptography meaning Converting an message to a Unreadable format is called Crypto graphy.

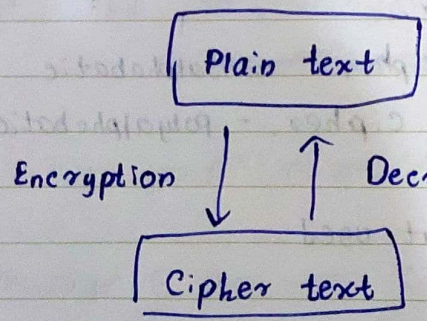


Services can be archeived by Cryptography.

- 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 cipher text to plain text.

- 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.

Varioues cipher methods that used.

Scytale
Caesar Cipher
Vigenere cipher
Jefferson's encryption device

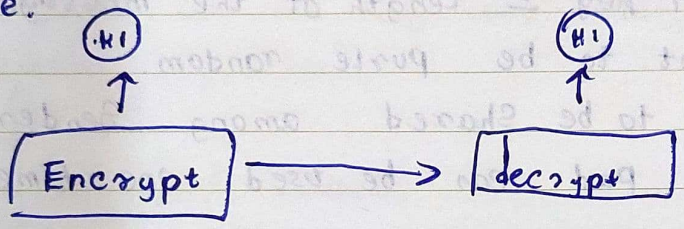
Date No

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, puplick key)
- also referred as public key Cryptography.

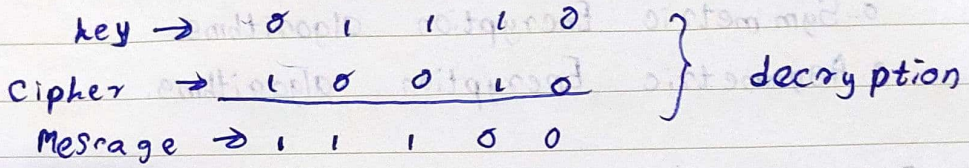
- One-Time pad Chiper text.

message ⊕ key = Cipher tex

↑
XOR

Message → 1 1 1 0 0
key → 0 1 1 1 0 → decryption.
Cipher → 1 0 0 1 0

~~Enc~~ decryption



Conditions in one time pad

- Length of key ≥ Length of the message.
- key want to be pure 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 message is vulnerable to brute-force attack.

- Cypher text only method.
  - using a Cypher text and using it attacker Could figure out the key and decrypte the message. (practically impossible).

- known plain text attack.
  - attacker using brute force attack to find the key and attacker already have a some idea about what original message looks like.

- Choosen plain text attack.
  - attacker can enter some data to the algorithem and observe the algorithm and figure out the message.

- Chosen cipher text attack.
  - attacker enter Cypher text and observ the decryption and figur out the key.

- Meet in the middle.
  - also some as known palin text attack.

Date No

frequency analysis.

o best way to crack the code is brute force attack. In here attacker may do a analysis and by using frequently used key trying to find the plain text.

Cryptography + Cryptoanalysis —> Cryptology.

Cryptology -> Science of making and braking Codes.