Cryptography

7/01/2025

Cryptography and Network Security

- Key Based
- Key less

- **Security**
- **Types of Security**
  1) No Security
  2) ID & Password
  3) Obscurity
  4) Security through encryption

Security Services / Principle of Security

i) Non-Repudiation
(False Identification or you can't denied anything)

ii) Authentication

iii) Access Control → Role Management (User Specific)
→ Rule Management (Resources)

CIA → Confidentiality Integrity Availability

Various types of security :-

Attack

Two Types :-

1) Passive Attacks (Doesn't do any modification of actual msg)
   - Detection Difficult
2) Active Attacks (modification of actual msg)
   - Detection easier compare than passive attacks

(Detection → Solution)

Man in the middle Attacks

Cryptography :—

The art / science of achieving security through encryption

method to convert plain text to cipher text

[Easily readable & Understandable] [Non-Meaningful Text]

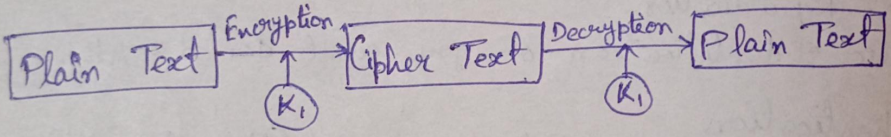
Key

① Symmetric key cryptography (Private key cryptography)

② Asymmetric key cryptography (public key cryptography)

[used → (i) public key (ii) private key]

① Symmetric key

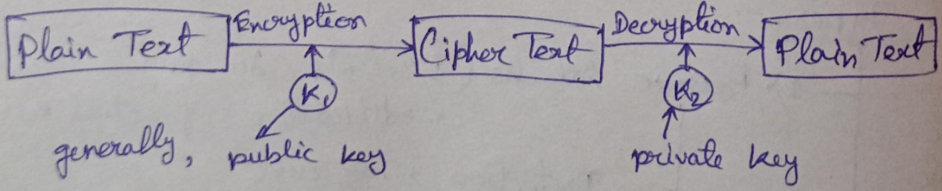


- One of algorithm

(i) Data Encryption Standard (DES) / DEA → Algorithm

② Assymmetric : (public)

(public key + private key)



- Spacial case → vice-versa

(*) A B C D . . . . . Z

0 1 2 3 25

(*) $K \geq 1$, non-negative , $K \leq 25$

$1 \leq K \leq 25$ for ceaser cipher

Ex: HELLO, key = 4

$e(H) = E(H, 4) = (H+4) \bmod 26 = (7+4) \bmod 26$

$= 11 \bmod 26$

$= 11$

$\Rightarrow L$

E → I
L → P
L → P
O → S

Cryptography Algorithm is divided into 2 parts

- Substitution
  +4 / +const
- Transposition (changing position of character)
  - Key based
  - Key less

Hash Code: → Do not use any key

→ Uses Hash fn

Message Digest:
Fixed length for var.

MD5

1st Algo. ever proposed

Ceaser Cipher → Mono alphabetic Cipher

C	B	A	S	E	R
+3 ↓	+3 ↓	+3 ↓	+3 ↓	+3 ↓	+3 ↓
F	H	D	V	H	U

Poly

H E Y THERE
+ + + + + + +
J G X A Y

Example:

Meet me at Two PM, key = 4

+4 +4 +4 +4 +4 +4

Cyclic after Z

W	X	Y	Z
+4 ↓	+4 ↓	+4 ↓	+4 ↓
A	B	C	D

Formula: → Encryption

$C = E(P, K) = (P+K) \bmod 26$

C → Cipher
26 → no. of Alphabet

$P = D(C, K) = (C-K) \bmod 26.$