Network Security & Cyber Laws

-Deepankar Sharma

1. Computer Security
2. Network Security
3. Internet Security

} Information Security

- Security Attack
- Security Mechanism
- Security Service

Cryptanalytic attack

1. Choosen Plain Text attack
2. Known Plain Text attack
3. Choosen Cipher-text attack
4. Ciphertext only attack

Security Mechanisms

1. Encipherment
2. Access control
3. Digital Signature

⋮ etc

Security Attacks

1. Interruption
2. Interception
3. Modification
4. Fabrication

Cryptographic Attacks

Passive Attacks

1. Release of Message Contents
2. Traffic Analysis

Active Attacks

1. Masquerade
2. Replay
3. Modification of Messages
4. Denial of Service (DOS)

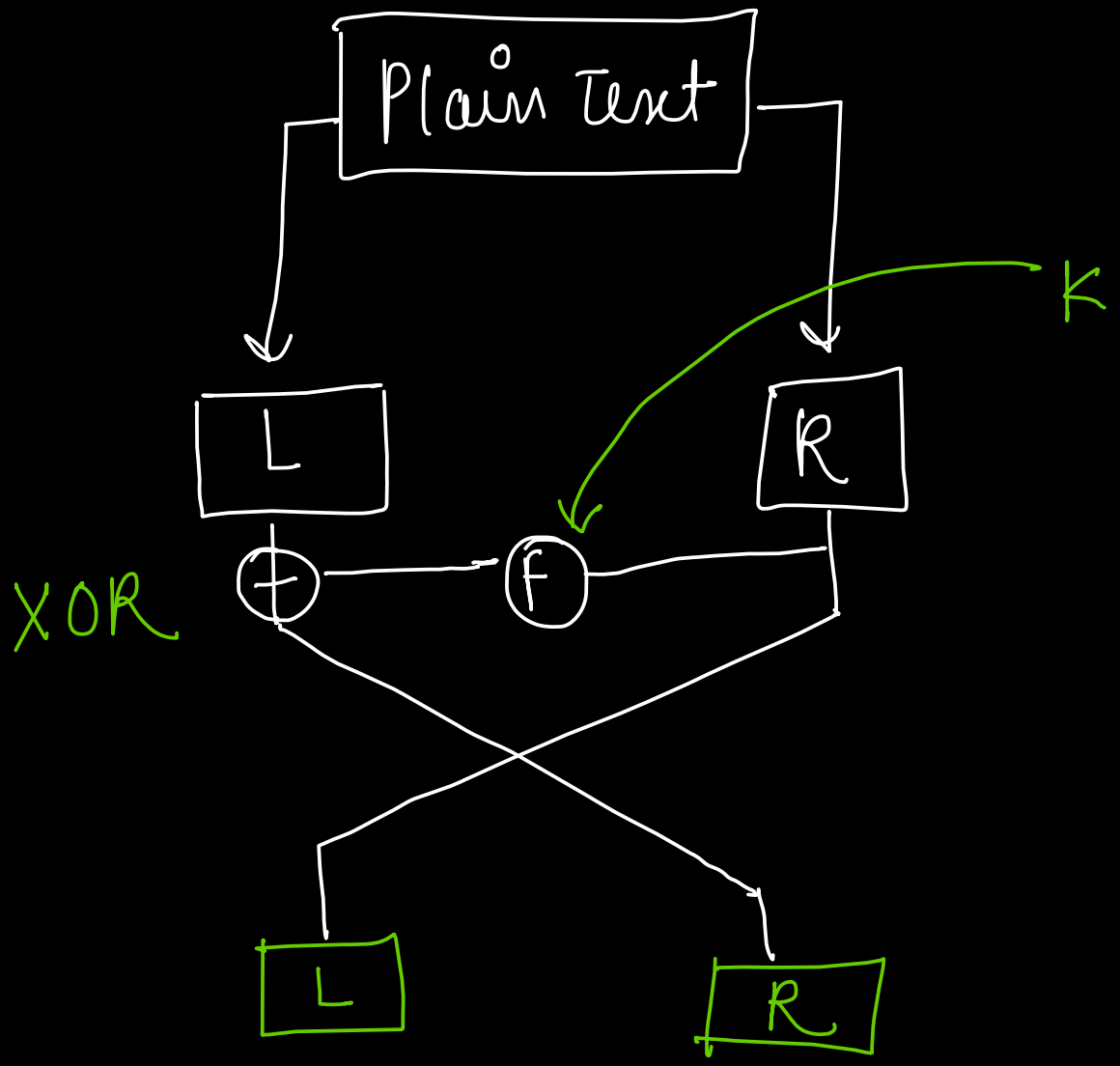
Conventional Encryption (Private key - Single key)

1. Plain Text → Random Nonsense

Classical Encryption Techniques

- 1. Substitution cipher
  - Caesar's cipher / Shift cipher
  - Playfair cipher
  - Polyalphabetic ciphers
    - Vigenere cipher
- 2. Transposition cipher
  - Rail fence cipher
  - Row Transposition cipher

Feistel Cipher Structure



DES ⇒ 16 feistel rounds

IDEA

Block Cipher Modes of operation

1. ECB (Electronic Code Book)
2. CBC (Cipher Block Chaining)
3. CFM (Cipher feedback Mode)
4. OFM (output feedback Mode)
5. Counter mode

RSA

1. p & q → 2 prime numbers
2. $n = pq$
3. $\phi(n) = (p-1)(q-1)$
4. Select e, $\gcd(e, \phi(n)) = 1$

   $1 < e \leq \phi(n)$
5. $d \equiv e^{-1} \pmod{\phi(n)}$
6. Public key $\{e, n\}$

   Private key $\{d, n\}$

$$C = M^e \bmod n$$

$$M = C^d \bmod n$$

Key Management

1. Public Announcement of public keys
2. Publicly available directory
3. Public key authority
4. Public key certificates
5. Diffie Hellman key exchange