Cryptanalysis and Data Security

Iris Shi

Cryptanalysis

Types –

- ➔ Brute force
- ➔ Chosen-plaintext
- ➔ Side-channel attacks

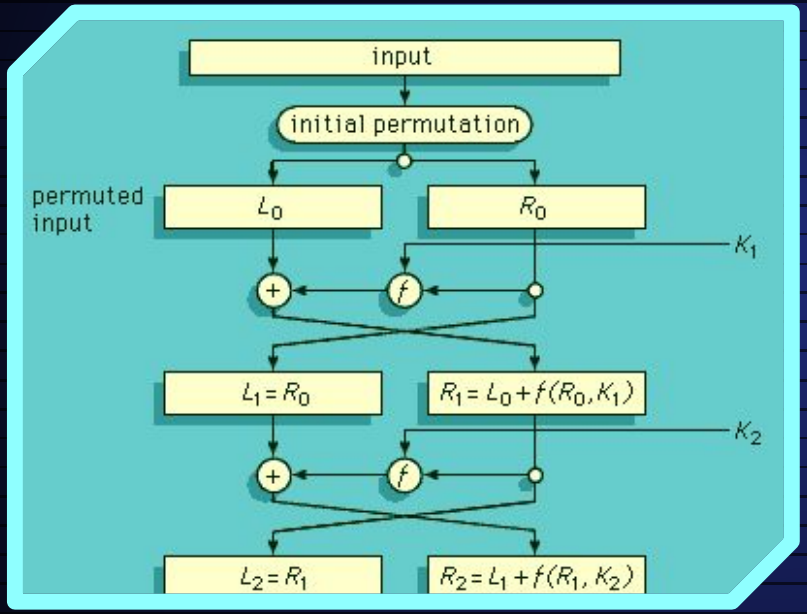
Examples –

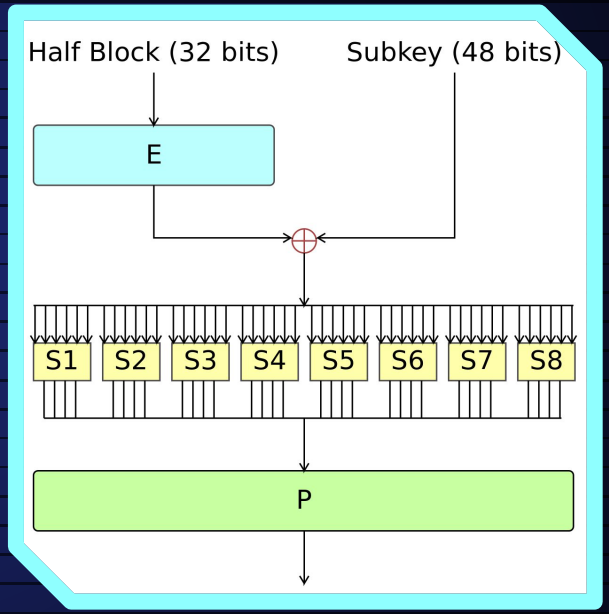
- ➔ Linear cryptanalysis
- ➔ Meet-in-the-middle attacks
- ➔ Birthday attack

Encryption

What is encryption?

Data Encryption Standard (DES)





$$f(e, n, M_i)$$

$$M_1, \ldots, M_k \rightarrow P_1, \ldots, P_k$$

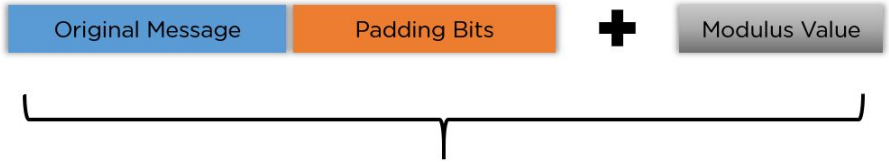
$$C_i = P_i^{\,e} \,\%\, n$$

$$P_i = C_i^{\,d} \,\%\, n = (P_i^{\,e})^{\,d} \,\%\, n = P_i^{\,e \cdot d} \,\%\, n$$

Public-key Encryption

Rivest-Shamir-Adleman (RSA)

Hashing Functions (SHA-256)



$H_0 = 6a09e667$ $H_1 = bb67ae85$ $H_2 = 3c6ef372$ $H_3 = a54ff53a$

$H_4 = 510e527f$ $H_5 = 9b05688c$ $H_6 = 1f83d9ab$ $H_7 = 5be0cd19$

Zero-Knowledge Proofs (ZKP)

- Prover and verifier
- Ali Baba Cave example
- Applications

Quantum Resistant Algorithms

- ➔ Shor's Algorithm
- ➔ Grover's Algorithm
- ➔ Hash Functions
- ➔ Code-Based Cryptography – McEliece

Modern Cyber Threats

- Phishing
  - Spear phishing
  - Ransomware
- Zero-day exploits
- Malware
- Man-in-the-Middle (MitM)
- Credentials stuffing

Conclusion

Thanks!

Do you have any questions?

youremail@freepik.com
+91 620 421 838
yourcompany.com