University Djilali Bounaâma of Khemis-Miliana

Department of Computer Science

L3 – Computer Systems (S6) - 2025/2026

Subject: Computer Security and Cryptography

Series of exercises N° 02

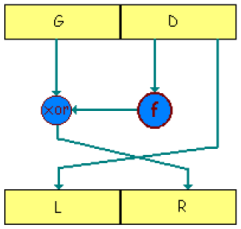
Exercise 01: Feistel Bijection

We want to encrypt the following plaintext block with a Feistel bijection repeated twice:

P = 11011110001010011101110010110101

The random function **f** is a **simple transposition** (**key = 2413**)

Diagram the encryption procedure for P, then write the ciphertext block.



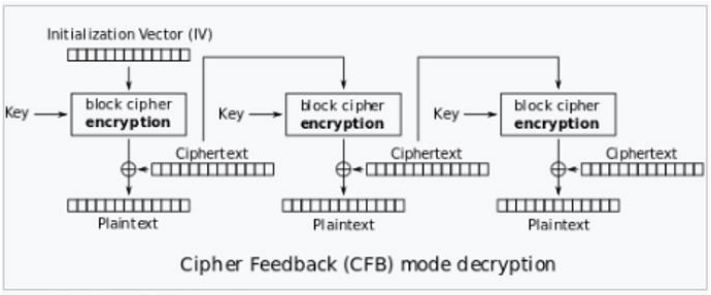
Encryption:L = D and R = G xor *f*(D)

Decryption:D = L and G = R xor *f*(L)

Feistel Bijection

Exercise 02: Full-Block CFB Decryption

We want to decrypt the following bitstream (**001111100111001101100001**) using a full-block CFB mode (**Block size = 8 bits**). The encryption function is a Feistel Bijection while the random function ***f*** is a simple transposition (**3421**). **IV = 11001101**



Cipher feedback (CFB) decryption

Exercise 03: Answer the following questions:

- Exact key length for DES and AES?
- Number of rounds for DES and AES?
- Number of keys required to encrypt transactions between 50 users for the two following cases:
  - Secret key encryption
  - Public key encryption

Exercise 04: Use the modular exponentiation method in order to calculate the following:

1) $5^{11} \pmod{14}$ 2) $41^{7} \pmod{187}$

Exercise 05: We aim to encrypt a message M using RSA, following these steps:

1- Choose two distinct prime numbers p and q, their product is n

Example: p=11, q=17

2- Choose e coprime with $\varphi(n)$, i.e., gcd(e, $\varphi(n)$)=1

Example: e=7

3- Calculate d such that $e \times d \equiv 1 \pmod{\varphi(n)}$

Example: d=23

- Calculate $\varphi(n)$, then deduce the values of the public and private keys?
- Write the encryption and decryption formulas for a message M?
- Calculate X, the encrypted message of M=88 using the method of modular exponentiation?

Exercise 06: RSA Signature

Ahmed wants to send a message m = 10 signed with RSA to Karim.

- Ahmed has the following data: n = 85, e = 5, d = 13.
- Karim has the following data: n = 187, e = 7, d = 23.

Upon receiving the message, Karim must verify its authenticity.

- Calculate the signed message to be sent by Ahmed, then verify the authenticity of the message received by Karim?

Exercise 07: Given n = 35 the public exponent of the RSA public key. Explain (step by step) how an attacker only uses this information to encrypt/decrypt messages and provides authenticity threats.

Exercise 08: Give the first and the last md5 50-bit input for the message "WORLD":
Knowing that WORLD $= (87, 79, 82, 76, 68)_{10}$

Exercise 09: Match each description in the left with the corresponding type of attack in the right:

1.Collecting information, Recovering secret keys, Destroying channels	a.Dictionary attack
2.Determining repetitions of symbols in text, comparing them with typical occurrences of a language	b.Exhaustive search attack
3.Require as input the name of the file to decode and a regular expression to apply	c.Statistical attack
4.Deciphering a password by trying a set of words (reversed, lowercase, uppercase)	d.Protocol attack