University Djilali Bounaâma of Khemis-Miliana

Department of Computer Science

3rd year Bachelor's Degree – Computer Systems (S6) - 2023/2024

Subject: IT Security and Cryptography

Series of exercises N° 02

Exercise 01: We want to encrypt the plaintext word '**EYE**' with the key '**S**' using **XORing** encryption: Knowing that the decimal values of the plaintext letters in the ASCII table are: E=69, Y=89, S=83. Provide the encrypted word in decimal?

Exercise 02: A system is protected by a **password**. After an unsuccessful attempt, the system waits for a while before asking for the password again (the total time for one attempt is **3 seconds**). How long (in seconds) will it take to penetrate the system knowing that the password consists of:

- **4 digits**?
- **4 letters**?
- **4 alphanumerics**?

Exercise 03: We want to encrypt the binary sequence "**110011010111011101011101**" using CBC mode with **8-bit** blocks, knowing that: The initialization vector **IV = "10010101"**. The key **K = "11101101"**. The encryption function is used to invert the block to be encrypted after XORing with K. Write down the encrypted binary sequence? Decrypt the encrypted sequence in order to get the initial binary sequence?

Exercise 04: 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**)

- Draw the standard Feistel schema, then write the encryption and decryption formulas?
- Diagram the encryption procedure for P, then write the ciphertext block?

Exercise 05: 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 06: Use the modular exponentiation method in order to Calculate the following:

- $5^{11} \pmod{14}$
- $41^{7} \pmod{187}$

Exercise 07: We want 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?
- Diagram the encryption/decryption procedure?

Exercise 08: 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?
- Diagram the authentication procedure?

Exercise 09: Answer the following questions:

- Given three integers a, n, and x, when do we say that x is the inverse of a modulo n?
- The vulnerability of RSA mainly stems from its public key:
  - Explain how?
  - What countermeasure should be considered to address this vulnerability?
- Match each PKI component with the right action:

a) Certification authority	1) Verify the enrollment request of a new entity in the infrastructure
b) Registration authority	2) Store the current certificates and those that have been revoked
c) Validation authority	3) Generate the certificate for an entity, containing the public identity and the certificate validity period