Assignment 2 : RSA and DH Algorithms

Exercise 1: RSA Encryption

1.1. Explain the RSA Encryption Algorithm

- Write a brief explanation of the RSA encryption/decryption algorithm, highlighting the key steps involved.
- Describe the role of the public key and private key in RSA encryption.
- Explain the concept of prime numbers and their significance in RSA.

1.2. Calculation of RSA Parameters

Ahmed and Fahd want to communicate and keep the message between them confidential using RSA encryption.

1. **Key generation**

- Ahmed chooses two prime numbers: p = 17 and q = 11.
- Calculate the value of n, φ(n) and put e = 13 for Ahmed's public key.
- Calculate Ahmed's private key.

2. **Encryption**

- Fahd wants to send a plaintext message: "SECRET" to Ahmed. He converts the plaintext into numeric representation using a predetermined mapping (A=1, B=2, C=3 and so on). Then, he encrypts the numeric representation of the message using Ahmed's public key (e, n).
- Show the **step-by-step encryption process** (use your **Windows scientific calculator** to perform the calculations accurately).

3. **Decryption**

- Ahmed receives another encrypted message from Fahd: "94 37 133 133 53".
- Show the **step-by-step decryption process** (use your **Windows scientific calculator** to perform the calculations accurately).

Exercise 2: Diffie–Hellman key exchange

Reem and Hala want to establish a shared secret key using the Diffie-Hellman key exchange protocol. They agree on the following parameters:

- Prime number (q) = 11
- Primitive root of q (a) = 6

1. Verify if the value of a = 6 is a primitive root of q = 11.

Reem chooses her private key $\mathbf{X_R}$ as 6, and Hala chooses his private key $\mathbf{X_H}$ as 5.

2. Calculate the following:

a) Reem's public key Y_R.
b) Hala's public key Y_H.
c) The shared secret key (K) that Reem and Hala will derive.

After establishing the shared secret key (K) using the Diffie-Hellman key exchange protocol, Reem and Hala decide to use the **Caesar cipher** for encrypting their messages. The Caesar cipher is a simple substitution cipher where each letter in the plaintext is shifted a certain number of positions down the alphabet.

The encryption function for the Caesar cipher is as follows:

$$\mathbf{Enc(x) = (x + K) \bmod 26}$$

- x is the letter to be encrypted ($0 \leq x \leq 25$, where A=0, B=1, ..., Z=25).
- K is the shared secret key ($0 \leq K \leq 25$).
- Enc(x) is the encrypted letter.

The decryption function for the Caesar cipher is as follows:

$$\mathbf{Dec(y) = (y - K + 26) \bmod 26}$$

- y is the encrypted letter ($0 \leq y \leq 25$)
- K is the shared secret key ($0 \leq K \leq 25$)
- Dec(y) is the decrypted letter

3. Using the shared secret key (K) derived in question 2(c), decrypt the following message sent by Reem to Hala: "**DPOHSBUVMBUJPOT**"

Submission Guidelines

- Submit your answers in a clear and organized format, showing all calculations and steps involved in the encryption and decryption processes. Provide explanations where necessary, and make sure to address all parts of each question.
- The **firm deadline** is **Tuesday, November 19th at 23:59**. Any submissions received after the deadline will not be considered.
- Submissions should be made through LMS in **PDF format**.
- Submissions made through email won't be accepted.
- For this assignment, you have the option to form groups of 3-4 students maximum. **Please note that no groups larger than 4 students will be accepted**.