Assignment 2: RSA and DH Algorithms

Abdullah Meraj Yazeed Alkhalaf Affan Mohammed
Bara Allam

November 19, 2024

Exercise 1: RSA Encryption

1.1: Explain the RSA Encryption Algorithm

1.2: Calculation of RSA Parameters

1. Key Generation

- Ahmed chooses two prime numbers: p = 17 and q = 11.
- Calculate $n,\ \phi(n)$:

$$n = p \times q = 17 \times 11 = 187$$
$$\phi(n) = (p-1) \times (q-1) = (17-1) \times (11-1)$$
$$= 16 \times 10 = 160$$

- Choose $e = 13$ for Ahmed's public key.
- Calculate Ahmed's private key d:

$$Here\ e = 13,\ \phi(n) = 160$$
$$ed \equiv 1(\mod \phi(n))$$
$$\implies ed \mod \phi(n) = 1 \mod \phi(n)$$
$$\implies ed \mod \phi(n) = 1$$
$$let\ ed = k \times \phi(n) + 1$$
$$13d = k \times 160 + 1$$
$$d = \frac{k \times 160 + 1}{13}$$

For k = 1:

$$d = \frac{1 \times 160 + 1}{13} = \frac{160 + 1}{13} = \frac{161}{13} = 12.38$$

For k = 2:

$$d = \frac{2 \times 160 + 1}{13} = \frac{320 + 1}{13} = \frac{321}{13} = 24.69$$

For k = 3:

$$d = \frac{3 \times 160 + 1}{13} = \frac{480 + 1}{13} = \frac{481}{13} = 37$$

d = 37
Ahmed's private key is (37,187)

2. Encryption

Question: 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).

Answer: S = 19, E = 5, C = 3, R = 18, T = 20 n = 187, e = 13

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

$$C = M^{13} \mod 187$$

$$C_S = 19^{13} \mod 187 = 83$$

$$C_E = 5^{13} \mod 187 = 37$$

$$C_C = 3^{13} \mod 187 = 148$$

$$C_R = 18^{13} \mod 187 = 35$$

$$C_T = 20^{13} \mod 187 = 80$$

"SECRET" is encrypted as "83 37 148 35 37 80"

3. Decryption

Question: Ahmed receives another encrypted message from Fahd: "94 37 133 133 53"

Answer: Here d = 37, n = 187

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

$$M = C^{37} \mod 187$$

$$M_94 = 94^{37} \mod 187 = 8 = "H"$$

$$M_37 = 37^{37} \mod 187 = 5 = "E"$$

$$M_{133} = 133^{37} \mod 187 = 12 = "L"$$

$$M_{53} = 53^{37} \mod 187 = 15 = "O"$$

"94 37 133 133 53" is decrypted as "HELLO"