RSA Practice Questions

Problem 1:

- Primes: $p = 17$, $q = 19$
- Public exponent: $e = 5$
- Message: $m = 12$

Step 1: Compute $n = p \times q$

$$n = 17 \times 19 = 323$$

Step 2: Compute $\phi(n) = (p - 1) \times (q - 1)$

$$\phi(n) = (17 - 1) \times (19 - 1) = 16 \times 18 = 288$$

Step 3: Check that $e = 5$ and $\phi(n)$ are coprime. Since $\gcd(5, 288) = 1$, $e = 5$ is valid.

Step 4: Compute the private key d such that $e \times d \equiv 1 \pmod{\phi(n)}$. We need to solve $5 \times d \equiv 1 \pmod{288}$.

Using the Extended Euclidean Algorithm, we find $d = 173$.

So, the public key is $(e, n) = (5, 323)$ and the private key is $d = 173$.

Step 5: Encrypt the message $m = 12$.

$$c = m^e \pmod{n} = 12^5 \pmod{323}$$

$$12^5 = 248832$$

$$c = 248832 \pmod{323} = 164$$

The ciphertext is $c = 164$.

Step 6: Decrypt the ciphertext to retrieve the original message.

$$m = c^d \pmod n = 164^{173} \pmod{323}$$

Using modular exponentiation, we get:

$$m = 12$$

The original message is $m = 12$.

Problem 2:

- Primes: $p = 23$, $q = 29$
- Public exponent: $e = 3$
- Message: $m = 15$

Step 1: Compute $n = p \times q$

$$n = 23 \times 29 = 667$$

Step 2: Compute $\phi(n) = (p-1) \times (q-1)$

$$\phi(n) = (23-1) \times (29-1) = 22 \times 28 = 616$$

Step 3: Check that $e = 3$ and $\phi(n)$ are coprime. Since $\gcd(3, 616) = 1$, $e = 3$ is valid.

Step 4: Compute the private key d such that $e \times d \equiv 1 \pmod{\phi(n)}$. We need to solve $3 \times d \equiv 1 \pmod{616}$.

Using the Extended Euclidean Algorithm, we find $d = 411$.

So, the public key is $(e, n) = (3, 667)$ and the private key is $d = 411$.

Step 5: Encrypt the message $m = 15$.

$$c = m^e \pmod{n} = 15^3 \pmod{667}$$

$$15^3 = 3375$$

$$c = 3375 \pmod{667} = 374$$

The ciphertext is $c = 374$.

Step 6: Decrypt the ciphertext to retrieve the original message.

$$m = c^d \pmod{n} = 374^{411} \pmod{667}$$

Using modular exponentiation, we get:

$$m = 15$$

The original message is $m = 15$.

Diffie-Hellman Practice Questions

Problem 1:

- Prime $p = 43$
- Generator $g = 7$

- Alice’s private key $a = 5$
- Bob’s private key $b = 9$

Step 1: Calculate Alice's public key

$$A = g^{a} \pmod p = 7^{5} \pmod{43}$$

$$A = 16807 \pmod{43} = 6$$

Alice's public key is $A = 6$.

Step 2: Calculate Bob's public key

$$B = g^{b} \pmod p = 7^{9} \pmod{43}$$

$$B = 40353607 \pmod{43} = 15$$

Bob's public key is $B = 15$.

Step 3: Compute the shared secret key

- Alice computes:

$$\text{Shared secret} = B^{a} \pmod p = 15^{5} \pmod{43} = 17$$

- Bob computes:

$$\text{Shared secret} = A^{b} \pmod p = 6^{9} \pmod{43} = 17$$

The shared secret key is 17.

Problem 2:

- Prime $p = 59$
- Generator $g = 11$
- Alice’s private key $a = 12$
- Bob’s private key $b = 19$

Step 1: Calculate Alice's public key

$$A = g^{a} \pmod{p} = 11^{12} \pmod{59} = 16$$

Alice's public key is $A = 16$.

Step 2: Calculate Bob's public key

$$B = g^{b} \pmod{p} = 11^{19} \pmod{59} = 32$$

Bob's public key is $B = 32$.

Step 3: Compute the shared secret key

- Alice computes:

$$\text{Shared secret} = B^{a} \pmod{p} = 32^{12} \pmod{59} = 17$$

- Bob computes:

$$\text{Shared secret} = A^{b} \pmod{p} = 16^{19} \pmod{59} = 17$$

The shared secret key is 17.

Caesar Cipher Practice Questions

Problem 1:

- Plaintext: "ATTACK AT DAWN"
- Shift: 4

Encryption: Shift each letter by 4 positions in the alphabet.

$$\text{ATTACK AT DAWN} \rightarrow \text{EXXEGO EX HEAR}$$

Decryption: Shift each letter back by 4 positions:

$$\text{EXXEGO EX HEAR} \rightarrow \text{ATTACK AT DAWN}$$

Problem 2:

- Ciphertext: "KHOOR ZRUOG"
- Shift: 3

Decryption: Shift each letter back by 3 positions:

$$\text{KHOOR ZRUOG} \rightarrow \text{HELLO WORLD}$$

Encryption:

- Plaintext: "HELLO WORLD"
- Shift: 7

$$\text{HELLO WORLD} \rightarrow \text{OLSSV DVYSK}$$

Vigenère Cipher Practice Questions

Problem 1:

- Plaintext: "SECURITY IS CRUCIAL"
- Key: "KEY"

Step 1: Encryption Using the Vigenère cipher, shift each letter by the corresponding key letter's position in the alphabet:

$$\text{SECURITY IS CRUCIAL} \rightarrow \text{CMWYVCWXS KC EYFOIVH}$$

Step 2: Decryption Use the key to reverse the shift:

$$\text{CMWYVCWXS KC EYFOIVH} \rightarrow \text{SECURITY IS CRUCIAL}$$

Problem 2:

- Ciphertext: "WYZGOS WP EFWX"
- Key: "CIPHER"

Step 1: Decryption Using the key "CIPHER", reverse the shift of each letter:

$$\text{WYZGOS WP EFWX} \rightarrow \text{SECRET GOAL SAFE}$$

Step 2: Encryption

- Plaintext: "DATA ENCRYPTION"
- Key: "ENCRYPT"

Encrypt using the Vigenère cipher:

$$\text{DATA ENCRYPTION} \rightarrow \text{ITVT SBTBBIQTD}$$

Columnar Transposition Cipher Practice Questions

Problem 1:

- Plaintext: "MEET ME AT MIDNIGHT"
- Key: "SECRET"

Step 1: Encryption Write the message in columns based on the key length, then rearrange the columns:

$$\text{Ciphertext} \rightarrow \text{MTTIIHEMMTDENEGTA}$$

Step 2: Decryption Rearrange the columns based on the key and read the plaintext:

$$\text{MTTIIHEMMTDENEGTA} \rightarrow \text{MEET ME AT MIDNIGHT}$$

Problem 2:

- Ciphertext: "NGETTMEEAIMTDHTIM"
- Key: "KEYWORD"

Step 1: Decryption Rearrange columns based on the key:

$$\text{Ciphertext} \rightarrow \text{MEET ME AT MIDNIGHT}$$