Lahore Garrison University

SUBMITTED BY:

Imtnan Khalid (071 C)

SUBMITTED TO:

Dr. Irshad Ahmed

Please define each cipher and give Two Examples to explain the encryption and decryption process of each cipher.

1. Viginire cipher

2. Playfair cipher

3. Hill cipher

4. Row-Column Transposition cipher

5. RSA Algorithm

1. Vigenère Cipher

Definition: The Vigenère cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution. A keyword is used to generate a series of different Caesar ciphers based on the letters of the keyword. The key is repeated to match the length of the plaintext.

Encryption Process:

1. Write the plaintext.
2. Write the key repeatedly below the plaintext to match its length.
3. Encrypt each letter of the plaintext by shifting it forward in the alphabet by the number of positions given by the corresponding letter of the key (A=0, B=1, C=2, ..., Z=25).

Decryption Process:

1. Write the cipher text.
2. Write the key repeatedly below the cipher text to match its length.
3. Decrypt each letter of the cipher text by shifting it backward in the alphabet by the number of positions given by the corresponding letter of the key.

Example 1:

- **Plaintext:** ATTACKATDAWN
- **Key:** LEMON
- **Cipher text:** LXFOPVEFRNHR

Encryption Steps:

- A (0) + L (11) = L (11)
- T (19) + E (4) = X (23)
- T (19) + M (12) = F (5)
- A (0) + O (14) = O (14)
- C (2) + N (13) = P (15)
- K (10) + L (11) = V (21)
- A (0) + E (4) = E (4)
- T (19) + M (12) = F (5)
- D (3) + O (14) = R (17)
- A (0) + N (13) = N (13)
- W (22) + L (11) = H (7)
- N (13) + E (4) = R (17)

Example 2:

- **Plaintext:** HELLOWORLD
- **Key:** KEY
- **Ciphertext:** RIJVSUYVJN

Encryption Steps:

- H (7) + K (10) = R (17)
- E (4) + E (4) = I (8)
- L (11) + Y (24) = J (9)
- L (11) + K (10) = V (21)
- O (14) + E (4) = S (18)
- W (22) + Y (24) = U (20)
- O (14) + K (10) = Y (24)
- R (17) + E (4) = V (21)
- L (11) + Y (24) = J (9)
- D (3) + K (10) = N (13)

2. Playfair Cipher

Definition: The Playfair cipher is a manual symmetric encryption technique and was the first literal digraph substitution cipher. The technique encrypts pairs of letters (digraphs), instead of single letters.

Encryption Process:

1. Create a 5x5 matrix using the key, filling in remaining letters in alphabetical order (combining I and J).
2. Divide the plaintext into pairs of letters.
3. For each pair, use rules based on the positions of the letters in the matrix to generate the cipher text
4. .

Decryption Process:

1. Create the 5x5 matrix using the key.
2. Divide the cipher text into pairs of letters.
3. For each pair, use rules based on the positions of the letters in the matrix to retrieve the plaintext.

Example 1:

- **Key:** MONARCHY
- **Plaintext:** BALLOON
- **Matrix:**

  M O N A R

  C H Y B D

  E F G I/J K

  L P Q S T

  U V W X Z

- **Cipher text:** ICMKONON

Encryption Steps:

- B and A are in the same column, replace each with the letter below: I and C
- L and L form a rectangle, replace with opposite corners: K and O
- O and N form a rectangle, replace with opposite corners: N and M
- O and N form a rectangle, replace with opposite corners: N and O

Example 2:

- **Key:** KEYWORD
- **Plaintext:** HELLO
- **Matrix:**

K E Y W O

R D A B C

F G H I/J L

M N P Q S

T U V X Z

- **Ciphertext:** LLMXVL

Encryption Steps:

- H and E form a rectangle, replace with opposite corners: G and K
- L and L are in the same row, replace each with the letter to the right: L and M
- O and W form a rectangle, replace with opposite corners: O and X

3. Hill Cipher

Definition: The Hill cipher is a polygraphic substitution cipher based on linear algebra. It uses matrix multiplication to encrypt and decrypt messages.

Encryption Process:

1. Convert the plaintext into numerical values.
2. Create an invertible key matrix.
3. Multiply the plaintext vector by the key matrix (mod 26) to get the ciphertext.

Decryption Process:

1. Convert the ciphertext into numerical values.
2. Find the inverse of the key matrix.
3. Multiply the ciphertext vector by the inverse key matrix (mod 26) to retrieve the plaintext.

Example 1:

- **Key Matrix:**

```
3 3
2 5
```

- **Plaintext:** HELLO
- **Plaintext Vector:** [7 4], [11 11], [14 14] (converted to pairs)
- **Ciphertext:** EGGCW (encrypted pairs: [4 6], [6 2], [22 3])

Encryption Steps:

1. [7 4] * [3 3 2 5] = [29 26] ≡ [3 0] = E G
2. [11 11] * [3 3 2 5] = [66 88] ≡ [6 2] = G C
3. [14 14] * [3 3 2 5] = [84 98] ≡ [22 3] = W D

Example 2:

- **Key Matrix:**

```
2 3
3 4
```

- **Plaintext:** TEST
- **Plaintext Vector:** [19 4], [18 19]

- **Ciphertext:** UBXH (encrypted pairs: [20 1], [23 7])

Encryption Steps:

1. [19 4] * [2 3 3 4] = [53 76] ≡ [20 1] = U B
2. [18 19] * [2 3 3 4] = [111 145] ≡ [23 7] = X H

4. Row-Column Transposition Cipher

Definition: The Row-Column Transposition cipher is a permutation cipher that rearranges the characters of the plaintext in a grid, by reading the characters off in a specific pattern.

Encryption Process:

1. Write the plaintext into a grid row by row.
2. Read the columns of the grid in a specified order to generate the ciphertext.

Decryption Process:

1. Write the ciphertext into the grid column by column.
2. Read the rows of the grid to retrieve the plaintext.

Example 1:

- **Plaintext:** HELLO
- **Key (order of columns):** 3 1 4 2 5
- **Grid:**

```
H E L L O
```

- **Ciphertext:** LELHO

Encryption Steps:

1. Write HELLO in rows:

```
H E L L O
```

2. Read columns in the order 3 1 4 2 5:
    - 3rd column: L
    - 1st column: H
    - 4th column: L
    - 2nd column: E
    - 5th column: O

Example 2:

- **Plaintext:** ATTACKATDAWN
- **Key (order of columns):** 4 3 1 2
- **Grid:**

```
A T T A
C K A T
D A W N
```

- **Ciphertext:** TADCTAKATANW

Encryption Steps:

1. Write ATTACKATDAWN in rows:

```
A T T A
C K A T
D A W N
```

2. Read columns in the order 4 3 1 2:
    - 4th column: A T N
    - 3rd column: T A W
    - 1st column: A C D
    - 2nd column: T K A

5. RSA Algorithm

Definition: The RSA algorithm is an asymmetric cryptographic algorithm used for secure data transmission. It involves a public key for encryption and a private key for decryption.

Encryption Process:

1. Select two large prime numbers, p and q.
2. Compute n = p * q.
3. Compute the totient, φ(n) = (p-1)(q-1).
4. Choose an encryption key e such that $1 < e < \varphi(n)$ and e is coprime with φ(n).
5. Compute the public key (n, e).
6. Encrypt the plaintext message M using the formula: C = M^e mod n.

Decryption Process:

1. Compute the decryption key d such that $e*d \equiv 1 \bmod \varphi(n)$.
2. Decrypt the ciphertext C using the formula: M = C^d mod n.

Example 1:

- **Primes:** p = 61, q = 53
- **n = p*q:** 61 * 53 = 3233
- **φ(n):** (61-1)(53-1) = 3120

- **e:** 17 (common choice, must be coprime with 3120)
- **d:** 2753 (calculated using extended Euclidean algorithm)
- **Public Key (n, e):** (3233, 17)
- **Private Key (d):** 2753
- **Plaintext (M):** 65
- **Ciphertext (C):** 2790 (65^17 mod 3233)

Encryption Steps: C = 65^17 mod 3233 = 2790

Decryption Steps: M = 2790^2753 mod 3233 = 65

Example 2:

- **Primes:** p = 47, q = 59
- **n = p*q:** 47 * 59 = 2773
- **φ(n):** (47-1)(59-1) = 2688
- **e:** 7 (chosen to be coprime with 2688)
- **d:** 1531 (calculated using extended Euclidean algorithm)
- **Public Key (n, e):** (2773, 7)
- **Private Key (d):** 1531
- **Plaintext (M):** 88
- **Ciphertext (C):** 2086 (88^7 mod 2773)

Encryption Steps: C = 88^7 mod 2773 = 2086

Decryption Steps: M = 2086^1531 mod 2773 = 88

These examples provide a basic understanding of the encryption and decryption processes for each cipher and algorithm.