INSTITUTE OF INFORMATION TECHNOLOGY

JAHANGIRNAGAR UNIVERSITY

Number of Assignment	**:** 01
Submission Date	**:** 21/04/2024
Course Tittle	**:** Cryptography and Network Security
Course Code	**:** ICT - 4257

Submitted To	**Submitted By**
Professor K M Akkas Ali	Md. Shakil Hossain
Professor	Roll – 2023
IIT – JU	4th year 2nd Semester
	IIT – JU

Question: Illustrate various Mono- and Poly-Alphabetic Substitution Ciphers.

1. **Monoalphabetic Substitution Ciphers:**
   - **Additive Cipher (Shift or Caesar Cipher):**
     - In the additive cipher, each letter in the plaintext is shifted a fixed number of positions in the alphabet to encrypt the message.

       Example:

       Plaintext: HELLO

       Shift: 3

       Ciphertext: KHOOR
   - **Multiplicative Cipher:**
     - The multiplicative cipher involves multiplying each letter's numerical value by a constant to encrypt the message.
   - **Affine Cipher:**
     - The affine cipher combines the additive and multiplicative ciphers by applying both operations to each letter in the plaintext.

       Example:

       Encryption: E(x) = (ax + b) mod 26

       Decryption: D(y) = a^-1(y - b) mod 26

2. **Polyalphabetic Substitution Ciphers:**
   - **Autokey Cipher:**
     - In the autokey cipher, a keyword is concatenated with the plaintext to create the keystream for encryption.
   - **Playfair Cipher:**
     - The Playfair cipher uses a 5x5 grid of letters to encrypt digraphs (pairs of letters) from the plaintext.

       Example:

       Key: MONARCHY

       Plaintext: HELLO

    Ciphertext: EGKLL

- **Vigenere Cipher:**
    - The Vigenere cipher uses a keyword to determine the amount of shift applied to each letter in the plaintext.

      Example:

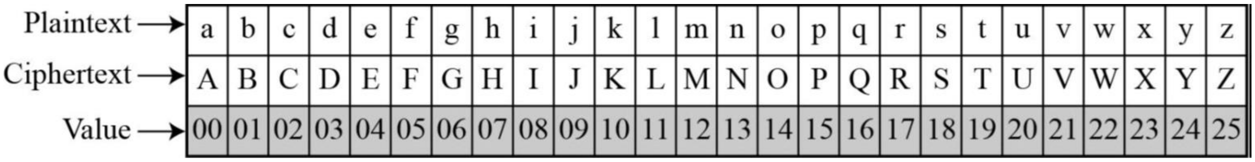
      Keyword: KEY

      Plaintext: HELLO

      Ciphertext: RIJVS
- **Hill Cipher:**
    - The Hill cipher involves matrix multiplication to encrypt blocks of letters in the plaintext

Mechanism:

1. **Monoalphabetic Ciphers:**
    - **Additive Cipher (Caesar Cipher):**
        1. Choose a shift value (key) for encryption.
        2. Each letter in the plaintext is shifted by the key value to encrypt the message.
        3. Encryption Formula: E(x) = (x + k) mod 26, where x is the plaintext letter's numerical value.
        4. Decryption is done by shifting the ciphertext letters back by the key value.



Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Figure: Additive Cipher

- **Affine Cipher:**
    1. Encryption Formula: E(x) = (ax + b) mod 26, where a and b are key values.
    2. Decryption Formula: D(y) = a^-1(y - b) mod 26, where y is the ciphertext letter's numerical value.
    3. Combines multiplication and addition operations for encryption and decryption.

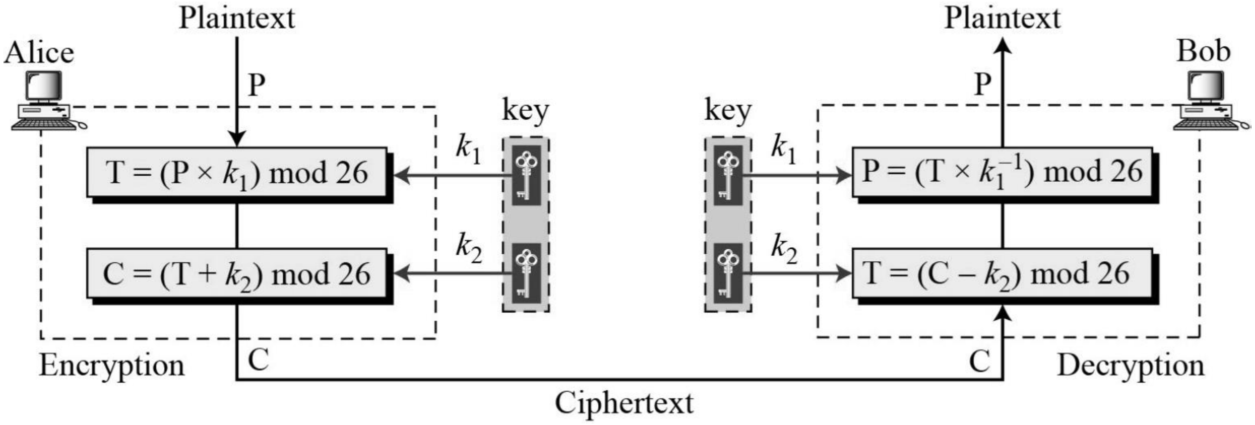
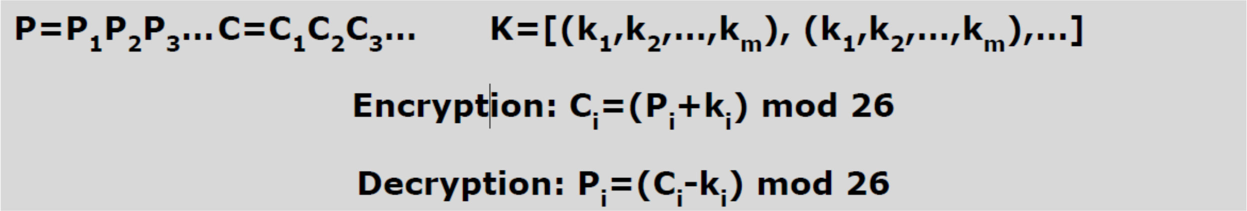


Figure: Affine Cipher

2. Polyalphabetic Ciphers:

- **Vigenere Cipher:**
    1. Choose a keyword repeated to match the length of the plaintext.
    2. Each letter in the plaintext is shifted by the corresponding letter in the keyword.
    3. Encryption Formula: E(x) = (x + k) mod 26, where k is the keyword letter's numerical value.
    4. Decryption is done by shifting the ciphertext letters back using the keyword.



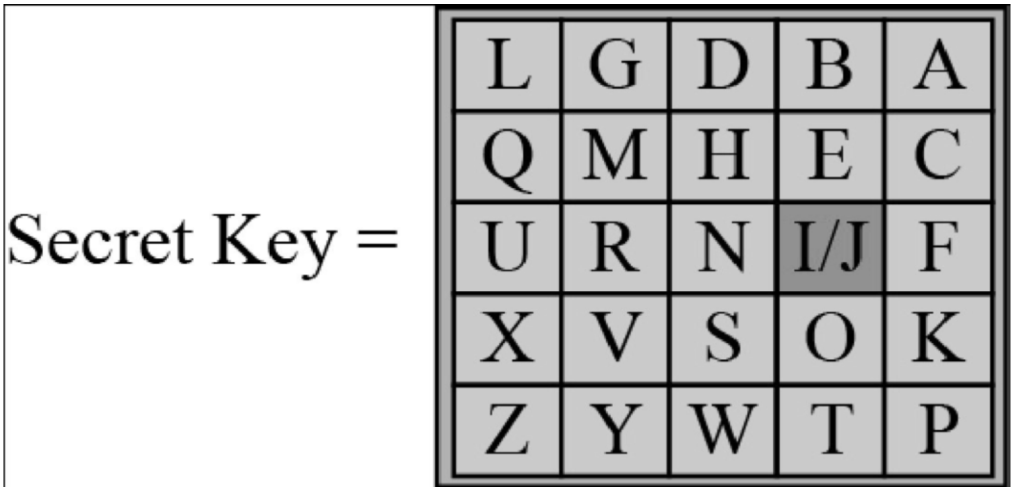
$P=P_1P_2P_3\ldots C=C_1C_2C_3\ldots \quad K=[(k_1,k_2,\ldots,k_m),\ (k_1,k_2,\ldots,k_m),\ldots]$

Encryption: $C_i=(P_i+k_i) \bmod 26$

Decryption: $P_i=(C_i-k_i) \bmod 26$

Figure: Vignere Cipher

- **Playfair Cipher:**
    1. Create a 5x5 grid with a keyword (excluding duplicates) for encryption.
    2. Process the plaintext in pairs (digraphs) and encrypt based on the grid rules.
    3. If the letters are in the same row, replace them with the letters to their immediate right (wrapping around if needed).
    4. If the letters are in the same column, replace them with the letters below.



Secret Key =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

Figure: Playfair Cipher

- **Hill Cipher:**
    1. Represent the plaintext as matrices and choose a key matrix for encryption.
    2. Multiply the plaintext matrix by the key matrix to get the ciphertext matrix.

3. Decryption involves multiplying the ciphertext matrix by the inverse of the key matrix.

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

$$\begin{aligned} C_1 &= P_1 k_{11} + P_2 k_{21} + \cdots + P_m k_{m1} \\ C_2 &= P_1 k_{12} + P_2 k_{22} + \cdots + P_m k_{m2} \\ &\cdots \\ C_m &= P_1 k_{1m} + P_2 k_{2m} + \cdots + P_m k_{mm} \end{aligned}$$

Figure: Hill Cipher

Similarities & Dissimilarities:

1. **Similarities:**
   - Both monoalphabetic and polyalphabetic ciphers are substitution ciphers that replace plaintext characters with ciphertext characters.
   - They aim to obscure the relationship between the plaintext and ciphertext to enhance security.
   - Both types of ciphers can be implemented using mathematical operations on the alphabet, such as shifting or matrix transformations.
2. **Dissimilarities:**
   - **Monoalphabetic Ciphers:**
     - Each letter in the plaintext is consistently replaced by the same letter in the ciphertext.
     - Vulnerable to frequency analysis due to fixed substitution patterns.
     - Limited key space compared to polyalphabetic ciphers.
   - **Polyalphabetic Ciphers:**
     - Each letter in the plaintext can be replaced by different letters based on the key or algorithm.
     - Resistant to frequency analysis due to varying substitution patterns.

- Larger key space, making them more secure than monoalphabetic ciphers.

The End