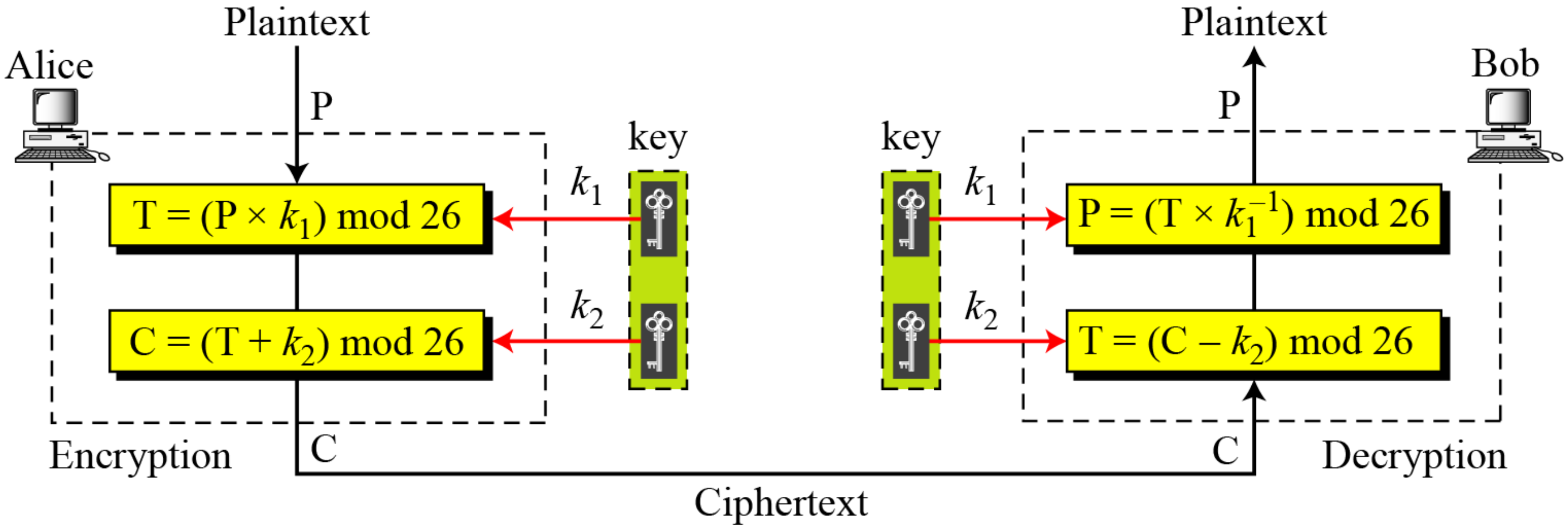
# Classical Cipher

PREPARED BY: DR. REEMA PATEL

# Affine Cipher

- Affine Ciphers




$$C = (P \times k_1 + k_2) \bmod 26$$

$$P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where $k_1^{-1}$ is the multiplicative inverse of $k_1$ and $-k_2$ is the additive inverse of $k_2$

# Affine Cipher

- In a multiplicative cipher,
  - the plaintext and ciphertext are integers in $Z_{26}$;
  - the key is an integer in $Z_{26^*}$.

- decrypt the message “ZEBBW”.
- Message is encrypted with the key pair (7, 2).

# Affine Cipher

- What is the key domain for any multiplicative cipher?
- The key needs to be in $Z_{26}*$. This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.
- We use a multiplicative cipher to encrypt the message “hello” with a key of 7. The ciphertext is “XCZZU”.

| | | |
|---|---|---|
| Plaintext: h $\rightarrow$ 07 | Encryption: $(07 \times 07)$ mod 26 | ciphertext: 23 $\rightarrow$ X |
| Plaintext: e $\rightarrow$ 04 | Encryption: $(04 \times 07)$ mod 26 | ciphertext: 02 $\rightarrow$ C |
| Plaintext: l $\rightarrow$ 11 | Encryption: $(11 \times 07)$ mod 26 | ciphertext: 25 $\rightarrow$ Z |
| Plaintext: l $\rightarrow$ 11 | Encryption: $(11 \times 07)$ mod 26 | ciphertext: 25 $\rightarrow$ Z |
| Plaintext: o $\rightarrow$ 14 | Encryption: $(14 \times 07)$ mod 26 | ciphertext: 20 $\rightarrow$ U |

# Affine Cipher

- The affine cipher uses a pair of keys in which the first key is from $Z_{26}^*$ and the second is from $Z_{26}$. The size of the key domain is $26 \times 12 = 312$.
- Use an affine cipher to encrypt the message "hello" with the key pair (7, 2).

| | | |
|---|---|---|
| P: h $\rightarrow$ 07 | Encryption: $(07 \times 7 + 2) \bmod 26$ | C: 25 $\rightarrow$ Z |
| P: e $\rightarrow$ 04 | Encryption: $(04 \times 7 + 2) \bmod 26$ | C: 04 $\rightarrow$ E |
| P: l $\rightarrow$ 11 | Encryption: $(11 \times 7 + 2) \bmod 26$ | C: 01 $\rightarrow$ B |
| P: l $\rightarrow$ 11 | Encryption: $(11 \times 7 + 2) \bmod 26$ | C: 01 $\rightarrow$ B |
| P: o $\rightarrow$ 14 | Encryption: $(14 \times 7 + 2) \bmod 26$ | C: 22 $\rightarrow$ W |

# Affine Cipher

- Use the affine cipher to decrypt the message "ZEBBW" with the key pair (7, 2) in modulus 26.

| | | |
|---|---|---|
| C: Z $\rightarrow$ 25 | Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$ | P:07 $\rightarrow$ h |
| C: E $\rightarrow$ 04 | Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$ | P:04 $\rightarrow$ e |
| C: B $\rightarrow$ 01 | Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$ | P:11 $\rightarrow$ l |
| C: B $\rightarrow$ 01 | Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$ | P:11 $\rightarrow$ l |
| C: W $\rightarrow$ 22 | Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$ | P:14 $\rightarrow$ o |

# Hill Cipher

- Invented by L. S. Hill in 1929.
- Inputs : String of English letters, A,B,…,Z.

  An $n \times n$ matrix **K**, with entries drawn from 0,1,…,25 (The matrix **K** serves as the secret key. )
- Divide the input string into blocks of size $n$.
- Identify A=0, B=1, C=2, …, Z=25.
- Encryption: Multiply each block by **K** and then reduce mod 26.
- Decryption: multiply each block by the inverse of **K**, and reduce mod 26

# Hill Cipher

- Plaintext: ATTACK Key: CDDG

So $k=\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$ Since KEY is **2x2** matrix, plaintext should be converted into vectors of length **2**

So $\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}, \begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix}, \begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

**Ciphertext C = K.P mod 26**

$$=\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \text{ X } \begin{bmatrix} A \\ T \end{bmatrix} \text{ mod } 26$$

$$=\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \text{ X } \begin{bmatrix} 0 \\ 19 \end{bmatrix} \text{ mod } 26$$

$$=\begin{bmatrix} 2*0+ & 3*19 \\ 3*0+ & 6*19 \end{bmatrix} \text{ mod } 26$$

$$=\begin{bmatrix} 57 \\ 114 \end{bmatrix} \text{ mod } 26$$

For mod 26, we are dividing numbers by 26 and considering remainders.

$$\mathbf{C} = \begin{bmatrix} 5 \\ 10 \end{bmatrix}$$, So corresponding alphabets **FK.**

**Ciphertext C = K.P mod 26**

$$=\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \text{X} \begin{bmatrix} T \\ A \end{bmatrix} \text{ mod } 26$$

$$=\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \text{X} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \text{ mod } 26$$

$$=\begin{bmatrix} 2*19+ & 3*0 \\ 3*19+ & 6*0 \end{bmatrix} \text{ mod } 26$$

$$=\begin{bmatrix} 38 \\ 57 \end{bmatrix} \text{ mod } 26$$

$$\mathbf{C} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}$$ , So corresponding alphabets **MF.**

**Ciphertext C = K.P mod 26**

$$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \text{ X } \begin{bmatrix} C \\ K \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \text{ X } \begin{bmatrix} 2 \\ 10 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 2 * 2 + & 3 * 10 \\ 3 * 2 + & 6 * 10 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 34 \\ 66 \end{bmatrix} \text{ mod } 26$$

$$\mathbf{C} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$$ , So corresponding alphabets **IO.**

So word **ATTACK** became **FKMFIO.**

# Decryption

- Find Inverse of Given Matrix
- Multiply Inverse Matrix with ciphertext against mod 26

# Example

- Plaintext: ”retreat now”
- Key Matrix:   “BACKUPABC”

$$\begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}$$

- Plaintext in group of three:

$$\begin{pmatrix} r \\ e \\ t \end{pmatrix} \begin{pmatrix} r \\ e \\ a \end{pmatrix} \begin{pmatrix} t \\ n \\ o \end{pmatrix} \begin{pmatrix} w \\ x \\ x \end{pmatrix} \qquad \begin{pmatrix} 17 \\ 4 \\ 19 \end{pmatrix} \begin{pmatrix} 17 \\ 4 \\ 0 \end{pmatrix} \begin{pmatrix} 19 \\ 13 \\ 14 \end{pmatrix} \begin{pmatrix} 22 \\ 23 \\ 23 \end{pmatrix}$$

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}\begin{pmatrix} r \\ e \\ t \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 17 \\ 4 \\ 19 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \times 17 + 0 \times 4 + 2 \times 19 \\ 10 \times 17 + 20 \times 4 + 15 \times 19 \\ 0 \times 17 + 1 \times 4 + 2 \times 19 \end{pmatrix}$$

$$= \begin{pmatrix} 55 \\ 535 \\ 42 \end{pmatrix}$$

$$= \begin{pmatrix} 3 \\ 15 \\ 16 \end{pmatrix} mod\ 26$$

$$= \begin{pmatrix} D \\ P \\ Q \end{pmatrix}$$

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}\begin{pmatrix} r \\ e \\ a \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 17 \\ 4 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \times 17 + 0 \times 4 + 2 \times 0 \\ 10 \times 17 + 20 \times 4 + 15 \times 0 \\ 0 \times 17 + 1 \times 4 + 2 \times 0 \end{pmatrix}$$

$$= \begin{pmatrix} 17 \\ 250 \\ 4 \end{pmatrix}$$

$$= \begin{pmatrix} 17 \\ 16 \\ 4 \end{pmatrix} \ mod\ 26$$

$$= \begin{pmatrix} R \\ Q \\ E \end{pmatrix}$$

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}\begin{pmatrix} t \\ n \\ o \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 19 \\ 13 \\ 14 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \times 19 + 0 \times 13 + 2 \times 14 \\ 10 \times 19 + 20 \times 13 + 15 \times 14 \\ 0 \times 19 + 1 \times 13 + 2 \times 14 \end{pmatrix}$$

$$= \begin{pmatrix} 47 \\ 660 \\ 41 \end{pmatrix}$$

$$= \begin{pmatrix} 21 \\ 10 \\ 15 \end{pmatrix} mod\ 26$$

$$= \begin{pmatrix} V \\ K \\ P \end{pmatrix}$$

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}\begin{pmatrix} w \\ x \\ x \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}\begin{pmatrix} 22 \\ 23 \\ 23 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \times 22 + 0 \times 23 + 2 \times 23 \\ 10 \times 22 + 20 \times 23 + 15 \times 23 \\ 0 \times 22 + 1 \times 23 + 2 \times 23 \end{pmatrix}$$

$$= \begin{pmatrix} 68 \\ 1025 \\ 69 \end{pmatrix}$$

$$= \begin{pmatrix} 16 \\ 11 \\ 17 \end{pmatrix} mod\ 26$$

$$= \begin{pmatrix} Q \\ L \\ R \end{pmatrix}$$

# Decryption

- Find Inverse Key Matrix

$$\begin{pmatrix} 0 & 11 & 15 \\ 7 & 0 & 1 \\ 4 & 19 & 0 \end{pmatrix}$$

$$\begin{vmatrix} 0 & 11 & 15 \\ 7 & 0 & 1 \\ 4 & 19 & 0 \end{vmatrix} = 0\begin{vmatrix} 0 & 1 \\ 19 & 0 \end{vmatrix} - 11\begin{vmatrix} 7 & 1 \\ 4 & 0 \end{vmatrix} + 15\begin{vmatrix} 7 & 0 \\ 4 & 19 \end{vmatrix}$$

- **find the determinant**

$$= 0(0-19) - 11(0-4) + 15(133-0)$$

$$= 0 + 44 + 1995$$

$$= 2039$$

$$= 11\ mod\ 26$$

# Decryption

- Inverse of determinant

$$dd^{-1} = 1 \, mod \, 26$$

$$11 \times 19 = 209 = 1 \, mod \, 26$$

# Decryption

- **find the adjugate matrix**

$$adj\begin{pmatrix} 0 & 11 & 15 \\ 7 & 0 & 1 \\ 4 & 19 & 0 \end{pmatrix} = \begin{pmatrix} +\begin{vmatrix} 0 & 1 \\ 19 & 0 \end{vmatrix} & -\begin{vmatrix} 11 & 15 \\ 19 & 0 \end{vmatrix} & +\begin{vmatrix} 11 & 15 \\ 0 & 1 \end{vmatrix} \\ -\begin{vmatrix} 7 & 1 \\ 4 & 0 \end{vmatrix} & +\begin{vmatrix} 0 & 15 \\ 4 & 0 \end{vmatrix} & -\begin{vmatrix} 0 & 15 \\ 7 & 1 \end{vmatrix} \\ +\begin{vmatrix} 7 & 0 \\ 4 & 19 \end{vmatrix} & -\begin{vmatrix} 0 & 11 \\ 4 & 19 \end{vmatrix} & +\begin{vmatrix} 0 & 11 \\ 7 & 0 \end{vmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} -19 & 285 & 11 \\ 4 & -60 & 105 \\ 133 & 44 & -77 \end{pmatrix}$$

$$= \begin{pmatrix} 7 & 25 & 11 \\ 4 & 18 & 1 \\ 3 & 18 & 1 \end{pmatrix} \mod 26$$

# Decryption

- **We need to multiply the inverse determinate (19) by each of the numbers in this new matrix**

$$19 \times \begin{pmatrix} 7 & 25 & 11 \\ 4 & 18 & 1 \\ 3 & 18 & 1 \end{pmatrix} = \begin{pmatrix} 133 & 475 & 209 \\ 76 & 342 & 19 \\ 57 & 342 & 19 \end{pmatrix} = \begin{pmatrix} 3 & 7 & 1 \\ 24 & 4 & 19 \\ 5 & 4 & 19 \end{pmatrix} \; mod\ 26$$

$$if\ K = \begin{pmatrix} 0 & 11 & 15 \\ 7 & 0 & 1 \\ 4 & 19 & 0 \end{pmatrix}, then\ K^{-1} = \begin{pmatrix} 3 & 7 & 1 \\ 24 & 4 & 19 \\ 5 & 4 & 19 \end{pmatrix}$$

# Decryption

- For decryption, multiply ciphertext with inverse key matrix mod 26.

# Columnar Transposition Cipher

- Columnar Transposition Cipher