

Cybersecurity Concepts

Prepared by Dr. Diao Salama

FNT625
Classical Encryption Techniques (part 3)

Lecture 7





مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY

Cybersecurity Concepts

Lecture 7

FNT625

Classical Encryption Techniques(part 3)

Prepared by
Dr. Diao Salama

www.midocean.ae

PLEASE
BE QUIET



10



Lecture

07

Lets Start the sixth Lecture



Classical Encryption Techniques **Part 3**



Matric Operation

Hill Cipher

Matric Operation

Hill Cipher

Matrices

Lecture

07

Operations with Matrices

Properties of Matrix Operations

The Inverse of a Matrix

Operations with Matrices

- Matrix:

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{bmatrix}_{m \times n} \in M_{m \times n}$$

(i, j) -th entry: a_{ij}

row: m

column: n

size: $m \times n$

Operations with Matrices

- i -th row vector

$$r_i = [a_{i1} \quad a_{i2} \quad \cdots \quad a_{in}]$$

row matrix

- j -th column vector

$$c_j = \begin{bmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{mj} \end{bmatrix}$$

column matrix

- Square matrix: $m = n$

Operations with Matrices

- i -th row vector

$$r_i = [a_{i1} \quad a_{i2} \quad \cdots \quad a_{in}]$$

row matrix

- j -th column vector

$$c_j = \begin{bmatrix} c_{1j} \\ c_{2j} \\ \vdots \\ c_{mj} \end{bmatrix}$$

column matrix

- Square matrix: $m = n$

Operations with Matrices

Lecture

07

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} = \begin{bmatrix} r_1 \\ r_2 \end{bmatrix}$$

$$\Rightarrow r_1 = [1 \quad 2 \quad 3], \quad r_2 = [4 \quad 5 \quad 6]$$

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} = [c_1 \quad c_2 \quad c_3]$$

$$\Rightarrow c_1 = \begin{bmatrix} 1 \\ 4 \end{bmatrix}, \quad c_2 = \begin{bmatrix} 2 \\ 5 \end{bmatrix}, \quad c_3 = \begin{bmatrix} 3 \\ 6 \end{bmatrix}$$

Operations with Matrices

- Equal matrix:

$$\text{If } A = [a_{ij}]_{m \times n}, B = [b_{ij}]_{m \times n}$$

$$\text{Then } A = B \text{ if and only if } a_{ij} = b_{ij} \quad \forall 1 \leq i \leq m, 1 \leq j \leq n$$

- Ex 1: (Equal matrix)

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \quad B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\text{If } A = B$$

$$\text{Then } a = 1, b = 2, c = 3, d = 4$$

Operations with Matrices

■ Matrix addition:

$$\text{If } A = [a_{ij}]_{m \times n}, B = [b_{ij}]_{m \times n}$$

$$\text{Then } A + B = [a_{ij}]_{m \times n} + [b_{ij}]_{m \times n} = [a_{ij} + b_{ij}]_{m \times n}$$

■ Ex 2: (Matrix addition)

$$\begin{bmatrix} -1 & 2 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 3 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} -1+1 & 2+3 \\ 0-1 & 1+2 \end{bmatrix} = \begin{bmatrix} 0 & 5 \\ -1 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 \\ -3 \\ -2 \end{bmatrix} + \begin{bmatrix} -1 \\ 3 \\ 2 \end{bmatrix} = \begin{bmatrix} 1-1 \\ -3+3 \\ -2+2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Operations with Matrices

■ Scalar multiplication:

If $A = [a_{ij}]_{m \times n}$, c : scalar

Then $cA = [ca_{ij}]_{m \times n}$

■ Matrix subtraction:

$$A - B = A + (-1)B$$

■ Ex 3: (Scalar multiplication and matrix subtraction)

$$A = \begin{bmatrix} 1 & 2 & 4 \\ -3 & 0 & -1 \\ 2 & 1 & 2 \end{bmatrix} \quad B = \begin{bmatrix} 2 & 0 & 0 \\ 1 & -4 & 3 \\ -1 & 3 & 2 \end{bmatrix}$$

Find (a) $3A$, (b) $-B$, (c) $3A - B$

Operations with Matrices

Sol:

$$(a) \quad 3A = 3 \begin{bmatrix} 1 & 2 & 4 \\ -3 & 0 & -1 \\ 2 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 3(1) & 3(2) & 3(4) \\ 3(-3) & 3(0) & 3(-1) \\ 3(2) & 3(1) & 3(2) \end{bmatrix} = \begin{bmatrix} 3 & 6 & 12 \\ -9 & 0 & -3 \\ 6 & 3 & 6 \end{bmatrix}$$

$$(b) \quad -B = (-1) \begin{bmatrix} 2 & 0 & 0 \\ 1 & -4 & 3 \\ -1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} -2 & 0 & 0 \\ -1 & 4 & -3 \\ 1 & -3 & -2 \end{bmatrix}$$

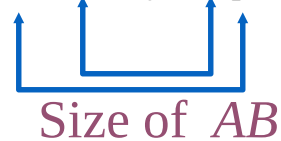
$$(c) \quad 3A - B = \begin{bmatrix} 3 & 6 & 12 \\ -9 & 0 & -3 \\ 6 & 3 & 6 \end{bmatrix} - \begin{bmatrix} 2 & 0 & 0 \\ 1 & -4 & 3 \\ -1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 6 & 12 \\ -10 & 4 & -6 \\ 7 & 0 & 4 \end{bmatrix}$$

Operations with Matrices

- Matrix multiplication:

If $A = [a_{ij}]_{m \times n}$, $B = [b_{ij}]_{n \times p}$

Then $AB = [a_{ij}]_{m \times n} [b_{ij}]_{n \times p} = [c_{ij}]_{m \times p}$



where $c_{ij} = \sum_{k=1}^n a_{ik} b_{kj} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj}$

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} b_{11} & \dots & b_{1j} & \dots & b_{1n} \\ b_{21} & \vdots & b_{2j} & \dots & b_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ b_{n1} & \dots & b_{nj} & \dots & b_{nn} \end{bmatrix} = \begin{bmatrix} c_{i1} & c_{i2} & \dots & c_{ij} & \dots & c_{in} \end{bmatrix}$$

- Notes: (1) $A+B = B+A$, (2) $AB \neq BA$

Operations with Matrices

■ Ex 4: (Find AB)

$$A = \begin{bmatrix} -1 & 3 \\ 4 & -2 \\ 5 & 0 \end{bmatrix} \quad B = \begin{bmatrix} -3 & 2 \\ -4 & 1 \end{bmatrix}$$

Sol:

$$\begin{aligned} AB &= \begin{bmatrix} (-1)(-3) + (3)(-4) & (-1)(2) + (3)(1) \\ (4)(-3) + (-2)(-4) & (4)(2) + (-2)(1) \\ (5)(-3) + (0)(-4) & (5)(2) + (0)(1) \end{bmatrix} \\ &= \begin{bmatrix} -9 & 1 \\ -4 & 6 \\ -15 & 10 \end{bmatrix} \end{aligned}$$

Operations with Matrices

- Matrix form of a system of linear equations:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$



$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

$\parallel$ $\parallel$ $\parallel$
 A x b

m linear equations



Single matrix equation

$$\underset{m \times n}{A} \underset{n \times 1}{x} = \underset{m \times 1}{b}$$

Operations with Matrices

- Transpose of a matrix:

$$\text{If } A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \in M_{m \times n}$$

$$\text{Then } A^T = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix} \in M_{n \times m}$$

Operations with Matrices

- Ex 8: (Find the transpose of the following matrix)

$$(a) A = \begin{bmatrix} 2 \\ 8 \end{bmatrix} \quad (b) A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \quad (c) A = \begin{bmatrix} 0 & 1 \\ 2 & 4 \\ 1 & -1 \end{bmatrix}$$

Sol:

$$(a) A = \begin{bmatrix} 2 \\ 8 \end{bmatrix} \Rightarrow A^T = \begin{bmatrix} 2 & 8 \end{bmatrix}$$
$$(b) A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \Rightarrow A^T = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix}$$
$$(c) A = \begin{bmatrix} 0 & 1 \\ 2 & 4 \\ 1 & -1 \end{bmatrix} \Rightarrow A^T = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 4 & -1 \end{bmatrix}$$

- Properties of transposes:

$$(1) (A^T)^T = A$$

$$(2) (A+B)^T = A^T + B^T$$

$$(3) (cA)^T = c(A^T)$$

$$(4) (AB)^T = B^T A^T$$

THEOREM Inverse of a Matrix Using Its Adjoint

If A is an invertible matrix, then

$$A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$$

Finding the Inverse of a 2x2 matrix

Step-1 First find what is called the Determinant

This is calculated as $ad-bc$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Step-2 Then swap the elements in the leading diagonal

$$\begin{bmatrix} d & b \\ c & a \end{bmatrix}$$

Step-3 Then negate the other elements

$$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Step-4 Then multiply the Matrix by 1/determinant

$$\frac{1}{ad - cb} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Find Inverse of A

Step 1 - Calc Determinant

$$A = \begin{pmatrix} 4 & 8 \\ 1 & 3 \end{pmatrix}$$

$$\text{Determinant (ad-cb)} = 4 \times 3 - 8 \times 1 = 4$$

Step 2 - Swap Elements on leading diagonal

$$\text{step2} \begin{pmatrix} 3 & 8 \\ 1 & 4 \end{pmatrix}$$

Step 3 - negate the other elements

$$\text{step3} \begin{pmatrix} 3 & -8 \\ -1 & 4 \end{pmatrix}$$

Step 4 - multiply by 1/determinant

$$\text{step4} \frac{1}{4} \begin{pmatrix} 3 & -8 \\ -1 & 4 \end{pmatrix}$$

$$A^{-1} = \begin{bmatrix} 0.75 & -2 \\ -0.25 & 1 \end{bmatrix}$$

inverse matrix

check

$$\begin{aligned}
 AA^{-1} &= \begin{bmatrix} 4 & 8 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 0.75 & -2 \\ -0.25 & 1 \end{bmatrix} \\
 &= \begin{bmatrix} 3-2 & -8+8 \\ 0.75-0.75 & -2+3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
 \end{aligned}$$

Find the inverses and check them

$$A = \begin{pmatrix} 2 & 6 \\ 1 & 5 \end{pmatrix}$$

$$A^{-1} = \frac{1}{4} \begin{pmatrix} 5 & -6 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 1.25 & -1.5 \\ -0.25 & 0.5 \end{pmatrix}$$

$$B = \begin{pmatrix} -5 & 20 \\ -1 & 2 \end{pmatrix}$$

$$B^{-1} = \frac{1}{10} \begin{pmatrix} 2 & -20 \\ 1 & -5 \end{pmatrix} = \begin{pmatrix} 0.2 & -2 \\ 0.1 & -0.5 \end{pmatrix}$$

$$C = \begin{pmatrix} 2 & 2 \\ 0 & -1 \end{pmatrix}$$

$$C^{-1} = \frac{1}{-2} \begin{pmatrix} -1 & -2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0.5 & 1 \\ 0 & -1 \end{pmatrix}$$

Find the inverses and check them

$$A = \begin{pmatrix} 2 & 6 \\ 1 & 5 \end{pmatrix}$$

$$A^{-1} = \frac{1}{4} \begin{pmatrix} 5 & -6 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 1.25 & -1.5 \\ -0.25 & 0.5 \end{pmatrix}$$

$$B = \begin{pmatrix} -5 & 20 \\ -1 & 2 \end{pmatrix}$$

$$B^{-1} = \frac{1}{10} \begin{pmatrix} 2 & -20 \\ 1 & -5 \end{pmatrix} = \begin{pmatrix} 0.2 & -2 \\ 0.1 & -0.5 \end{pmatrix}$$

$$C = \begin{pmatrix} 2 & 2 \\ 0 & -1 \end{pmatrix}$$

$$C^{-1} = \frac{1}{-2} \begin{pmatrix} -1 & -2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0.5 & 1 \\ 0 & -1 \end{pmatrix}$$

We can use A^{-1} to solve a system of equations

$$x + 3y = 1$$

$$2x + 5y = 3$$

To see how, we can re-write a system of equations as matrices.

$$A\mathbf{x} = \mathbf{b}$$

coefficient
matrix

variable
matrix

constant
matrix

$$\begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}$$

$$\begin{bmatrix} x \\ y \end{bmatrix}$$

=

$$\begin{bmatrix} 1 \\ 3 \end{bmatrix}$$

Why will it help us solve equations?

Because if we can express a system of equations in the form

$$Ax = b$$

Then we can multiply both sides by the inverse matrix

$$A^{-1}Ax = A^{-1}b$$

And we can then know the values of x because

$$A^{-1}A = I$$

$$x = A^{-1}b$$

Solving systems of equations

We can use our 2x2 matrices to express these systems of equations

$$\left. \begin{array}{rcl} x + y & = & 240 \\ x - 3y & = & 0 \end{array} \right\} \text{Becomes in matrix form}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 240 \\ 0 \end{pmatrix}$$

constants from the
left hand side

UNKNOWNNS
 $x \sim x_1$
 $y \sim x_2$

inverse matrix

constants from the
right hand side

Your Turn solve the following

$$3x + 4y = 5$$

$$5x = 7 - 6y$$

$$\begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5 \\ 7 \end{pmatrix}$$

$$\text{Answer } x = -1 \ y = 2$$

$$x + 7y = 1.24$$

$$3y - x = 0.76$$

$$\begin{pmatrix} 1 & 7 \\ -1 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1.24 \\ 0.76 \end{pmatrix}$$

$$\text{Answer } x = -0.16 \ y = 0.2$$

$$8x = 3y - 1$$

$$x + y = -7$$

$$\begin{pmatrix} 8 & -3 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1 \\ -7 \end{pmatrix}$$

$$\text{Answer } x = -2 \ y = -5$$

DETERMINANTS BY COFACTOR EXPANSION

DETERMINANTS BY COFACTOR EXPANSION

For A (2x2) matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

The expression is called the determinant of the matrix and is denoted by the symbol $\det A$ or $|A|$

the formula for A^{-1} given in Theorem is

$$A^{-1} = \frac{1}{\det(A)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

THEOREM

If A is an $n \times n$ triangular matrix (upper triangular, lower triangular, or diagonal), then $\det(A)$ is the product of the entries on the main diagonal of the matrix; that is, $\det(A) = a_{11}a_{22}\cdots a_{nn}$

EXAMPLE Determinant of an Upper Triangular Matrix

$$\begin{vmatrix} 2 & 7 & -3 & 8 & 3 \\ 0 & -3 & 7 & 5 & 1 \\ 0 & 0 & 6 & 7 & 6 \\ 0 & 0 & 0 & 9 & 8 \\ 0 & 0 & 0 & 0 & 4 \end{vmatrix} = (2)(-3)(6)(9)(4) = -1296$$

Adjoint of a Matrix

DEFINITION

If A is any $n \times n$ matrix and C_{ij} is the cofactor of a_{ij} , then the matrix

$$\begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{bmatrix}$$

is called the *matrix of cofactors from A* . The transpose of this matrix is called the *adjoint of A* and is denoted by $\text{adj}(A)$.

EXAMPLE 6 Adjoint of a Matrix

Let

$$A = \begin{bmatrix} 3 & 2 & -1 \\ 1 & 6 & 3 \\ 2 & -4 & 0 \end{bmatrix}$$

The cofactors of A are

$$\begin{aligned} C_{11} &= 12 & C_{12} &= 6 & C_{13} &= -16 \\ C_{21} &= 4 & C_{22} &= 2 & C_{23} &= 16 \\ C_{31} &= 12 & C_{32} &= -10 & C_{33} &= 16 \end{aligned}$$

so the matrix of cofactors is

$$\begin{bmatrix} 12 & 6 & -16 \\ 4 & 2 & 16 \\ 12 & -10 & 16 \end{bmatrix}$$

and the adjoint of A is

$$\text{adj}(A) = \begin{bmatrix} 12 & 4 & 12 \\ 6 & 2 & -10 \\ -16 & 16 & 16 \end{bmatrix}$$

$$A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$$

- Find the inverse of a matrix by Gauss-Jordan Elimination:

$$\left[A \mid I \right] \xrightarrow{\text{Gauss-Jordan Elimination}} \left[I \mid A^{-1} \right]$$

- Ex 2: (Find the inverse of the matrix)

$$A = \begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix}$$

Sol:

$$AX = I$$

$$\begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} x_{11} + 4x_{21} & x_{12} + 4x_{22} \\ -x_{11} - 3x_{21} & -x_{12} - 3x_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- Ex : (Find the inverse of the following matrix)

$$A = \begin{bmatrix} 1 & -1 & 0 \\ 1 & 0 & -1 \\ -6 & 2 & 3 \end{bmatrix}$$

Sol:

$$[A : I] = \begin{bmatrix} 1 & -1 & 0 & \vdots & 1 & 0 & 0 \\ 1 & 0 & -1 & \vdots & 0 & 1 & 0 \\ -6 & 2 & 3 & \vdots & 0 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{r_{12}^{(-1)}} \begin{bmatrix} 1 & -1 & 0 & \vdots & 1 & 0 & 0 \\ 0 & 1 & -1 & \vdots & -1 & 1 & 0 \\ -6 & 2 & 3 & \vdots & 0 & 0 & 1 \end{bmatrix} \xrightarrow{r_{13}^{(6)}} \begin{bmatrix} 1 & -1 & 0 & \vdots & 1 & 0 & 0 \\ 0 & 1 & -1 & \vdots & -1 & 1 & 0 \\ 0 & -4 & 3 & \vdots & 6 & 0 & 1 \end{bmatrix}$$

$$\xrightarrow{r_{23}^{(4)}} \begin{bmatrix} 1 & -1 & 0 & \vdots & 1 & 0 & 0 \\ 0 & 1 & -1 & \vdots & -1 & 1 & 0 \\ 0 & 0 & -1 & \vdots & 2 & 4 & 1 \end{bmatrix} \xrightarrow{r_3^{(-1)}} \begin{bmatrix} 1 & -1 & 0 & \vdots & 1 & 0 & 0 \\ 0 & 1 & -1 & \vdots & -1 & 1 & 0 \\ 0 & 0 & 1 & \vdots & -2 & -4 & -1 \end{bmatrix}$$

$$\xrightarrow{r_{32}^{(1)}} \begin{bmatrix} 1 & -1 & 0 & \vdots & 1 & 0 & 0 \\ 0 & 1 & 0 & \vdots & -3 & -3 & -1 \\ 0 & 0 & 1 & \vdots & -2 & -4 & -1 \end{bmatrix} \xrightarrow{r_{21}^{(1)}} \begin{bmatrix} 1 & 0 & 0 & \vdots & -2 & -3 & -1 \\ 0 & 1 & 0 & \vdots & -3 & -3 & -1 \\ 0 & 0 & 1 & \vdots & -1 & -4 & -1 \end{bmatrix}$$

$$= [I \vdots A^{-1}]$$

So the matrix A is invertible, and its inverse is

$$A^{-1} = \begin{bmatrix} -2 & -3 & -1 \\ -3 & -3 & -1 \\ -2 & -4 & -1 \end{bmatrix}$$

▪ Check:

$$AA^{-1} = A^{-1}A = I$$

Matric Operation

Hill Cipher

Hill Cipher

- ❑ The Hill Cipher was invented by Lester S. Hill in 1929
- ❑ The Hill Cipher based on linear algebra
- ❑ Encryption
 - 2 x 2 Matrix Encryption
 - 3 x 3 Matrix Encryption

Hill Cipher

- square matrix M by the equation $MM^{-1} = M^{-1}M = I$, where I is the identity matrix.

- $C = P * K \text{ mod } 26$

Hill Cipher

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Hill Cipher

□ Example of Key 2 x 2

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$\square K = \begin{pmatrix} H & I \\ L & L \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

□ plaintext message "short example"

□ P = short example

$$\square P = \begin{pmatrix} S \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

Hill Cipher

$$\square P = \begin{pmatrix} S \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

$$\square C = K * P \text{ mod } 26$$

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$\square \begin{bmatrix} k_0 & k_1 \\ k_2 & k_3 \end{bmatrix} * \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} = \begin{bmatrix} k_0 * p_0 + k_1 * p_1 \\ k_2 * p_0 + k_3 * p_1 \end{bmatrix}$$

$$\square \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} * \begin{bmatrix} 18 \\ 7 \end{bmatrix} = \begin{bmatrix} 7 * 18 + 8 * 7 \\ 11 * 18 + 11 * 7 \end{bmatrix} = \begin{bmatrix} 182 \\ 275 \end{bmatrix}$$

$$\square C = \begin{bmatrix} 182 \\ 275 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 0 \\ 15 \end{bmatrix} = \begin{bmatrix} a \\ p \end{bmatrix}$$

Hill Cipher Encryption

$$\square P = \begin{pmatrix} S \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix}$$

$$7 \times 14 + 8 \times 17 = 234$$

$$11 \times 14 + 11 \times 17 = 341$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} = \begin{pmatrix} 234 \\ 341 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} = \begin{pmatrix} 234 \\ 341 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \text{ mod } 26$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} = \begin{pmatrix} 234 \\ 341 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} A \\ D \end{pmatrix}$$

$$\square P = \begin{pmatrix} S \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix}$$

$$7 \times 19 + 8 \times 4 = 165$$

$$11 \times 19 + 11 \times 4 = 253$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 165 \\ 253 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 165 \\ 253 \end{pmatrix} = \begin{pmatrix} 9 \\ 19 \end{pmatrix} \text{ mod } 26$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 165 \\ 253 \end{pmatrix} = \begin{pmatrix} 9 \\ 19 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} J \\ T \end{pmatrix}$$

Hill Cipher Encryption

$$\square P = \begin{pmatrix} S \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix}$$

$$7 \times 23 + 8 \times 0 = 161$$

$$11 \times 23 + 11 \times 0 = 253$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} = \begin{pmatrix} 161 \\ 253 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} = \begin{pmatrix} 161 \\ 253 \end{pmatrix} = \begin{pmatrix} 5 \\ 19 \end{pmatrix} \text{ mod } 26$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} = \begin{pmatrix} 161 \\ 253 \end{pmatrix} = \begin{pmatrix} 5 \\ 19 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} F \\ T \end{pmatrix}$$

Hill Cipher Encryption

$$\square P = \begin{pmatrix} S \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix}$$

$$7 \times 12 + 8 \times 15 = 204$$

$$11 \times 12 + 11 \times 15 = 297$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 204 \\ 297 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 204 \\ 297 \end{pmatrix} = \begin{pmatrix} 22 \\ 11 \end{pmatrix} \text{ mod } 26$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 204 \\ 297 \end{pmatrix} = \begin{pmatrix} 22 \\ 11 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} W \\ L \end{pmatrix}$$

$$\square P = \begin{pmatrix} S \\ h \end{pmatrix} \begin{pmatrix} o \\ r \end{pmatrix} \begin{pmatrix} t \\ e \end{pmatrix} \begin{pmatrix} x \\ a \end{pmatrix} \begin{pmatrix} m \\ p \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 18 \\ 7 \end{pmatrix} \begin{pmatrix} 14 \\ 17 \end{pmatrix} \begin{pmatrix} 19 \\ 4 \end{pmatrix} \begin{pmatrix} 23 \\ 0 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix}$$

$$7 \times 11 + 8 \times 4 = 109$$

$$11 \times 11 + 11 \times 4 = 165$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 109 \\ 165 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 109 \\ 165 \end{pmatrix} = \begin{pmatrix} 5 \\ 9 \end{pmatrix} \text{ mod } 26$$

$$\begin{pmatrix} H & I \\ L & L \end{pmatrix} \begin{pmatrix} l \\ e \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 11 \\ 4 \end{pmatrix} = \begin{pmatrix} 109 \\ 165 \end{pmatrix} = \begin{pmatrix} 5 \\ 9 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} F \\ J \end{pmatrix}$$

$$\square C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix}$$

□ This gives us a final ciphertext of "APADJ TFTWLFJ"

$$\square C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix}$$

$\square$ This gives us a final ciphertext of "APADJ TFTWLFJ"

$$\square K = \begin{pmatrix} H & I \\ L & L \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

$\square$ We want to find K^{-1}

□ *Step 1 – Find the Multiplicative Inverse of the Determinant*

➤ $D(K) = 7 * 11 - 8 * 11 = -11 \bmod 26 = 15$

➤ $DD^{-1} = 1 \bmod 26 = 15 * D^{-1}$

➤ Try and Test $1 \bmod 26 = 105$

➤ $D^{-1} = 7$

Hill Cipher Decryption

□ *Step 2 – Find the Adjugate Matrix of Key*

$$\blacktriangleright \text{adj} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$$\blacktriangleright \text{adj} \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} = \begin{pmatrix} 11 & -8 \\ -11 & 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix}$$

□ *Step 3 Multiply the Multiplicative Inverse of the Determinant
by the Adjugate Matrix*

$$\square 7 * \begin{pmatrix} 11 & 18 \\ 15 & 7 \end{pmatrix} = \begin{pmatrix} 77 & 126 \\ 165 & 49 \end{pmatrix} \text{ mod } 26 = \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} = K^{-1}$$

$$\square C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \end{pmatrix}$$

$$\begin{aligned} \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} A \\ P \end{pmatrix} &= \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 0 \\ 15 \end{pmatrix} \\ &= \begin{pmatrix} 25 \times 0 + 22 \times 15 \\ 1 \times 0 + 23 \times 15 \end{pmatrix} \\ &= \begin{pmatrix} 330 \\ 345 \end{pmatrix} \\ &= \begin{pmatrix} 18 \\ 7 \end{pmatrix} \text{ mod } 26 \\ &= \begin{pmatrix} s \\ h \end{pmatrix} \end{aligned}$$

$$\square C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \end{pmatrix}$$

$$\begin{aligned} \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} A \\ D \end{pmatrix} &= \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} \\ &= \begin{pmatrix} 25 \times 0 + 22 \times 3 \\ 1 \times 0 + 23 \times 3 \end{pmatrix} \\ &= \begin{pmatrix} 66 \\ 69 \end{pmatrix} \\ &= \begin{pmatrix} 14 \\ 17 \end{pmatrix} \text{ mod } 26 \\ &= \begin{pmatrix} 0 \\ r \end{pmatrix} \end{aligned}$$

$$\square C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \end{pmatrix}$$

$$\begin{aligned} \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} J \\ T \end{pmatrix} &= \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix} \\ &= \begin{pmatrix} 25 \times 9 + 22 \times 19 \\ 1 \times 9 + 23 \times 19 \end{pmatrix} \\ &= \begin{pmatrix} 643 \\ 446 \end{pmatrix} \\ &= \begin{pmatrix} 19 \\ 4 \end{pmatrix} \text{ mod } 26 \\ &= \begin{pmatrix} t \\ e \end{pmatrix} \end{aligned}$$

$$\square C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \end{pmatrix}$$

$$\begin{aligned} \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} F \\ T \end{pmatrix} &= \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \\ &= \begin{pmatrix} 25 \times 5 + 22 \times 19 \\ 1 \times 5 + 23 \times 19 \end{pmatrix} \\ &= \begin{pmatrix} 543 \\ 442 \end{pmatrix} \\ &= \begin{pmatrix} 23 \\ 0 \end{pmatrix} \text{ mod } 26 \\ &= \begin{pmatrix} x \\ a \end{pmatrix} \end{aligned}$$

$$\square C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \end{pmatrix}$$

$$\begin{aligned} \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} W \\ L \end{pmatrix} &= \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix} \\ &= \begin{pmatrix} 25 \times 22 + 22 \times 11 \\ 1 \times 22 + 23 \times 11 \end{pmatrix} \\ &= \begin{pmatrix} 792 \\ 275 \end{pmatrix} \\ &= \begin{pmatrix} 12 \\ 15 \end{pmatrix} \text{ mod } 26 \\ &= \begin{pmatrix} m \\ p \end{pmatrix} \end{aligned}$$

$$\square C = \begin{pmatrix} a \\ p \end{pmatrix} \begin{pmatrix} a \\ d \end{pmatrix} \begin{pmatrix} j \\ t \end{pmatrix} \begin{pmatrix} f \\ t \end{pmatrix} \begin{pmatrix} w \\ l \end{pmatrix} \begin{pmatrix} f \\ j \end{pmatrix} = \begin{pmatrix} 0 \\ 15 \end{pmatrix} \begin{pmatrix} 0 \\ 3 \end{pmatrix} \begin{pmatrix} 9 \\ 19 \end{pmatrix} \begin{pmatrix} 5 \\ 19 \end{pmatrix} \begin{pmatrix} 22 \\ 11 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \end{pmatrix}$$

$$\begin{aligned} \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} F \\ J \end{pmatrix} &= \begin{pmatrix} 25 & 22 \\ 1 & 23 \end{pmatrix} \begin{pmatrix} 5 \\ 9 \end{pmatrix} \\ &= \begin{pmatrix} 25 \times 5 + 22 \times 9 \\ 1 \times 5 + 23 \times 9 \end{pmatrix} \\ &= \begin{pmatrix} 323 \\ 212 \end{pmatrix} \\ &= \begin{pmatrix} 11 \\ 4 \end{pmatrix} \text{ mod } 26 \\ &= \begin{pmatrix} l \\ e \end{pmatrix} \end{aligned}$$

□ Using Hill Cipher how to implement 3x3 matrix encryption ? The key for a hill cipher is a matrix

e.g. $k = \begin{pmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{pmatrix}$ and **message**= ATTACK AT DAWN



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

