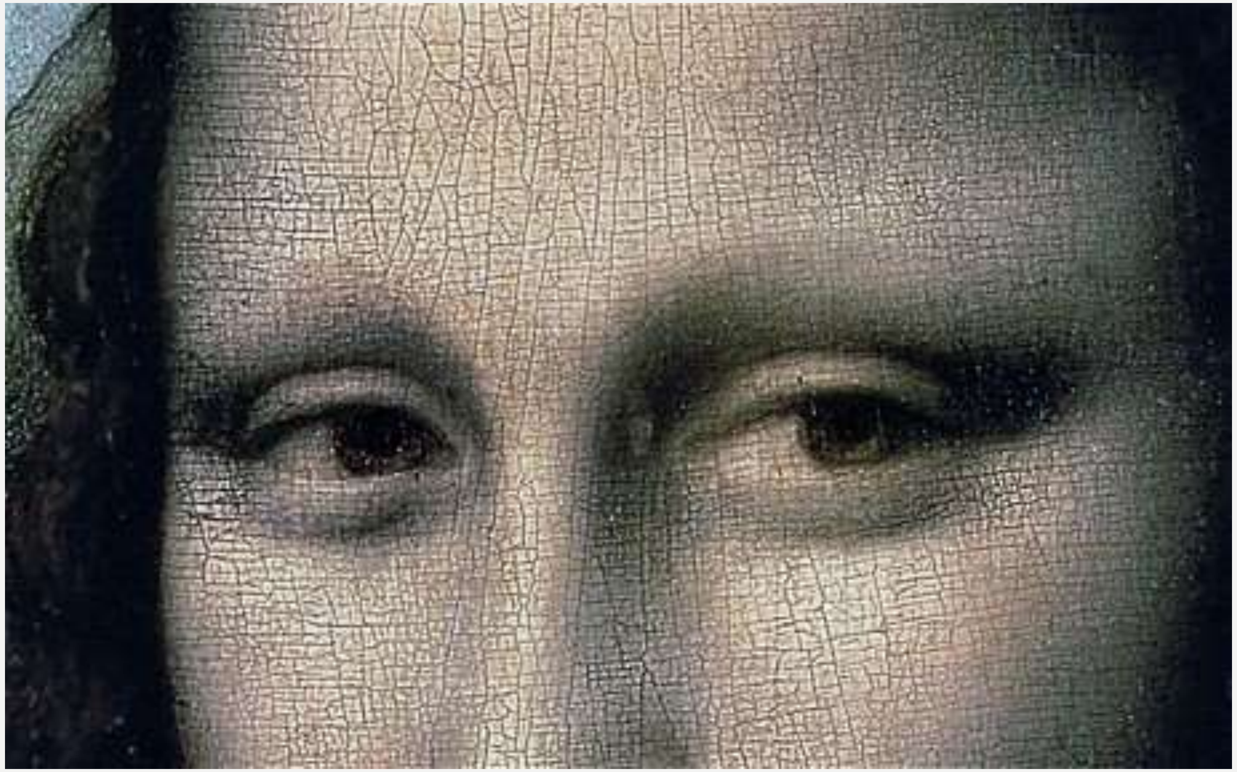
HILL CIPHER

Since times , security of data to maintain its confidentially has been major issue.

Codes form an important part of history starting from painting of da vinci and Michelangelo



TERMINOLOGY

- **Encipher/ encode/ encrypt** : A set of steps that converts information into a secret text (not for all).
- **Plaintext** : Original information
- **Ciphertext** : Encrypted form of plaintext. It contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it.

CRYTOGRAPHY

- a **cipher** (or cypher) is an algorithm for performing encryption or decryption

- Cryptography is the study of Secret (crypto-)-Writing (-graphy).It is the science or art of

  encompassing the principles and methods of transforming an intelligible message into

  one that is intelligible and then transforming the message back to its original for

ENCRYPTION TECHNIQUE

- There are basically two types of encryption techniques

- Substitution :In this technique letters of plaintext are replaced by or by numbers and symbols.

- Transposition: Transposition (or permutation) does not alter any of the bits in the plaintext, but instant moves the position around within it.

CAESAR CIPHER

- Caesar Cipher replaces each letter of the message by a fixed letter a fixed distance away

For example:

Plaintext: I CAME I SAW I CONQUERED

Cipher text: L FDPH L VDZ L FRQTXHUHG

Mapping is:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Can describe the Cipher as:

Encryption: $C=E\ (P)=(P+3)\text{mod } 26$

Decryption: $P=D(C)\ =(C-3)\ \text{mod}26$

PLAY FAIR CIPHER

- The technique encrypts pairs of letters, instead of single letters as in the simple substitution cipher.
- The Playfair is significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it.
- A typical scenario for Playfair use would be to protect important secrets during actual combat. By the time the enemy cryptanalysts could break the message the information was useless to them.

Original Text	Cipher Text
SECRET MESSAGE	NO RD KU NK QZ PC ND
SECRETMESSAGE	NORDKUNKQZPCND
SE CR ET ME SX SA GE	

MONO-ALPHABETIC-CIPHER

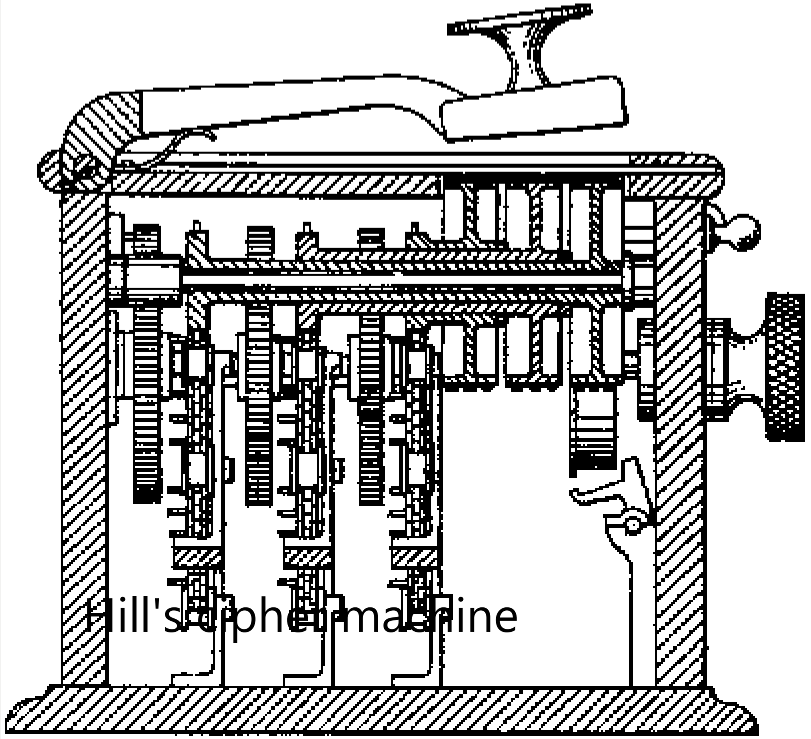
- A *monoalphabetic substitution cipher*, also known as a simple substitution cipher, relies on a fixed replacement structure. That, is if "a" is encrypted to "R", then every time we see the letter "a" in the plaintext, we replace it with the letter "R" in the ciphertext.

- A B C D E F G H

  f g h I j k l m n o p

HILL CIPHERS

- The core of Hill-cipher is matrix manipulations. It is a multi-letter cipher, developed by the mathematician Lester Hill in 1929.
- Uses matrices to encrypt and decrypt
- Uses modular arithmetic (Mod 26)

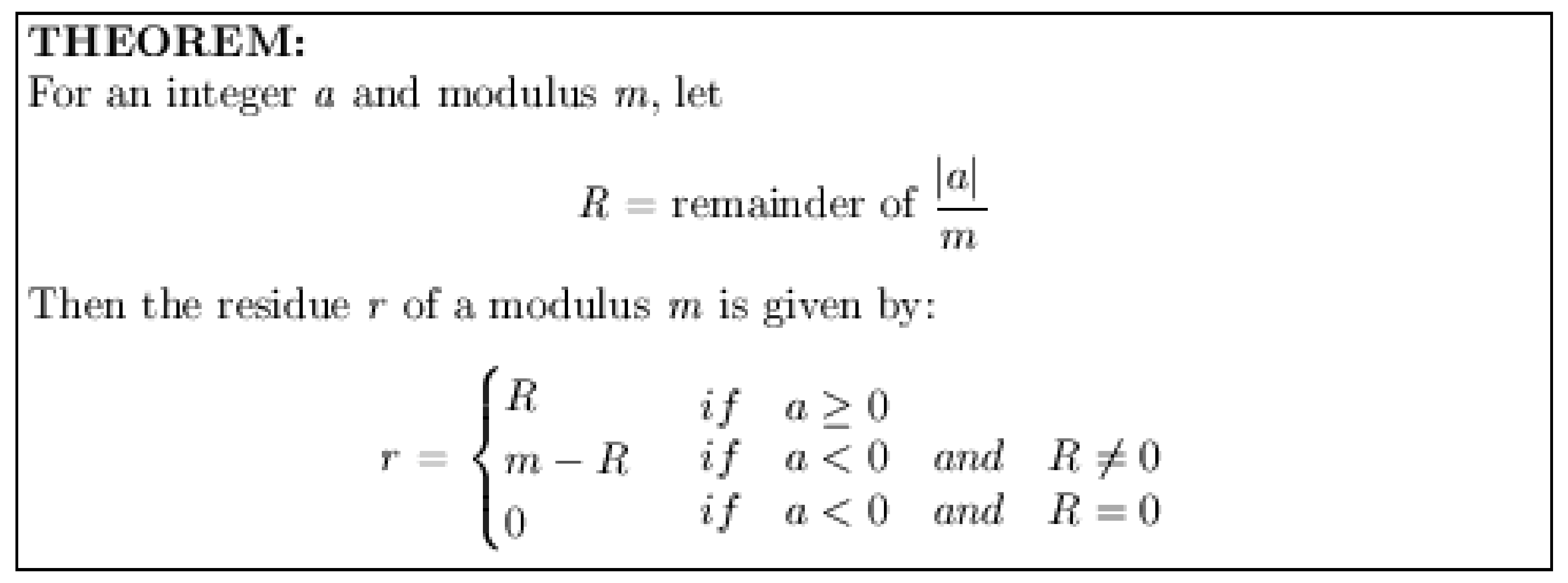


Hill's cipher machine

HISTORY

- Invented by Lester S. Hill in 1929.
- The Hill cipher is a polygraphic substitution cipher based on linear algebra, as it can work on digraphs, trigraphs (3 letter blocks) or theoretically any sized blocks.
- To counter charges that his system was too complicated for day to day use, Hill constructed a cipher machine for his system using a series of geared wheels and chains. However, the machine never really sold.

MODULUS THEOREM



THEOREM:
For an integer a and modulus m, let

$$R = \text{remainder of } \frac{|a|}{m}$$

Then the residue r of a modulus m is given by:

$$r = \begin{cases} R & if \quad a \geq 0 \\ m - R & if \quad a < 0 \quad and \quad R \neq 0 \\ 0 & if \quad a < 0 \quad and \quad R = 0 \end{cases}$$

MODULAR INVERSES

- Inverse of 2 is ½ (2 · ½ = 1)
- Matrix Inverse: $AA^{-1} = I = A^{-1}A$
- **modular inverse** of an integer *a* modulo *m* is an integer *x* such that **a x = 1 (mod m).**

For example:

a = 3 and m = 26.

3 x = 1 (mod 26) => x must be 9

i.e. modular inverse of 3 modulo 26 is 9.

- The modular inverse of *a* modulo *m* exists if and only if *a* and *m* are coprime

  i.e. If Gcd(a, m) = 1.

HILL CIPHER MATRICES

- One matrix to encrypt, one to decrypt
- Must be n x n, invertible matrices
- Decryption matrix must be modular inverse of encryption matrix in Mod 26
- the determinant of encryption matrix must be nonzero, and must not be divisible by 2 or 13
- If the determinant of encryption matrix is 0, or divisible by 2 or 13 then it has common factors with 26 so modular inverse doesn’t exist and the matrix cannot be used in the Hill cipher.

ENCRYPTION

- Assign each letter in alphabet a number between 0 and 25

  a=0,b=1,c=2……., z=25
- Change message into 2 x 1 letter vectors
- Change each vector into 2 x 1 numeric vectors
- Multiply each numeric vector by encryption matrix
- Convert product vectors to letters

EXAMPLE

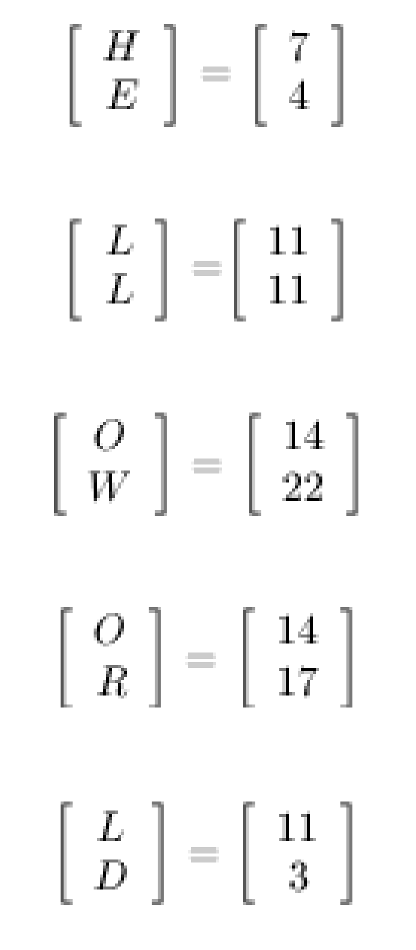
LETTER TO NUMBER SUBSTITUTION

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

CHANGE MESSAGE TO VECTORS

Message to encrypt = HELLO WORLD



$$\begin{bmatrix} H \\ E \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix}$$

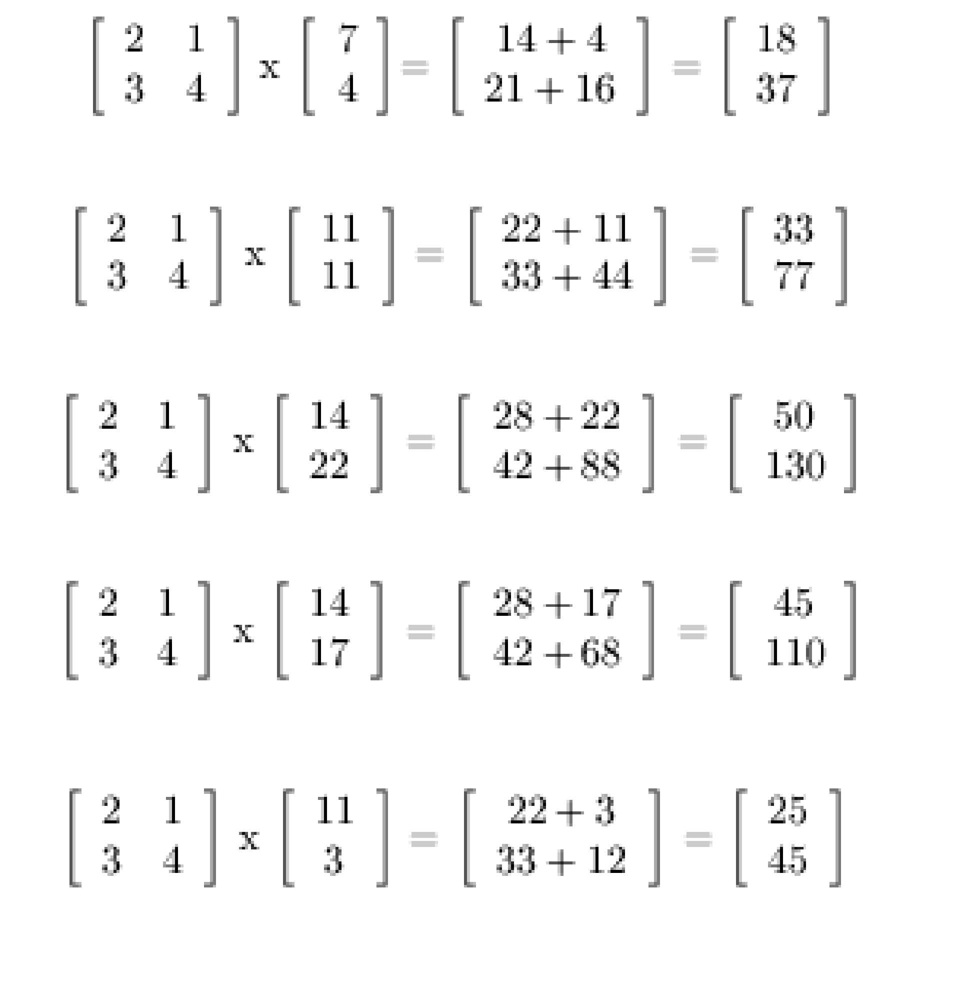
$$\begin{bmatrix} L \\ L \end{bmatrix} = \begin{bmatrix} 11 \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} O \\ W \end{bmatrix} = \begin{bmatrix} 14 \\ 22 \end{bmatrix}$$

$$\begin{bmatrix} O \\ R \end{bmatrix} = \begin{bmatrix} 14 \\ 17 \end{bmatrix}$$

$$\begin{bmatrix} L \\ D \end{bmatrix} = \begin{bmatrix} 11 \\ 3 \end{bmatrix}$$

MULTIPLY MATRIX BY VECTORS



$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \text{x} \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 14+4 \\ 21+16 \end{bmatrix} = \begin{bmatrix} 18 \\ 37 \end{bmatrix}$$

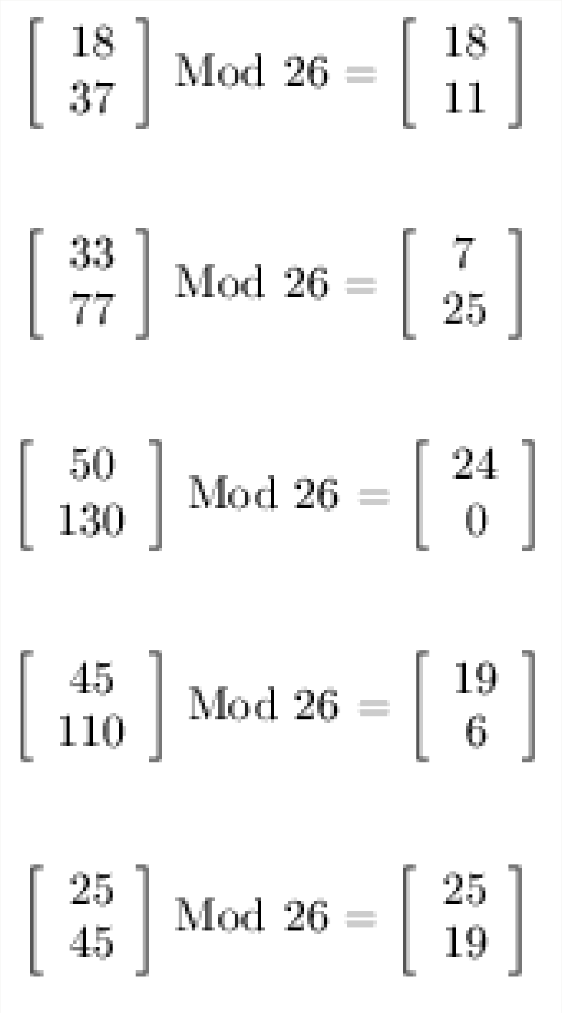
$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \text{x} \begin{bmatrix} 11 \\ 11 \end{bmatrix} = \begin{bmatrix} 22+11 \\ 33+44 \end{bmatrix} = \begin{bmatrix} 33 \\ 77 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \text{x} \begin{bmatrix} 14 \\ 22 \end{bmatrix} = \begin{bmatrix} 28+22 \\ 42+88 \end{bmatrix} = \begin{bmatrix} 50 \\ 130 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \text{x} \begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} 28+17 \\ 42+68 \end{bmatrix} = \begin{bmatrix} 45 \\ 110 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix} \text{x} \begin{bmatrix} 11 \\ 3 \end{bmatrix} = \begin{bmatrix} 22+3 \\ 33+12 \end{bmatrix} = \begin{bmatrix} 25 \\ 45 \end{bmatrix}$$

CONVERT TO MOD 26



$$\begin{bmatrix} 18 \\ 37 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 18 \\ 11 \end{bmatrix}$$

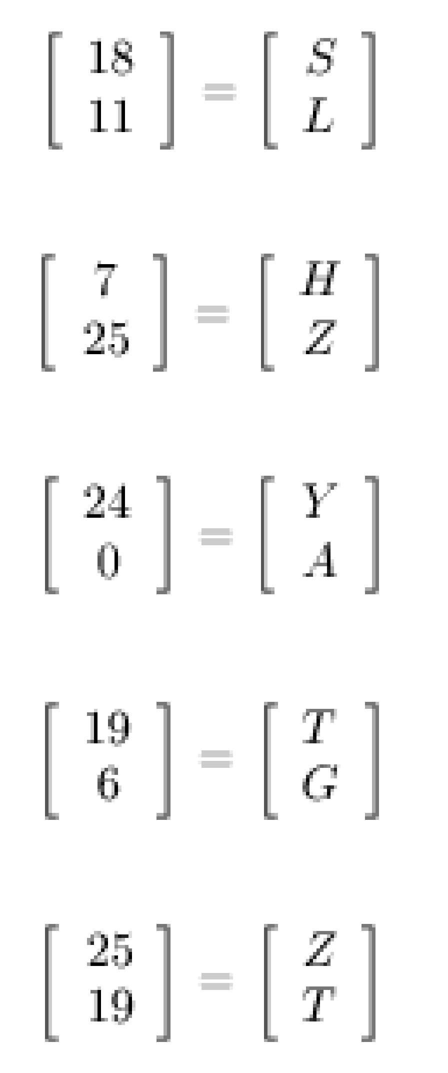
$$\begin{bmatrix} 33 \\ 77 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 7 \\ 25 \end{bmatrix}$$

$$\begin{bmatrix} 50 \\ 130 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 24 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 45 \\ 110 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 19 \\ 6 \end{bmatrix}$$

$$\begin{bmatrix} 25 \\ 45 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 25 \\ 19 \end{bmatrix}$$

CONVERT NUMBERS TO LETTERS



$$\begin{bmatrix} 18 \\ 11 \end{bmatrix} = \begin{bmatrix} S \\ L \end{bmatrix}$$

$$\begin{bmatrix} 7 \\ 25 \end{bmatrix} = \begin{bmatrix} H \\ Z \end{bmatrix}$$

$$\begin{bmatrix} 24 \\ 0 \end{bmatrix} = \begin{bmatrix} Y \\ A \end{bmatrix}$$

$$\begin{bmatrix} 19 \\ 6 \end{bmatrix} = \begin{bmatrix} T \\ G \end{bmatrix}$$

$$\begin{bmatrix} 25 \\ 19 \end{bmatrix} = \begin{bmatrix} Z \\ T \end{bmatrix}$$

HELLO WORLD has been encrypted to
SLHZY ATGZT

DECRYPTION MATRIX

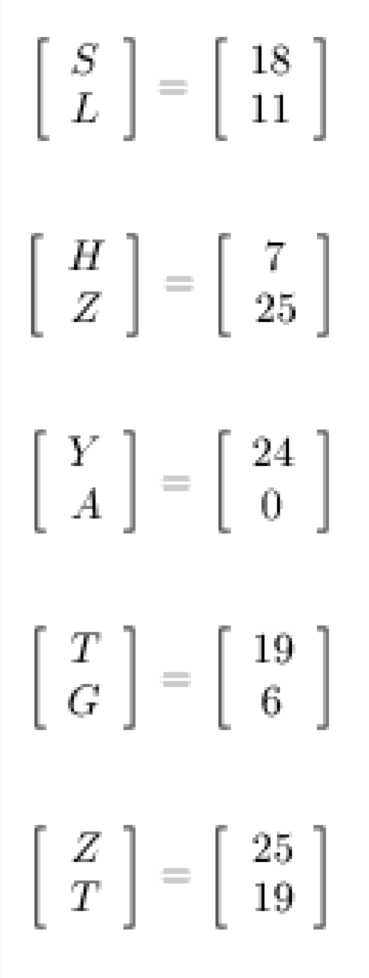
- Calculate determinant of given encryption matrix A, det A
- Make sure that det A has a modular inverse for Mod 26
- Calculate the adjoint of A, adj A
- Multiply adj A by modular inverse of det A
- Calculate Mod 26 of the result to get B
- Use A to encrypt, B to decrypt

DECRYPTION

- Change message into 2 x 1 letter vectors
- Change each vector into 2 x 1 numeric vectors
- Multiply each numeric vector by decryption matrix
- Convert new vectors to letters

CHANGE MESSAGE TO VECTORS

Message to encrypt = SLHZYATGZT



$$\begin{bmatrix} S \\ L \end{bmatrix} = \begin{bmatrix} 18 \\ 11 \end{bmatrix}$$

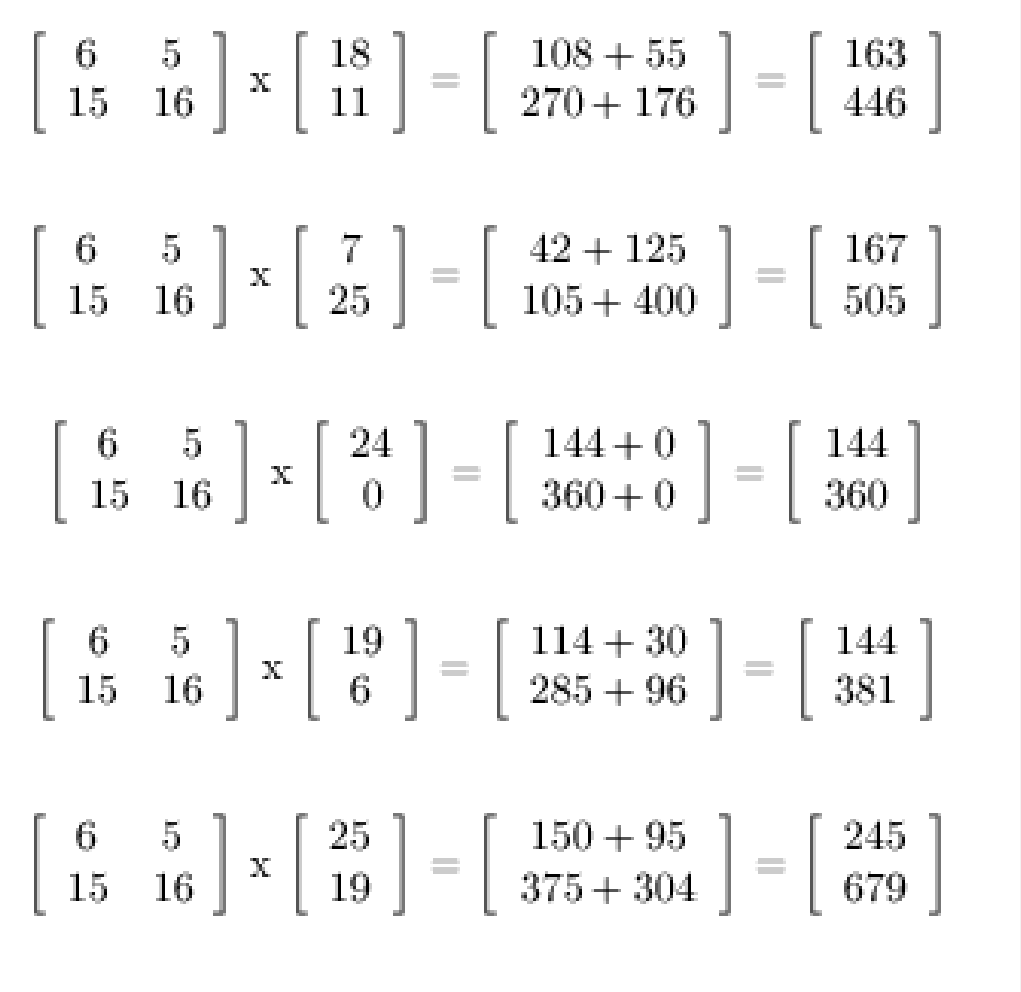
$$\begin{bmatrix} H \\ Z \end{bmatrix} = \begin{bmatrix} 7 \\ 25 \end{bmatrix}$$

$$\begin{bmatrix} Y \\ A \end{bmatrix} = \begin{bmatrix} 24 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} T \\ G \end{bmatrix} = \begin{bmatrix} 19 \\ 6 \end{bmatrix}$$

$$\begin{bmatrix} Z \\ T \end{bmatrix} = \begin{bmatrix} 25 \\ 19 \end{bmatrix}$$

MULTIPLY MATRIX BY VECTORS



$$\begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix} \text{x} \begin{bmatrix} 18 \\ 11 \end{bmatrix} = \begin{bmatrix} 108 + 55 \\ 270 + 176 \end{bmatrix} = \begin{bmatrix} 163 \\ 446 \end{bmatrix}$$

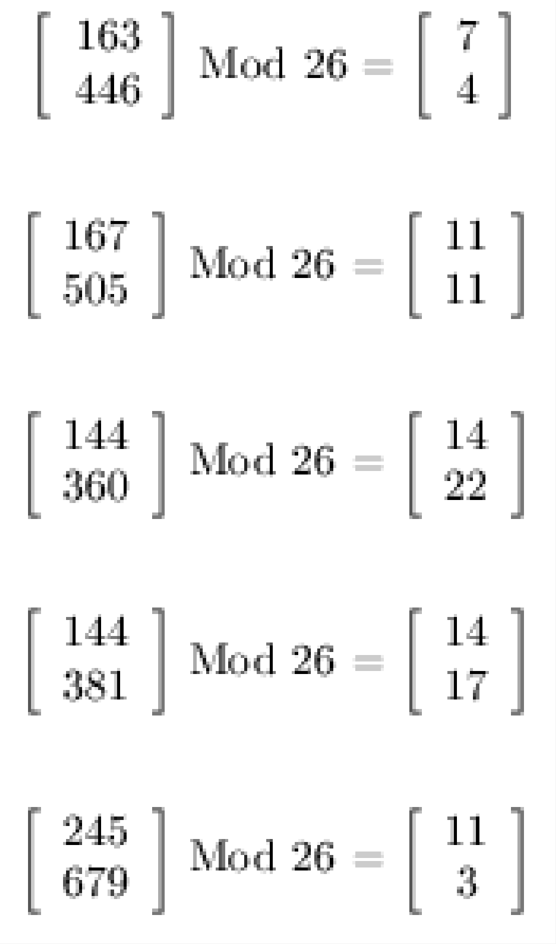
$$\begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix} \text{x} \begin{bmatrix} 7 \\ 25 \end{bmatrix} = \begin{bmatrix} 42 + 125 \\ 105 + 400 \end{bmatrix} = \begin{bmatrix} 167 \\ 505 \end{bmatrix}$$

$$\begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix} \text{x} \begin{bmatrix} 24 \\ 0 \end{bmatrix} = \begin{bmatrix} 144 + 0 \\ 360 + 0 \end{bmatrix} = \begin{bmatrix} 144 \\ 360 \end{bmatrix}$$

$$\begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix} \text{x} \begin{bmatrix} 19 \\ 6 \end{bmatrix} = \begin{bmatrix} 114 + 30 \\ 285 + 96 \end{bmatrix} = \begin{bmatrix} 144 \\ 381 \end{bmatrix}$$

$$\begin{bmatrix} 6 & 5 \\ 15 & 16 \end{bmatrix} \text{x} \begin{bmatrix} 25 \\ 19 \end{bmatrix} = \begin{bmatrix} 150 + 95 \\ 375 + 304 \end{bmatrix} = \begin{bmatrix} 245 \\ 679 \end{bmatrix}$$

CONVERT TO MOD 26



$$\begin{bmatrix} 163 \\ 446 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 7 \\ 4 \end{bmatrix}$$

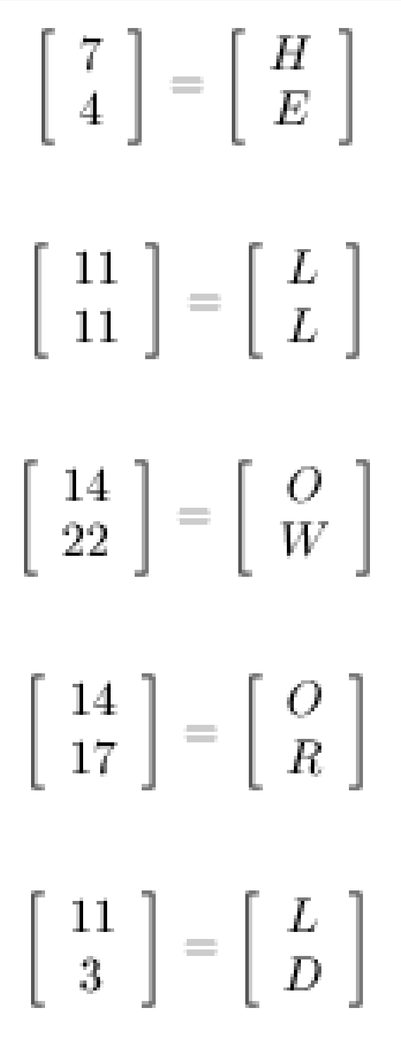
$$\begin{bmatrix} 167 \\ 505 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 11 \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} 144 \\ 360 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 14 \\ 22 \end{bmatrix}$$

$$\begin{bmatrix} 144 \\ 381 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 14 \\ 17 \end{bmatrix}$$

$$\begin{bmatrix} 245 \\ 679 \end{bmatrix} \text{Mod } 26 = \begin{bmatrix} 11 \\ 3 \end{bmatrix}$$

CONVERT NUMBERS TO LETTERS



$$\begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} H \\ E \end{bmatrix}$$

$$\begin{bmatrix} 11 \\ 11 \end{bmatrix} = \begin{bmatrix} L \\ L \end{bmatrix}$$

$$\begin{bmatrix} 14 \\ 22 \end{bmatrix} = \begin{bmatrix} O \\ W \end{bmatrix}$$

$$\begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} O \\ R \end{bmatrix}$$

$$\begin{bmatrix} 11 \\ 3 \end{bmatrix} = \begin{bmatrix} L \\ D \end{bmatrix}$$

SLHZYATGZT has been decrypted to
HELLO WORLD

OBJECTIVES

- In the next presentation, we will see how to break through the hill cypher, requirements for breaking it and we will one or two examples using that.

THANK YOU

REFERENCES

- Wikipedia
  - https://en.wikipedia.org/wiki/Hill_cipher