ISC

Week#4 – Lab next week
(26 Jan 2024 – Holiday – Home study)

Dhiren Patel

Polygram ciphers – Hill cipher

- Polygram ciphers are a type of substitution cipher that encrypts text by substituting groups of letters (called "polygrams") rather than individual letters.
- They operate on groups of letters (typically 2-6 letters per group)
- Increase difficulty of frequency analysis attacks
- Examples are: Playfair cipher (Di-gram cipher) and Hill cipher

Hill cipher

Invented by mathematician Lester S. Hill in 1929 (paper - "Cryptography in an Algebraic Alphabet")

Key characteristics:

- A specific type of polygram cipher that uses matrix multiplication to encrypt text
- Employs a square matrix as the key

Advantages:

- Can encrypt multiple letters at once
- Difficult to break without the key
- When operating on 2 symbols at once, a Hill cipher offers no particular advantage over Playfair.
- As the dimension increases, the Hill cipher rapidly becomes infeasible for a human to operate by hand.

Encryption and Decryption – Hill cipher

- Encryption process:
- Assign numerical values to letters (e.g., A=0, B=1, ..., Z=25)
- Divide plaintext into blocks of letters equal to the size of the key matrix
- Represent each block of plaintext as a column vector
- Multiply the column vector by the key matrix (modulo 26) to get the ciphertext vector
- Convert the ciphertext vector back into letters
- Decryption process:
- Use the inverse of the key matrix to multiply ciphertext vectors and obtain plaintext

Example#1

Let

$$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

Letter	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
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

be the key and suppose the plaintext message is 'HELP'. Then this plaintext is represented by two pairs

$$HELP \to \begin{pmatrix} H \\ E \end{pmatrix}, \begin{pmatrix} L \\ P \end{pmatrix} \to \begin{pmatrix} 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 11 \\ 15 \end{pmatrix}$$

Then we compute

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 7 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 8 \end{pmatrix} \pmod{26}, \text{ and}$$

$$\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 11 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 19 \end{pmatrix} \pmod{26}$$

Cipher text ➔ $\begin{pmatrix} H \\ I \end{pmatrix}, \begin{pmatrix} A \\ T \end{pmatrix}$

Example#1 Decryption

- Inverse matrix of key is $\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}$

$$HIAT \rightarrow \begin{pmatrix} H \\ I \end{pmatrix}, \begin{pmatrix} A \\ T \end{pmatrix} \rightarrow \begin{pmatrix} 7 \\ 8 \end{pmatrix}, \begin{pmatrix} 0 \\ 19 \end{pmatrix}$$

Then we compute

$$\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} 241 \\ 212 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 4 \end{pmatrix} \pmod{26}, \text{ and}$$

$$\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \begin{pmatrix} 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 323 \\ 171 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 15 \end{pmatrix} \pmod{26}$$

Therefore,

$$\begin{pmatrix} 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 11 \\ 15 \end{pmatrix} \rightarrow \begin{pmatrix} H \\ E \end{pmatrix}, \begin{pmatrix} L \\ P \end{pmatrix} \rightarrow HELP.$$

Hill cipher – example#2

- Encrypt "Meet B" using a 2 X 2 Hill Cipher
- with the keys k = $\begin{bmatrix} 3 & 1 \\ 5 & 2 \end{bmatrix}$ and decryption key k^{-1} = $\begin{bmatrix} 2 & -1 \\ -5 & 3 \end{bmatrix}$
- $c_1 = (k_{11}x_1 + k_{12}x_2) \bmod 26$
- $c_2 = (k_{21}x_1 + k_{22}x_2) \bmod 26$
- Plain text is: me et bx (x added to complete last (pair) digram)
- Numerical equivalent = 12 4 4 19 1 23, read as pairs x_1x_2, x_3x_4, x_5x_6.

- $c_1 = (36 + 4) \bmod 26 = 14$ (O), $c_2 = (60 + 8) \bmod 26 = 16$ (Q)
- Encrypted as → oq fg az

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Hill Cipher Example#2 (Decryption)

- Decryption key $K^{-1} = \begin{bmatrix} 2 & -1 \\ -5 & 3 \end{bmatrix}$
- ***Decryption X*** $= D_K(C) = \boldsymbol{K^{-1}C} \bmod 26$
- $x_1 = (k_{11}c_1 + k_{12}c_2) \bmod 26$
- $x_2 = (k_{21}c_1 + k_{22}c_2) \bmod 26$
- oq fg az <14, 16><5,6><0,25>
- $x_1 = (28 - 16) \bmod 26 = 12 = m$
- $x_2 = (-70 + 48) \bmod 26 = -22 = 4 = e$
- me et bx

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Hill cipher example#3 (Tri-gram)

- 3x3 matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n × n matrices (modulo 26)
- Consider the message 'ACT'

Key matrix is ➔ $$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Encryption of “ACT” and “CAT”

Thus the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

which corresponds to a ciphertext of 'POH'. Now, suppose that our message is instead 'CAT', or:

$$\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix}$$

Letter	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
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

This time, the enciphered vector is given by:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}\begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} = \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$$

Decryption

Letter	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
Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- Key inverse matrix is ➔

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \pmod{26} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}$$

Taking the previous example ciphertext of 'POH', we get:

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} = \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

which gets us back to 'ACT', as expected.

Hill cipher .. More examples

- 3 X 3 Hill cipher using tri-grams
- Encrypt “ACT” using given key matrix and decrypt its corresponding cipher text using given inverse key matrix
- E.g. key matrix $K = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 0 & -2 \end{bmatrix}$ and $K^{-1} = \begin{bmatrix} 2 & -2 & -1 \\ -4 & 5 & 3 \\ 1 & -1 & -1 \end{bmatrix}$

Lab next week

- Part 1: Implement Hill Cipher (2 x 2)
- Input plaintext and key matrix and inverse key matrix
- Output ciphertext
- Input ciphertext and decrypt it to plaintext
- Part 2:
- Generating and testing key matrix – there has to be suitable inverse matrix for use for Hill cipher
- Part 3: Implement Hill Cipher (n x n), where n could be 2 to 5

More – Hill cipher

What are the flaws here ?
1.Key matrix ne select karvanu
 (karan ae matrix nu to inverse pan exists karvu joie.)
2.Matrix ni amuk properties to ana predictable banavi de 6e

- **Implementation issues**
- Key generation and distribution
- Matrix and its inverse (elements (integer))
- Matrix Calculator (open source/on-line)
- **Attacks** – besides frequency analysis (di-grams and tri-grams), Cryptanalyst - John Tiltman discovered vulnerabilities in the cipher's key selection and matrix properties, making it susceptible to certain attacks