Wednesday, December 30, 2020 8:19 AM

Chapter-II Cryptography

Classical Cipher Schemes

Classical Substitution Cipher

Here, the ciphertext is obtained by replacing the letters of plaintext with other letters, symbols or numbers. If the plaintext is viewed as a sequence of bits, the ciphertext is obtained by replacing the plaintext bit patterns with ciphertext bit patterns.

Caesar Cipher

→ easiest known substitution cipher invented by Julius Caesar for communicating with his military generals in war.

→ Here, the ciphertext is obtained by substituting each letter by an arbitrary letter (say m) and so on.

→ Example.

plaintext : MEET ME AFTER THE PARTY

Using the key m = 3.

ciphertext = PHHW PH DIWHU DKH SDUWB

Here the following transformation is used

a	b	c	d	e	f	----------	x	y	z
d	e	f	g	h	i	----------	a	b	c

Mathematically, we assign each letter to a number starting from a = 0 to z = 25. Then, we have the Caesar Cipher as:

$$C = E(P) = (X + K) \bmod 26$$

$$P = D(C) = (X - K) \bmod 26$$

The widely used ROT13 encryption is simply a Caesar Cipher with an offset value of 13.

Vigenere is also an encryption technique where Caesar Cipher is employed.

offset value of 13.
Vigenere is also an encryption technique where Caesar Cipher is employed.

Cryptanalysis of Caesar Cipher

1. Predictable
2. less number of possible Cipher (26)
3. a letter 'A' maps to a b c ..... to z (any one of them)
4. With simple tries, one can easily crack the ciphertext in very less time.

Hill Cipher

- Invented by Lester S. Hill in 1929
- Polygraphic Substitution cipher.
- Best example of block substitution Cipher where group of letters are encrypted together in equal block length.

Encryption Scheme

The receiver & Sender both must agree upon a key matrix in order to encrypt a message using the Hill Cipher. The key matrix 'A' of size $n \times n$ is used and A should be invertible against modulo 26. The plaintext is represented as a vector of size 'n'. The following example uses a matrix of size 2×2 and plaintext will be enciphered in blocks of 2 characters.

Let the key matrix A be $A = \begin{bmatrix} 3 & 25 \\ 24 & 17 \end{bmatrix}$

The message to be converted into Ciphertext is 'MISSISSIPI'

A-0	N-13
B-1	O-14
C-2	P-15
D-3	Q-16
E-4	R-17
F-5	S-18
G-6	T-19

Using the translation alongside, the vector for MI will be $\begin{bmatrix} 12 \\ 8 \end{bmatrix}$.

The sender then calculates

$$\begin{bmatrix} 3 & 25 \\ 24 & 17 \end{bmatrix} \begin{bmatrix} 12 \\ 8 \end{bmatrix} \bmod 26$$

$$= \lceil 3 \times 12 + 25 \times 8 \rceil \bmod 26$$

F-5	S-18
G-6	T-19
H-7	U-20
I-8	V-21
J-9	W-22
K-10	X-23
L-11	Y-24
M-12	Z-25

$$= \begin{bmatrix} 3\times12 + 25\times8 \\ 12\times24 + 17\times8 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 236 \\ 424 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 8 \end{bmatrix} = \begin{bmatrix} C \\ I \end{bmatrix}$$

Using the same translation, the first two letter of Ciphertext correspond to 2, 8 which return CI. The same process is used for the entire text.

[Note: If there are not enough letters to form block of 2 (in this case n=2), the message is padded with some arbitrary letter say 'z']

Continuing in the similar fashion we get the following translations:

Plaintext (P.T.) : MI SS IS SI PP IK

Ciphertext (C.T.): CI KK GE OW ER OY

Encrypt the string DOG Using the key 'GYBMQKURP'

$$\begin{bmatrix} D \\ O \\ G \end{bmatrix} = \begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix} \qquad \begin{pmatrix} G & Y & B \\ M & Q & K \\ U & R & P \end{pmatrix} = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Now,

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 6\times3 + 24\times14 + 1\times6 \\ 13\times14 + 16\times14 + 10\times6 \\ 20\times3 + 17\times14 + 15\times6 \end{bmatrix} \bmod 26 = \begin{bmatrix} 360 \\ 323 \\ 388 \end{bmatrix} \bmod 26 = \begin{bmatrix} 22 \\ 11 \\ 24 \end{bmatrix} = \begin{bmatrix} W \\ L \\ Y \end{bmatrix}$$

$\begin{bmatrix} 20\times3+17\times14+15\times6 \end{bmatrix}$ $\begin{bmatrix} 380 \end{bmatrix}$ $\begin{bmatrix} C \\ I \end{bmatrix}$ $\begin{bmatrix} K \end{bmatrix}$

Decryption of Message

→ Calculate inverse of Key A

adj (A)

$$A^{-1} = [\det(A)]^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{26}$$

Next we multiply the inverse of the Key by each pair of Ciphertext letters (mod 26) to recover the original letters.

For $A = \begin{bmatrix} 3 & 25 \\ 24 & 17 \end{bmatrix}$ $A^{-1} = 17 \begin{bmatrix} 17 & -24 \\ -25 & 3 \end{bmatrix} \bmod 26$

$$= \begin{bmatrix} 289 & -425 \\ -408 & 51 \end{bmatrix} \bmod 26$$

[It is the modular inverse (multiplicative inverse) of det(A)] $= \begin{bmatrix} 3 & 17 \\ 8 & 25 \end{bmatrix}$

Recall our encrypted message : CIKKGEUWEROY

The recovery is calculated as

$$A^{-1} * \begin{bmatrix} C \\ I \end{bmatrix} = \begin{bmatrix} 3 & 17 \\ 8 & 25 \end{bmatrix} * \begin{bmatrix} 2 \\ 8 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 12 \\ 8 \end{bmatrix} = \begin{bmatrix} M \\ I \end{bmatrix}$$

Proceeding in similar fashion, we decrypt other remaining pats of the Ciphertext and the decrypted message is MISSISSIPIK.

#Worked Out Example

Encrypt "ATTACK" Using the key $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

Soln:

Encrypt "ATTACK" using the key $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

⇒ Soln:

As the key is 2×2 matrix we split the word ATTACK into vectors of size 2×1 as given below:

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

Encryption Process

$$\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$$

$$C = KP \bmod 26$$

$$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26 = \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$$

Similarly,

$$\begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix} \quad C = KP \bmod 26$$

$$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$$

Also,

$$\begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 2 \\ 10 \end{bmatrix} \quad C = KP \bmod 26$$

$$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \bmod 26 = \begin{bmatrix} 34 \\ 66 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$$

∴ ATTACK becomes FKMFIO.

For decryption,

Determinant of matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is given as $ad - bc$.

So, $D = \begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix} = 12 - 9 = 3$

Next we find the multiplicative inverse of D (i.e 3 in our case)

Next we find the multiplicative inverse of D (i.e 3 in our case)

i.e $DD^{-1} \equiv 1 \bmod 26$

or, $3D^{-1} \equiv 1 \bmod 26$

$D^{-1} = 9.$

$adj(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ for matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\therefore$ adj of $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$ is given as $\begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$

Now to remove negative signs we add 26 to all negative numbers as we perform modulo 26 operation.

$$\therefore adj(K) = \begin{bmatrix} 6 & -3+26 \\ -3+26 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

Now, $K^{-1} = D^{-1} adj(K)$

$$= 9 \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix}$$

Finding its modulo 26 we have

$$K^{-1} = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

Now lets decrypt FKMFIO

$$C = \begin{bmatrix} F \\ K \end{bmatrix} = \begin{bmatrix} 5 \\ 10 \end{bmatrix}$$

$$P = K^{-1}C \bmod 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}\begin{bmatrix} 5 \\ 10 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 260 \\ 305 \end{bmatrix} \bmod 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$$

FK becomes AT.

Also, for MF $\begin{bmatrix} M \\ F \end{bmatrix} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}$

$$P = K^{-1}C \bmod 26$$

$$= \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}\begin{bmatrix} 12 \\ 5 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 149 \\ 390 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} T \\ A \end{bmatrix}$$

MF becomes TA

and finally for IO $\begin{bmatrix} I \\ O \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$

$$P = K^{-1}C \bmod 26$$

$$= \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}\begin{bmatrix} 8 \\ 14 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 366 \\ 452 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$$

IO becomes CK.

Hence, ATTACK is encrypted as FKMFIO and FKMFIO is successfully decrypted as ATTACK using the given key matrix $A = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$.

$$A = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}.$$

Monoalphabetic Cipher

- rather than shifting alphabets, shuffle the letters arbitrarily.
- each plaintext letter maps to a different random cipher letter.
- key is 26 letter long.
- each letter in plaintext is encoded by one & only one letter from cipher alphabet & each letter in ciphertext represents only one letter from the plaintext.

Polyalphabetic Cipher

→ each letter in plaintext can be encoded by any letter in the ciphertext alphabet & each letter in the alphabet represents different letters from plaintext each time it appears.

ATBASH Cipher (eg of monoalphabetic cipher)

Plaintext	A - M	N - Z
Ciphertext	Z - N	M - A

Using ATBASH Cipher

Plaintext	B	I	K	A	S	H
	1	8	10	0	18	7
	24	17	15	25	7	18
Ciphertext	Y	R	P	Z	H	S

Affine Cipher

Encryption : $E(x) = (ax + b) \bmod m$

Decryption : $D(x) = c(x - b) \bmod m$

where a & b are the key values.

→ c is the multiplicative inverse of a i.e $a \times c = 1 \bmod m$.

Encode & Decode the text "Affine Cipher" using key $a = 5$ & $b = 8$

Encode & Decode the text "Affine Cipher" using Key $a=5$ & $b=8$.

Encryption:

Plaintext	A	F	F	I	N	E	C	I	P	H	E	R
X	0	5	5	8	13	4	2	8	15	7	4	17
$ax+b$	8	33	33	48	73	28	18	48	83	43	28	93
$ax+b \bmod M$	8	7	7	22	21	2	18	22	5	17	2	15
Ciphertext	I	H	H	W	U	C	S	W	F	R	C	P

Now, to calculate the multiplicative inverse of 5.
It is found to be -5. So adding 26 to it we get 21 as its Multiplicative inverse.

Decryption

Ciphertext	I	H	H	W	U	C	S	W	F	R	C	P
X	8	7	7	22	21	2	18	22	5	17	2	15
$C(x-b)$	0	-21	-21	294	273	-126	210	294	-63	189	-126	147
$C(x-b) \bmod 26$	0	5	5	8	13	4	2	8	15	7	4	17
Plaintext	A	F	F	I	N	E	C	I	P	H	E	R

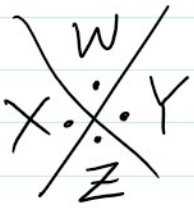
What happens if we take $a=4$ & $b=5$?

Pigpen Cipher → Visual Cipher

Key:

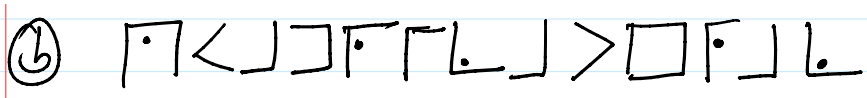
A	B	C
D	E	F
G	H	I

J.	K.	L.
M.	N.	O.
P.	Q.	R.



Decipher the following using Pigpen Cipher

(a) 

⑥ 

Steganography

⇒ A plaintext message may be hidden in any message nowadays. The method of steganography conceals the existence of message, whereas the method of cryptography renders message into unintelligible from outsider by various transformation of text.

⇒ A simple form of steganography, but one that is time consuming to construct is one in which words arrangement or letters within an apparently innocous text spells out the real message.

Examples:

① Sequence of the first letter of each word of the overall msg may spell out the real message.

② Subset of word of overall message is used to carry / convey the hidden message.

Various techniques have been used previously. Some of them are:

Character Marking: Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held to an angle to bright light.

Invisible Ink: a no. of substances can be used for writing but leave no visible traces until heat or some chemicals is applied to the paper.

Pin Structure: A small pin structure on selected letters are ordinarily not visible unless the paper is held in front of light.

Drawbacks

- Requires a lot of overhead to hide relatively few bits

- Requires a lot of overhead to hide relatively few bits of information.
- Once system is discovered, it becomes virtually worthless.