1. Playfair Cipher numericals

Rules for encryption using playfair cipher

1. Diagram.
2. Repeating letters, - filler letter.
3. Same column ↓↓ wrap around.
4. Same row →→ wrap around.
5. Rectangle ⇆ swap

M	O	N	A →	R
C ←	H	Y	B →	D
E ←	F	G	H	K
L	P	Q	S ←	T
U	V	W	X	Z

Eg. 1: attack

Diagram: at ta ck

for at → 1st create rectangle in matrix

2nd for ck

at	ta	ck
RS	SR	DE

Cipher text → RSSRDE

Eg. 2: mosque

Diagram: mo sq ue.

mo	sq	ue
ON	TS	ML

same row →→

M →	O →	N	A	R
C	H	Y	B	D
E ↓	F	G	I/J	K
L	P	Q →	S →	T → same row →→
U	V	W	X	Z

↑ same column ↓↓

Hill cipher :

Multi letter cipher.
Developed by Lester hill in 1929.
Encrypts a group of letters : digraph, trigraph, or polygraph

Mathematical concepts required :

matrix arithmetic modulo 26.
Square matrix.
Determinant
Multiplicative Inverse

Algorithm : Can be expressed as

$$C = E(K, P) = P \times K \bmod 26$$

$$P = D(K, C) = CK^{-1} \bmod 26 = P \times K \times K^{-1} \bmod 26$$

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

← Encryption

← key matrix size 3 means 3 letters encrypted together.

$$C_1 = (P_1 k_{11} + P_2 k_{21} + P_3 k_{31}) \bmod 26$$

$$C_2 = (P_1 k_{12} + P_2 k_{22} + P_3 k_{32}) \bmod 26$$

$$C_3 = (P_1 k_{13} + P_2 k_{23} + P_3 k_{33}) \bmod 26$$

Eg:→ Hill cipher

Question: Encrypt "pay more money" using hill cipher with key.

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Solution:

p	a	y	m	o	r	e	m	o	n	e	y
15	0	24	12	14	17	4	12	14	13	4	24

key = 3×3 matrix

Plaintext = pay more emo ney ← if not enough letter to make a trigraph or any other add extra letter (filler)

$$(C_1\ C_2\ C_3) = (15\ 0\ 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$C_1 = (15\times17 + 0\times21 + 24\times2) \bmod 26 = 303 \bmod 26$

$C_2 = (15\times17 + 0\times18 + 24\times2) \bmod 26 = 303 \bmod 26$

$C_3 = (15\times5 + 0\times21 + 24\times19) \bmod 26 = 531 \bmod 26$

$(C_1\ C_2\ C_3) = (303\ 303\ 531) \bmod 26$

$= (17\ 17\ 11)$

Ciphertext for pay is = (R R L)

II nd Plaintext = mor

same process

$$= (12\ 14\ 17)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$(C_1 C_2 C_3) = (532\ 490\ 677) \bmod 26$

$= (12, 22, 1)$ mod

P.T.(mor) = C.T.(M W B)

III rd Plaintext = emo

$= (10, 0, 18)$

emo = (K A S)

IV th Plaintext = neg

$= (348\ 312\ 538) \bmod 26$

$= (15\ 3\ 7)$

neg = (P D H)

whole P.T.: Plaintext = pay more money

Ciphertext = R R L M W B K A S P D H

Hill cipher Decryption

Decryption requires K^{-1}, the inverse matrix K

$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K.$$

To find Det K, Adj K

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

$$\text{Det } |K| \bmod 26 = \begin{pmatrix} +17 & -17 & +5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$\text{Det}[K] = 17(18\times19 - 2\times21) - 17(21\times19 - 2\times21) + 5(21\times2 - 18\times2)$$

$$= 5100 - 6069 + 30 \bmod 26$$

$$= -939 \bmod 26$$

$$= -3 \bmod 26 \quad \text{i.e. } (+26 - 3)$$

whenever get a -ve value add with modulo

$$\text{Det}|K| \equiv 23$$

$$\text{adj}|K| = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix}$$

$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K$$

$$= \frac{1}{23} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$$= (23^{-1}) \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

$23^{-1} \times 23 = 1 \bmod 26$ (multiplicative inverse of 23 is 17)

$1 \times 23 = 23 \bmod 26$

$2 \times 23 = 20 \bmod 26$

$3 \times 23 = 17 \bmod 26$

$4 \times 23 = [illegible] \bmod 26$

$17 \times 23 = 1 \bmod 26$

inverse of 23 is = 17 find a no. which when multiplied by 23 then taken modulo on 26 gives remainder = 1

Can we extended euclidian algo. to find that

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

To check if it is right or not do when K^{-1} will be multiplied by K is give you Identity matrix or unique matrix

$$K \times K^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

$$= \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Q. Decrypt "RRLMWBKASPDH" using hill cipher with key

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Solution: $P = C k^{-1} \bmod 26$

R	R	L	M	W	B	K	A	S	P	D	H
17	17	11	12	22	1	10	0	18	15	3	7

C.T. = R R L

$$(P_1 P_2 P_3) = (R\ R\ L) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (17\ 17\ 14) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

Similarly get results for all

Polyalphabetic ciphers

To improve the simple monoalphabetic technique.
General name: polyalphabetic substitution cipher

Common features:

1. A set of related monoalphabetic substitution rules is used.
2. A key determines which particular rule is chosen for a given transformation.

Vigenere Cipher → (Polyalphabetic)

It consists of the 26 Ceasar ciphers with shifts of 0 through 25.

Encryption process:

$C_i = (P_i + k_i \bmod m) \bmod 26$

C_i → ciphertext character (1 or 2 ...)

Decryption Process:

$P_i = (C_i - k_i \bmod m) \bmod 26$

Eg. key: deceptive deceptive deceptive

Plaintext: wearediscoveredsaveyourself

If the no. of characters are less in key then it will get repeated.

corresponding no. key: deceptivedeceptivedeceptive

PT: wearediscoveredsaveyourself

Ciphertext:

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4
PT	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3	18	0	21	4	24	14	20	17	18	4	11	5
CT	25	8	2	21	19	22	16	13	6	17	25	6	21	19	22	0	21	25	7	2	16	24	6	11	12	6	9
	Z	I	C	V	T	W	Q	N	G	R	Z	G	V	T	W	A	V	Z	H	C	Q	Y	G	L	M	G	J

Encryption

$C_i = (P_i + k_i \bmod m) \bmod 26$

$C_1 = (3 + 22) \bmod 26$

$= 25$

$C_2 = (4 + 4) \bmod 26$

$= 8 \bmod 26 = 8$ . . . .

Security attacks - can check same (e) is represented as diff^n C.T. letter.

Imp^n point is to determine the length of the keyword. for cryptanalysis.

key and P.T. share the same frequency distribution of letters, a statistical technique can be applied.

Autokey system:

The periodic nature of the keyword can be eliminated by using a non-repeating keyword i.e as long as the msg itself.

Vigner proposed autokey system, in which a keyword is concatenated with the P.T. itself to provide a running key.

Eg.

key : deceptive we arediscovered save

P.T. : we arediscove a dsave yourself

C.T : ZICVTWQNGKZEIIGASXSTSLVVWLA

Better security with Autokey system.

One time pad - (Substitution cipher) (Vernam cipher) -