20/08/2021

OPEN BOOK TEST - 1

Page No.:
Date:

Q1. Vigenere cipher

Plaintext = Practice Problem

Key = CNS

cipher text = ?

1. Encryption : Plain text = practiceproblem.

p	r	a	c	t	i	c	e	p	r	o	b	l	e	m
15	17	0	2	19	8	2	4	15	17	14	1	11	4	12

2. Key = CNS

2 13 18

3. Divide the plain text in no. of char in key.

pra cti cep rob lem

	p	r	a	c	t	i	c	e	p	r	o	b	l	e	m
PT -	15	17	0	2	19	8	2	4	15	17	14	1	11	4	12
K -	2	13	18	2	13	18	2	13	18	2	13	18	2	13	18

4. Cipher Text = $(P + K) \bmod 26$

$C_1 = (15 + 2) \bmod 26 = 17 \bmod 26 = 17 = r$

$C_2 = (17 + 13) \bmod 26 = 30 \bmod 26 = 4 = e$

$C_3 = (0 + 18) \bmod 26 = 18 \bmod 26 = 18 = s$

$C_4 = (2 + 2) \bmod 26 = 4 \bmod 26 = 4 = e$

$C_5 = (19 + 13) \bmod 26 = 32 \bmod 26 = 6 = g$

$C_6 = (8 + 18) \bmod 26 = 26 \bmod 26 = 0 = a$

$C_7 = (2 + 2) \bmod 26 = 4 \bmod 26 = 4 = e$

$C_8 = (4 + 13) \bmod 26 = 17 \bmod 26 = 17 = r$

$C_9 = (15 + 18) \bmod 26 = 33 \bmod 26 = 7 = h$

$C_{10} = (17 + 2) \bmod 26 = 19 \bmod 26 = 19 = t$

$C_{11} = (14 + 13) \bmod 26 = 27 \bmod 26 = 1 = b$

$C_{12} = (1 + 18) \bmod 26 = 19 \bmod 26 = 19 = t$

$C_{13} = (11 + 2) \bmod 26 = 13 \bmod 26 = 13 = n$

$C_{14} = (4 + 13) \bmod 26 = 17 \bmod 26 = 17 = r$

$C_{15} = (12 + 18) \bmod 26 = 30 \bmod 26 = 4 = e$

∴ cipher Text = resegaerhtbtnre

Q2. Hill cipher

Plain text = ACT

Key = YashShah

Cipher text = ?

1. Key matrix = 3×3 = $\begin{bmatrix} y & a & s \\ h & s & h \\ a & h & x \end{bmatrix} = \begin{bmatrix} 24 & 0 & 18 \\ 7 & 18 & 7 \\ 0 & 7 & 23 \end{bmatrix}$

Plain text matrix = 3×1 = $\begin{bmatrix} a \\ c \\ t \end{bmatrix} = \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$

$C_1 = P_1 \times K \bmod 26 = \begin{bmatrix} a \\ c \\ t \end{bmatrix} \times \begin{bmatrix} y & a & s \\ h & s & h \\ a & h & x \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \times \begin{bmatrix} 24 & 0 & 18 \\ 7 & 18 & 7 \\ 0 & 7 & 23 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0\times24 + 2\times0 + 18\times19 \\ 0\times7 + 2\times18 + 19\times7 \\ 0\times0 + 2\times7 + 19\times23 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 342 \\ 169 \\ 451 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 4 \\ 13 \\ 9 \end{bmatrix} = \begin{bmatrix} e \\ n \\ j \end{bmatrix}$

∴ Cipher text = enj

Q3. Keyless Transposition (Row) Cipher.

Plaintext = Practiceproblem

Key = CNS

Cipher text = ?

1. Total number of character in Plain text = 15

1. Enter all char in Plain text into square matrix.

p	r	a	c
t	i	c	e
p	r	o	b
l	e	m	x

p	t	p	l
r	i	r	e
a	c	o	m
c	e	b	x

We will write text from rows.

∴ cipher text = ptpl rire acom cebx

Q4. Keyed (column) cipher.

Plain text = Practice Problem

Key = Fire

Cipher text = ?

1. No. of columns = 4

f	i	r	e
5	8	17	4

p	r	a	c
t	i	c	e
p	r	o	b
l	e	m	x

Cipher text = cebx ptpl rire acom

Q5. Encrypt using Affine cipher

Plain text = Good Morning

Key = (7, 9)

$E = (p \times K_1 + K_2) \bmod 26$

K_1 = multiplicative key = 9

K_2 = Additive key = 7

g o o d m o r n i n g

6 14 14 3 12 14 17 13 8 13 6

$E = (P \times K_1 + K_2) \bmod 26$

$C_1 = (6 \times 9 + 7) \bmod 26 = 61 \bmod 26 = 9 = j$

$C_2 = (14 \times 9 + 7) \bmod 26 = 133 \bmod 26 = 3 = d$

$C_3 = (14 \times 9 + 7) \bmod 26 = 133 \bmod 26 = 3 = d$

$C_4 = (3 \times 9 + 7) \bmod 26 = 34 \bmod 26 = 8 = i$

$C_5 = (12 \times 9 + 7) \bmod 26 = 115 \bmod 26 = 11 = l$

$C_6 = (14 \times 9 + 7) \bmod 26 = 133 \bmod 26 = 3 = d$

$C_7 = (17 \times 9 + 7) \bmod 26 = 160 \bmod 26 = 4 = e$

$C_8 = (13 \times 9 + 7) \bmod 26 = 124 \bmod 26 = 20 = u$

$C_9 = (8 \times 9 + 7) \bmod 26 = 79 \bmod 26 = 1 = b$

$C_{10} = (13 \times 9 + 7) \bmod 26 = 124 \bmod 26 = 20 = u$

$C_{11} = (6 \times 9 + 7) \bmod 26 = 61 \bmod 26 = 9 = j$

cipher text = jddildeubuj

Q6. Decrypt using affine cipher.

Plain text = ?

cipher text = aevjvjztsdvch

Key = (17, 15)

K_1 = multiplicative key = 15

K_2 = additive key = 17

$D = K_1^{-1}(P - K_2) \bmod 26$.

1. To find key inverse.

$26 = 15 \times 1 + 11$

$15 = 11 \times 1 + 4$

$11 = 4 \times 2 + 3$

~~$8 = 3 \times 2 + 0$~~

$4 = 3 \times 1 + 1$

$3 = 1 \times 3 + 0$

$1 = 4 + 3(-1)$

$1 = 4 + (11 + 4(-2))(-1)$

$1 = 4(3) + 11$

$1 = (15 + 11(-1))(3) + 11$

$1 = 15(3) + 11(-2)$

$1 = 15(3) + (26 + 15(-1))(-2)$

$1 = 15(3) + 26(-2) + 15(2)$

$1 = 15(5) + 26(-2)$

Q7. Encrypt using playfair cipher.
Plain-text = good morning
key = stayhappy.

s	t	a	y	h
p	b	c	d	e
f	g	i/j	k	l
m	n	o	q	r
u	v	w	x	z

5×5

go od mo rn in gx

in qc nq mo go kv
∴ cipher text = inqc nqmogokv

Q8. Playfair cipher
Cipher text = qo mq ye kc xl
key = hello
Plain-text = ?

h	e	l	o	a
b	c	d	f	g
i/j	k	m	n	p
q	r	s	t	u
v	w	x	y	z

5×5

qo = th
mq = is
ye = wo
kc = ce
xl = sx

Plain ~~Cipher~~ text = this wocesx

Q9. Affine cipher.
Plain text = Hello Everyone.
key = (7, 5)
Cipher text = ?

h	e	l	l	o	e	v	e	r	y	o	n	e
7	4	11	11	14	4	21	4	17	24	14	13	4

$C = (P \times K1 + K2) \bmod 26$.

2 21 20 20 1 21 0 21 8 7 1 16 21

∴ Cipher text = cvuubvavihbqv

Q10. Affine cipher.

cipher text = cvuubvavihbqv

key = (11, 3)

Plain text = hello everyone.

Q11. Additive cipher.

cipher text = axeehxoxkrhgx

key = T = 19

Plain text = ?

a	x	e	e	h	x	o	x	k	r	h	g	x
0	23	4	4	7	23	14	23	10	17	7	6	23

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

7	4	11	11	14	4	21	4	17	24	14	13	4
h	e	l	l	o	e	v	e	r	y	o	n	e

Plain text = hello everyone.

Q13. C = horeeeyxlovxlenx Keyless transposition.

h	o	r	e
e	e	y	x
l	v	o	x
l	e	n	x

Plain text = hello everyone

Q14. Keyed transposition.

cipher text = eeyxlovxhorelenx

Key = HACK.

3 1 2 4

e	e	y	x
l	v	o	x
h	o	r	e
l	e	n	x

3 1 2 4

e	l	h	l
e	v	o	e
y	o	r	n
x	x	e	x

⇒

h	e	L	l
o	e	v	e
r	y	o	n
e	x	x	x

Plain text = hello everyone.