CNS ASSIGNMENT

(1)

18DCS007

Q1.

(1) FOR ADDITIVE CIPHER, $C_i = P_i + K \mod 26$

$C_a = 0 + 13 \mod 26 = 13 = n$
$C_t = 19 + 13 \mod 26 = 6 = g$
$C_c = 2 + 13 \mod 26 = 15 = p$
$C_K = 10 + 13 \mod 26 = 23 = x$
$C_i = 8 + 13 \mod 26 = 21 = v$
$C_s = 18 + 13 \mod 26 = 5 = f$
$C_o = 14 + 13 \mod 26 = 1 = b$
$C_d = 3 + 13 \mod 26 = 16 = q$
$C_y = 24 + 13 \mod 26 = 11 = l$

CT = nggnpx vf ghqnl

(2) FOR MULTIPLICATIVE CIPHER, $C_i = P_i \times \mod 26$

$C_w = 22 \times 13 \mod 26 = 0 = a$
$C_e = 4 \times 13 \mod 26 = 0 = a$
$C_l = 11 \times 13 \mod 26 = 13 = n$
$C_i = 8 \times 13 \mod 26 = 0 = a$
$C_v = 21 \times 13 \mod 26 = 13 = n$
$C_n = 13 \times 13 \mod 26 = 13 = n$
$C_s = 18 \times 13 \mod 26 = 0 = a$
$C_c = 2 \times 13 \mod 26 = 0 = a$
$C_u = 20 \times 13 \mod 26 = 0 = a$
$C_m = 17 \times 13 \mod 26 = 13 = n$
$C_o = 14 \times 13 \mod 26 = 0 = a$
$C_d = 3 \times 13 \mod 26 = 13 = n$

CT = aa naina an anaaaan
aannnn

Substitution is not unique because GCD(13,26) ≠ 1

(3) FOR AFFINE CIPHER, $C_i = (P_i \times K_1) + K_2 \bmod 26$

$C_t = (19 \times 15) + 20 \bmod 26 = 19 = t$
$C_h = (7 \times 15) + 20 \bmod 26 = 21 = v$
$C_i = (8 \times 15) + 20 \bmod 26 = 10 = k$
$C_s = (18 \times 15) + 20 \bmod 26 = 4 = e$
$C_a = (0 \times 15) + 20 \bmod 26 = 20 = u$
$C_n = (13 \times 15) + 20 \bmod 26 = 7 = h$
$C_g = (6 \times 15) + 20 \bmod 26 = 6 = g$
$C_m = (12 \times 15) + 20 \bmod 26 = 18 = s$
$C_e = (4 \times 15) + 20 \bmod 26 = 2 = c$

CT = tvke ke vh ueekghscht

(4) FOR SHIFT CIPHER

7 ch. →

... V [W] X Y Z A B C [D] E F ...

By same method CT = dLsjvtl av aol dvgsk vm
jyfwavnyhwof

(5)

PT	h	o	w	w	a	s	t	h	e	a	t	t	a	c	k
Value	7	14	22	22	0	18	19	7	4	0	19	19	0	2	10
Key	10	7	14	22	22	0	18	19	7	4	0	19	19	0	2
Enc	17	21	10	18	22	18	11	0	11	4	19	12	19	2	12
CT	r	v	k	s	w	s	l	a	l	e	t	m	t	c	m

CT = rvk sws lal etmtcm

(6)

PT	h	o	p	e	y	o	u	a	r	e	s	a	f	e
Value	7	14	15	4	24	14	20	0	17	4	18	0	5	4
key	2	14	21	8	3	14	21	8	3	2	14	21	21	8
Enc	9	2	10	12	1	16	8	21	25	7	20	14	0	12
CT	j	c	k	m	b	q	i	v	z	h	u	o	a	m

PT	a	n	d	s	o	u	n	d
Value	0	13	3	18	14	20	13	3
key	3	2	14	21	8	3	2	14
Enc	3	15	17	13	22	23	15	17
CT	d	p	r	n	w	x	p	r

CT = jckm haji vzh uoam dpm nwxpr

(7) Key =

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

PT = ch ec ky ou ri nt er ne tc on ne ct iv it yx (bogus character)

CT = qp av mw cw sv tz lx lg pd dk dp di ds zy

CT = qpavm wcws vtztxlgp ddklgdidszy

(8). Backup is 6 letters long so key will be of 3×3 order

$$PT = \begin{bmatrix} B & E & Y & R & E & A & N & I \\ E & A & F & T & E & M & A & D \\ R & D & I & O & H & X & I & T & N \end{bmatrix} \qquad K = \begin{bmatrix} B & A & C \\ K & U & P \\ B & B & B \end{bmatrix}$$

bogus

$$= \begin{bmatrix} 1 & 4 & 24 & 17 & 4 & 0 & 13 & 8 \\ 4 & 0 & 5 & 19 & 4 & 12 & 0 & 14 \\ 17 & 3 & 14 & 7 & 23 & 8 & 19 & 13 \end{bmatrix}$$

$CT = K \times PT \bmod 26$

$$CT = \begin{bmatrix} 35 & 10 & 52 & 31 & 50 & 16 & 51 & 34 \\ 345 & 85 & 550 & 655 & 485 & 360 & 415 & 555 \\ 22 & 7 & 43 & 45 & 31 & 20 & 32 & 35 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 9 & 10 & 0 & 5 & 24 & 16 & 25 & 8 \\ 7 & 7 & 4 & 5 & 23 & 22 & 25 & 9 \\ 22 & 7 & 17 & 17 & 5 & 20 & 16 & 9 \end{bmatrix}$$

$$= \begin{bmatrix} J & K & A & F & Y & Q & Z & I \\ H & H & E & F & X & W & Z & J \\ W & H & R & R & F & U & G & J \end{bmatrix}$$

CT = JHWKHHAERFFRYZFQWUZZGIJJ

(9) e i g h t Key = 13425
1 4 2 3 5

TABLE: t r a n s t a n r s
p o s i t p s i o t
i o n c i i n c h o i
p h e r s p e h r s
a r e v u a e v r u
l n e r a l e r n a
b l e t o b e t l o
s e v e r s v e e r
a l k i n ⇒ a k i l n
d s o f c d o f s c
i p h e r i h e p r
t e x t o t x t e o
n l y a t n y a l t
s t a c k s t c k a s

CT = tpipalbs aditrit as neee vkoh xy cnicr vrteifeta kroohrm tel spelastisvarn crnts

(10) m a a t e d
e e t m h n h l n e a
e m t j a o e a t n y
t a l v i

CT = maatedeetmhnhlneaemtjaoeatnytalvi

Q2.

(1) FOR ADDITIVE CIPHER, $P_i = C_i - K \bmod 26$

$P_J = 9 - 13 \bmod 26 = 22 = W$
$P_X = 23 - 13 \bmod 26 = 10 = K$
$P_U = 20 - 13 \bmod 26 = 7 = H$
$P_Q = 2 - 13 \bmod 26 = 15 = P$
$P_D = 16 - 13 \bmod 26 = 3 = D$
$P_M = 3 - 13 \bmod 26 = 16 = Q$
:

PT = WKHPQZKRKDVFRQILGHQFHLQKLPVHOIJOLQVWKHFRQILGHQFHRIR
WKHUV

If key = 16, PT = THE MAN WHO HAS CONFIDENCE IN HIMSELF
GAINS THE CONFIDENCE OF OTHERS

(2) FOR MULTIPLICATIVE CIPHER, $P_i = C_i \times K^{-1} \bmod 26$

GCD(26,17) = GCD(17,9) = GCD(9,8) = GCD(8,1) = GCD(1,0) = 1

Using extended euclideon algorithm

q	r_1	r_2	r	t_1	t_2	$t = t_1 - qt_2$
1	26	17	9	0	1	-1
1	17	9	8	1	-1	2
1	9	8	1	-1	2	-3
8	8	1	0	2	-3	26
	1	0		-3		
	GCD			Inverse		

$-3 \bmod 26 = 23 \bmod 26 = K^{-1}$

$P_V = (21 \times 23) \mod 26 = 15 = P$
$P_Q = (16 \times 23) \mod 26 = 4 = E$
$P_E = (4 \times 23) \mod 26 = 14 = O$
$P_F = (5 \times 23) \mod 26 = 11 = L$
$P_K = (10 \times 23) \mod 26 = 22 = W$
:

PT = PEOPLE WHO ARE CRAZY ENOUGH TO THINK THEY CAN CHANGE THE WORLD ARE THE ONES WHO DO

(3) FOR AFFINE CIPHER, $P_i = (C_i - k_2) \times k_1^{-1} \mod 26$

GCD (26,7) = GCD(7,5) = GCD(5,2) = GCD(2,7) = GCD(1,0) = 1

Using extended euclidean algo

q	r_1	r_2	r	t_1	t_2	$t = t_1 - qt_2$
3	26	7	5	0	1	-3
1	7	5	2	1	-3	4
2	5	2	1	-3	4	-11
2	2	1	0	4	-11	-18
	1	0		-11	-18	

GCD Inverse

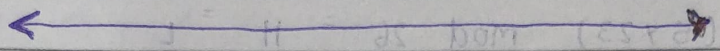
$-11 \mod 26 = 15 \mod 26$

$P_F = (5-15) \times 15 \mod 26 = 6 = G$
$P_Z = (25-15) \times 15 \mod 26 = 20 = U$
$P_A = (0-15) \times 15 \mod 26 = 9 = J$
:

PT = GUJARAT COUNCIL ON SCIENCE AND TECHNOLOGY

(4) USING CIPHER SHIFT

... S | T | U V W X Y Z A B C D E F G H I J K L | M | N O ...



$\therefore P_m = T$

PT = THE PESSIMIST SEES DIFFICULTY IN EVERY OPPORTUNITY
THE OPTIMIST SEES OPPORTUNITY IN EVERY DIFFICULTY

(5)

CT:	G	H	C	Z	E	H	R	H	G	Q	R	H	E	U	N	...
Value	6	7	2	25	4	7	17	7	6	16	17	7	4	20	13	...
Key	13	19	14	14	11	19	14	3	4	2	14	3	4	0	20	...
Dec	19	14	14	11	19	14	3	4	2	14	3	4	0	20	19	...
PT	T	O	O	L	T	O	D	E	C	O	D	E	A	U	T	...

PT: TOOL TO DECODE AUTOKEY AUTOMATICALLY

(6)

CT	C	Y	K	T	W	O	H	R	D	P	O	K	E	Q	...
Value	2	24	10	19	22	14	7	17	3	15	14	10	4	16	...
Key	0	7	12	4	3	0	1	0	3	0	7	12	4	3	...
Dec	2	17	24	15	19	14	6	17	0	15	7	24	0	13	...
PT	C	R	Y	P	T	O	G	R	A	P	H	Y	A	N	

PT: CRYPTOGRAPHY AND NETWORK SECURITY

(7) KEY:

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

CT = LA ZS MC YF TQ HE IM FC PV CS LA XV

PT = HE YT HI SI SP LA HF AI RC IP HE RX

= bogus

PT = HEY THIS IS PLAYFAIR CIPHER

(8) $KEY = \begin{bmatrix} B & A & G \\ K & U & P \\ B & B & B \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 1 & 1 & 1 \end{bmatrix}$

$\Delta = 1(20-15) + 2(110-20)$

$= 5 + 2(-10)$

$= 5 + (-20) = -15 \bmod 26 = 11$

$K^T = \begin{bmatrix} 1 & 10 & 1 \\ 0 & 20 & 1 \\ 2 & 15 & 1 \end{bmatrix}$ $Adj(K) = \begin{bmatrix} 5 & 2 & -40 \\ 5 & -1 & 5 \\ -10 & -1 & 20 \end{bmatrix}$

Using extended euclidean algorithm

q	r_1	r_2	r	t_1	t_2	$t = t_1 - t_2 q$
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	

GCD

Inverse

$-7 \bmod 26 = 19 \bmod 26$

$A^{-1} = \begin{bmatrix} 19\times5 & 19\times2 & 19\times(-40) \\ 19\times5 & 19\times(-1) & 19\times5 \\ 19\times(-10) & 19\times(-1) & 19\times20 \end{bmatrix} \bmod 26 = \begin{bmatrix} 17 & 12 & 20 \\ 17 & 7 & 17 \\ 18 & 7 & 16 \end{bmatrix}$

FOR HILL CIPHER : $P = K^{-1} \times C$

CT = BAP HVF JIX GGC HZH MYZ

$$\begin{bmatrix} B \\ A \\ P \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 15 \end{bmatrix} \Rightarrow P \begin{bmatrix} 17 & 12 & 20 \\ 17 & 7 & 17 \\ 18 & 7 & 16 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 15 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 12 \\ 24 \end{bmatrix} = \begin{bmatrix} F \\ M \\ Y \end{bmatrix}$$

$$\begin{bmatrix} H \\ V \\ F \end{bmatrix} = \begin{bmatrix} 7 \\ 24 \\ 5 \end{bmatrix} \Rightarrow P = \begin{bmatrix} 17 & 12 & 20 \\ 17 & 7 & 17 \\ 18 & 7 & 16 \end{bmatrix} \begin{bmatrix} 7 \\ 24 \\ 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} 13 \\ 8 \\ 20 \end{bmatrix} = \begin{bmatrix} N \\ I \\ K \end{bmatrix}$$

$$\begin{bmatrix} J \\ I \\ Y \end{bmatrix} = \begin{bmatrix} 9 \\ 8 \\ 23 \end{bmatrix} \Rightarrow P = \begin{bmatrix} 17 & 12 & 20 \\ 17 & 7 & 17 \\ 18 & 7 & 16 \end{bmatrix} \begin{bmatrix} 9 \\ 8 \\ 23 \end{bmatrix} \bmod 26 = \begin{bmatrix} 6 \\ 22 \\ 0 \end{bmatrix} = \begin{bmatrix} G \\ W \\ A \end{bmatrix}$$

$$\begin{bmatrix} H \\ Z \\ H \end{bmatrix} = \begin{bmatrix} 7 \\ 25 \\ 7 \end{bmatrix} \Rightarrow P = \begin{bmatrix} 17 & 12 & 20 \\ 17 & 7 & 17 \\ 18 & 7 & 16 \end{bmatrix} \begin{bmatrix} 7 \\ 25 \\ 7 \end{bmatrix} \bmod 26 = \begin{bmatrix} 13 \\ 23 \\ 23 \end{bmatrix} = \begin{bmatrix} N \\ X \\ X \end{bmatrix}$$

$$\begin{bmatrix} M \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 12 \\ 24 \\ 25 \end{bmatrix} \Rightarrow P = \begin{bmatrix} 17 & 12 & 20 \\ 17 & 7 & 17 \\ 18 & 7 & 16 \end{bmatrix} \begin{bmatrix} 12 \\ 24 \\ 25 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 \\ 17 \\ 4 \end{bmatrix} = \begin{bmatrix} E \\ R \\ E \end{bmatrix}$$

PT = FMYNIHCOGWANXXERE

(9) KEY = I N S E R T ∴ KEY = 412536

~~2 3 1 4~~ KEY^{-1} = 235146

2 3 5 1 4 6

TABLE:

G	I	M	I	A	N
U	E	Y	R	O	L
I	I	F	S	F	P
E	E	R	C	F	T
V	I	N	E	E	R
S	Y	R	P	E	T
H	C	T	A	W	I
L	W	O	D	U	I
O	T	L	K	O	L
	I	K			

POS = 1 2 3 4 5 6

KEY = 2 3 5 1 4 6

I	M	A	G	I	N
M	Y	O	U	R	L
I	F	E	I	S	P
E	R	F	I	S	P
E	R	F	E	C	T
I	N	E	V	E	R
Y	R	E	S	P	E
C	T	W	H	A	T
W	O	U	L	D	I
T	L	O	O	D	I
T	K	E			

PT: IMAGINE YOUR LIFE IS PERFECT IN EVERY RESPECT WHAT WOULD IT LOOK LIKE

(10) TABLE

S		I		A	I	E
E		Y	S	Y	S	T	T	F
C	T	M	L	A	U	S	L	I
U	I	O	T	O	P	R	O	L
R		S		E		N		

PT = SECURITY IS MOSTLY A SUPERSTITION LIFE IS EITHER A DARING ADVENTURE OR NOTHING

Q3.

(1) PT = YES

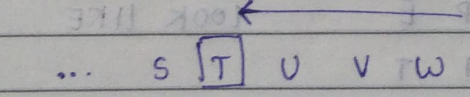
CT = CIW

FOR SHIFT CIPHER, Ci is shift down of K characters of Pi

We get C by shifting y down by 4 characters
We get I by shifting e down by 4 characters
We get W by shifting s down by 4 characters

KEY: 4

To get plaintext from ciphertext, we shift them up by 4



PT = TREASURE

→ attack = known plaintext attack

(2) We are not given any info

→ attack = Brute Force Attack

We known $P_i = C_i - K \bmod 26$

FOR KEY = +1,

PT = MBIZDYQBKZRIXKXNCDOQKXYQBKZ ... not possible

FOR KEY +2,

PT = LAHYCXPAJYQHJWMBCNPI ... not making sense

⋮

FOR KEY = +11,

PT = CRYPTOGRAPHY AND STEGANOGRAPHY ARE TWO SIDES OF A COIN

→ KEY = +11

(3) PT = ab

CT = GL

FOR AFFINE CIPHER WE KNOW THAT,

$C_i = (P_i \times K_1) + K_2 \bmod 26$

$\therefore \quad 6 = (0 \times K_1) + K_2 \bmod 26$

$11 = (1 \times K_1) + K_2 \bmod 26$

→ $\therefore K_2 = 6 \implies K_1 = 5$

Possible because GCD(26,5) = 1

Using extended euclidean algorithm

q	r_1	r_2	r	t_1	t_2	$t = t_1 - t_2 q$
5	26	5	1	0	1	-5
5	5	1	0	1	-5	26
	1	0		-5	26	

GCD — Inverse

$-5 \bmod 26 = 21 \bmod 26$

$\therefore \quad P_i = (C_i - K_2) \times K_1^{-1} \bmod 26$

$P_X = (23-6) \times 21 \bmod 26 = 19 = T$

$P_P = (15-6) \times 21 \bmod 26 = 7 = H$

$P_A = (0-6) \times 21 \bmod 26 = 4 = E$

$P_L = (11-6) \times 21 \bmod 26 = 1 = B$

PT = THE BEST OF A FIGHT IS MAKING UP AFTERWARDS

→ Attack : known plaintext attack

Q4. KEY = cryptography

We need to take alphabets plus numbers ∴ 6×6 matrix

TABLE:

c	r	y	p	t	o
g	a	h	b	1	2
3	4	5	6	7	8
9	b	d	e	f	j
j	k	l	m	n	q
s	u	v	w	x	z

PT: 18 DC 5D 07 RU DR AB AR AD

CT: 72 9Y ZC 8T AR BY 4K A4 HB

Q5. $KEY = \begin{bmatrix} b & a & c \\ R & U & p \\ b & b & b \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 1 & 1 & 1 \end{bmatrix}$

$PT = \begin{bmatrix} I & C & O & U & A & R \\ 8 & S & 7 & D & B & A \\ D & O & R & R & A & D \end{bmatrix} = \begin{bmatrix} 1 & 2 & 0 & 20 & 0 & 17 \\ 8 & 18 & 7 & 3 & 1 & 1 \\ 3 & 0 & 17 & 17 & 0 & 3 \end{bmatrix}$

$CT = Key \times PT \bmod 26$

$= \begin{bmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 0 & 20 & 0 & 17 \\ 8 & 18 & 7 & 3 & 1 & 1 \\ 3 & 0 & 17 & 17 & 0 & 3 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 7 & 2 & 34 & 54 & 0 & 23 \\ 215 & 380 & 395 & 515 & 20 & 235 \\ 12 & 20 & 24 & 40 & 1 & 21 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 7 & 2 & 8 & 2 & 0 & 23 \\ 7 & 16 & 5 & 21 & 20 & 1 \\ 12 & 20 & 24 & 14 & 1 & 21 \end{bmatrix} = \begin{bmatrix} H & C & I & A & X \\ H & Q & F & U & B \\ M & U & Y & B & V \end{bmatrix}$

CT = HHMCQUIFYAUBXBV

Miracle
Page
Date

Q6. $p = 18 + 7 = 25$ ($\because$ 18DCS007)

(i) $GCD(132,25) = GCD(25,7) = GCD(7,4) = GCD(4,3) = GCD(3,1)$
$= GCD(1,0)$

using extended euclidean algorithm

q	r_1	r_2	r	t_1	t_2	$t = t_1 - t_2 q$
5	132	25	7	0	1	-5
3	25	7	4	1	-5	16
1	7	4	3	-5	16	-21
1	4	3	1	16	-21	37
3	3	1	0	-21	37	-90

1

GCD

Inverse 37

37 mod 26 = 11

(ii) $GCD(80,25) = GCD(25,5) = GCD(5,0)$ $\because GCD = 5 \neq 1$

~~Using extented~~ $\therefore$ Inverse not possible

Q7. $p = 18 + 07 = 25$ ($\because$ 18DCS007)

Total numbers of keys in affine for $Z_p = p \times \# Z^*_p$

$\# Z^*_p = 5^2 - 5$
$= 25 - 5 = 20$

$\therefore$ TOTAL POSSIBLE KEYS $= 25 \times 20$
$= 500$

Q8. PT = 18DCS007RUDRABA KEY = (7,2)

$C_1 = (1 \times 7) + 2 \mod 26 = 9 = J$
$C_8 = (8 \times 7) + 2 \mod 26 = 6 = G$
$C_D = (3 \times 7) + 2 \mod 26 = 23 = X$
$C_C = (2 \times 7) + 2 \mod 26 = 16 = Q$
$C_S = (18 \times 7) + 2 \mod 26 = 24 = Y$
$C_0 = (0 \times 7) + 2 \mod 26 = 2 = C$
$C_0 = (0 \times 7) + 2 \mod 26 = 2 = C$
$C_7 = (7 \times 7) + 2 \mod 26 = 24 = Y$
⋮

∴ CT = JGXQYCCYRMXRCJC

→ For AFFINE, $P_i = (C_i - K_2) \times K_1^{-1} \mod 26$

Using extended euclidean algo,

q	r_1	r_2	r	t_1	t_2	$t = t_1 - q t_2$
3	26	7	5	0	1	-3
1	7	5	2	1	-3	4
2	5	2	1	-3	4	-11
2	2	1	0	4	-11	26
	1	0		-11	26	
	GCD			Inverse		

$-11 \mod 26 = 15 \mod 26$

∴ CT = JGXQYCCYRMXRCJC

$P_J = (9-2) \times 15 \mod 26 = 1$
$P_G = (6-2) \times 15 \mod 26 = 8$
$P_X = (23-2) \times 15 \mod 26 = 3 = D$

$P_R = (16-2) \times 15 \mod 26 = 2 = C$

$P_Y = (24-2) \times 15 \mod 26 = 18 = S$

$P_C = (2-2) \times 15 \mod 26 = 0 = A$

$P_C = (2-2) \times 15 \mod 26 = 0 = A$

$P_{RA} = ES$

⋮

PT = 18DCSOO7RUDRABA

(I) Suppose Key = (1,2)

then $CT = (PT \times 1) + 2 \mod 26 = PT + 2 \mod 26$

For eg. PT = 18DCSOO7RUDRABA

CT = 30FEU229TWFTCDC

Using $PT = CT - 2 \mod 26$,

PT = 18DCSOO7RUDRABA

∴ Additive Cipher is special case of affine cipher

(II) Suppose Key = (7,0)

then $CT = (PI \times 7) + 0 \mod 26 = PI \times 7 \mod 26$

Eg. PT = 18DCSOO7RUDRABA

CT = 7HVOWOOXPKVPAHA

Using $PT = CI \times 7^{-1} \mod 26$

CT = 18DCSOO7RUDRABA

∴ Multiplicative cipher is special case of affine cipher

Miracle
Page
Date

Q9. $K = (18007)_{10} = (1000110010010111)$

$\therefore K = 1000110010$

(I) Permutation on 10 bit Key

I/P = 1000110010 ⟶ initial permutation

O/P = 0100001101

3	5	2	7	4	10	1	9	8	6

(II) Circular left shift on both halves

I/P = 01000 01101

O/P = 00100 10110

(III) Apply compression D box ⟶

6	3	7	4	8	5	10	9

I/P = 00100 10110

O/P = 11001001 — K_1

(IV) Apply shift left operation on O/P of step (II)

I/P = 00100 10110

O/P = 01000 01100

(V) Apply compression D box

I/P = ~~000100111~~ 01000 01100

O/P = ~~00100000~~ 00101000

└ K_2

K_1 = 11001001

K_2 = 00101000

Q10. KEY = ~~RUDRA ARVIND BARAD~~ RUDRA ARVIND BARAD

= ADDAA AA E16DBAAAD

KEY = $^{1}1010\ ^{5}1101\ ^{9}1101\ ^{13}1010$
$^{17}1010\ ^{21}1010\ ^{25}1010\ ^{29}1110$
$^{33}0001\ ^{37}0110\ ^{41}1101\ ^{45}1011$
$^{49}1010\ ^{53}1010\ ^{57}1010\ ^{61}1101$

(i) Apply parity drop & permutation

O/P = 1110 1111 0010 1101
0001 0111 1110 1011
1001 1110 1111 0010
0110 1101

(ii) Dividing into 2 parts

L = 1110 1111 0010 1101 0001 0111 1110
R = 1011 1001 1110 1111 0010 0110 1101

(iii) Apply 1 bit circular shift on both halves

$^{1}\ \ ^{5}\ \ ^{9}\ \ ^{13}\ \ ^{17}\ \ ^{21}\ \ ^{25}$
L = 1101 1110 0101 1010 0010 1111 1101
$^{29}\ \ ^{33}\ \ ^{37}\ \ ^{41}\ \ ^{45}\ \ ^{49}\ \ ^{53}$
R = 0111 0011 1101 0100 1101 1011 0110

(iii) Apply compression D box

O/p → 0001 1101 1111 1111
1001 0011 0111 0111
1101 0100 0011 0101 → K_1

Thus we get first round key 1 $K_1 = (1DFF9377D835)_{16}$