

CNS ASSIGNMENT

①

18DCS007

Miracle

Page _____

Date _____

Q1.

as hom os t(13x7) = 13 + 8936 CIPHER 207 (8)

(1) FOR ADDITIVE CIPHER, $c_i = p_i + k \pmod{26}$

$$c_0 = 0 + 13 \pmod{26} = 13 = n$$

$$c_1 = 19 + 13 \pmod{26} = 0 \pmod{26} = 9$$

$$c_2 = 2 + 13 \pmod{26} = 15 = p$$

$$c_3 = 10 + 13 \pmod{26} = 23 = x$$

$$c_4 = 8 + 13 \pmod{26} = 21 = v$$

$$c_5 = 18 + 13 \pmod{26} = 5 = f$$

$$c_6 = 14 + 13 \pmod{26} = 1 = b$$

$$c_7 = 3 + 13 \pmod{26} = 16 = g$$

$$c_8 = 24 + 13 \pmod{26} = 11 = L$$

CT = nggnpaxvf ghqnl

(2) FOR MULTIPLICATIVE CIPHER, $c_i = p_i \times k \pmod{26}$

$$c_0 = 22 \times 13 \pmod{26} = 0 = a$$

$$c_1 = 13 \times 13 \pmod{26} = 0 \pmod{26} = a$$

$$c_2 = 11 \times 13 \pmod{26} = 13 = n$$

$$c_3 = 8 \times 13 \pmod{26} = 0 = a$$

$$c_4 = 21 \times 13 \pmod{26} = 13 = n$$

$$c_5 = 13 \times 13 \pmod{26} = 13 = n$$

$$c_6 = 18 \times 13 \pmod{26} = 0 \pmod{26} = a$$

$$c_7 = 22 \times 13 \pmod{26} = 0 \pmod{26} = a$$

$$c_8 = 20 \times 13 \pmod{26} = 0 \pmod{26} = a$$

$$c_9 = 17 \times 13 \pmod{26} = 13 = n$$

$$c_{10} = 14 \times 13 \pmod{26} = 0 \pmod{26} = a$$

$$c_{11} = 3 \times 13 \pmod{26} = 13 = n$$

(2)

(3) FOR AFFINE CIPHER, $C_i = (P_i \times k_1) + k_2 \pmod{26}$

$$C_t = (19 \times 15) + 20 \pmod{26} = 19 = t$$

$$C_h = (7 \times 15) + 20 \pmod{26} = 21 = v \quad \text{bom } El + 0 = h$$

$$C_i = (8 \times 15) + 20 \pmod{26} = 10 = k \quad \text{bom } El + P1 = i$$

$$C_s = (18 \times 15) + 20 \pmod{26} = 4 = e \quad \text{bom } El + S = s$$

$$C_a = (0 \times 15) + 20 \pmod{26} = 20 = u \quad \text{bom } El + Q1 = a$$

$$C_n = (13 \times 15) + 20 \pmod{26} = 7 = h \quad \text{bom } El + 8 = n$$

$$C_g = (6 \times 15) + 20 \pmod{26} = 6 = g \quad \text{bom } El + 61 = g$$

$$C_m = (12 \times 15) + 20 \pmod{26} = 18 = s \quad \text{bom } El + N1 = m$$

$$C_e = (4 \times 15) + 20 \pmod{26} = 2 = C \quad \text{bom } El + E = e$$

$$I = (1 \times 15) + 20 \pmod{26} = I \quad \text{bom } El + H1 = I$$

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 = d l s j v t l a v a o l d v g s k v m
" j y f w a v n y h w o f "

(5) PT: o h n o n w r w a s t h e a t t a c k

Value 7 14 22 22 0 18 19 17 4 0 19 19 0 2 10

Key 10 7 14 22 22 0 18 19 7 4 0 0 19 19 8 0 2

Encr. 17 21 10 18 22 18 11 0 11 4 0 19 12 19 2 12

CT: g n v k s w s t a l s t o n t x c o s m

CT = g n v k s w s t a l s t o n t x c o s m

n = 81 = as bom El + S = n

(3)

(6) PT ex: h7o adpilc y o u l a n t e s a f c
 Value 7 14 15 4 24 14 20 0 17 4 18 0 5 4

key 2 14 8 21 8 3 14 21 18 8 3 28 14 21 21 8

Enc 9 0 2 10 12 1 16 8 21 25 7 3 20 14 0 12

CT j 8 c 8 k m b q i t v z o h u o a m

PT a n d s o 8 u o n d n i

Value 0 13 3 18 14 20 5 13 3 2 0 n

key 19 3 2 7 14 21 8 1 3 8 2 8 14 11 3 11

Enc 3 15 17 13 22 23 15 17

CT d p s n w w d p o p 1 e n s a t 2 8 = 73
 as boni 222 24 28 28 222 022 22 22 22 22 22 22

CT = jckm hai vzh ssudam dpm nwdxry

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

PT = ch ec ky ou ni nt en netc on ne ct iv it y x

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

CT = qpavm wcmws vtztzlgp ddklgdidszy

bogus character

(4)

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

P E O S I N T A O S N H S N 2 I N I T E N D V

S P T I S = [B E Y R E A N I] \times K = [B H A C] Key

S I O N I C E A F T E M A D \times K = [K U P P] 103

M O O I O R D I O H X I T N \times K = [B B B I] T2

bogus

$$= \begin{bmatrix} 1 & 4 & 24 & 17 & 4 & 0 & 13 & 8 \\ 4 & 0 & 5 & 19 & 4 & 12 & 0 & 14 \\ 17 & 3 & 14 & 7 & 23 & 18 & 19 & 13 \end{bmatrix} \times \begin{bmatrix} 2 & 6 & 11 & 0 & 19 \\ 8 & 1 & 8 & 1 & 0 \\ 18 & 15 & 13 & 11 & 10 \end{bmatrix} \times K = K \times PT \text{ mod } 26$$

$$CT = \begin{bmatrix} 35 & 10 & 52 & 31 & 50 & 16 & 51 & 34 \\ 345 & 85 & 550 & 655 & 485 & 360 & 415 & 555 \\ 22 & 7 & 17 & 11 & 5 & 20 & 16 & 9 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 9 & 10 & 0 & 5 & 24 & 16 & 25 & 18 \\ 7 & 7 & 4 & 5 & 23 & 22 & 25 & 9 \\ 22 & 7 & 17 & 11 & 5 & 20 & 16 & 9 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \text{key} \quad (1)$$

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

$$CT = J H W K H H A E R F F R Y Z F Q W U Z Z G I J J$$

(5)

(9) eight key = 13425

1 4 2 3 5 bom 21 = 13 4 2 5

TABLE: t m a n s = s t a n n s 13 - P = 29

p o s i t = o p s i o t 10 - 83 = 49

j o n c i = j i n c b o i 15 - 89 = 60

p h e n s = p e s h n s 13 - 89 = 60

a n e v u = a e v n u 13 - 11 = 29

l n e n a = l e n n a 13 - 8 = 59

b l e t o b e t l o

s e r v e n u s v e r u s 13 - P = 49

a L k i n \Rightarrow a k i l n v u t a c s

d s o f c d o f s c

a s t h a c k i s i 9 - t i c k a s

e x t e r i o r i t e x t i t e o

n l y a t n y a l t

a s t h a c k i s i 9 - t i c k a s

C T = t p i p a l b s a d i t i t a s n e e v k o h x y c n i c y v r t e i f e t a k n o o h n m t e l

s p e l a s t i s u a n c m t s g l o m o r b i b u s h a b u h x s g n i a l i

(10) m a a t a t f e d s t e r e v

e c t l m h n h l n e a r i 25 1

c m t j a o e a t n y p 11 1

t a a L s v i t 8 P 1

35 8- 5 0 17 8 8

C T = m a a t e d e e t m h n h l n e a e m t j a p e a t n y t a l v i

- A = 35 bom 85 = 35 bom 8-

$$P_V = (121 \times 23) \bmod 26 = 15 \equiv P_2 \text{ (mod } 26)$$

$$P_Q = (16 \times 23) \bmod 26 = 4 = E$$

$$PE = (4 \times 23) \bmod 26 = 14 \neq 0$$

$$P_F = (5 \times 23) \bmod 26 = 11 = L \rightarrow$$

$$P_K = (10 \times 23) \bmod 26 = 22 = w$$

卷二

PTE = PEOPLE WHO ARE CRAZY ENOUGH TO THINK THEY CAN

CHANGE THE WORLD ARE THE ONES WHO DO IT

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

$$\text{GCD}(26,7) = \text{GCD}(7,5) = \text{GCD}(5,2) = \text{GCD}(2,1) = \text{GCD}(1,0) = 1$$

Using extended Euclidean algo $p_1 \text{ II } p_2 \text{ II } p_3$

$$3 \quad 26 \quad 7 \quad 5 \quad 0 \quad 1 \quad -3$$

400 TO NEED 3-4 BURGUNDY 2-3 BROWN 1-2 BROWNISH VIOLET

2 5 2 1 -3 4 -11
12 5 1 2 3 4 5 6 7 8

$$2 - 1 + 3 - 0 + 5 - 4 - 11 = 18$$

GCD 3 8 1 9 Inverse 7 15 5 9 6 14 11

$$ns \equiv r^{21} \cdot g \cdot p^3 - 11 \pmod{26} \equiv 15 \pmod{26}$$

$$P_F = (5-15) \times 15 \bmod 26 = 6 = G_1$$

$$P_2 = (25 - 15) \times 15 \bmod 26 = 20 \equiv U$$

$$P_A = (0 - 15) \times 15 \bmod 26 = 9 = J$$

PT = GUJARAT COUNCIL ON SCIENCE AND TECHNOLOGY

(8)

(4) USING CIPHER SHIFT $21 = \text{as bom } (85 \times 1) = 49$

$\dots S[T]UVWXYZABCDEFHIJKLMNOP\dots$

$\leftarrow J = H = \text{as bom } (85 \times 1) = 49$

$W = S = \text{as bom } (85 \times 1) = 49$

$$\therefore P_m = T$$

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

(5) CT: GASHOGZXE(H-R)H/GQRDHETU NO... (8)

Value 6 7 2 25 4 7 17 7 6 16 17 7 4 20 13 ...

Key (0, 13, 19, 15, 8, 14, 11, 19, 21, 17, 3) = 42, 20, 14, 3, 14, 0, 11, 20 ...

Dec 19 14 14 11 19 14 13 14 21 14 3 14 10 20 19 ...

PT: O L T O D E C O D E A U P T ...

E T I H O S R G D S A

PT: TOOL TO DECODE AUTOKEY AUTOMATICALLY

(6) CT: 8C Y K T W O H R D P S O K E Q ...

Value 2 24 10 8 19 22 14 7 17 3 15 14 10 4 16 ...

Key 0 7 12 4 3 2 3 0 1 0 3 0 7 12 4 3 ...

Dec 23 17 24 15 28 19 17 14 6 17 0 15 7 24 0 13 ...

PT: C R Y P T O G R A P H Y A N

T = 0 = as bom $81 \times (21-0) = 49$

PT: CRYPTOGRAPHY AND NETWORK SECURITY $85 = 49$

T = P = as bom $81 \times (21-0) = 49$

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

HO JI NUOJ TATRBLU = TP

(9)

Miracle

Page _____
Date _____

CT = LA ZS MC YF TQ HE IM FC PV CS (LA) XV JH 901

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

SKM HSH IAD KIC FVH bogus T

PT = HEY THIS IS PLAYFAIR CIPHER

$$(8) \text{ KEY} = \begin{bmatrix} -B & A & G \\ K & U & P \\ B & B & B \end{bmatrix} \quad \begin{bmatrix} 10 & 21 \\ 10 & 20 & 15 \\ 1 & 1 & 1 \end{bmatrix} \quad q \leftarrow 0 \quad 8$$

$$\Delta = 81(20-15) + 2(110-20) \\ = 81 + 2(-10) \\ = 5 + (-20) = -15 \bmod 26 = 11$$

$$K^T = \begin{bmatrix} 81 & 10 & 1 \\ 0 & 20 & 1 \\ 2 & 15 & 1 \end{bmatrix} \quad \text{Adj}(K) = \begin{bmatrix} 5 & 2 & -40 \\ 5 & -1 & 5 \\ -10 & -1 & 20 \end{bmatrix}$$

Using extended euclidean algorithm

$$\begin{array}{ccccccc} q & g_1 & g_2 & g_1 & t_1 & t_2 & t = t_1 - t_2 q \\ 2 & 26 & 11 & 4 & 0 & 1 & -2 \\ 2 & 11 & 4 & 3 & 0 & 1 & -5 \\ 3 & 3 & 1 & 0 & 5 & 1 & 26 \\ 1 & 0 & & & -7 & & 26 \end{array}$$

GCD

inverse of 19 mod 26

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

$$A^{-1} = \begin{bmatrix} 19 \times 5 & 19 \times 2 & 19 \times (-40) \\ 19 \times 5 & 19 \times (-1) & 19 \times 5 \\ 19 \times (-10) & 19 \times (-1) & 19 \times 20 \end{bmatrix} \bmod 26 = \begin{bmatrix} 17 & 12 & 20 \\ 17 & 7 & 17 \\ 18 & 7 & 16 \end{bmatrix}$$

(10)

Miracle

Page _____
Date _____

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

CT = BAP HVF JIX GIGC HZM ZLY

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

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

$$\begin{bmatrix} J \\ I \\ Y \end{bmatrix} = \begin{bmatrix} 9 \\ 8 \\ 23 \end{bmatrix} \Rightarrow P = \begin{bmatrix} 17 & 12 & 20 \\ 17 & 7 & 17 \\ 18 & 7 & 16 \end{bmatrix} \begin{bmatrix} 9 \\ 8 \\ 23 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 6 \\ 22 \\ 10 \end{bmatrix} = \begin{bmatrix} G \\ W \\ A \end{bmatrix}$$

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

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

PT = FMYNIHCOGWANXXERE

as bom PI = as bom PI

OF SI PI	(ON-)XPI	SXPI	EXPI	= FA
SI SI PI	= 38 boms	EXPI	(I-)XPI	EXPI
DI PI PI	OSXPI	(I-)XPI	(OI-)XPI	

(11)

Miracle

Page _____
Date _____

(9) KEY = I N S E R T

2 3 → 4

∴ KEY = 41253697

(Q1)

KEY⁻¹ = 235146

3	2	3	5	1	4	6	A	T	e
7	P	R	P	a	r	a	r	e	

TABLE: G J I M I U A N N T C

J U E Y R O L O I U

H I I F S S F P a R

E E R C F T

N I T C N E E R M H O M 2 7 8

S Y M R H P E T D E N T

H C T A W I

L W O D V I

O T L K O L

231 = 19

(Q1)

I K 610 = 10

POS = 11 2 3 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

KEY = 2 3 5 1 4 6

G J I M I U A N N T C

J U E Y R O L O I U

H C T A W I

I F E I S P

E R F I S P PT: IMAGINE YOUR LIFE IS

E R F E C T PERFECT IN EVERY

I N E V E R R E S P E C T WHAT WOULD IT

Y R E S P E C T LOOK LIKE

C A T S W R H X A W T V O F T e

W O U L D I

T L O O D I

T K E d i o f t a l s t a i o l a o w n d = d i o f t a l s

(10) TABLE

T E R S H I N

(10)

S	I	A	D	M	I	E	S	E
E	Y	S	Y	S	T	T	F	
C	T	N	H	L	A	V	I	S
U	I	O	T	O	P	R	E	O
R	S	9	3	2	E	I	I	N
		T	3	0	C	E	3	

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

Q3.

(1) PT = YES

I W A T C H

CT = CIW

K I

FOR SHIFT CIPHER, C_i is shift down of K characters of P_i

We get C by shifting Y down by 4 characters

We get I by shifting W down by 5 characters

We get W by shifting S down by 6 characters

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

... S \boxed{T} U V W \boxed{X} Y Z T A ...

PT = TREASURE

→ attack = known plaintext attack

(13)

(2) We are not given any info
 → attack = Brute Force Attack

We know $P_i = C_i - k \pmod{26}$

$\begin{array}{ccccccc} 2 & - & 1 & 0 & 1 & 2 & 3 \\ 2 & - & 1 & 0 & 1 & 2 & 3 \end{array}$

FOR KEY = +1, $\begin{array}{ccccccc} 2 & - & 1 & 0 & 1 & 2 & 3 \end{array}$

PT = MBIZDYQBKZRIKXNCDOQKXYQBKZ ... not possible

FOR KEY + 2, $\begin{array}{ccccccc} 2 & - & 1 & 0 & 1 & 2 & 3 \end{array}$

PT = LAHYCXPAJYQHTWMBCNPJ ... not making sense

\vdots $\begin{array}{ccccccc} 2 & - & 1 & 0 & 1 & 2 & 3 \end{array}$

FOR KEY = +11, $T = P_1 = 28 \pmod{26} \text{ is } 28 \times (2-11) = 19$

PT = CRYPTOGRAPHY = AND = STEGANOGRAPHY = ARE = TWO SIDES

OF A COIN $3 = N = 28 \pmod{26} \text{ is } 28 \times (2-11) = 19$

$8 = 1 = 28 \pmod{26} \text{ is } 28 \times (2-11) = 19$

→ KEY = +11

(3) PT = ab

CT = GL

FOR AFFINE CIPHER WE KNOW THAT, $C_i = (P_i \times K_1) + K_2 \pmod{26}$

$$\therefore 6 = (0 \times K_1) + K_2 \pmod{26}$$

$$11 = (1 \times K_1) + K_2 \pmod{26}$$

$$\rightarrow \therefore K_2 = 6 \Rightarrow K_1 = 5$$

Possible because $\text{GCD}(26, 5) = 1$

Using extended euclidean algorithm to find t_2 (5)

$$912 = 26 \times 35 + 16 \quad t_2 = -5 \quad t = t_1 - t_2 q$$

$$26 = 5 \times 5 + 1 \quad t_1 = 1$$

$$5 = 1 \times 5 + 0 \quad -5 \cdot 1 = -5$$

GCD

Inverse

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

Decipher text ..

$$\therefore P_i = (C_i - k_2) \times k_1^{-1} \bmod 26$$

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

$$P_p = (15 - 6) \times 21 \bmod 26 = 17 = H$$

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

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

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 n y a p h t m o s d f i k x o = 3

g a h n o b i m 2 e t f i k x l = 11

3 4 5 6 7 8

9 b d e f j p k ← e s ←

j k l m o n g p c o r e a d i s e o p

s u v w x z

15

PT: 18 DC SD 07 RU DR AB AR SAD

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

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

$$PT = \begin{bmatrix} 1-C O U A R \\ 8 5 7 D B A \\ 1-D O R R A D \end{bmatrix} = \begin{bmatrix} 1 & 2 & 0 & 20 & 0 & 17 \\ 8 & 18 & 7 & 3 & 1 & 1 \\ 3 & 0 & 17 & 17 & 0 & 3 \end{bmatrix}$$

$$CT = \text{Key} \times PT \bmod 26$$

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

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

$$= \begin{bmatrix} 7 & 2 & 8 & 2 & 0 & 23 \\ 7 & 16 & 5 & 21 & 20 & 1 \\ 12 & 20 & 24 & 40 & 1 & 21 \end{bmatrix} \quad \text{or} \quad \begin{bmatrix} H & C & I & 8 & A & X \\ H & Q & F & U & B \\ M & V & Y & B & V \end{bmatrix}$$

$$CT = H H M C Q U I F Y A U B X B V$$

Q6. $P = 18 + 7 = 25 \quad (\because 18 \text{ DC } 0007)$

(i) $\text{GCD}(132, 25) = \text{GCD}(25, 7) = \text{GCD}(7, 4) = \text{GCD}(4, 3) = \text{GCD}(3, 1)$

$= \text{GCD}(1, 0)$

Using extended euclidean algorithm

a	g_1	g_2	g_i	t_1	t_2	$t = t_1 - t_2 g_i$
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	<u>-21</u>	37	as bmod -90
<u>1</u>						37
GCD	0	0	37	0 mod 26	= 1	
as bmod	1	1	3	7	81	8
	8	0	1	0	8	1

(ii) $\text{GCD}(80, 25) = \text{GCD}(25, 5) = \text{GCD}(5, 0) \quad \therefore \text{GCD} = 5 \neq 1$

Using extended Euclidean algorithm Inverse not possible

Q7. $P = 18 + 07 = 25 \quad (\because 18 \text{ DC } 0007)$

Total numbers of keys in affine form $Z_P = p \times \# Z^*_P$

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

$$\therefore \text{TOTAL POSSIBLE KEYS} = 25 \times 20 \\ = 500$$

(17)

$$Q8. PT = 18DCS007RUDRABA \text{ as ham key } = (7, 12) \quad \text{for part}$$

$$P = 81 = \text{as ham } 31 \times (S-H) \quad \text{for part}$$

$$C_1 = (1 \times 7) + 2 \pmod{26} \Rightarrow 9 = 3^5 \times (S-S) \quad \text{for part}$$

$$C_8 = (8 \times 7) + 2 \pmod{26} \Rightarrow 66 = 2^6 \times (S-S) \quad \text{for part}$$

$$C_D = (3 \times 7) + 2 \pmod{26} = 23 = X \quad \text{for part}$$

$$C_C = (2 \times 7) + 2 \pmod{26} = 16 = Q \quad \text{for part}$$

$$C_S = (18 \times 7) + 2 \pmod{26} = 124 = 2^5 D \Rightarrow Y = 79 \quad \text{for part}$$

$$C_O = (0 \times 7) + 2 \pmod{26} = 2 = C \quad \text{for part}$$

$$C_0 = (0 \times 7) + 2 \pmod{26} = 2 \pmod{26} \quad \text{for part}$$

$$C_7 = (7 \times 7) + 2 \pmod{26} = 51 = 2^5 C \quad \text{for part}$$

$$\vdots$$

$$\therefore CT = JG_1 \times QYCCYRMXRCJC \Rightarrow 18DCS007RUDRABA = 79 \quad \text{for part}$$

$$CT = 30E933D1M3LDC \quad \text{for part}$$

$$\rightarrow \text{For AFFINE, } P_i = (c_i - k_2) \times k_1^{-1} \pmod{26}$$

$$\text{as ham } S-T = 79 \quad \text{part}$$

Using extended euclidean algo,

$$q \quad g_1 \quad g_2 \quad n \quad t_1 \quad t_2 \quad t = t_1 - q t_2$$

$$3 \quad 26 \quad 7 \quad 5 \quad 6 \quad 1 \quad -3 \quad \text{for part}$$

$$1 \quad 7 \quad 5 \quad 2 \quad 1 \quad -3 \quad \text{for part}$$

$$2 \quad 5 \quad 2 \quad 1 \quad -3 \quad \text{for part}$$

$$2 \quad 2 \quad 1 \quad -3 \quad \text{for part}$$

$$\underline{1} \quad 0 \quad -11 \quad 26 \quad \text{for part}$$

$$\text{GCD} \quad \text{Inverse} \quad 18DCS007RUDRABA = 79 \quad \text{for part}$$

$$-11 \pmod{26} = 15 \pmod{26} \quad \text{for part}$$

$$\therefore CT = JG_1 \times QYCCYRMXRCJC \Rightarrow 18DCS007RUDRABA = 79 \quad \text{for part}$$

$$P_J = (9-2) \times 15 \pmod{26} = 15 \pmod{26} \quad \text{for part}$$

$$P_{G_1} = (6-2) \times 15 \pmod{26} = 15 \pmod{26} \quad \text{for part}$$

$$P_X = (23-2) \times 15 \pmod{26} = 3 = D \quad \text{for part}$$

$$P_8 = (16-2) \times 15 \bmod 26$$

$$P_y = (24-2) \times 15 \bmod 26 = 18 = S$$

$$P_C = (2-2) \times 15 \mod 26 = 0 \neq 05 + (1+1) = 10$$

$$P_C = (2-2) \times 15 \bmod 26 = 10 \text{ mod } 26 = 10$$

$$P_{87} = 65 \quad v = 88 = \text{as soon as } st(1x^2) = 65$$

$$g = \partial f = \text{as hom } s + (fx) = c$$

~~PT~~ PT = 180 CS007 RUDRABA M 5t (RXB1) = 3

$\phi = g \circ \text{asym} \circ f(rx_0) = \phi$

(1) Suppose key = (1,2) is as best st (fxo) = o

$$\text{then } CT = (PT \times 1) + 2 \bmod 26 = PT + 2 \bmod 26$$

For eg. PT = 18D(S007 RUDRA BARYA X 10) = P

CT = 30FEU229 TWFTC DC

for define , $p_i = (c_i - p_s) \times p_i$ we get see

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

PT = 18DCSOOTRUDRAFBIAJG bbbmixs pnieu

\therefore Additive cipher is special case of affine cipher

(ii) Suppose $\text{Rey} = (7, 0)$

$$\text{then } CT = (PI \times 7) + 0 \pmod{26} = PI \times 7 \pmod{26}$$

then $Ct = (P \times t) + b \pmod{2^8}$

Eg. PT = 18DCS0107RUDRABA

as (TME 21) VOW OX PKVPAHA

$$\text{Using } PT = CT \times 7^{-1} \pmod{26} \Rightarrow 17 \times 7^{-1} \pmod{26} = 13$$

CT = 18D(5007 RUDRA BA 21 x (S-P) + 18

\therefore Multiplicative cipher is special case of affine cipher

$$D = 3 \text{ kg/m}^3 \quad (35-5) \times 10^3 \text{ kg/m}^3$$

Q9. $K = (18007)_{10} = (100011001010111)_2$

$$\therefore K = 1000110010101110$$

(i) Permutation on 10 bit Key

I/P = 1000110010 → initial permutation

O/P = 0100001101 [using 8 qmb]

3	5	2	7	4	10	1	9	8	6
---	---	---	---	---	----	---	---	---	---

(ii) Circular left shift on both halves = 9(0)

I/P = 010001010111101000

O/P = 00100101011010111001
1011 0110

(iii) Apply compression D box →

6	3	7	4	8	5	10	9
---	---	---	---	---	---	----	---

I/P = 00100 10110 [using 8 qmb & only 6 bits] (ii)

O/P = 11001001 —

K ₁

(iv) Apply shift left operator on O/P of step (ii)

I/P = 00100 10110

O/P = 01000 01100 [using 8 qmb & only 6 bits] (iii)

(v) Apply compression D box

I/P = ~~0001001110~~ 01000 01100

O/P = ~~0001000000~~ 00101000

L

K ₂

 [using 8 qmb & only 6 bits] (iii)

$$K_1 = 1100100110111000 \leftarrow 9(0)$$

$$K_2 = 0010100011001001$$

$$[K_2] \leftarrow 1010011011011011$$

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

$(228077 = P + 1) = 12$ ADD A A A A E 16 DBA AAD

KEY = $1010^{5} 1101^{9} 0101^{13} 0101001 \dots$ (10081) = A
 $1010^{17} 1010^{21} 1010^{25} 1010^{29} 1110 \dots$ (1000110001) = B
 $0001^{33} 0110^{37} 1101^{41} 1011^{45} \dots$
 $1010^{49} 1010^{53} 1010^{57} 1010^{61} 1101 \dots$ (Circular shift of H101)

Initial State

(ii) Apply parity drop & permutation

O/P = 1110 1111 0010 1101 (Initial state)
 $0001 0111 1110 / 1011 0000 1010 = 912$
 $1001 1110 1111 / 0010 0111 0101 = 910$
 $0110 1101$

Initial State \rightarrow Apply compression D box (iii)

(iii) Dividing into 2 parts

$L = 00100 10110$

$R = 1110 1111 0010 1101 0001 0111 1100$

$R = 1110 1111 1001 1110 1111 0010 0110 0110$ (Initial state) (iv)

(iii) Apply 1 bit circular shift on both halves

$L = 1101 1110 0101 1010 0010 1111 1101$
 $R = 0111 0010 1011 1011 0001 1010 1010$ (Initial state) (v)

Initial State \rightarrow Apply compression D box = 910

(iii) Apply compression D box

O/P \rightarrow 0001 1101 1111011111

1001 0010 1111 0110 = K₁

1101 0100 0011 1010 \rightarrow [K₁]

Thus we get first round key₁ $K_1 = (1D649377D835)_{16}$