ANKIT GOYAL
Roll No - 17103011
CSE Final Year

1. letter ⇒ (a-z) = 26
digits ⇒ (0-9) = 10
$\overline{\quad 36 \quad}$

(a) Key size = 36, modulus = 36

(b) Key size ⇒ only values whose gcd (a, 36) ≡ 1 will be in key domain.

Hence key domain ⇒ possible values of a
≡ (1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35)

Key size = 12
modulus = 36

(c) Key domain = (Key domain of additive) * (Key domain of multiplicative)

= 12 * 36 = 432

modulus = 36

2.

(a) Additive cipher with key 20.

Encryption formula ⇒ (character No. + key) % 26

Message = "this is an exercise"

t → n
h → b
i → c
s → m
i → c
s → m

a → u
n → h
e → y
x → r
e → y
r → l

c → w
i → c
s → m
e → y

Encrypted text ⇒ nbcn cn uh yrylwcmy

Decryption formula ⇒

$$\left(\text{Character No} - \underset{+26}{\text{Key}}\right) \% \; 26$$

Decryption ⇒ .

n → t	m → s	y → e
b → h	u → a	d → r
c → i	h → n	w → c
h → s	y → e	c → i
c → i	r → x	m → s
		y → e

Decrypted text ⇒ this is an exercise.

(b) Multiplicative cipher :- (With Key 15)

Encryption formula ⇒ (Character No * Key) % 26

message ⇒ " this is an exercise".

t → z	a → a	c → e
h → 6	n → n	i → q
i → q	e → i	s → k
s → k	x → h	e → i
i → q	e → i	
s → k	r → v	

encrypted string ⇒ ~~zb qk qk an~~
26 qK ak on ihiveqki

Decryption formula ⇒
(character No. * (Key^{-1})) % 26
Key^{-1} ⇒ 15^{-1} = (7) mod 26

z → t		
b → h	a → a	v → r
q → i	n → n	e → c
k → s	i → e	q → i
q → i	h → x	k → s
k → s	i → e	i → e

Decrypted string ⇒ this is an exercise

(c) Affine Cipher with key (15, 20)

Encryption formula ⇒ (character No * 15 + 20) % 26

t → t	n → h	i → K
h → v	e → c	s → e
i → k	x → c	e → c
s → e	r → p	
a → u	c → y	

Encrypted string ⇒ tvke ke uh cb cpykec

Decryption formula ⇒ ((character No − 20) * (15^{-1})) % 26

t → t	u → a	y → c
v → h	h → n	K → i
K → i	c → e	e → s
e → s	b → x	c → e
K → i	c → e	
e → s	p → r	

Decrypted string ⇒ this is an exercise.

3. Vigegnre table :- A table of 26 X 26 size with each alphatics in different row, each alphabet shifted equvically to left compared to previous alphabet. corrosponding to 26 possible shift ciphers.

Text ⇒ LIFE IS FULL OF SURPRISES

Key ⇒ HEAL TH HEAL TH HEALTHHEA

Encrypted ⇒ smfpbzmy lw hn zy ra kpzis

4. We live in an insecure world ⇒

$$K = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}$$

we live in an secure worldz.

we $\begin{bmatrix} 22 \\ 4 \end{bmatrix} \Rightarrow \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 22 \\ 4 \end{bmatrix} = \begin{pmatrix} 56 \\ 138 \end{pmatrix} = \begin{bmatrix} 4 \\ 8 \end{bmatrix}$ = EI

li: $\begin{bmatrix} 11 \\ 8 \end{bmatrix} \Rightarrow \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 11 \\ 8 \end{bmatrix} = \begin{bmatrix} 46 \\ 111 \end{bmatrix} = \begin{bmatrix} 20 \\ 7 \end{bmatrix}$ = UH

ve: $\begin{bmatrix} 21 \\ 4 \end{bmatrix} \Rightarrow \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 21 \\ 4 \end{bmatrix} = \begin{bmatrix} 54 \\ 133 \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$ = CD

in: $\begin{bmatrix} 8 \\ 13 \end{bmatrix} \Rightarrow \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 8 \\ 13 \end{bmatrix} = \begin{bmatrix} 55 \\ 131 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$ = DB

an: $\begin{bmatrix} 0 \\ 13 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 0 \\ 13 \end{bmatrix} = \begin{bmatrix} 39 \\ 91 \end{bmatrix} = \begin{bmatrix} 13 \\ 13 \end{bmatrix}$ = NN

in: $\begin{bmatrix} 8 \\ 13 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 8 \\ 13 \end{bmatrix} = \begin{bmatrix} 55 \\ 131 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$ = DB

se: $\begin{bmatrix} 18 \\ 4 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 18 \\ 4 \end{bmatrix} = \begin{bmatrix} 48 \\ 118 \end{bmatrix} = \begin{bmatrix} 22 \\ 14 \end{bmatrix}$ = WO

cu: $\begin{bmatrix} 2 \\ 20 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 2 \\ 20 \end{bmatrix} = \begin{bmatrix} 64 \\ 150 \end{bmatrix} = \begin{bmatrix} 12 \\ 20 \end{bmatrix}$ = MU

re: $\begin{bmatrix} 17 \\ 4 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 17 \\ 4 \end{bmatrix} = \begin{bmatrix} 46 \\ 113 \end{bmatrix} = \begin{bmatrix} 20 \\ 9 \end{bmatrix}$ = UJ

wo = $\begin{bmatrix} 22 \\ 14 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 22 \\ 14 \end{bmatrix} = \begin{bmatrix} 86 \\ 208 \end{bmatrix} = \begin{bmatrix} 8 \\ 0 \end{bmatrix}$ = IA

rl: $\begin{bmatrix} 17 \\ 11 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 17 \\ 11 \end{bmatrix} = \begin{bmatrix} 67 \\ 162 \end{bmatrix} = \begin{bmatrix} 15 \\ 6 \end{bmatrix}$ = PG

dz: $\begin{bmatrix} 3 \\ 25 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}\begin{bmatrix} 3 \\ 25 \end{bmatrix} = \begin{bmatrix} 81 \\ 190 \end{bmatrix} = \begin{bmatrix} 3 \\ 8 \end{bmatrix}$ = DI

Encoded string ⇒ EIUH CDD BNNDB MOMUUJIAPGDI

5. 5X5 matrix ⇒

$$\begin{array}{c|ccccc} & 1 & 2 & 3 & 4 & 5 \\ \hline 1 & m & o & n & a & r \\ 2 & c & h & y & b & d \\ 3 & e & f & g & i & k \\ 4 & l & p & q & s & t \\ 5 & u & v & w & x & z \end{array}$$

↓ row

message ⇒ instruments ⟶ Z- added explicitly

in ① st ② ru ③ me ④ nt ⑤ sz ⑥

		row	col		encoded
① in ⇒	i :	3	4	⇒	ga
	n :	1	3		
② st ⇒	s :	4	4	⇒	tl
	t :	4	5		
③ ru ⇒	r :	1	5	⇒	mz
	u :	5	1		
④ me ⇒	m :	1	1	⇒	cl
	e :	3	1		
⑤ nt ⇒	n :	1	3	⇒	rq
	t :	4	5		
⑥ sz ⇒	s :	4	4	⇒	tx
	z :	5	5		

encoded string ⇒ gatlmzclrqtx