Final

1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M
14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Ceasar Cipher

Cipher, $C = E(K,P) = (P+k) \bmod 26$

plain, $P = D(K,C) = (C-K) \bmod 26$

Example:

- $m \rightarrow 13+3 = 16 \bmod 26 = 16$
  $16 \rightarrow P$
- $y \rightarrow 25+3 = 28 \bmod 26 = 2$
  $2 \rightarrow B$

⊞ For $K=3$

Plain text: meet me after the toga party

Cipher text: PHHW PH DIWHU WKH WRJD SDUWB

→ can be written in both uppecase or lowercase

⊞ For $K=5$

Plain text: classes have not been held property due to many socio cultural issues

Cipher text: hqfxxjx mfaj sty gjjs mjqi uwtujwqd izj yt rfsd xthnt hzqyzwfq nxxzjx

Mono Alphabetic Substitution

Plain-text:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y
Cipher-text:	Q	W	E	R	M	R	T	Y	U	I	O	P	S	D	F	G	H	J	K	L	Z	X	C	V	B

For : 'attack'

Cipher: 'QLLQEO'

Poly-Alphabetic Substitution

Plain-text: MEET

Keyword : KEYK

key: KEY → 11 5 25

M with K shift (10) 11-1

- M → (13 + 10) → 23rd letter → W

E with E shift (4) → 5-1

- E → (5 + 4) → 9th letter → I

E with Y shift (24) → 25-1

- E → (24 + 5) → 29th letter → (29-26) → 3rd letter → C

T with K shift (10)

- T → (10 + 20) → 30th letter → (30-26) → 4th letter → D

∴ Encrypted : WICD

Rail Fence Cipher

For 2 rows:

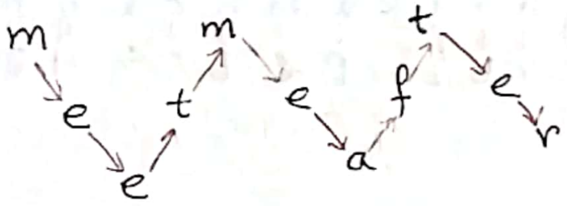
Plain text: meet me after

```
m   e   m   a   t   r
  e   t   e   f   e
```

Ciphertext: mematretefe

For 3 rows:

Plain-text: meet me after



Cipher-text: mmtetefeear

Row Transposition Cipher

- First the letters are included according to the number ~~of~~ or alphabet sequence (012..., abc...) then the columns are exchanged according to the sequence of the keys. Then row-wise write them

Key: 41532

Plain text: the simplest possible transpositions

1	2	3	4	5
t	h	e	s	i
m	p	l	e	s
t	p	o	s	s
i	b	l	e	t
r	a	n	s	p
o	s	i	t	i
o	n	s	x	x

4	1	5	3	2
s	t	i	e	h
e	m	s	l	p
s	t	s	o	p
e	i	t	l	b
s	r	p	n	a
t	o	i	i	s
x	o	x	s	n

∴ Cipher Text: stiehemslpstsopeitlbsrpnatoiisxoxsn

Q1 (Set-A)

2 Key: 4132

Plaintext: The man who passes the sentence should swing the sword

1	2	3	4
t	h	e	m
a	n	w	h
o	p	a	s
s	e	s	t
h	e	s	e
n	t	e	n
c	e	s	h
o	u	l	d
s	w	i	n
g	t	h	e
s	w	o	r
d	x	x	x

4	1	3	2
m	t	e	h
h	a	w	n
s	o	a	p
t	s	s	e
e	h	s	e
n	n	e	t
h	c	s	e
d	o	l	u
n	s	i	w
e	g	h	t
r	s	o	w
x	d	x	x

∴ cipher text: mtehhawnsoaptsseehsennethesedolunsiweghtrsowxdxx

Columnar Transposition Cipher

- According to the sequence number of key, put the values and then column wise • write• them-according to the actual sequence of the numbers.

Keyword: HACK
Plain text: meet me after the party
order of keyword: 3124

H	A	C	K
3	1	2	4
m	e	e	t
m	e	a	f
t	e	r	t
h	e	p	a
r	t	y	x

Cipher text: eeeetearpymmthrtftax

⊞ Keyword: ANALYST
Plain text: the nose is pointing down and the houses are getting bigger
order: 1423756

A	N	A	L	Y	S	T
1	4	2	3	7	5	6
t	h	e	n	o	s	e
i	s	p	o	i	n	t
i	n	g	d	o	w	n
a	n	d	t	h	e	h
o	u	s	e	s	a	r
e	g	e	t	t	i	n
g	b	i	g	g	e	r

ciphertext: tiiaoegepgdseinodtetghsnnugbsnweaieetnhrnr oiohstg

~~128^{23} mod 160~~

~~$= \{[(128^2 \text{ mod } 160) \times 10] \times 128^1 \text{ mod } 160\} \text{ mod } 160$~~

RSA

* M is smaller than n.

- Select two large prime number at random
  $p = 17$ and $q = 11$
- $n = p \times q = 17 \times 11 = 187$
- $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$
- $e = 7$
- $d = \frac{1 + K \times \phi(n)}{e}$

$= \frac{1 + K \times 160}{7}$

$= \frac{1 + (1 \times 160)}{7}$

$= 23$

$\gcd(7, 160) = 1$

$; e \times d = 1 \text{ mod } \phi(n)$

$e \times d = 1 + K \times \phi(n)$

PU (Public key) = {e, n}

PR (Private key) = {d, n}

$C = M^e \text{ mod } n$

$D = C^d \text{ mod } n$

Text = How are you?

H = 02
o = 03
w = 04
– = 05

a = 06
r = 07
e = 08
– = 09

Y = 10
o = 11
u = 12
? = 13

$C_1 = (2)^7 \text{ mod } 187 = 128$

$C_2 = (3)^7 \text{ mod } 187 = 130$

$C_3 = (4)^7 \text{ mod } 187 = 115$

$C_4 = (5)^7 \text{ mod } 187 = 146$

$C_5 = (6)^7 \text{ mod } 187 = 184$

$C_6 = (7)^7 \text{ mod } 187 = 182$

$C_7 = (8)^7 \text{ mod } 187 = 134$

$C_8 = (9)^7 \text{ mod } 187 = 70$

$C_9 = (10)^7 \text{ mod } 187 = 175$

$C_{10} = (11)^7 \text{ mod } 187 = 88$

$C_{11} = (12)^7 \text{ mod } 187 = 177$

$C_{12} = (13)^7 \text{ mod } 187 = 106$

$M_1 = 128^{23} \text{ mod } 187 = 2$

$M_2 = 130^{23} \text{ mod } 187 = 3$

$M_3 =$

$M_4 =$

$M_5 =$

$M_6 =$

$M_7 =$

$M_8 =$

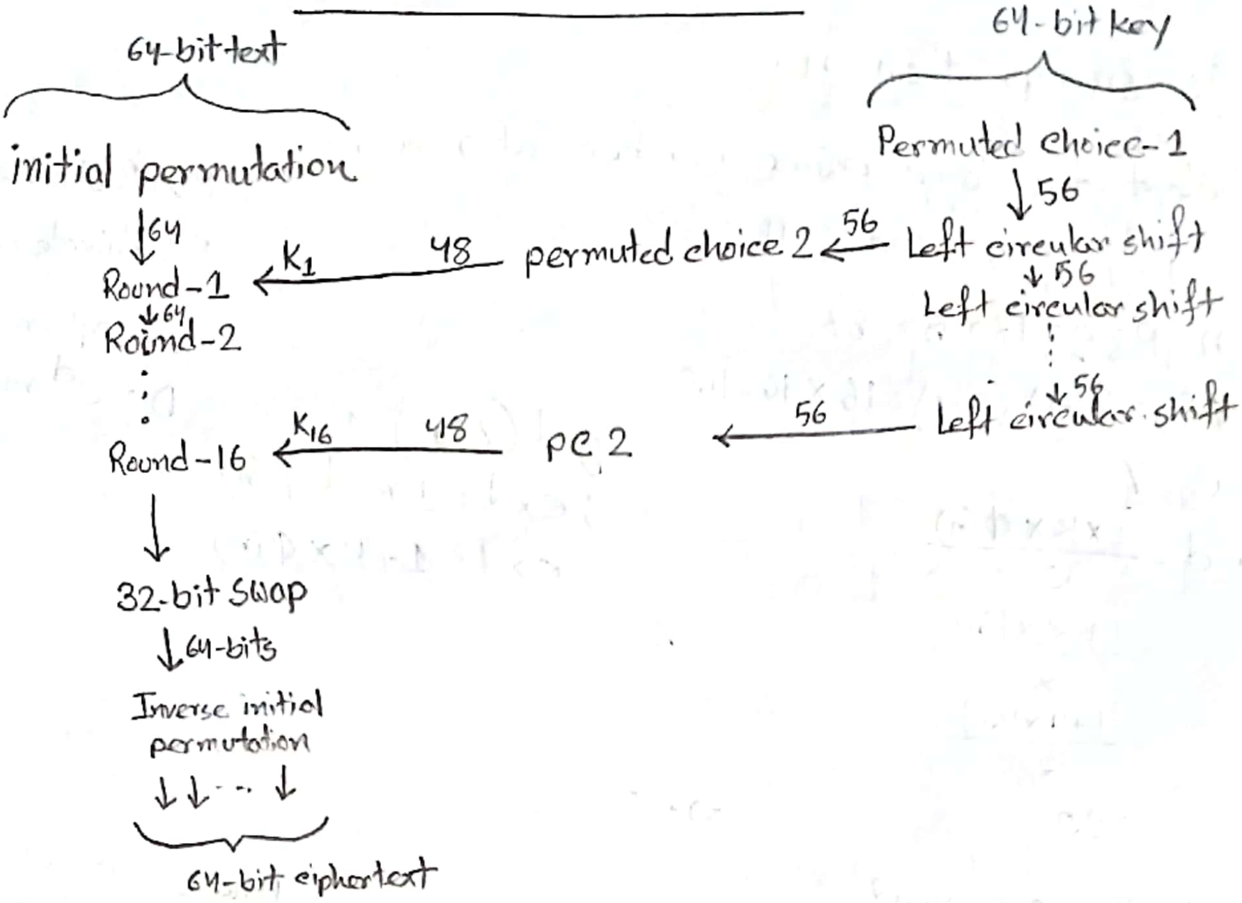
$M_9 =$

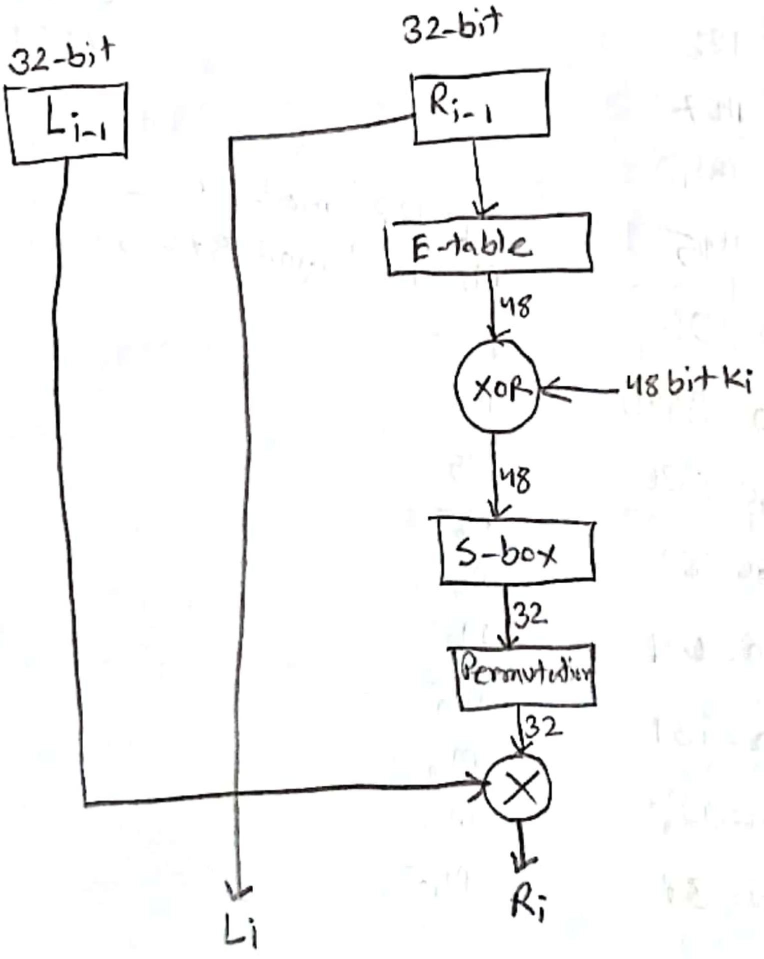
$M_{10} =$

$M_{11} =$

$M_{12} =$

DES (Single Round)





ASCII values:

A → 65
⋮ +32 (for lowercase)
Z → 90

a → 97
⋮
z → 122

space → 32
! → 33
? → 63
. → 46

, → 44

Step-1: Converting the text to Binary and add padding (10000000)

Input Text: "Ansary"

A =	01000001	1-8
n =	01101110	9-16
s =	01110011	17-24
a =	01100001	25-32
r =	01110010	33-40
y =	01111001	41-48
	10000000	49-56
	10000000	57-64

Step-2: Initial Permutation (IP) For input text

$$L_0 \left\{ \begin{array}{cccccccc} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{array} \right.$$

$$R_0 \left\{ \begin{array}{cccccccc} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array} \right.$$

Step-3: Takes the key in Binary and Apply PC1

$$\begin{array}{ccccccccl} 0&0&1&1&0&1&0&0&1\text{-}8\\ 0&0&1&0&1&1&0&1&9\text{-}16\\ 1&0&1&1&0&1&0&1&17\text{-}24\\ 1&0&1&0&1&0&0&0&25\text{-}32\\ 0&0&0&1&1&1&0&1&33\text{-}40\\ 1&1&0&1&1&0&1&1&41\text{-}48\\ 1&0&0&1&0&0&0&0&49\text{-}56\\ 0&0&0&0&0&1&0&0&57\text{-}64 \end{array} \longrightarrow \begin{array}{rccccccc} C: &0&1&1&0&1&1&0\\ &0&0&0&1&0&0&0\\ &0&0&0&0&0&0&1\\ &1&1&1&0&1&1&1\\ D: &0&0&1&0&0&0&0\\ &0&1&0&0&1&0&1\\ &1&1&0&0&1&1&1\\ &0&1&0&0&1&0&1 \end{array}$$

Step-4: Key generation

ⓐ Left circular shift (once) ⓑ PC-2

$$\begin{array}{lccccccc} 1\text{-}7 &1&1&0&1&1&0&0\\ 8\text{-}14 &0&0&1&0&0&0&0\\ 15\text{-}21 &0&0&0&0&0&1&1\\ 22\text{-}28 &1&1&0&1&1&1&0\\ 29\text{-}35 &0&1&0&0&0&0&0\\ 36\text{-}42 &1&0&0&1&0&1&1\\ 43\text{-}49 &1&0&0&1&1&1&0\\ 50\text{-}56 &1&0&0&1&0&1&0 \end{array} \longrightarrow \left.\begin{array}{cccccc} 0&0&0&0&1&1\\ 0&0&0&0&1&1\\ 1&0&0&1&1&0\\ 0&0&1&1&0&1\\ 1&0&0&0&1&1\\ 1&0&0&0&0&1\\ 0&0&1&0&0&1\\ 1&1&1&1&0&0 \end{array}\right\} K_1$$

Step-5: Round-1 : $\overset{\rightarrow 32\,\text{bit}}{R_0} \rightarrow$ e-bit → 48-bit

$$R_0: \begin{array}{cccccccc} 1&1&0&0&0&0&0&0\\ 0&0&1&1&1&1&1&0\\ 0&0&1&0&0&0&1&0\\ 0&0&0&1&0&1&1&0 \end{array} \longrightarrow \begin{array}{cccccc} 0&1&1&0&0&0\\ 0&0&0&0&0&0\\ 0&0&0&1&1&1\\ 1&1&1&1&0&0\\ 0&0&0&1&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 1&0&1&1&0&1 \end{array}$$

XOR → Same : 0
diff : 1

48 bit R0
48 bit

- XOR with K1

Row
Column

0 1 1 0 1 1
0 0 0 0 1 1
1 0 0 0 0 1
1 1 0 0 0 1
1 0 0 1 1 1
1 0 0 1 0 1
0 0 1 0 1 1
0 1 0 0 0 1

- S-boxes:

S1 :	Row : 01 = 1	Column : 1101 = 13	value from S1 : 5 → 0101
S2 :	01 = 1	0001 = 1	: 13 → 1101
	11 = 3	0000 = 0	: 1 → 0001
	11 = 3	1000 = 8	: 9 → 1001
	11 = 3	0011 = 3	: 7 → 0111
	11 = 3	0010 = 2	: 2 → 0010
	01 = 1	0101 = 5	: 9 → 1001
	01 = 1	1000 = 8	: 12 → 1100

- Permutation:

1-4	0 1 0 1	→	1 0 1 0
5-8	1 1 0 1		1 1 1 0
9-12	0 0 0 1		0 0 1 0
13-16	1 0 0 1		1 1 0 0
17-20	0 1 1 1		1 1 0 0
21-24	0 0 1 0		0 0 0 0
25-28	1 0 0 1		1 1 1 1
29-32	1 1 0 0		0 0 1 1

- XOR with L_0

```
0 0 1 1 1 1 1 1         1 0 1 0 1 1 1 0         1 0 0 1 0 0 0 1
0 0 1 1 0 1 0 0    ⊕    0 0 1 0 1 1 0 0    →    0 0 0 1 1 0 0 0
0 0 0 0 0 0 1 0         1 1 0 0 0 0 0 0         1 1 0 0 0 0 1 0
0 0 1 0 1 1 0 1         1 1 1 1 0 0 1 1         1 1 0 1 1 1 1 0
```

32-bit swap → - L_1 is initial R_0 ; R_1 is the latest output - Putting R_i under L_1

```
1-8   1 1 0 0 0 0 0 0
9-16  0 0 1 1 1 1 1 0
17-24 0 0 1 0 0 0 1 0
25-32 0 0 0 1 0 1 1 0
33-40 1 0 0 1 0 0 0 1
41-48 0 0 0 1 1 0 0 0
49-56 1 1 0 0 0 0 1 0
57-64 1 1 0 1 1 1 1 0
```

- Apply IP^{-1} :

```
1 0 0 0 0 0 0 0
0 0 0 1 1 1 1 1
0 0 0 1 0 0 1 1
0 0 1 1 0 0 1 0
1 0 1 1 0 0 1 1
0 0 0 1 0 1 0 0
0 1 0 0 1 0 1 0
1 1 0 0 1 0 1 0
```

(Ans) after Round-1

Quiz-1:

1(a) PlainText: WINTER IS COMING

1-8	W	=	0 1 0 1 0 1 1 1
9-16	I	=	0 1 0 0 1 0 0 1
17-24	N	=	0 1 0 0 1 1 1 0
25-32	T	=	0 1 0 1 0 1 0 0
33-40	E	=	0 1 0 0 0 1 0 1
41-48	R	=	0 1 0 1 0 0 1 0
49-56	_	=	0 0 1 0 0 0 0 0
57-64	I	=	0 1 0 0 1 0 0 1

Block-1

1-8	S	=	0 1 0 1 0 0 1 1
9-16	_	=	0 0 1 0 0 0 0 0
17-24	C	=	0 1 0 0 0 0 1 1
25-32	O	=	0 1 0 0 1 1 1 1
33-40	M	=	0 1 0 0 1 1 0 1
41-48	I	=	0 1 0 0 1 0 0 1
49-56	N	=	0 1 0 0 1 1 1 0
57-64	G	=	0 1 0 0 0 1 1 1

Block-2

1(b)

For Block-1:

1 0 1 1 1 1 1 1
0 0 1 0 1 0 0 1
0 0 0 1 1 1 0 1
1 0 0 1 0 0 1 1
0 0 0 0 0 0 0 0
0 1 0 0 0 0 0 0
1 0 0 0 0 1 1 0
0 0 1 0 0 1 0 1

For Block-2:

1 1 1 1 1 1 0 1
0 0 0 0 0 0 0 1
1 1 0 1 1 0 0 0
1 0 1 1 1 1 0 1
0 0 0 0 0 0 0 0
0 0 0 0 0 0 1 0
0 1 1 1 1 0 0 0
1 1 0 0 1 1 0 1