Ques-1. Encrypt the Plain text "she is listening" and its key is "PASCAL" using method-2 of Vigenere Cipher.

Plain text ⇒ she is listening

Key = PASCAL

(15, 0, 18, 2, 0, 11) (according to ceaser cipher table)

Key value differs

Plain text	S	H	E	I	S	L	I	S	T	E	N	I	N	G
Plain is ~~text~~ value	18	7	4	8	18	11	8	18	19	4	13	8	13	6
~~P's value~~	~~15~~	~~0~~	~~18~~											
Key Stream	15	0	18	2	0	11	15	0	18	2	0	11	15	0
C's value	7	7	22	10	18	22	23	18	11	6	13	19	2	6
Cipher text	H	H	W	K	S	W	X	S	L	G	N	T	C	G
Plain	18	7	4	8	18	11	8	18	19	4	13	8	13	6
Value	S	H	E	I	S	L	I	S	T	E	N	I	N	G

Decryption Method

→ (C - K) mod 26

= (7 - 15) mod 26

= -8 mod 26

= -8 + 26

= 18

Ques-No:2. Difference between Block Cipher and Stream Cipher.

Block Cipher	Stream Cipher
• In Block cipher, keys and algorithms are applied to block of data.	• In stream cipher, keys and algorithms are applied to each binary digit or to one bit at a time.

• Block cipher is more time consuming.	• Stream cipher is less time consuming.
• It is slower than stream cipher.	• It is faster than block cipher.
• It is used in chaining modes of operation.	• Stream cipher is not used in chaining modes of operation.
• Software implementation is easy using block cipher.	• Hardware implementation is easy using stream cipher.

Ques-3. What is Transposition cipher? Explain.

(a) Rail Fench
(b) Row Transposition
(c) Double Transposition

Transposition cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

Ex→ Plain text → Hello World

H	e	l	l
o	w	o	r
l	d		

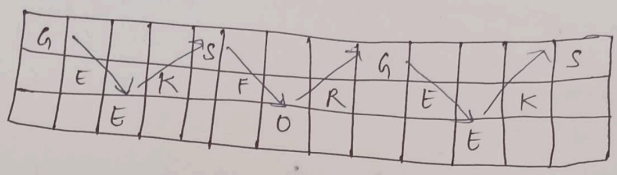
Cipher text Holewdlolr.

(a) Rail Fence Cipher–

The Rail Fence Cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.

Ex→ Input: "Geeks for Geeks"
key = 3

(3) Using



Output: GSGSEKFREKEOE

(b) Row Transposition Cipher –

Plain text → written row by row in a rectangle.
Cipher text → write out the columns in an order specified by a key.

Ex → Plain text → Attack postponed until two am.

key ⇒ 3 4 2 1 5 6 7

a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

Dummy bits

Cipher text →

TTNAAPTMTSUOAODWCOIXKNLYPETZ.

(c) Double Transposition Cipher –

Double transposition cipher consists of two applications of columnar transposition to a message. The two application may use the same key for each of the two steps, or they may use different keys. Now ~~the~~ number the letters in the keyword in alphabetic order.

Ex → ~~from the~~ Plain text → Attack started down

③ ... and uses a 56-bit key during ... from full 64-bit

key ⇒ 123

a	t	t
a	c	k
x	a	t
x	d	a
w	n	x → dummy bit

Ciphers ⇒ aa xxaw t cadu t k t ax

for double transposition →

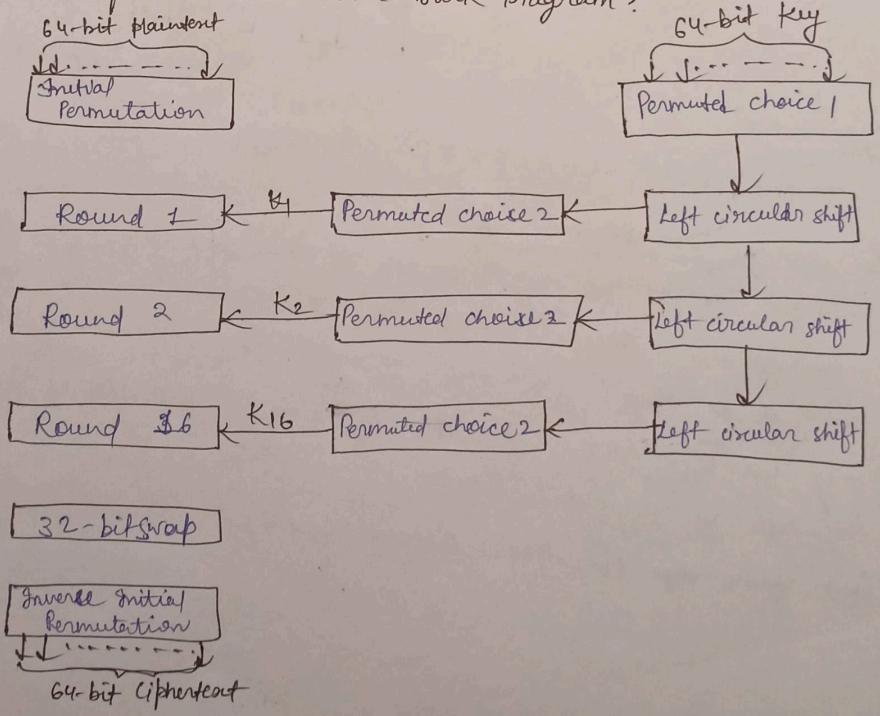
plain text ⇒ aaxxawtcadutktax

a	a	x
x	w	t
c	a	d
n	t	k
t	a	x

new cipher text by double transposition cipher is –

⇒ axcnt awatarxtdkx

Ques 4. Explain DES with Block Diagram?



③ Uses ....

DES has a 64-bit block size and uses a 56-bit key during execution (8 parity bits are stripped off from full 64-bit key). DES is a symmetric cryptosystem, specifically a 16-round Feistel cipher.

DES is generally used for encrypting plain text messages in various algorithm modes such as electronic code book (ECB), cipher-block chaining (CBC), cipher feedback (CFB) & output feedback.

Step-

① 64-bit plain text passed to initial permutation func^n.
② IP performed on plain text.
③ IP produce two halves of LPT & RPT block.
④ LPT & RPT go through 16 rounds.
⑤ LPT & RPT combined and finally permutation is performed.
⑥ Result produces 64-bit ciphertext.

Ques-5. Use the additive cipher with key = 5 to encrypt and decrypt the plain text = Awesome.

{A = 0 . . . . . z=25}

Plain text = A W E S O M E
0 22 4 18 14 12 4

Key = 5

C(P) = (P+K) mod 26 formula Encryption

C(A) = (0+5) mod 26
= 5 mod 26
C(A) = F

C(W) = (22+5) mod 26
= 27 mod 26
= 27-26
= 1
C(W) = B

C(E) = (4+5) mod 26
= 9 mod 26
C(E) = J

C(S) = (18+5) mod 26
= 23 mod 26
C(S) = X

C(O) = (14+5) mod 26
= 19 mod 26
C(O) = T

C(M) = (12+5) mod 26
= 17 mod 26
C(M) = R

AWESOME → encrypted as → FBJXTRJ

Plain text — Cipher text

Decryption formula → $P(c) = (C-K) \bmod 26$

FBJXTRJ

5 1 9 23 19 17 9

$P(F) = (5-5) \bmod 26$

$= 0$

$P(F) = A$

$P(B) = (1-5) \bmod 26$

$= -4 + 26$

$= 22$

$P(B) = W$

$P(J) = (9-5) \bmod 26$

$= 4 \bmod 26$

$= 4$

$P(J) = E$

$P(X) = (23-5) \bmod 26$

$= 18$

$P(X) = S$

$P(T) = (19-5) \bmod 26$

$= 14 \bmod 26$

$= 14$

$P(T) = O$

$P(R) = (17-5) \bmod 26$

$= 12 \bmod 26$

$P(R) = 12$

$P(R) = M$

Cipher text — Plain text

FBJXTRJ → decrypted as → AWESOME