Dated..01/03/2023.....

ASSIGNMENT-1.

Name: Sahil Kaundal
UID: 21BCS8197
Branch: CSE (Lateral Entry)
Group: 616-A
Semester: 6th
Subject Code :- 20CST-354
Subject: Information Security and Cryptography.

Q1.(a) What does "CAESAR" become with a shift of F?

Ans. Given plain text → "CAESER"

Shift Key → F

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Equation to get cipher text is $C = E(P, K) \bmod 26$

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

where C → cipher text letter
P → Plain text letter
K → Key or No. of shifts

Plain text :- CAESAR

So, from above numbering we get.

C → 2 which is first letter of Plain text

F → 5 which is key for encryption.

putting these values in the equation

$C = (P+K) \bmod 26 \Rightarrow C = (2+5) \bmod 26$

$C = 7 \bmod 26$

So, cipher text letter which replaces C from plain text is

Teacher Signature

Dated.....

Letter placed at position 7

So; C → H — (I)

∴ Repeating the same process for every letter for plain text

Letter A. A → 0

$C = (P+K) \bmod 26 \Rightarrow C = (0+5) \bmod 26$

$C = 5$

So, we will replace A from F — (II)

For plain text letter E. E → 4

$C = (4+5) \bmod 26$

$C = 9$

So, we will replace E from J → (III)

For plain text letter S S → 18

$C = (18+5) \bmod 26$

$C = 23$

So, we will replace S from X → (IV)

For plain text letter A. A → 0

we have already calculated in eq (II) so A → F

For plain text letter R: R → 17

$C = (17+5) \bmod 26$

$C = 22$

So, we will replace R from W — (V)

After combining all the cipher text letters we get

Plain Text ⇒ CAESAR

CIPHER TEXT :- H F J X F W

Dated.....

(b) What key do we need to make "CAESER" become "MKOCKB"?

Ans. Given: Plain text "CAESER"
Cipher text "MKOCKB"

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

From plain text letter C we get number 2 and cipher text letter M we get number 12.

So, equation to find key of the cipher is

$K = C - P$

where K → Key

C → Number of position of cipher text letter

P → Number or position of plain text letter.

So, we get

$K = C - P$

$C = 12$, $P = 2$ $\quad K = 12 - 2$

$K = 10$

So, the key used to cipher the plain text is K.

(c) What key do we need to make "CIPHER" become "SYFXUH"?

Ans: Given: Plain text : "CIPHER"

Cipher Text : "SYFXUH"

From above alphabet tabel we get that letter C is placed at position 2. And cipher Text S is placad at position 18.

So; eq. we get $K = C - P$

$K = 18 - 2 = 16$; So, Key is Q.

Teacher Signature

Dated.....

(d) Use the Caesar cipher to encrypt your first name.

Ans. Plain Text : SAHIL

In caesar cipher we take key as 3 which is conventional julias caesar cipher method.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

So, from equation $C = (p + K) \bmod 26$

C → Cipher text

P → Plain text

K → 3 or key.

- for letter S ; S → 18

$C = (18 + 3) \bmod 26$

$C = 21$

So, S will be encrypted by V

- for letter A ; A → 0

$C = (0 + 3) \bmod 26$

$C = 3$

So, A will be encrypted by D.

- for letter H ; H → 7

$C = (7 + 3) \bmod 26$

$C = 10$

So, H will be encrypted by K

- for letter I ; I → 8

$C = (8 + 3) \bmod 26$

$C = 11$ So, I will encrypted by L

Teacher Signature

Dated.....

for letter L : L → 11

$C = (11+3) \bmod 26$

$C = 14$ So, L will encrypted by O.

So, result of Plain Text as encrypted Text is

Plaintext :- S A H I L

Cipher text :- V D K L O

Q2 :- To use a substitution cipher we replace (substitute) each letter of the plain text with a different letter in the cipher text. To use this cipher we need a table of letter replacements. For example, look at the following table.

Plain	C	D	E	H	I	N	P	R	S	T	Y
Cipher	X	J	L	A	Z	E	V	K	H	O	M

Using this substitution this plain text is changed into

Plain Text :- THIS SENTENCE IS ENCRYPTED

Cipher Text :- OAZH HLEOLEXL ZH LEXKMVOLJ

Crack the cipher Text

(a) HAL ZH VKZM

Ans. So, from the above two tables of plain text & cipher text we get.

H is substitution of S

A → H

L → E

Z → I

H → S

V → P

K → R

Z → I

M → Y

Teacher Signature

Dated.....

So, creating a table for cipher Text and plain Text.

	CIPHER TEXT								
PLAIN TEXT	H	A	L	Z	H	V	K	Z	M
	S	H	E	I	S	P	R	I	Y

So; Decryption of Cipher Text.

Cipher Text : H A L ZH VKZM

Plain Text : S H E IS PRIY

(b) OAZH HAL IZJ

From the tables given of Plain Text & Cipher Text we

O is substitution of T

A ⟶ H

Z ⟶ I

H ⟶ S

L ⟶ E

J ⟶ D

So, creating a table for cipher Text and plain text

	CIPHER TEXT									
PLAIN TEXT	O	A	Z	H	H	A	L	J	Z	J
	T	H	I	S	S	H	E	D	I	D

So, Decryption of Cipher Text

Cipher Text → O AZH HAL IZJ

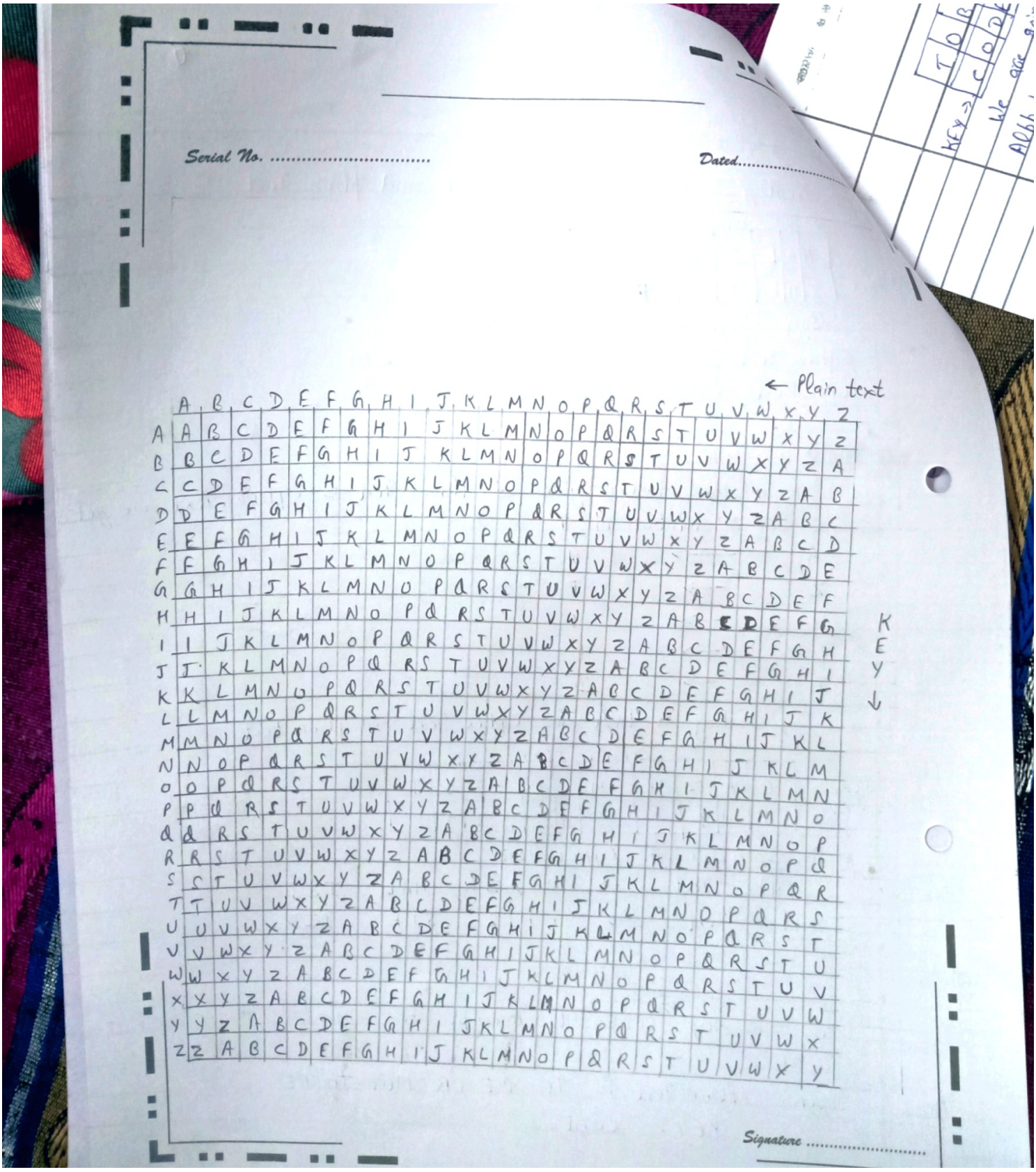
Plain Text → THIS SHE DID.

Q3. Use the key "CODE" to encrypt the sentence "TO BE OR N TO BE".

Ans. Given: Plain Text :- TO BE OR NOT TO BE

KEY :- CODE

Teacher Signature


Serial No. .....
Dated.....
← Plain text
KEY ↓
Signature .....

Dated.....

	Plain Text →													
	T	O	B	E	O	R	N	O	T	T	O	B	E	
KEY →	C	O	D	E	C	O	D	E	C	O	D	E	C	

We are going to use vignere cipher Table of 26 x 26 Alphabet to decrypt the plain text.

From the table or Vignere table of 26 x 26 Alphabets where Rows are key given and columns are for plain text.
So, from table we take key & Plain text intersection in order to decrypt the plain text.

Taking intersecting column T and row C from the Vignere table we get, taking all the intersection from Key + Plain Text

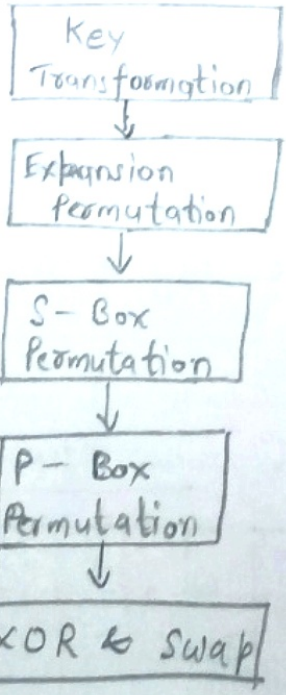
P.T	T	O	B	E	O	R	N	O	T	T	O	B	E	
KEY	C	O	D	E	C	O	D	E	C	O	D	E	C	
C.T	V	C	E	I	Q	F	Q	S	V	H	R	F	G	

We get cipher Text as VCEI QF QSV HR FG.

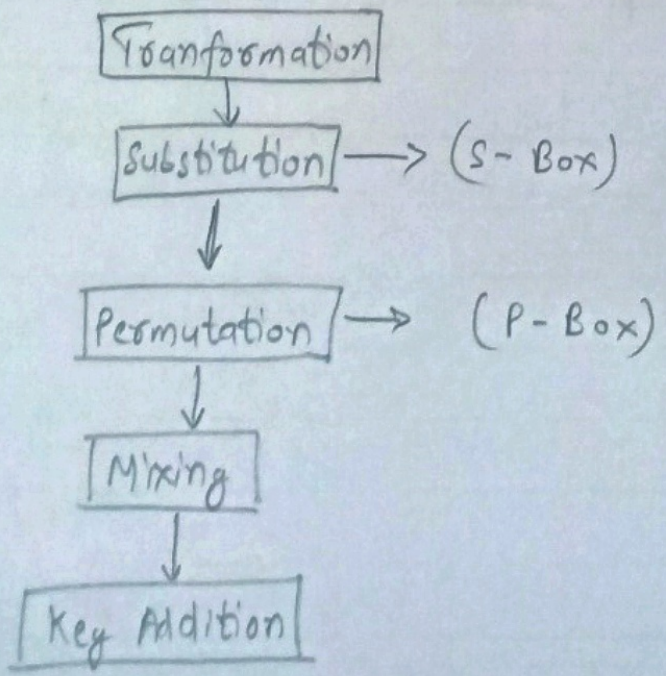
Teacher Signature

Serial No. ..... Dated .....

- Block Diagram of round of DES



Block diagram of rounds of AES



Dated.....

4(a) Explain the complete difference in AES and DES with each rounds.

Advanced Encryption Standard	Data Encryption Standard
1. AES is Byte Oriented	1. DES is Bit Oriented
2. Key length is not fixed. It can be of 128 bit or 192 bit or 256 bit	2. Key length is fixed i.e. of 56 bit.
3. In AES the number of rounds depends on the key length for 128 bit we have 10 rounds, 12 rounds for 192 bit and 14 rounds for 256 bit.	3. DES involves 16 rounds of identical operations.
4. AES can encrypt 128 bits of plain text.	4. DES can encrypt 64 bits of plain text.

In DES 16 rounds are divided into two halves, with each half performing eight rounds of encryption. Each round involves following steps.

1. Expansion
2. Key Mixing
3. Substitution
4. Permutation.

AES on the other hand perform rounds depending upon the key size, where each round performs series of substitution & permutations on the data. Each round involves

(1) Substitution (2.) Permutation (3) Mixing (4) Key Mixing

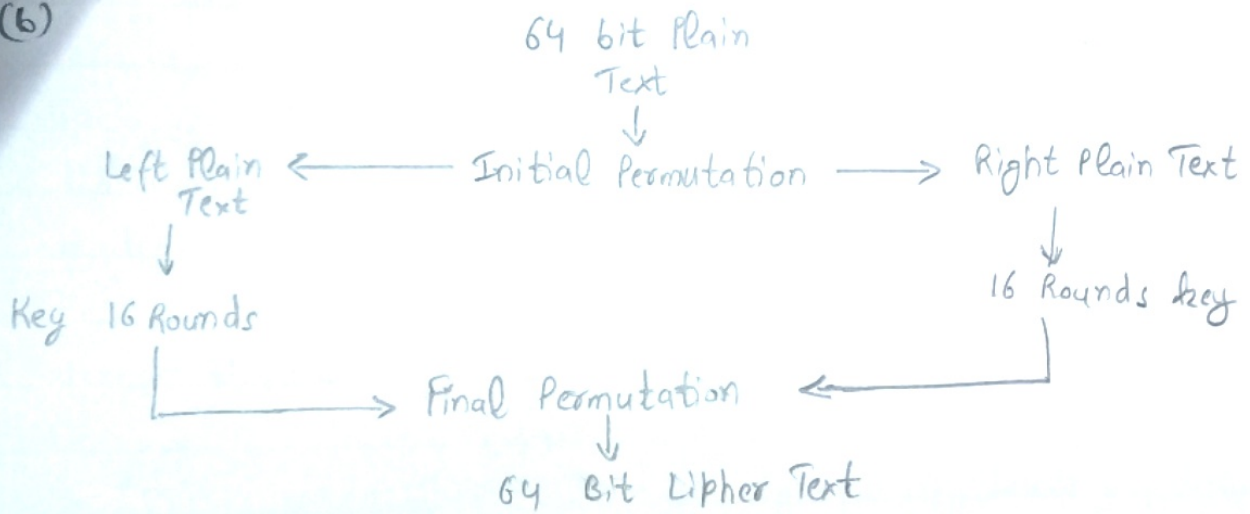
(b) How the 64 bit PT can be xored with 48 bit key in DES.

Data Encryption standard (DES) is a block cipher and encrypt data block of size of 64 bits each which mean 64 bit of cipher text. The same algorithm & key are used for decryption and encryption with minor differences, Their key length is 56 Bits.

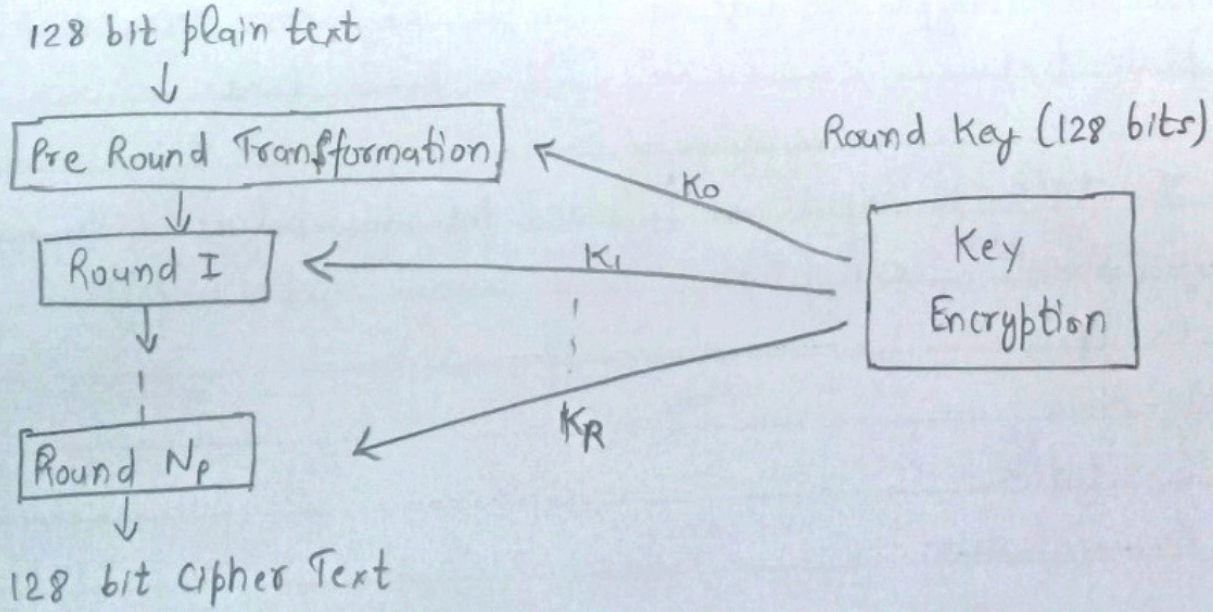
Teacher Signature

Serial No. ..... Dated.....

(b)



(c)



Dated.....

Also explain how the 14 subset keys input in 10 rounds transformation in AES.

Advanced Encryption Standard (AES) is an iterative rather than Feistal cipher. The no. of rounds in AES is variable and depends upon the key length.

AES uses 10 rounds for 128 bit key
12 rounds for 192 bit key
14 rounds for 256 bit key

(d) How the s box convert 6 bits into 4 bit. and how the 32 PT expanded to 48 bit using FPGA MAX + ver 7.2 Rijndael VHDL bit.

The resulting 64 bit performed text block is divident into 2 half blocks. Each half block consist of 32 bits and each of the 16 rounds in turn.

Key → Expansion ⟶ S-Box ⟶ P-Box ⟶ XOR and Swap
Tranformation Permutation Permutation Permutation.

tep-1. Key Transformation –

From the 56 bit key, a different 48 bit subkey is generated during each round using a process.

ep-2. Expansion Permutation –

Original right plain text (RPT) of 32 bits

↓ ↓ ↓

Block I (4 Bit) Block II (4 Bit) ----- Block VII (8 bit)

The Expansion Permutation process expands the 32 bit RPT to 48 bit. Now the key - 48 bit is XOR with 48 bit RPT and the resulting output is given to the next step, which is S-Box Substitution.

Teacher Signature