USN | | | | | | | | | |

CMRIT
CMR INSTITUTE OF TECHNOLOGY, BENGALURU.
ACCREDITED WITH A+ GRADE BY NAAC

Internal Assessment Test I – Nov. 2021

Sub:	**Cryptography**				Sub Code:	**18EC744**	Branch:	**EC**
Date:	**13/11/2021**	Duration:	90 min's	Max Marks: **50**	Sem / Sec:	**7 A, B, C, D**		OBE

	Answer any FIVE FULL Questions	MARKS	CO	RBT
1	Encrypt the message "Work is worship" using, play fair cipher with the keyword "COMPUTER" and decrypt the cipher text to recover the original message. Give the rules for encryption and decryption.	**[10]**	CO1	L3
2 (a)	Develop a set of additive and multiplication tables for modulo 8.	**[5]**	CO1	L2
2 (b)	Explain the procedure to calculate the GCD using Euclidean algorithm. Determine the GCD of (24140, 16762) using Euclidean algorithm	**[5]**	CO1	L2
3 (a)	Define modular arithmetic operation with necessary properties and prove the same.	**[5]**	CO1	L1
3 (b)	Using extended Euclidean algorithm, find the multiplicative inverse of 550 mod 1769.	**[5]**	CO1	L2
4	Explain the types of cryptanalytic attacks on encrypted messages.	**[10]**	CO1	L1
5	Illustrate the following with necessary diagrams: (i) Feistel encryption and decryption process. (ii) Single DES encryption.	**[10]**	CO2	L2
6	Encrypt the plain text "MONDAY" using Hill cipher with key = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Show your calculations to obtain the cipher text. (Use a =0, b=1 …z=25).	**[10]**	CO1	L3
7 (a)	Distinguish between block cipher and stream cipher with examples.	**[5]**	CO2	L1
7 (b)	Explain the process of **DES** encryption with necessary diagram.	**[5]**	CO2	L1

----------All The Best---------

CMR INSTITUTE OF TECHNOLOGY

USN

Scheme and Solution of Internal Assesment Test – I

Sub:	**Cryptography**		Sec	7 A, B, C, D			Code:	**18EC744**
Date:	**13/11/2021**	Duration:	90 mins	Max Marks:	50	Sem: VII	Branch:	ECE

Solution

1 *Encrypt the message "Work is worship" using, play fair cipher with the keyword "COMPUTER" and decrypt the cipher text to recover the original message. Give the rules for encryption and decryption.* **[10 marks]**

Ans **Play fair matrix:**

C	**O**	**M**	**P**	**U**
T	**E**	**R**	A	B
D	F	G	H	I/J
K	L	N	Q	S
V	W	X	Y	Z

Playfair matrix [2 marks]

Plaintext is encrypted two letters at a time. If a pair is a repeated letter, insert filler like 'X'.

Encryption Rule of Play-Fair Cipher:

(1) If both letters fall in the same row, replace each with the letter to its right (circularly).
(2) If both letters fall in the same column, replace each with the letter below it (circularly).
(3) Otherwise, each letter is replaced by the letter in the same row but in the column of the other letter of the pair.

+ Encryption rule [2 marks]

Ciphertext is decrypted two letters at a time.

Decryption Rules of Play-Fair Cipher:

(1) Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the left, with the first element of the row circularly following the last.
(2) Two plaintext letters that fall in the same column are each replaced by the letter above, with the top element of the column circularly following the last.
(3) Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

+ Decryption rule [2 marks]

Encryption:

Plain Text	wo	rk	is	wo	rs	hi	px
Rule	2	3	2	2	3	1	3
Cipher Text	OE	TN	SZ	OE	BN	ID	MY

Decryption:

Cipher Text	OE	TN	SZ	OE	BN	ID	MY
Rule	2	3	2	2	3	1	3
Plain Text	wo	rk	is	wo	rs	hi	px

+ Encryption [2 marks]

+ Decryption [2 marks]

Plain Text: WO RK IS WO RS HI PX

Cipher Text: OE TN SZ OE BN ID MY

2(a) *Develop a set of additive and multiplication tables for modulo 8.* **[5 marks]**

Ans **Arithmetic Modulo 8**

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2

w	$-w$	w^{-1}
0	0	-
1	7	1
2	6	-
3	5	3
4	4	-
5	3	5
6	2	-

Addition [2.5 marks]

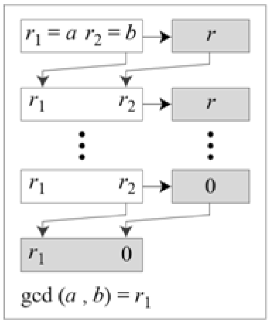
+

Multiplication [2.5 marks]

7	7	0	1	2	3	4	5	6		**7**	0	7	6	5	4	3	2	1	7	1	7

2(b) *Explain the procedure to calculate the GCD using Euclidean algorithm. Determine the GCD of (24140, 16762) using Euclidean algorithm.* **[5 marks]**

Ans



Algorithm

```
r1 ← a;    r2 ← b;
while (r2 > 0)
{
  q ← r1 / r2;
  r  ← r1 − q × r2;
  r1 ← r2;  r2 ← r;
}
gcd (a, b) ← r1
```

q	r_1	r_2	r
1	24140	16762	7378
2	16762	7378	2006
3	7378	2006	1360
1	2006	1360	646
2	1360	646	68
9	646	68	34
2	68	34	0
	34	0	

Procedure [2 marks]

+

Solution [3 marks]

3(a) *Define modular arithmetic operation with necessary properties and prove the same.* **[5 marks]**

Ans

Property	Expression
Commutative Laws	$(a+b) mod\ n = (b+a)\ mod\ n$ $(a \times b) mod\ n = (b \times a)\ mod\ n$
Associative Laws	$[(a+b)+c] mod\ n = [a+(b+c)] mod\ n$ $[(a \times b) \times c] mod\ n = [a \times (b \times c)] mod\ n$
Distributive Law	$[a \times (b+c)] mod\ n = [(a \times b)+(a \times c)] mod\ n$ $[a+(b \times c)] mod\ n = [(a+b) \times (a+c)] mod\ n$
Identities	$(0+a) mod\ n = a\ mod\ n$ $(1 \times a) mod\ n = a\ mod\ n$
Inverse	$a+k = 0\ mod\ n \quad where\ k = (-a)$ $a \times k = 1\ mod\ n \quad where\ k = a^{-1}$

Properties [2 marks]

+

Proof [3 marks]

Let a = 1, b = 5, c = 3 and n = 8

Commutative Laws:

1. $(a+b) mod\ n = (1+5) mod\ 8 = 6 \quad (LHS)$
   $(b+a)\ mod\ n = (5+1) mod\ 8 = 6 \quad (RHS)$
   LHS = RHS (proved)
2. $(a \times b) mod\ n = (1 \times 5) mod\ 8 = 5 \quad (LHS)$
   $(b \times a)\ mod\ n = (5 \times 1) mod\ 8 = 5 \quad (RHS)$
   LHS = RHS (proved)

Associative Laws:

1. $[(a+b)+c] mod\ n = [(1+5)+3] mod\ 8 = [6\ mod\ 8 + 3\ mod\ 8] mod\ 8 = [9] mod\ 8 = 1 \quad (LHS)$
   $[a+(b+c)] mod\ n = [1+(5+3)] mod\ 8 = [1\ mod\ 8 + 0\ mod\ 8] mod\ 8 = [1] mod\ 8 = 1 \quad (RHS)$
   LHS = RHS (proved)
2. $[(a \times b) \times c] mod\ n = [(1 \times 5) \times 3] mod\ 8 = [5\ mod\ 8 \times 3\ mod\ 8\ ] mod\ 8 = [15\ ] mod\ 8 = 7 \quad (\ LHS)$
   $[a \times (b \times c)] mod\ n = [1 \times (5 \times 3)] mod\ 8 = [1\ mod\ 8 \times 15\ mod\ 8\ ] mod\ 8 = [7] mod\ 8 = 7 \quad (RHS)$
   LHS = RHS (proved)

Distributive Law:

1. $[a \times (b+c)] mod\ n = [1 \times (5+3)] mod\ 8 = [1\ mod\ 8 \times 8\ mod\ 8] = [0] mod\ 8 = 0 \quad (LHS)$
   $[(a \times b)+(a \times c)] mod\ n = [(1 \times 5)+(1 \times 3)] mod\ 8 = [5+3] mod\ 8 = 0 \quad (RHS)$
   LHS = RHS (proved)
2. $[a+(b \times c)] mod\ n = [1+(5 \times 3)] mod\ 8 = [1\ mod\ 8 + 15\ mod\ 8] = [1+7] mod\ 8 = 0 \quad (LHS)$
   $[(a+b) \times (a+c)] mod\ n = [(1+5) \times (1+3)] mod\ 8 = [6\ mod\ 8 \times 4\ mod\ 8] = 24\ mod\ 8 = 0 \quad (RHS)$

Identities:

1. $(0+a) mod\ n = (0+1) mod\ 8 = 1$

2. $(1 \times a) mod\ n = (1 \times 1) mod\ 8 = 1$

Inverse:

1. $b + k = 0\ mod\ n \quad where\ k = (-b) \qquad here\ k = -5$
   $[5 + (-5)] mod\ 8 = 0$
2. $b \times k = 1\ mod\ n \quad where\ k = b^{-1} \qquad here\ k = 5$
   $[5 \times 5] mod\ 8 = [25] mod\ 8 = 1$

3(b) *Using extended Euclidean algorithm, find the multiplicative inverse of 550 mod 1769.* **[5 marks]**

Ans

q	r_1	r_2	r	t_1	t_2	$t = t_1 - qt_2$
3	1769	550	119	0	1	-3
4	550	119	74	1	-3	13
1	119	74	45	-3	13	-16
1	74	45	29	13	-16	29
1	45	29	16	-16	29	-45
1	29	16	13	29	-45	74
1	16	13	3	-45	74	-119
4	13	3	1	74	-119	550
3	3	1	0	-119	550	-1769
	1	0		**550**	-1769	

Solution [5 marks]

$550^{-1} mod\ 1769 = 550$

4 *Explain the types of cryptanalytic attacks on encrypted messages.* **[10 marks]**

Ans

TABLE 1: TYPES OF ATTACKS ON ENCRYPTED MESSAGES

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key. • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.

Table [4 marks]

+

Description with diagram [6 marks]

Cryptanalysis:

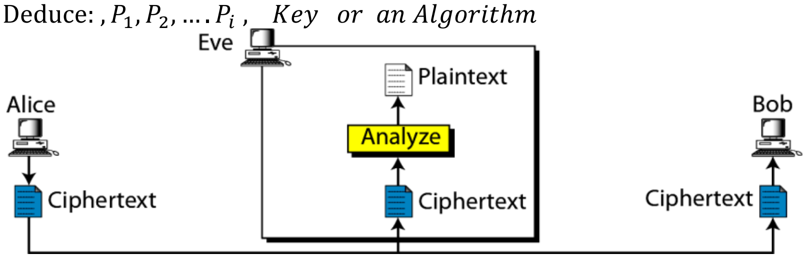
The whole point of cryptography is to keep the plain text secret from the eavesdropper. Cryptanalysis is the art or science of recovering the plain text without access to the key. Successful cryptanalysis may recover the plain text or the key. It also may find the weakness in a cryptosystem. An attempted cryptanalysis is called an attack. In real world cryptanalysts don't always have such detailed information. But it is assumed that the cryptanalyst has the knowledge of the encryption algorithm. There are several types of cryptanalytic attacks.

a) Cipher text only attack
b) Known Plain text attack
c) Chosen Plain text attack
d) Adaptive chosen Plain text attack
e) Chosen cipher text attack
f) Rubber-hose cryptanalysis

Cipher text only attack:

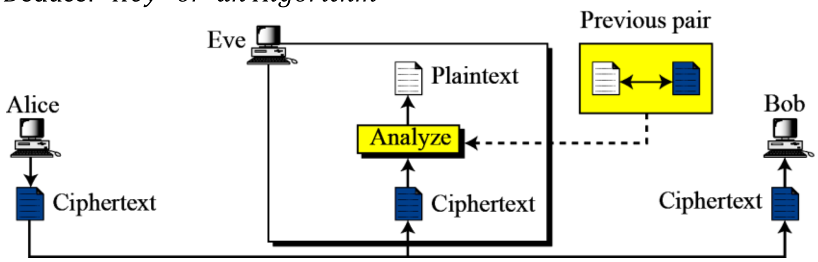
1. The cryptanalysts have the cipher text of several messages and all these cipher text has been encrypted using same key.

2. The cryptanalyst's job is to recover the key used to decrypt the message with the same key.
   Given: $C_1, C_2, \dots \dots C_i$
   Deduce: , $P_1, P_2, \dots . P_i$, $Key\ \ or\ \ an\ Algorithm$



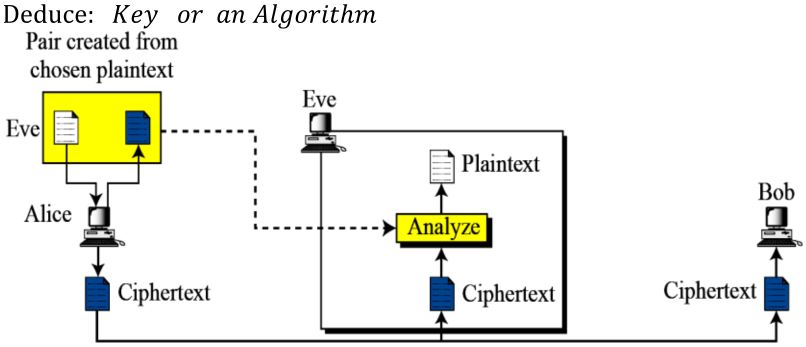
Known Plain text attack:

1. The cryptanalysts have access not only to the cipher text of several message, but also the plain text of those messages.
2. Here the cryptanalyst's job is to deduce the key or an algorithm.
   Given: $(P_1, C_1), (P_2, C_2), \dots . . (P_i, C_i)$
   Deduce: $Key\ \ or\ \ an\ Algorithm$



Chosen Plain text attack:

1. The cryptanalysts not only have access to the cipher text and the associated plaintext, but it also can choose the plain text that gets encrypted.
2. It is more powerful than a known plaintext attack, because the cryptanalysts can choose specific plain text to encrypt, so that one might get more information about the key.
3. Here the cryptanalyst's job is to deduce the key
   Given: $(P_1, C_1), (P_2, C_2), \dots . . (P_i, C_i)$ where the cryptanalyst gets to choose $P_1, P_2, \dots . P_i$
   Deduce: $Key\ \ or\ \ an\ Algorithm$

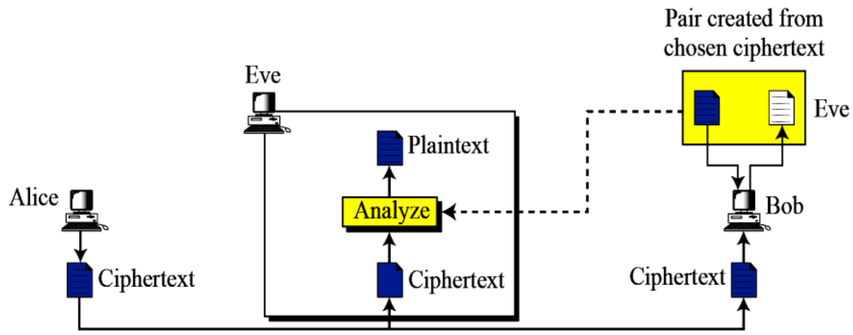


Adaptive chosen Plain text attack:

1. This is a special case of a chosen plain text attack, not only can the cryptanalyst chose the plain text that is encrypted, but he also can modify his choice based on the results of the previous encryption.
2. The chosen plain text attack, a cryptanalyst might just be able to choose a large block of plain text to be encrypted, in additive chosen plain text attack, the cryptanalyst can choose a smaller block of plain text and then choose another based on the results of the first.
   Given: $(P_1, C_1), (P_2, C_2), \dots . . (P_i, C_i)$ where the cryptanalyst gets to choose $P_1, P_2, \dots . P_i$
   Deduce: $Key\ \ or\ \ an\ Algorithm$

Chosen cipher text attack:

1. The cryptanalysts can choose different cipher text to be decrypted and has access to the decrypted plain text.
2. E.g. the cryptanalyst has access to a tamperproof box that does automatic decryption
3. The cryptanalyst job is to deduce the key.
   Given: $C_1, P_1 = D_K(C_1),\ C_2, P_2 = D_K(C_2) \dots \dots \dots C_i, P_i = D_K(C_i)$
   Deduce: Key



Chosen key attack:

1. This attack doesn't mean that the cryptanalyst can choose the key; it means he has some knowledge about the relationship between different keys. It is not very practical

Rubber-hose cryptanalysis:

The cryptanalyst threatens blackmails or tortures someone until they give him the key. To bribe someone to get the key is known as purchase key attack. These are very powerful attacks and often the best way to break the algorithm.

5 *Illustrate the following with necessary diagrams:* **[10 marks]**

(i) Feistel encryption and decryption process.

(ii) Single DES encryption.

Ans **(i) FEISTEL CIPHER STRUCTURE:**

Feistel structure [5 marks]

+

Single round DES [5 marks]

1. The inputs to the encryption algorithm are a plaintext block of length $2w$ bits and a key K.
2. The plaintext block is divided into two halves, $L0$ and $R0$.
3. The two halves of the data pass through n rounds of processing and then combine to produce the ciphertext block.
4. Each round i has as inputs L_{i-1} and R_{i-1} derived from the previous round, as well as a subkey K_i derived from the overall K. The subkeys K_i are different from K and from each other.
5. 16 rounds are used, although any number of rounds could be implemented. All rounds have the same structure.
6. A **substitution** is performed on the left half of the data. This is done by applying a *round function* F to the right half of the data and then taking the exclusive-OR of the output of that function and the left half of the data.
7. The round function F has the same general structure for each round. The round function F is represented as $F(RE_i, K_{i+1})$
8. Following this substitution, a **permutation** is performed that consists of the interchange of the two halves of the data.
9. Feistel network depends on the choice of the following parameters and design features:
   a) **Block size:** larger block sizes mean greater security, but it reduces encryption/decryption speed for a given algorithm. The greater security is achieved by greater diffusion. Traditionally, a block size of 64 bits has been considered a reasonable tradeoff and was nearly universal in block cipher design. However, the new AES uses a 128-bit block size.
   b) **Key size:** Larger key size means greater security but may decrease encryption decryption speed. The greater security is achieved by greater resistance to brute-force attacks and greater confusion. Key sizes of 64 bits or less are now widely considered being inadequate and 128 bits has become a common size.
   c) **Number of rounds:** The essence of the Feistel cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16 rounds.
   d) **Subkey generation algorithm:** Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.
   e) **Round function F:** Again, greater complexity generally means greater resistance to cryptanalysis.
10. There are two other considerations in the design of a Feistel cipher:
   a) **Fast software encryption/decryption:** Encryption is embedded in applications hence the speed of execution of the algorithm becomes a concern.
   b) **Ease of analysis:** Although we would like to make our algorithm as difficult as possible

to cryptanalyze, there is great benefit in making the algorithm easy to analyze. That is, if the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a higher level of assurance as to its strength. DES, for example, does not have an easily analyzed functionality.

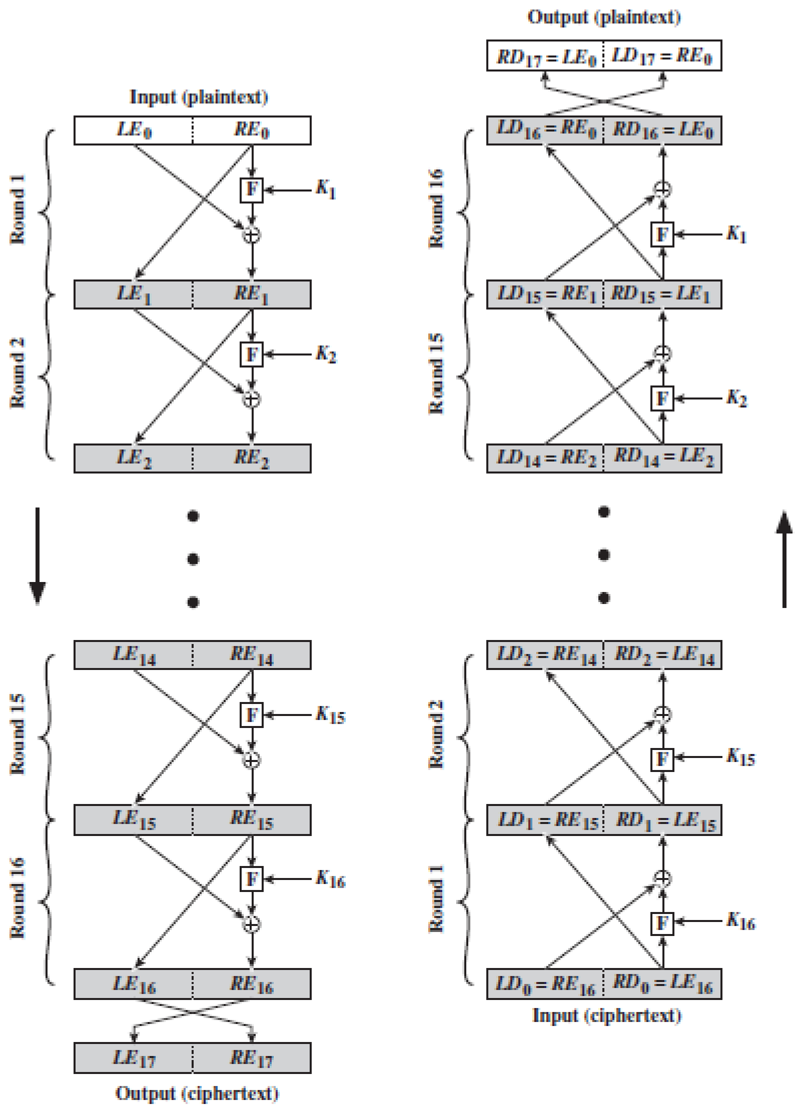


Figure: Feistel Encryption and Decryption (16 rounds)

11. **Feistel Decryption Algorithm:**
    a) Decryption with a Feistel cipher is same as the encryption process.
    b) In decryption the ciphertext is used as input to the algorithm, and the subkeys K_i are used in reverse order.
    c) That is, K_n is used in the first round, K_{n-1} in the second round, and so on, until K_1 is used in the last round. It is an advantage because no need to implement two different algorithms; one for encryption and one for decryption.
    d) For clarity, the notation LE_i *and* RE_i is used for data traveling through the encryption algorithm and LD_i *and* RD_i for data traveling through the decryption algorithm.
    e) The diagram indicates that, at every round, the intermediate value of the decryption process is equal to the corresponding value of the encryption process with the two halves of the value swapped. i.e. $RE_i||LE_i = LD_{16-i}||RD_{16-i}$
    f) Example: (for better clarity)

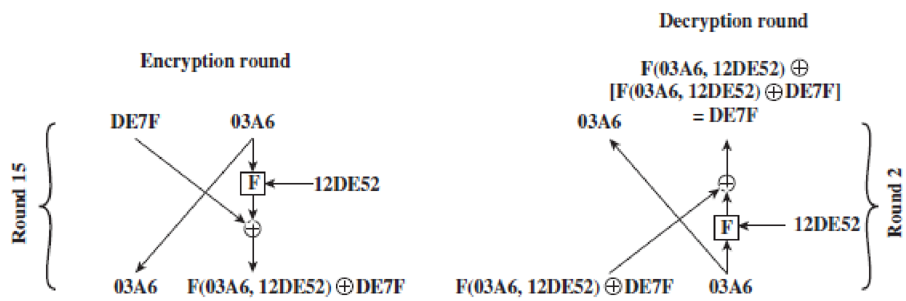
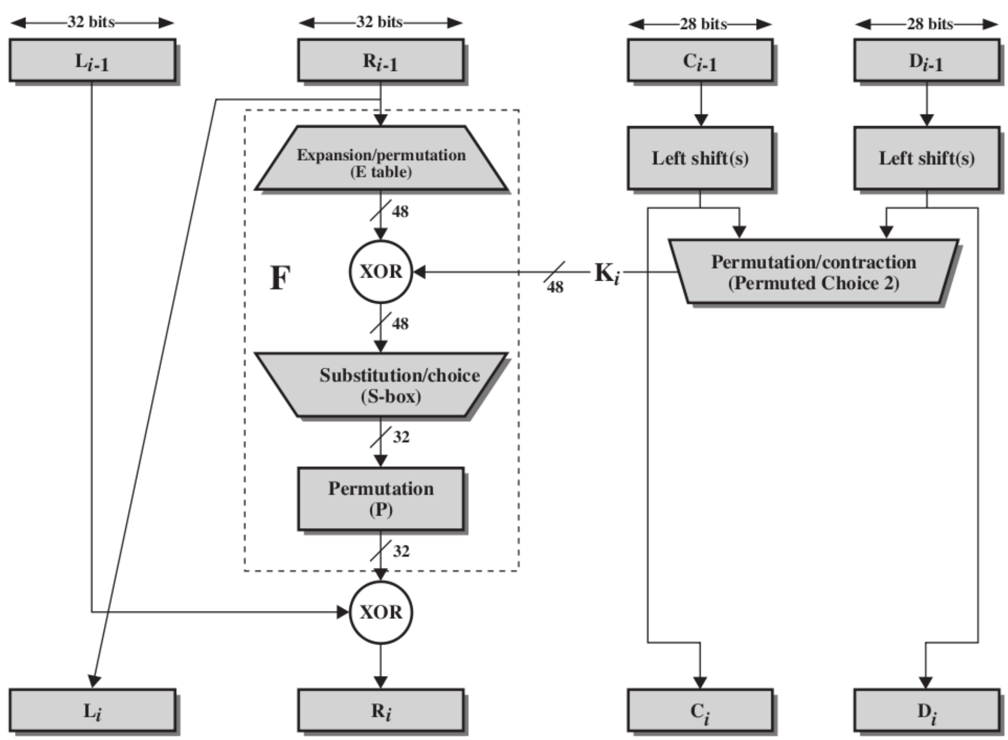


Figure: Feistel Example

(ii) Details of Single Round DES:

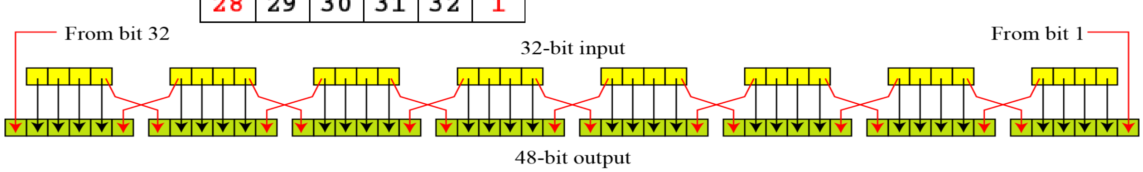
Figure below shows the internal structure of a single round. Again, begin by focusing on the left-hand side of the diagram. The left and right halves of each 64-bit intermediate value are treated as separate 32- bit quantities, labelled L (left) and R (right). As in any classic Feistel cipher, the overall processing at each round can be summarized in the following formulas:

$$L_i = R_{i-1}$$
$$R_i = L_{(i-1)} \oplus F\left(R_{(i-1)}, K_i\right)$$



Expansion: The round key K_i is 48 bits, and the R is 32 bits. The R is first expanded to 48 bits by using permutation plus expansion table as shown below.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	28
24	25	26	27	28	29
28	29	30	31	32	1



XOR: The resulting 48 bits are XOR with K_i

Substitution Table: These 48 bits are passed through the substitution function that produces a 32 bits output which is permuted based on predefined rule as shown in table below.

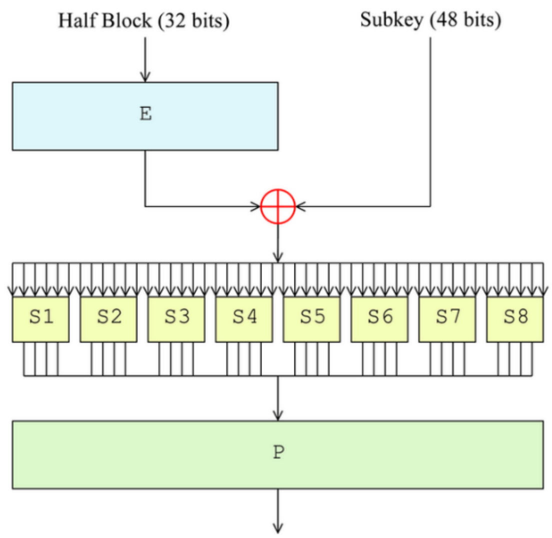
The round key K_i is 48 bits. The R input is 32 bits. This R input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits. The resulting 48 bits are XORed with K_i. This 48-bit result passes through a substitution function that produces a 32-bit output. The role of the S-boxes in the function is illustrated in figure shown below. The substitution consists of a set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

The substitution consists of 8 S-Boxes, which accepts 6 bits as input and produces 4 bits as output. The 1st and last bit of the input to S-Box S_i forms the row and the remaining 4 bits represents the column.

E.g. In S_1, for the input 011001, the row is 01 i.e. 1st row and 1100 i.e. 12th column, the value at 1st row and 12th column is 9 i.e. 1001.

The output of the S-Boxes is again permuted as

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25



6 *Encrypt the plain text "MONDAY" using Hill cipher with key =* $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$*. Show your calculations to obtain the cipher text. (Use a =0, b=1 ...z=25).* **[10 marks]**

Ans Divide the plain text into block of 2(as here key is a 2×2 matrix)

Plain Text: MO ND AY **[10 marks]**

$C = KP \bmod 26$

$$\begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix} \times \begin{bmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \end{bmatrix} \ mod\ 26$$

$$\begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \end{bmatrix} = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \times \begin{bmatrix} M & N & A \\ O & D & Y \end{bmatrix} mod26 = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \times \begin{bmatrix} 12 & 13 & 0 \\ 14 & 3 & 24 \end{bmatrix} mod26$$

$$\begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \end{bmatrix} = \begin{bmatrix} 164 & 129 & 96 \\ 158 & 86 & 168 \end{bmatrix} mod26 = \begin{bmatrix} 8 & 25 & 18 \\ 2 & 8 & 12 \end{bmatrix} mod26 = \begin{bmatrix} I & Z & S \\ C & I & M \end{bmatrix}$$

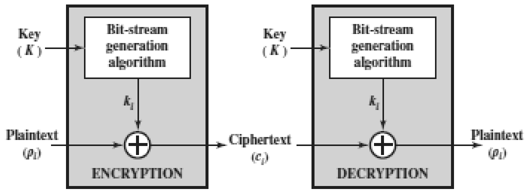
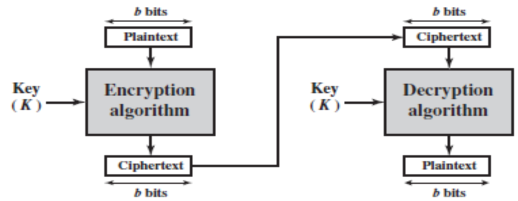
Cipher Text : ICZISM

7(a) *Distinguish between block cipher and stream cipher with examples.* **[5 marks]**

Ans **Difference between stream cipher and block cipher:**

Stream cipher	Block cipher
1. Processing or encoding of plain text is done bit by bit. 2. Bits are processed one by one in a chain 3. Different key bit is used to encrypt each of the bits. 4. E.g. One Time Pad, Vigenère cipher, Vernam cipher 5. It is usually very simple and much faster.	1. Processing or encoding of the plaintext is done as a fixed length block one by one. E.g. 64 or 128 bit in size 2. A pad is added to short length block 3. Same key is used to encrypt each of the blocks. 4. E.g. DES (Data Encryption Standard) ,AES (Advance Encryption Standard) 5. Usually more complex and slower in

[5 marks]

6. Equally secure if properly designed 7. Statistically random 8. Requires less coding 	operation. 6. More secure in most cases. 7. Most block ciphers are based on fiestel cipher structure. 8. Requires more coding. 

7(b) *Explain the process of DES encryption with necessary diagram.* **[5 marks]**

Ans

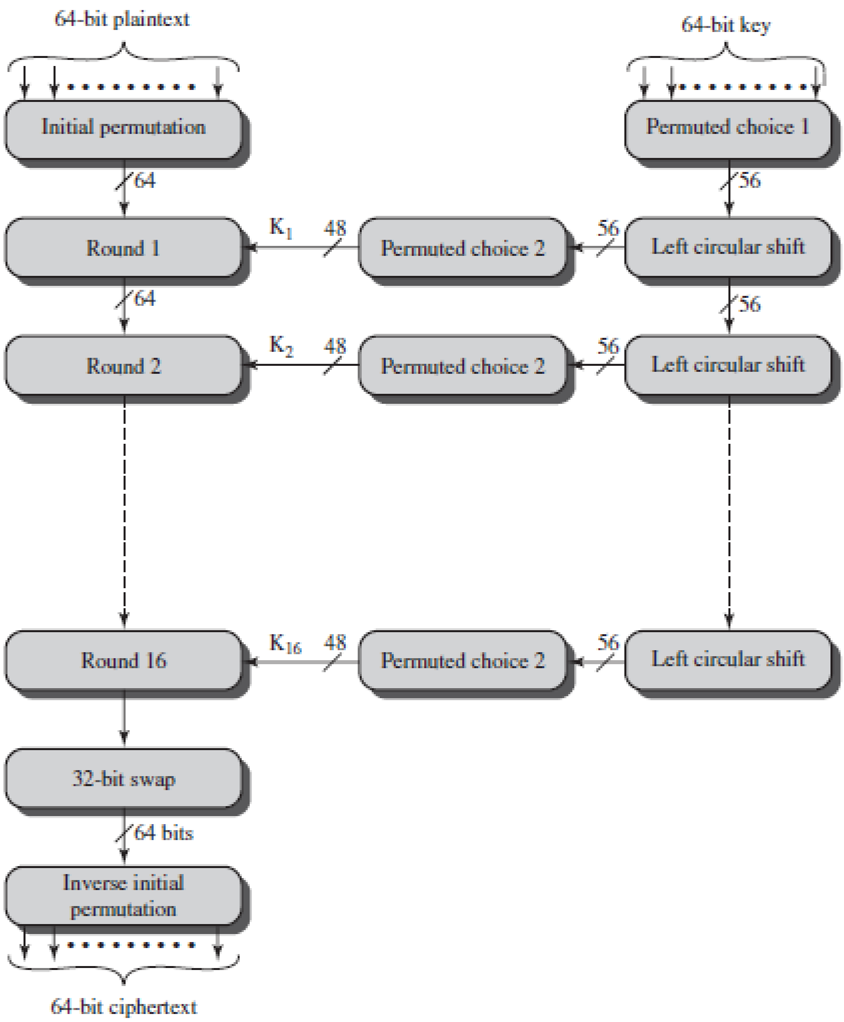


diagram [3 marks]

+

Description [2 marks]

Figure: General Depiction of DES Encryption Algorithm

64 bit key is used but every 8th bit is the parity bit hence it is taken as 56 bit key. Initially the key is passed through the permutation function. For each 16 round, a sub key K_i is produced by the combination of left circular shift and permutation. The same permutation function is used in each round.

The plain text are processed through these phases

a) Initial Permutation
b) 16 rounds of same function
c) Swap
d) Final Permutation

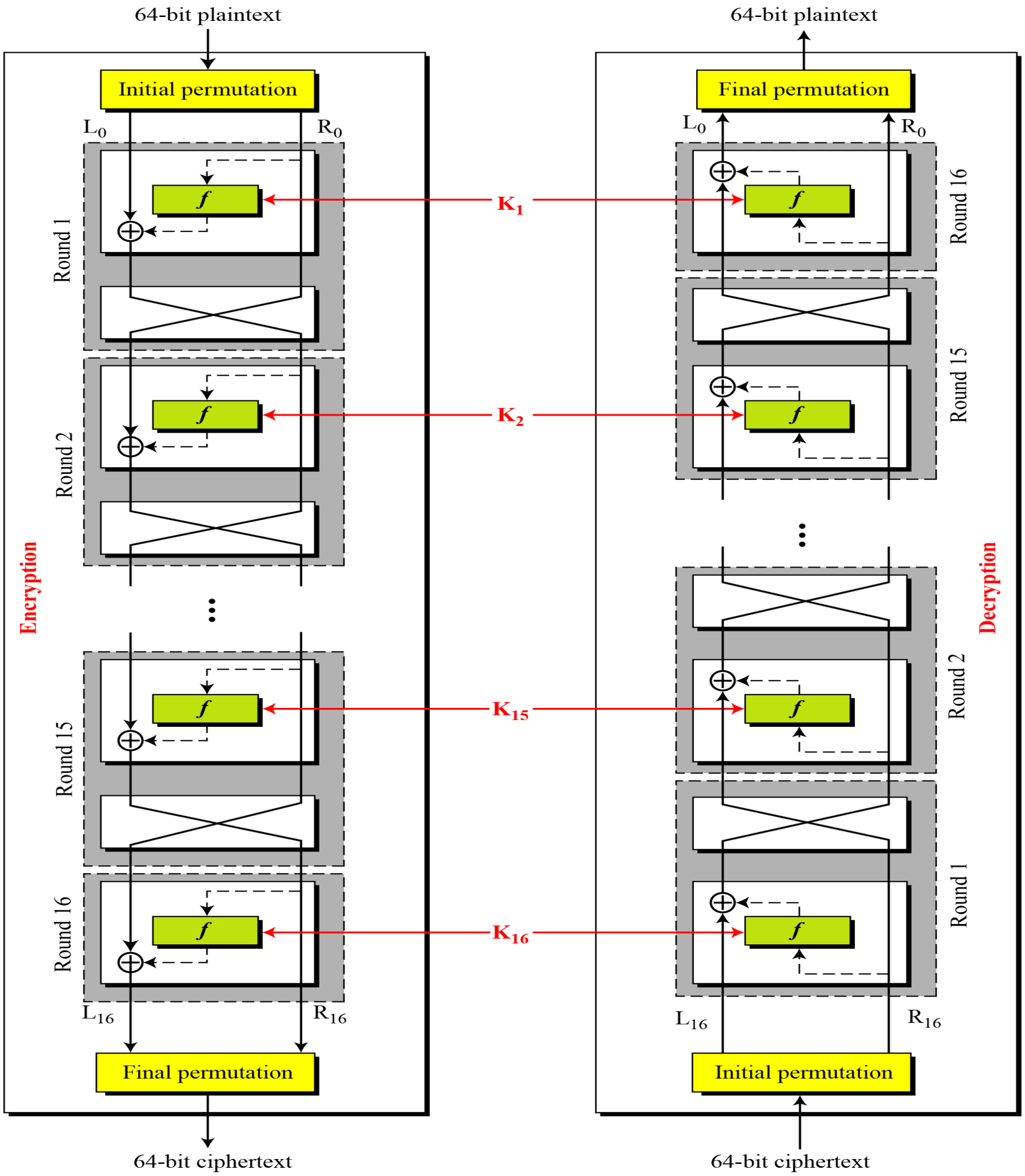


Figure: DES Encryption and Decryption

Initial Permutation and Final Permutation:

The input is 64 bit. These inputs are permuted according to a predefined rule. The permutation table contains a permutation of the number from 1 to 64. These permutation table and inverse permutation table can be designed such that the original bits can be restored.

Initial Permutation	*Final Permutation*
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

DES Encryption:

a) In DES Encryption, there are two inputs to the encryption function:

    i. the plaintext to be encrypted
    ii. Key
b) In this case, the plaintext must be 64 bits in length and the key is 56 bits in length.
c) The processing of the plaintext proceeds in three phases.
    i. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the *permuted input.*
    ii. This is followed by a phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions.
    iii. The left and right halves of the output are swapped to produce the **preoutput**.
    iv. Finally, the pre-output is passed through a permutation $[\mathrm{IP}^{-1}]$ that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.
d) With the exception of the initial and final permutations, DES has the exact structure of a Feistel cipher.

Key Generation:

a) In DES, 56-bit key is used.
b) Initially, the key is passed through a permutation function.
a) Then, for each of the sixteen rounds, a *subkey* (K_i) is produced by the combination of a left circular shift and a permutation.
b) The permutation function is the same for each round, but a different subkey is produced because of the repeated shifts of the key bits.

DES Decryption:

a) As with any Feistel cipher, decryption uses the same algorithm as encryption, except that the application of the subkeys is reversed.
b) Additionally, the initial and final permutations are reversed.