GALGOTIAS UNIVERSITY

ADMISSION NUMBER												

School of Computing Science and Engineering

Bachelor of Technology in Computer Science and Engineering
Mid Term Examination - Nov 2023

Duration : 90 Minutes
Max Marks : 50

Sem V - E2UG501B - Network Security

General Instructions
Answer to the specific question asked
Draw neat, labelled diagrams wherever necessary
Approved data hand books are allowed subject to verification by the Invigilator

1) Build a procedure for securing network data using: (i) Validating the encryption and decryption (ii) Validating with Computer security Programs — K3 (6)

2) Explain the purpose of S-boxes in DES. — K3 (9)

3) Examine a simple four-function calculator in GF(2^4). You may use table lookups for the multiplicative inverses. — K4 (8)

4) This problem provides a numerical example of encryption using a one round version of DES. We start with 64-bit key (K): 1101111000010000100111000101100011101000101001001010011000110000 and 64-bit plaintext (M): 0101011011101001100111101010110011011110010 — K5 (15)

Permuted Choice 1 (PC-1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Permuted Choice 2 (PC-2)

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

1. Derive first round key **(K1)**
2. Derive **L0** and **R0.**

Evaluate.

5) A disadvantage of the general monoalphabetic cipher is that both sender and receiver must commit the permuted cipher sequence to memory. A common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. For example, using the keyword *CIPHER*, write out the keyword followed by unused letters in normal order and match this against the plaintext letters: K6 (12)

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

If it is felt that this process does not produce sufficient mixing, write the remaining letters on successive lines and then generate the sequence by reading down the columns:

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

This yields the sequence
C A K S Y I B L T Z P D M U H F N V E G O W R J Q X
Estimate the keyword.