Topic _____ Date. 01st May 2023

Name: Fariha Salman
Roll no: 19BCS048
Class: B. Tech. 8th Semester Computer Engineering
Subject: Network Security Assignment

Tutorial Sheet - 3

1. A) Data Encryption Standard (DES) is a symmetric key block cipher that uses a 64-bit key and operates on 64-bit blocks of plaintext. It works by repeating a series of operations called rounds.

⇒ DES uses 16 rounds. Each round of DES is a Feistal cipher.

DES follows the following basic structure:-

i) Expansion :- The 32-bit right half of the previous rounds output is expanded to 48 bits using a fixed permutation table called E-box. The resultant 48-bit block is then X-ORed with a 48-bit subkey.

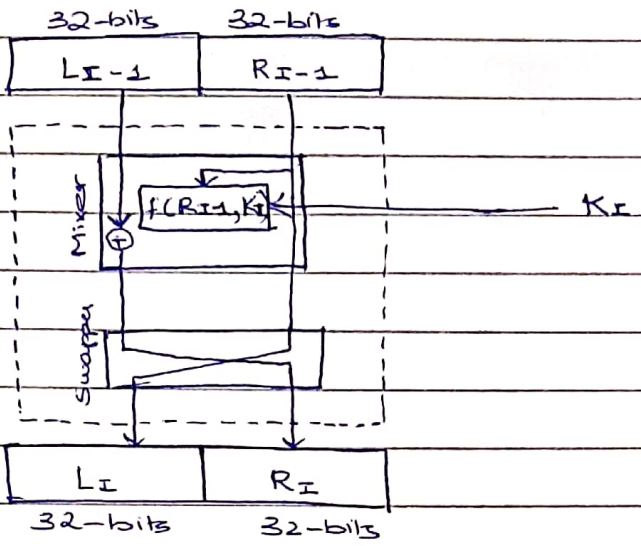
ii) Substitution :- The resulting 48-bit block is divided into 8 6-bit blocks and each block is substituted using a separate S-box. Each S-box takes a 6-bit input and produces a 4-bit output, resulting into a 32-bit output.

iii) Permutation :- The 32-bit output is then subjected to a fixed permutation using a table called P-box. The P-box shuffles the bits of the output in a non-linear way to produce the final 32-bit output of round.

iv) Key mixing :- The output of the P-box is then X-ORed with the 32-bit half of the previous round output to produce the input for the next round.

Topic. Date.

⇒ A round in DES (at the encryption site) is shown as follows:-



2.A) Plaintext given:- 123456ABCD132536

8421

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
0	0	0	1	0	0	1	0	0	0	1	1	0	1	0	0	0	1	0	1	0	1	1	0	1	0	1	0	1	0	1	1	1	1	0	0	1	1	0	1

47	44	46	48	50	52	54	56	58	60	62	64
0	0	0	1	0	0	1	1	0	0	1	0	0	1	0	1	0	0	1	1	0	1	1	0

41	43	45	47	49	51	53	55	57	59	61	63

Initial permutation :-

0 0 0 1, 0 1 0 0 ⇒ 1 4 A 7 D 6 7 8 1 8 C A 1 8 A D

1 0 1 0, 0 1 1 1

1 1 0 1, 0 1 1 0

0 1 1 1, 1 0 0 0

0 0 0 1, 1 0 0 0

1 1 0 0, 1 0 1 0

0 0 0 1, 1 0 0 0

1 0 1 0, 1 0 0 1

TELCO

Teacher's Sign.....

Topic _____ Date. _____

Inverse Initial Permutation :-

1 0 1 0 1 0 0 1 ⇒ A96 79E81 761B8481
0 1 1 0 0 1 1 1
1 0 0 1 1 1 1 0
1 0 0 0 0 0 0 1
0 1 1 1 0 1 1 0
0 0 0 1 1 0 1 1
1 0 0 0 0 1 0 0
1 0 0 0 0 0 0 1

3.A) IDEA (International Data Encryption Algorithm) is a symmetric key block cipher that was developed in 1991 as a replacement for the aging DES algorithm. IDEA uses a 128-bit key and operates on 64-bit blocks of data.

⇒ The sub-key generation process is as follows:-

i) Key expansion
ii) The 128-bit IDEA key is split into eight 16-bit subkeys. These are then used to generate 52 additional 16-bit subkeys
iii) Encryption / decryption rounds
iv) IDEA uses 8 rounds enc/dec of input block. Each round input block is divided into two 16-bit halves, the left half and the right half.
v) Multiply L by a 16-bit subkeys (K1-K6).
vi) Add R to result of previous step.
vii) Modulo 2^16.
viii) Multiply the result of previous step by 16-bit subkey.
ix) Add result of previous step to L.
x) Modulo 2^16.
xi) Exchange L and R.

After 8 rounds, L and R halves are concatenated and passed

TELCO

Teacher's Sign.....

Topic _____ Date. _____

through final permutation to obtain the ciphertext.

4.A) 01000011 01001111 01001101 01010000 01010101
41 43 45 47 49 51 53 55 57 59 61 63
01010100 01000101 01010010
42 44 46 48 50 52 54 56 58 60 62 64

Initial permutation :-

1 1 1 1 1 1 1 1	⊗
1 0 1 1 1 0 0 0	⊗
0 1 1 1 0 1 1 0	v
0 1 0 1 0 1 1 1	W
0 0 0 0 0 0 0 0	⊗
0 0 0 0 0 0 0 0	⊗
0 0 0 0 0 1 1 0	⊗
1 0 0 0 0 0 1 1	⊗

⊗ ⇒ no valid character

Final permutation :-

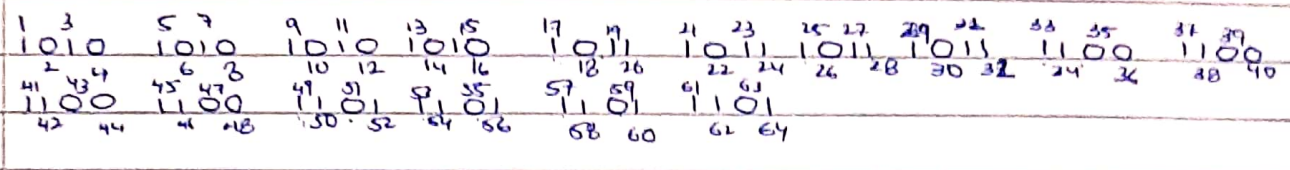
1 1 0 1 1 1 0 0	⊗
0 1 0 1 0 0 1 0	R
1 0 1 1 1 1 0 0	⊗
0 0 0 1 0 1 0 0	⊗
1 0 1 0 0 0 1 1	⊗
0 0 0 0 0 0 0 0	⊗
1 1 1 1 1 1 1 1	⊗
0 0 0 0 0 0 0 0	⊗

Topic Date.

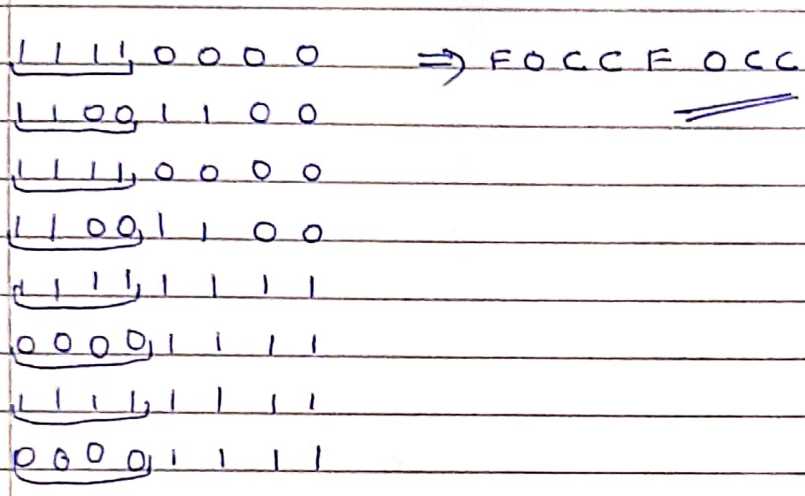
5.A) Plaintext:- AAAA BBBB CCCC DDDD (hexadecimal)

8421

10 - A
11 - B
12 - C
13 - D
14 - E
15 - F

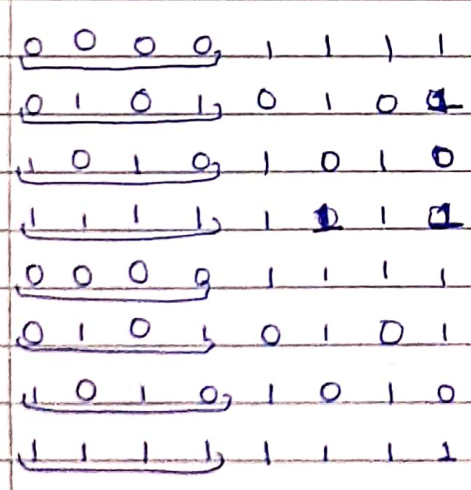


Initial permutation:-



⇒ F0CCF0CCFF0FF0F

Final permutation:-



⇒ 0F55AAFF0F55AAFF

Topic _____ Date. _____

6.A) The Advanced Encryption Standard (AES) is a symmetric key block cipher that operates on 128-bit blocks of data.

⇒ The states of AES in Round 1:-

i) SubBytes :- In this state, each byte of input block is substituted with a corresponding byte from an S-box. The S-box is a fixed 256-bit byte table that is generated during the key expansion phase of the cipher.

Example:-

19	3D	E3	BE		D4	29	11	AE
A0	F4	E2	2B	→	E0	BF	98	F1
9A	C6	8D	2A		B8	B4	5D	E5
E9	F8	4B	08		1E	41	52	30

ii) Shift Rows :- The rows of input are shifted cyclically by certain no. of bytes (to the left).

Example:-

D4	29	11	AE		D4	29	11	AE
E0	BF	98	F1	→	BF	98	F1	E0
B8	B4	5D	E5		5D	E5	B8	B4
1E	41	52	30		30	1E	41	52

iii) MixColumns :- In this state, each column is transformed using matrix multiplication.

Example:-

04	A0	8E	D5
88	52	2B	2F
D2	7F	80	D6
BC	9E	17	68

Topic _____ Date. _____

iv) Add Round Key :- In this state, the input block is combined with a round key.

04	2A	6C	78
46	F2	F9	9B
DA	F4	C7	C2
5D	60	13	18

7.A) COMPUTER ENGINEER

C ⇒ 02 ⇒ 02
O ⇒ 14 ⇒ 0E
M ⇒ 12 ⇒ 0C
P ⇒ 15 ⇒ 0F
U ⇒ 20 ⇒ 14
T ⇒ 19 ⇒ 13
E ⇒ 4 ⇒ 04
R ⇒ 17 ⇒ 11
E ⇒ 4 ⇒ 04
N ⇒ 13 ⇒ 0D
G ⇒ 6 ⇒ 06
I ⇒ 8 ⇒ 08
N ⇒ 13 ⇒ 0D
E ⇒ 4 ⇒ 04
E ⇒ 4 ⇒ 04
R ⇒ 17 ⇒ 11

$$\begin{bmatrix} C & U & E & N \\ O & T & N & E \\ M & E & G & E \\ P & R & I & R \end{bmatrix} \Rightarrow \begin{bmatrix} 02 & 14 & 04 & 0D \\ 0E & 13 & 0D & 04 \\ 0C & 04 & 06 & 04 \\ 0F & 11 & 08 & 11 \end{bmatrix}$$

TELC

Teacher's Sign. _____

Topic _____ Date. _____

8.A) For AES – 192,

IP = $x^8 + x^4 + x^3 + x + 1$ (prime).

RCon[11] ⇒ RC_{11}

⇒ $x^{11-1} = x^{10}$ mod prime

⇒ $x(x^9)$ mod prime

⇒ $x(x^5 + x^4 + x^2 + x)$ mod $x^8 + x^4 + x^3 + x + 1$

⇒ $x^6 + x^5 + x^3 + x^2$

⇒ 01101100 ⇒ $(6C\ 00\ 00\ 00)_{16}$

RCon[12] ⇒ RC_{12}

⇒ x^{12-1} ⇒ x^{12} mod prime

⇒ $x(x^{10})$ mod prime

⇒ $x(x^6 + x^5 + x^3 + x^2)$ mod $x^8 + x^4 + x^3 + x + 1$

⇒ $x^7 + x^6 + x^4 + x^3$ mod $x^8 + x^4 + x^3 + x + 1$

⇒ $x^7 + x^6 + x^4 + x^3$

⇒ 11011000 ⇒ $(D8\ 00\ 00\ 00)_{16}$

For AES – 256, IP = $x^8 + x^4 + x^3 + x + 1$ (prime).

RCon[13] ⇒ RC_{13}

⇒ x^{13-1} ⇒ x^{12} mod prime

⇒ $x(x^{11})$ mod prime

⇒ $x(x^7 + x^6 + x^4 + x^3)$ mod $x^8 + x^4 + x^3 + x + 1$

⇒ $x^8 + x^7 + x^5 + x^4$ mod $x^8 + x^4 + x^3 + x + 1$

⇒ $x^7 + x^5 + x^3 + x + 1$

⇒ 10101011

⇒ $(AB\ 00\ 00\ 00)_{16}$.

Topic _____ Date. _____

RCon[14] $\Rightarrow$ RC_{14}

$\Rightarrow x^{14-1} \Rightarrow x^{13}$ mod prime

$\Rightarrow x(x^{12})$ mod prime

$\Rightarrow x(x^7 + x^5 + x^3 + x + 1)$ mod $x^8 + x^4 + x^3 + x + 1$

$\Rightarrow (x^8 + x^6 + x^4 + x^2 + x)$ mod $x^8 + x^4 + x^3 + x + 1$

$\Rightarrow x^6 + x^3 + x^2 + 1$

$\Rightarrow 01001101 \Rightarrow (4D\ 00\ 00\ 00)_{16}$.

9.A) $t = \text{SubWord}(\text{RotWord}(w[i-1])) \oplus \text{RCon}[i/4]$

For round 1,

$\frac{i}{4} = 1$

$\Rightarrow i = 4$.

$w[i-1] \Rightarrow w_{4-1} \Rightarrow w_3 \Rightarrow 13AA5487$

$\Downarrow$

$\Rightarrow AA548713$ (RotWord)

$\Downarrow$

$\Rightarrow AC2017 7D$ (SubWord)

AC2017 7D

$\oplus$ 01000000

A [1100] 2017 7D

$\oplus$ 0 [0001] 0000 00

$\Rightarrow$ A [1101] 2017 7D.

$\Rightarrow$ A02017 7D $\Rightarrow t_4$.

TELCO

Teacher's Sign.....

Topic _____ Date. _____

10.A)

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{bmatrix}$$

pre-define matrix — state array

$$= \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 40 & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix}$$

$= (02 \times 87) \oplus (03 \times 6E) \oplus (01 \times 4C) \oplus (01 \times A6) \Rightarrow 47$

$02 \Rightarrow 00000010 \Rightarrow x$

$87 \Rightarrow 10000111 \Rightarrow x^7 + x^2 + x + 1$

$02 \times 87 \Rightarrow x^8 + x^3 + x^2 + x \bmod x^8 + x^4 + x^3 + x + 1$

$\Rightarrow x^4 + x^2 + 1$

$\Rightarrow 00010101 \Rightarrow 15$

8421

$03 \times 6E$

$03 \Rightarrow 00000011 \Rightarrow x + 1$

$6E \Rightarrow 01101110 \Rightarrow x^6 + x^5 + x^3 + x^2 + x$

$02 \times 6E \Rightarrow (x^6 + x^5 + x^3 + x^2 + x + x^7 + x^6 + x^4 + x^3 + x^2)$

$\Rightarrow x^7 + x^5 + x^4 + x$

$\Rightarrow 10110010 \Rightarrow B2$

00010101
10110010 $\Rightarrow 47$
01000110
10100110

01000111

Topic _____ Date. _____

11.A)
$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix} \xrightarrow{\text{Shift rows}} \begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 00 & 23 & 04 \\ 13 & 19 & 12 & 12 \\ 19 & 14 & 00 & 11 \end{bmatrix}$$

12.A)
$w_0 = w[i-4] = EAD27321$

$w_3 = 7F\ 8D\ 29\ 2F = temp \rightarrow$

7F	8D	29	2F
B_0	B_1	B_2	B_3

After RotWord $\Rightarrow$ 8D 29 2F 7F

After SubWord $\Rightarrow$ 5D A5 15 D2 $\rightarrow \oplus \rightarrow t$

RCon[9] $\Rightarrow$ RC9

$\Rightarrow x^{9-1} \Rightarrow x^8$ mod prime

$\Rightarrow x^8 \bmod x^8 + x^4 + x^3 + x + 1$

$\Rightarrow x^4 + x^3 + x + 1$

$\Rightarrow 00011011$

$\Rightarrow (1B\ 00\ 0000)_{16}$

5D A5 15 D2
1B 00 00 00 $\rightarrow \oplus \rightarrow$ (5D ⊕ 1B) A5 15 D2

$\Rightarrow$ (0100 0110) A5 15 D2

$\Rightarrow$ 46 A5 15 D2 $\Rightarrow$ temp.

01011101
00011011
0100 0110

$w_i = 46\ A5\ 15\ D2 \oplus EA\ D2\ 73\ 21$ (temp ⊕ w[i-4])

$= AC\ 77\ 66\ F3$