NETWORK SECURITY ASSIGNMENT.

TUTORIAL SHEET-3

Name:- Tabish Khan

Roll No:- 19BCS037.

T-1

DES (Data Encryption standard) is a symmetric key encryption algorithm that uses a 64-bit block size and a 56-bit key length. A single round of DES consist of several key operations, permutations and substitution boxes.

i) Key generation:- The 56-bit key is first permuted using a predefined table called "PC-1" table, which results in 56 bit permutation of original key. The resulting key is then split into two 28-bit halves and each half is circularly shifted by one or two bits to create new 28-bit keys. These new keys are then combined and permuted again using another predefined table called the "PC-2" table.

ii) Data Permutation. The 64-bit plain text is then permuted using the "Initial Permutation" (IP) table. This rearranges the bits of the plain text so that they are in a new order before the undergo further processing.

(ii) Data Encryption : The 64-bit plaintext block is then permuted using the

(iii) Substitution : The permuted plaintext is then split into two 32-bits values, the left half (L_0) and the right half (R_0). The right half is expanded to 48 bits using another predefined table called the "Expansion table". The expanded right half is then XORed with the round key generated in step 2. The resulting 48-bit value is then split into 8, 6-bit boxes, which are used as inputs to eight different substitution boxes (S-boxes). Each S-box takes a 6-bit input and produces a 4-bit output based on predefined lookup table. The outputs of the S boxes are concatenated to form a 32-bit value.

(iv) Permutation :- The 32-bit value obtained from S-boxes is then permuted using a predefined table called "Permutation table" to obtain a new 32-bit value. The permutation is designed to increase the diffusion of the bits, which means that changing one bit in the input should result in most multiple bits being

change in output.

v) Output : The new 32-bit value obtained from the permutation in step 4 is XORed with the left half (L_0) to produce the new right half (R_1). The left half (R_0) is unchanged and becomes the left half of next round (L_1). The new left half (L_1) and right half (R_1) is combined to form the 64-bit cipher text block.

I-2.

Initial Permutation

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

19BCS091 - TARUSH LOHANI

Date:
Page

Function Initial Permutation (IP).

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

Plain Text: 123456ABCD132536.

Converting to Binary.

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
0 0 0 1 0 0 1 1
0 0 1 0 0 1 0 1
0 0 1 1 0 1 1 0

Converting it accordingly to permutation table.

19BCS037 - TABISH KHAN

0 0 0 1 0 1 0 0
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 1 0 1

= 14A7D67818CA18AD

Converting the above table according the inverse permutation table.

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
0 0 0 1 0 0 1 1
0 0 1 0 0 1 0 1
0 0 1 1 0 1 1 0

= 123456ABCD132536

Date
Page

Q3

IDEA (International Data Encryption Algorithm) is a symmetric key block cipher that operates on 64-bit blocks of data using a 128-bit key. It was developed by James Massey and Xuejia Lai in 1991 and it became very popular in 1990s due to its strong security, speed and simplicity.

IDEA encryption process involves a series of 8 rounds, each of which consists of a series of operations including substitution, permutation, and modular arithmetic. The subkey generation process of each round of IDEA is as follows:

1. Key Expansion: 128 bit key is divided into 8 - 16 bit subkeys and 6-16 bit "round keys" are generated from the original key using modular arithmetic.

2. Round Keys: For each round, 6 - 16 bit round keys are used. The first 4 keys are used in substitution operation, while the last two keys are used in the multiplication and addition operation.

3. Subkey Mixing :- In each round, the 64-bit plaintext block is divided into 4 16-bit sub blocks. Each sub block is combined with a different 16-bit round key by bitwise addition modulo 2^{16}.

4. Substitution :- Each 16-bit sub block is substituted by another 16-bit value using a lookup table.

5. Permutation :- The 64-bit block is permuted by swapping the positions of two adjacent 16-bit sub blocks and then shifting all the bits of the block to left by 1.

6. Multiplication :- Each of the 4 sub-blocks is multiplied by a different 16-bit round key using modulo arithmetic and then the resulting products are added modulo 2^{16} to obtain the final encrypted value.

7. Output :- After 8 rounds of encryption, the resulting 64-block is the ciphertext.

IP & SDES - TARUN (CHAN)

Date
Page

T-4

Initial permutation table.

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

Inverse initial permutation table.

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

19B6S037 - TABISH ICHAN

Plaintext

0 1 0 0 0 0 1 1
0 1 0 0 1 1 1 1
0 1 0 0 1 1 0 1
0 1 0 1 0 0 0 0
0 1 0 1 0 1 0 1
0 1 0 1 0 1 0 0
0 1 0 0 0 1 0 1
0 1 0 1 0 0 1 0

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
1 0 0 0 0 0 1 1
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.

19BCS037 - TABLSHI CHAN

Date
Page

Final permutation using inverse permutation table

0 1 0 0 0 0 1 1
0 1 0 0 1 1 1 1
0 1 0 0 1 1 0 1
0 1 0 1 0 0 0 0
0 1 0 1 0 1 0 1
0 1 0 1 0 1 0 0
0 1 0 0 0 1 0 1
0 1 0 1 0 0 1 0

T-5

Initial permutation table

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

Inverse initial permutation table -

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

19BCS037 - TABISH KHAN

Plaintext:

AAAA BBBB CCCC DDDD

1 0 1 0 1 0 1 0
1 0 1 0 1 0 1 0
1 0 1 1 1 0 1 1
1 0 1 1 1 0 1 1
1 1 0 0 1 1 0 0
1 1 0 0 1 1 0 0
1 1 0 1 1 1 0 1
1 1 0 1 1 1 0 1

Text after going through initial permutation table.

1 1 1 1 0 0 0 0
1 1 0 0 1 1 0 0
1 1 1 1 0 0 0 0
0 0 0 0 1 1 0 0
1 1 1 1 1 1 1 1
0 0 0 0 1 1 0 0
1 1 1 1 0 0 0 0
0 0 0 0 1 1 0 0

19BCS037 - TANISH CHAN

Prove the converted text through Vernam cipher

1 0	1 0	1 0 1 0
1 0	1 0	1 0 1 0
1 0	1 1	1 0 1 1
1 0	1 1	1 0 1 1
1 1	0 0	1 1 0 0
1 1	0 0	1 1 0 0
1 1	0 1	1 1 0 1
1 1	0 1	1 1 0 1

19BCS037 - TABISH KHAN

T-6

The round of AES consist of four different steps -

1) SubBytes
2) Shift Rows
3) Mix Columns
4) AddRoundKey.

- SubBytes :- In this steps, each byte in the STATE matrix is replaced with a corresponding byte from the S-box lookup table. The Sbox is a 256 ~~bit~~ byte substitution table that is used to provide non-linearity in the encryption process.

- ShiftRows :- In this steps, the byte in each row of the STATE matrix are shifted cyclically to the left. The first row is not shifted, the second row is shifted by 1 byte, the third row is shifted by 2 byte to the left and the fourth row is shifted by 3 byte to the left.

- **MixColumns:-** In this step, each column of the STATE matrix is multiplied by a fixed polynomial to produce a new value for each byte in the column.

- **Add RoundKey:-** In this step, the STATE matrix is combined with a key schedule, which is derived from the master key. Each byte in the STATE matrix is XORed with the corresponding byte in the key schedule.

I.7

COMPUTERENGINEER

A B C D E F G H I J K L M N O P
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

Q R S T U V W X Y Z
16 17 18 19 20 21 22 23 24 25.

Computer Engineer can be written as.

02 14 12 15 21 19 04 17 04 13 06 08
13 04 04 17

STATE MATRIX

02	21	04	13
14	19	13	04
12	04	06	04
15	17	08	17

14BCS057 - TABISH ICHAN

Date
Page

T-8

AES-192 polynomial is $x^8 + x^4 + x^3 + x + 1$

Rcon[11]:

$= x^{11-1} = x^{10}$

$x^8 + x^4 + x^3 + x + 1 \;\big[\; x^{10} \;\big(\; x^2$

$x^{10} + x^6 + x^5 + x^3 + x^2$

$x^6 + x^5 + x^3 + x^2$

$= 00110110$

$= 36_{16}$

Rcon[12]

$= x^{12-1} = x^{11}$

$x^8 + x^4 + x^3 + x + 1 \;\big|\; x^{11} \;\big(\; x^3$

$x^{11} + x^7 + x^6 + x^4 + x^3$

$x^7 + x^6 + x^4 + x^3$

01101100

$= 6C_{16}$

AES-256 polynomial - $x^8+x^4+x^3+x+1$.

Rcon(13)

$= x^{13-1} = x^{12}$.

$$x^8+x^4+x^3+x+1 \;\big]\; x^{12} \;\big(\; x^4 + 1$$

$$x^{12}+x^8+x^7+x^5+x^4$$

$$x^8+x^7+x^5+x^4$$

$$x^8+x^4+x^3+x+1$$

$$x^7+x^5+x^4+x^3+x+1$$

01010101

55 16

Rcon(14)

$= x^{14-1} = x^{13}$

$$x^8+x^4+x^3+x+1 \;\big]\; x^{13} \;\big(\; x^5 + x + 1$$

$$x^{13}+x^9+x^8+x^6+x^5$$

$$x^9+x^8+x^6+x^5$$

$$x^9+x^5+x^4+x^2+x$$

$$x^8+x^6+x^4+x^2+x$$

$$x^8+x^4+x^3+x+1$$

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

: 00100110

: 26 16

19BCSD9-TABISH MAJID

T-9

Round	Value of t	First word	Second word	Third word	Fourth word
—	—	2475A2B3	34755688	31E21200	13AA5487
1	AD2077D	8955B52E	BD2DE356	BCC2A146	9B59A3C1
2	470678DB	C553CD45	7373BE53	A4B1DA15	8CD97A14
3	31DA40DD	A7898B25	8CFAA7B8	734B7483	9A5D7AB3
4	47A5B3AD	B022DEB8	31DB752E	479301AD	5401F92
5	6C76LD49	D454F390	ED8C8666	A71F871B	F31E8BEA
6	5414F00D	8640DB95	861C8D23	4103DA38	521D8209
7	4E413353	62833EB6	049FB395	C59CB9AD	F70B3B74
8	8CE29268	CE61ACDE	EAFE1F4B	2F62A8E6	D83E9D92
9	DA5E4F61	E43FE3BF	DEC1FCF4	21A35A12	F40C780
10	3FC6CD94	D8F92E26	D538D242	F4958860	DDB4F92

19BCS032 - TANISH KUMAR

T-10

STATE

00	12	0C	08
04	04	00	23
12	12	13	19
14	00	11	19

STATE after shift rows

00	12	0C	08
04	00	23	04
13	19	12	12
19	14	00	11