Date ____ 20__

IS assignment 1

21K-3153

BCS-7A

(Q1). Symmetric encryption applied to a unit of data larger than a single 64-bit or 128-bit block.

Email messages, network packets etc must be broken into fixed length blocks.

Simplest approach is ECB, in which plaintext is handled b bits at a time & each plaintext is encrypted using the same key. Typically b=64 or 128

Consider a scenario in which a password is:

"123123 ..." repeated. If this password is broken into blocks, each block would have the same encrypted block. Decrypting one block would lead to the entire password being decrypted.

ECB is not secure as identical plaintext block result in identical cipher blocks.

Repetitive patterns can be detected easily as change in plaintext do not propagate to other blocks.

Date ____ 20__

Q2 (a) PT = 0000000000000000

K = 0000000000000000 =

Binary PT = all zeros

Binary key = all zeros

After PC1:

K+ = 56 bit 0's

C0 = 28 bits 0's = 0000000 → in Hexa

D0 = 28 bit 0's = 0000000

After PC1:

K+ = 56 bit 0's

0000000000000000 → in Hexa

C0 = 28 bits 0's

0000000 → in Hexa

D0 = 28 bits 0's

0000000 → in Hexa

After Left shift (1 bit bec DES standard ↑)

C0 = same = 0000000 → in Hexa

D0 = same = 0000000

Date _____ 20__

After R2:

K_1 = 48 bits 0

000000000000 → in Hex

Now Applying IP to M:

M after IP = all zeros - 64 bit 0's

L_0 = 32 bit 0's = 00000000 → in Hex

R_0 = 32 bit 0's = 00000000

after expansion of R_0 = 48 bit 0's = 000000000000 → in Hex

$E(R_0)$ = 48 bit 0's

000000000000 → in Hex

$K \oplus E(R_0)$:

48 bit 0's

000000000000 → in Hex

Sboxes:

$K_1 \oplus E(R_0)$:

000000 000000 000000 000000 000000 000000 000000 000000

column

row

all zeros

for each S box, row 0 & column 0

Date 20

S1 = 14 = 1110
S2 = 15 = 1111
S3 = 10 = 1010
S4 = 07 = 0111
S5 = 02 = 0010
S6 = 12 = 1100
S7 = 04 = 0100
S8 = 13 = 1101

After permutation (P) table of Sbox:

1101 1000 1101 1000 1101 1011
1101

L1 = R0 = 32 bit 0's

R1 = 1101 1000 1101 1000 1101 1011

1101 1000 1101 1000 1101 1011 1101

(A) 0000 0000 0000 0000 0000 0000 0000

1101 1000 1101 1000 1101 1011 1101

R1

L1 = 00000

Date _____ 20__

(b) PT = 64 bit 1's
K = 64 bits 1's

After PC1:
K+ = 56 bit 1's

C_0 = 28 bits 1's
D_0 = 28bit 1's

Left shift (1 bit because DES Round 1)

C_0 = same
D_0 = same

After PC2:
K_1 = 48 bits 1's

Applying IP to M:

M = 64 bit 1's

L_0 = 32 bit 1's
R_0 = 32bit 1's

Expansion of R_0 (E(R_0)) = 48 bit 1's

$K_1 \oplus E(R_0)$ = 48 bits 0's

for

→

Sboxes:

for each Sbox → row & column is 0

S1 = 14 → 1110
S2 → 15 → 1111
S3 → 10 → 1010
S4 → 07 → 0111
S5 → 02 0010
S6 → 12 1100
S7 → 04 0100
S8 → 13 1101

After permutation:

~~1100~~ 11011000110110001101101110111011

1101 → f(R0,K)

L1 = R0 = 32 bits 1's → L1

R1 = L0 ⊕ f(R0,K)

~~11011 000 11011 000 11011 0111 0111 01~~

~~⊕ 11111111111111111111111111111111~~

~~0 1 1 100 100 11 100 100 1000 100 0010~~

11011000 11011000 11011 0111 011 1101

⊕ 11111111111111111111111111111111

00100111 00100111 00100 1000 100 0010 → R1

Date ____ 20 ____

(c) Ans-

i) $x1 = 000000$ $x2 = 000001$

0,0

$S_1(x1) = 14 \rightarrow 01110$

$S_1(x2) = 1,0 = 00 \rightarrow 0000$

$$\begin{array}{r} 1110 \\ 0000 \\ \hline 1110 \end{array}$$

$S_1(x1 \oplus x2)$: $x_1 \oplus x_2 = 000001$

1,0

$S_1(x1 \oplus x2) = 00$

$S_1(x) \oplus S_1(x2) \neq S_1(x1 \oplus x2)$

$1110 \neq 0000$

(ii) →

Date _____ 20__

2) $x_1 = 111111$ $x_2 = 100000$

$S_1(x_1) = 11, 1111$	$S_1(x_2) = 1, 0$
↓	
3, 15	0
↓	↓
13 ⇒ 1101	0000

$x_1 \oplus x_2 = 011111$

$S_1(x_1 \oplus x_2) = 1, 15$

↓

$08 \Rightarrow 1000$

1101
0000
1101

$S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$

$1101 \neq 1000$

Date ____ 20 ____

3) $x_1 = 01010$ $x_2 = 010101$

$S_1(x_1)$:	$S_1(x_2)$:
10, 0101	01, 1010
↓	↓
2, 5	1, 10
↓	↓
06	12
↓	↓
0110	1100

$(x_1 \oplus x_2)$ = 111111

3, 15

$S_1(x_1 \oplus x_2) = 13 \Rightarrow 1101$

0110
1100
1010

$S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$

1010 ≠ 1101

→

Date 20

Q3 (a) First 64 bit key is mapped to a 56 bit key. Bit 1 becomes bit 8 of C0. Propogation of flipped bit is felt throughout and if one S-box is affected, at the next atleast 4 S-boxes are affected. Thus flipped bit can very quickly affect all S-boxes.

R1: Sbox 4 → 1 bit left shifted
R2: S box 1, 2, 3, 5, 6, 7, 8 → 1 bits left shifted
R3: Sbox 1, 2, 3, 4, 5, 6, 7, 8 → 2 bits L.S
R4 = Sboxes 1, 2, 3, 4, 5, 6, 7, 8 → 2 bits L.S
R5 = all sboxes → 2 bit L.S
R6 = all S-boxes → 2 bit L.S
R7 = all S-boxes → 2 bit L.S
R8 = all S-boxes → 2 bit L.S
R9 = all S-boxes → 1 bit L.S
R10 = all S-boxes → 2 bit L.S
R11 = All S-boxes → 2 bit L.S
R12 = All S boxes → 2 bit L.S
R13 = All S-boxes → 2 bit L.S
R14 = All S-boxes → 2 bit L.S
R15 = All S-boxe → 2 bit L.S
R16 = All S-boxes → 2 bit L.S

Date _____ 20___

Since decryption is the reverse of encryption, the bit would still affect 5-bits but in reverse order.

The first sub key used in encryption is the last sub key used in decryption.

If SBox 4 was affected in R1 of encryption, SBox 4 would be affected in R16 of decryption

Date _____ 20__

Q4(a) Cryptanalysis is the process of analyzing & breaking cryptographic algos by observing weakness & patterns in the encryption process

- Brute-force attacks involve trying all possible keys until one is found.

Cryptanalysis requires techniques, brute force requires time and error

- If a weak key is found, cryptanalysis is faster. Brute force is slower, especially with longer keys.
- Cryptanalysis depends on the algorithm's complexity, brute force depends on the key length.

(b)
- Brute force: Try all keys until correct one is found
- Known-Plaintext Attack: This is done when the plaintext is known. Goal is to deduce encryption key.
- Chosen-Plaintext attack:
  Plaintexts can be chosen and ciphertexts can be studied. Goal is to identify weaknesses in encryption standard.
- Ciphertext only attack:
  Only ciphertexts are known. Goal is to identify weaknesses in encryption patterns.

Date _____ 20___

Q5 Emerging Sciences

Emerging Sciences

Plaintex in Hexs:

45 6D 65 72 67 69 6F 67 20 53 63 69
65 6E 63 65

Key: Two One Nine Two

54 77 6F 20 4F 6E 65 20 39 69 6E 65
20 54 77 6F

45 6D 65 72
67 69 6F 67
20 53 63 69
65 6E 63 65

Key

54 77 6F 20
4F 6E 65 20
39 69 6E 65
20 54 77 6F

11 1A 0A 52
28 07 0B 47
19 3A 0D 0C
45 3A 14 0A

S Box:

				Mashift
F2	A2	67	00	1 bit L.S
34	C5	2B	A0	2 bit L.S
D4	80	D7	FE	3 bit L.S
6C	80	FA	67	

Date _____ 20___

After shifting:

82	A2	67	00
C5	2B	A0	34
D7	FF	D4	80
67	6E	80	FA

Mix column

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

×

82	A2	67	00
C5	2B	A0	34
D7	FE	D4	80
67	6E	80	FA

~~× 82 ⊕ 03 × C5 ⊕ 01 × D7 ⊕ 01 × 67~~

Date ____ 20__

02 x82 ⊕ 03x C5 ⊕ 01xD7 ⊕ 01x67

02 = x

82 = $x^7 + x$

↓

$x^8 + x^2 = x^4 + x^3 + x + 1 + x^2$ = 00011111

~~03x C5 =~~ x

03 = x+1

C5 = 11000101 = $x^7 + x^6 + x^2 + 1$ = ~~$x^6 + x^4$~~ $+x^2$

$x^8 + x^7 + x^3 + x + x^7 + x^6 + x^2 + 1$

$x^4 + x^3 + x + 1 + x^3 + x + x^6 + x^2 + 1$

$x^6 + x^4 + x^2$ = 01010100

01 * D7 ⇒

D7

01 x67 = 67

00011111

01010100

10101011

⊕ 01100111

11111011

FB

Date ____ 20 ____

after performing same steps:
final matrix

FB	09	79	F4
16	3A	8D	B2
57	EB	2A	83
41	26	06	DC

(+)

Add key:

(3) key:	75	3A	74	54
	82	EC	85	D1
	C7	A7	CC	BB
	97	B7	D2	BD

Ans ←

8E	33	0D	A0
94	D6	0F	63
90	F9	E6	8F
D6	91	D7	61