Name: Ashna Wasif
Class: BSCS 7B (Morning)
Subject: Information Security
Roll No: 2791.
Submitted To: Dr. Zia ur Rehman

"ASSIGNMENT # 02"

MIX COLUMN:

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

X

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95

SOLUTION:

Before moving towards its working, the following table will help:

HexaDecimal	Binary	Equivalent Equation
02	00000010	X
03	00000011	$X+1$
01	00000001	1
87	10000111	X^7+X^2+X+1
F2	11110010	$X^7+X^6+X^5+X^4+X$
4D	01001101	$X^6+X^3+X^2+1$
97	10010111	$X^7+X^4+X^2+X+1$
6E	01101110	$X^6+X^5+X^3+X^2+X$
46	01000110	X^6+X^2+X
A6	10100110	$X^7+X^5+X^2+X$
4C	01001100	$X^6+X^3+X^2$
90	10010000	X^7+X^4

EC	11101100	$x^7+x^6+x^5+x^3+x^2$
E7	11100111	$x^7+x^6+x^5+x^2+x+1$
4A	01001010	x^6+x^3+x
C3	11000011	x^7+x^6+x+1
8C	10001100	$x^7+x^2+x^3$
DB	11011000	$x^7+x^6+x^4+x^3$
95	10010101	$x^7+x^4+x^2+1$

- $(02 \times B7) \oplus (03 \times 6E) \oplus (01 \times 46) \oplus (01 \times AC)$

$02 \times B7$: $x(x^7+x^2+x+1)$

$x^8+x^3+x^2+x$

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

$= x^4+x^2+1$

$03 \times 6E$: $(x+1)(x^6+x^5+x^3+x^2+x)$

$x^7+x^6+x^4+x^3+x^2+x^6+x^5+x^3+x^2+x$

$= x^7+x^5+x^4+x$

01×46: $1(x^6+x^2+x)$

$= x^6+x^2+x$

$01 \times A6$: $1(x^7+x^5+x^2+x)$

$= x^7+x^5+x^2+x$

x^4+x^2+1 : 0 0 0 1 0 1 0 1

$x^7+x^5+x^4+x$: 1 0 1 1 0 0 1 0

x^6+x^2+x : 0 1 0 0 0 1 1 0

$x^7+x^5+x^2+x$: $\oplus$ 1 0 1 0 0 1 1 0

0 1 0 0 0 1 1 1

$(01000111)_2 = (47)_{16}$

- $(02 \times F2) \oplus (03 \times 4C) \oplus (01 \times E7) \oplus (01 \times 8C)$

$02 \times F2$: $x(x^7+x^6+x^5+x^4+x)$

$x^8+x^7+x^6+x^5+x^2$

$x^4+x^3+x+1+x^7+x^6+x^5+x^2$

$= x^7+x^6+x^5+x^4+x^3+x^2+x+1$

03 x 4C : $(x+1)(x^6+x^3+x^2)$

$x^7+x^4+x^3+x^6+x^3+x^2$

$= x^7+x^6+x^4+x^2$

01 x E7 : $1(x^7+x^6+x^5+x^2+x+1)$

$= x^7+x^6+x^5+x^2+x+1$

01 x 8C : $1(x^7+x^3+x^2)$

$= x^7+x^3+x^2$

$x^7+x^6+x^5+x^4+x^3+x^2+x+1$: 1 1 1 1 1 1 1 1

$x^7+x^6+x^4+x^2$: 1 1 0 1 0 1 0 0

$x^7+x^6+x^5+x^2+x+1$: 1 1 1 0 0 1 1 1

$x^7+x^3+x^2$: 1 0 0 0 1 1 0 0

0 1 0 0 0 0 0 0

$(01000000)_2 = (4B)_{16}$

- (02 x 4D) ⊕ (03 x 90) ⊕ (01 x 4A) ⊕ (01 x DB)

02 x 4D : $x(x^6+x^3+x^2+1)$

$= x^7+x^4+x^3+x$

03 x 90 : $(x+1)(x^7+x^4)$

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

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

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

01 x 4A : $1(x^6+x^3+x)$

$= x^6+x^3+x$

01 x DB : $1(x^7+x^6+x^4+x^3)$

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

$x^7+x^4+x^3+x$: 1 0 0 1 1 0 1 0

$x^7+x^5+x^3+x+1$: 1 0 1 0 1 0 1 1

x^6+x^3+x : 0 1 0 0 1 0 1 0

$x^7+x^6+x^4+x^3$: 1 1 0 1 1 0 0 0

1 0 1 0 0 0 1 1

$(10100011)_2 = (A3)_{16}$

- $(02 \times 97) \oplus (03 \times EC) \oplus (04 \times C3) \oplus (01 \times 95)$

$02 \times 97 : \quad x\,(x^7 + x^4 + x^2 + x + 1)$

$x^8 + x^5 + x^3 + x^2 + x$

$x^4 + x^3 + x + 1 + x^5 + x^3 + x^2 + x$

$= x^5 + x^4 + x^2 + 1$

$03 \times EC : \quad (x+1)\,(x^7 + x^6 + x^5 + x^3 + x^2)$

$x^8 + x^7 + x^6 + x^4 + x^3 + x^7 + x^6 + x^5 + x^3 + x^2$

$= x^8 + x^5 + x^4 + x^2 \rightarrow x^4 + x^3 + x + 1 + x^5 + x^4 + x^2$

$\hookrightarrow x^5 + x^3 + x^2 + x + 1$

$01 \times C3 = 1(x^7 + x^6 + x + 1)$

$= x^7 + x^6 + x + 1$

$01 \times 95 : \quad 1\,(x^7 + x^4 + x^2 + 1)$

$= x^7 + x^4 + x^2 + 1$

$x^5 + x^4 + x^2 + 1 : \quad 00110101$

$x^5 + x^3 + x^2 + x + 1 : \quad 00101111$

$x^7 + x^6 + x + 1 : \quad 11000011$

$x^7 + x^4 + x^2 + 1 : \quad 10010101$

01001100

$(01001100)_2 = (4C)_{16}$

- $(01 \times B7) \oplus (02 \times 6E) \oplus (03 \times 46) \oplus (01 \times A6)$

$01 \times B7 : \quad 1\,(x^7 + x^2 + x + 1)$

$= x^7 + x^2 + x + 1$

$02 \times 6E : \quad x\,(x^6 + x^5 + x^3 + x^2 + x)$

$= x^7 + x^6 + x^4 + x^3 + x^2$

$03 \times 46 : \quad (x+1)\,(x^6 + x^2 + x)$

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

$= x^7 + x^6 + x^3 + x$

$01 \times A6 : \quad 1\,(x^7 + x^5 + x^2 + x)$

$= x^7 + x^5 + x^2 + x$

$x^7 + x^2 + x + 1$: 10000111

$x^7 + x^6 + x^4 + x^3 + x^2$: 11011100

$x^2 + x^6 + x^3 + x$: 11001010

$x^7 + x^5 + x^2 + x$: 10100110

00110111

$(00110111)_2 = (37)_{16}$

- $(01 \times F2) \oplus (02 \times 4C) \oplus (03 \times E7) \oplus (01 \times 8C)$

$01 \times F2$: $1 (x^7 + x^6 + x^5 + x^4 + x)$

$= x^7 + x^6 + x^5 + x^4 + x$

$02 \times 4C$: $x (x^6 + x^3 + x^2)$

$= x^7 + x^4 + x^3$

$03 \times E7$: $(x+1)(x^7 + x^6 + x^5 + x^2 + x + 1)$

$x^8 + x^7 + x^6 + x^3 + x^2 + x + x^7 + x^6 + x^5 + x^2 + x + 1$

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

$= x^5 + x^4 + x$

$01 \times 8C$: $1 (x^7 + x^2 + x^3)$

$= x^7 + x^3 + x^2$

$x^7 + x^6 + x^5 + x^4 + x$: 11110010

$x^7 + x^4 + x^3$: 10011000

$x^5 + x^4 + x$: 00110010

$x^7 + x^3 + x^2$: 10001100

11010100

$(11010100)_2 = (D4)_{16}$

- $(01 \times 4D) \oplus (02 \times 90) \oplus (03 \times 4A) \oplus (01 \times D8)$

$01 \times 4D$: $1 (x^6 + x^3 + x^2 + 1)$

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

02×90 : $x (x^7 + x^4)$

$x^8 + x^5$

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

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

$03 \times 4A$: $(x+1)(x^6+x^3+x)$

$= x^7+x^4+x^2+x^6+x^3+x$

$01 \times DB$: $1\,(x^7+x^6+x^4+x^3)$

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

$x^6+x^3+x^2+1$: 0 1 0 0 1 1 0 1

$x^7+x^4+x^3+x+1$: 0 0 1 1 1 0 1 1

$x^7+x^6+x^4+x^3+x^2+x$: 1 1 0 1 1 1 1 0

$x^7+x^6+x^4+x^3$: 1 1 0 1 1 0 0 0

0 1 1 1 0 0 0 0

$(01110000)_2 = (70)_{16}$

$(01 \times 97) \oplus (02 \times EC) \oplus (03 \times C3) \oplus (01 \times 95)$

01×97 : $1\,(x^7+x^4+x^2+x+1)$

$= x^7+x^4+x^2+x+1$

$02 \times EC$: $x\,(x^7+x^6+x^5+x^3+x^2)$

$x^8+x^7+x^6+x^4+x^3$

$x^4+x^3+x+1+x^7+x^6+x^4+x^3$

$= x^7+x^6+x+1$

$03 \times C3$: $(x+1)(x^7+x^6+x+1)$

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

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

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

01×95 : $1\,(x^7+x^4+x^2+1)$

$= x^7+x^4+x^2+1$

$x^7+x^4+x^2+x+1$: 1 0 0 1 0 1 1 1

x^7+x^6+x+1 : 1 1 0 0 0 0 1 1

$x^6+x^4+x^3+x^2+x$: 0 1 0 1 1 1 1 0

$x^7+x^4+x^2+1$: 1 0 0 1 0 1 0 1

1 0 0 1 1 1 1 1

$(10011111)_2 = (9F)_{16}$

- $(01 \times 57) \oplus (01 \times 6E) \oplus (02 \times 46) \oplus (03 \times A6)$

02×57 : $1\,(x^7 + x^2 + x + 1)$

$= x^7 + x^2 + x + 1$

$01 \times 6E$: $1\,(x^6 + x^5 + x^3 + x^2 + x)$

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

02×46 : $x\,(x^6 + x^2 + x)$

$= x^7 + x^3 + x^2$

$03 \times A6$: $(x+1)(x^7 + x^5 + x^2 + x)$

$x^8 + x^6 + x^3 + x^2 + x^7 + x^5 + x^2 + x$

$x^7 + x^3 + x + 1 + x^6 + x^3 + x^7 + x^5 + x$

$= x^7 + x^6 + x^5 + x^4 + 1$

$x^7 + x^2 + x + 1$: 1 0 0 0 0 1 1 1

$x^6 + x^5 + x^3 + x^2 + x$: 0 1 1 0 1 1 1 0

$x^7 + x^3 + x^2$: 1 0 0 0 1 1 0 0

$x^7 + x^6 + x^5 + x^4 + 1$: 1 1 1 1 0 0 0 1

1 0 0 1 0 1 0 0

$(10010100)_2 = (94)_{16}$

- $(01 \times F2) \oplus (01 \times 4C) \oplus (02 \times E7) \oplus (03 \times 8C)$

$01 \times F2$: $1\,(x^7 + x^6 + x^5 + x^4 + x)$

$= x^7 + x^6 + x^5 + x^4 + x$

$01 \times 4C$: $1\,(x^6 + x^3 + x^2)$

$= x^6 + x^3 + x^2$

$02 \times E7$: $x\,(x^7 + x^6 + x^5 + x^2 + x + 1)$

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

$x^4 + x^3 + x + 1 + x^7 + x^6 + x^3 + x^2 + x$

$= x^7 + x^6 + x^4 + x^2 + 1$

$03 \times 8C$: $(x+1)(x^7 + x^3 + x^2)$

$x^8 + x^4 + x^3 + x^7 + x^3 + x^2$

$x^4 + x^3 + x + 1 + x^4 + x^7 + x^2$

$= x^7 + x^3 + x^2 + x + 1$

$x^7 + x^6 + x^5 + x^4 + x$: 1 1 1 1 0 0 1 0

$x^6 + x^3 + x^2$: 0 1 0 0 1 1 0 0

$x^8 + x^6 + x^4 + x^2 + 1$: 1 1 0 1 0 1 0 1

$x^7 + x^3 + x^2 + x + 1$: 1 0 0 0 1 1 1 1

1 1 1 0 0 1 0 0

$(11100100)_2 = (E4)_{16}$

- $(01 \times 4D) \oplus (01 \times 90) \oplus (02 \times 4A) \oplus (03 \times DB)$

$01 \times 4D$: $1 (x^6 + x^3 + x^2 + 1)$

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

01×90: $1 (x^7 + x^4)$

$= x^7 + x^4$

$02 \times 4A$: $x (x^6 + x^3 + x)$

$= x^7 + x^4 + x^2$

$03 \times D8$: $(x+1)(x^7 + x^6 + x^4 + x^3)$

$x^8 + x^7 + x^5 + x^4 + x^7 + x^6 + x^4 + x^3$

$x^4 + x^3 + x + 1 + x^5 + x^6 + x^3$

$= x^6 + x^5 + x^4 + x + 1$

$x^6 + x^3 + x^2 + 1$: 0 1 0 0 1 1 0 1

$x^7 + x^4$: 1 0 0 1 0 0 0 0

$x^7 + x^4 + x^2$: 1 0 0 1 0 1 0 0

$x^6 + x^5 + x^4 + x + 1$: 0 1 1 1 0 0 1 1

0 0 1 1 1 0 1 0

$(00111010)_2 = (3A)_{16}$

- $(01 \times 97) \oplus (01 \times EC) \oplus (02 \times C3) \oplus (03 \times 95)$

01×97: $1 (x^7 + x^4 + x^2 + x + 1)$

$= x^7 + x^4 + x^2 + x + 1$

$01 \times EC$: $1 (x^7 + x^6 + x^5 + x^3 + x^2)$

$= x^7 + x^6 + x^5 + x^3 + x^2$

$02 \times C3$: $x (x^7 + x^6 + x + 1)$

$x^8 + x^7 + x^2 + x$

$x^4+x^3+x+1+x^7+x^2+x$

$= x^7+x^4+x^3+x^2+1$

03x95: $(x+1)(x^7+x^4+x^2+1)$

$x^8+x^5+x^3+x+x^7+x^4+x^2+1$

$x^4+x^3+x+1+x^5+x^3+x+x^7+x^4+x^2+1$

$= x^7+x^5+x^2$

$x^7+x^4+x^2+x+1$:	1 0 0 1 0 1 1 1
$x^7+x^6+x^5+x^3+x^2$:	1 1 1 0 1 1 0 0
$x^7+x^4+x^3+x^2+1$:	1 0 0 1 1 1 0 1
$x^7+x^5+x^2$:	1 0 1 0 0 1 0 0
	0 1 0 0 0 0 1 0

$(01000010)_2 = (42)_{16}$

- $(03x87) \oplus (01x6E) \oplus (01x46) \oplus (02xA6)$

03x87: $(x+1)(x^7+x^2+x+1)$

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

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

x^7+x^4+x

01x6E: $1(x^6+x^5+x^3+x^2+x)$

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

01x46: $1(x^6+x^2+x)$

$= x^6+x^2+x$

02xA6: $x(x^7+x^5+x^2+x)$

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

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

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

x^7+x^4+x:	1 0 0 1 0 0 1 0
$x^6+x^5+x^3+x^2+x$:	0 1 1 0 1 1 1 0
x^6+x^2+x:	0 1 0 0 0 1 1 0
$x^6+x^4+x^2+x+1$:	0 1 0 1 0 1 1 1
	1 1 1 0 1 1 0 1

$(11101101)_2 = (ED)_{16}$

- $(03 \times F2) \oplus (01 \times 4C) \oplus (01 \times E7) \oplus (02 \times 8C)$

$03 \times F2$: $(x+1)(x^7+x^6+x^5+x^4+x)$

$x^8+x^7+x^6+x^5+x^7+x^6+x^5+x^4+x$

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

$= x^3+x^2+1$

$01 \times 4C$: $1(x^6+x^3+x^2)$

$= x^6+x^3+x^2$

$01 \times E7$: $1(x^7+x^6+x^5+x^2+x+1)$

$= x^7+x^6+x^5+x^2+x+1$

$02 \times 8C$: $x(x^7+x^2+x^3)$

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

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

$= x+1$

x^3+x^2+1 : 00001101

$x^6+x^3+x^2$: 01001100

$x^7+x^6+x^5+x^2+x+1$: 11100111

$x+1$: 00000011

10100101

$(10100101)_2 = (A5)_{16}$

- $(03 \times 4D) \oplus (01 \times 90) \oplus (01 \times 4A) \oplus (02 \times DB)$

$03 \times 4D$: $(x+1)(x^6+x^3+x^2+1)$

$x^7+x^4+x^3+x+x^6+x^3+x^2+1$

$= x^7+x^6+x^4+x^2+x+1$

01×90 : $1(x^7+x^4)$

$= x^7+x^4$

$01 \times 4A$: $1(x^6+x^3+x)$

$= x^6+x^3+x$

$02 \times DB$: $x(x^7+x^6+x^4+x^3)$

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

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

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

$x^7 + x^6 + x^4 + x^2 + x + 1$:	1 1 0 1 0 1 1 1
$x^7 + x^4$:	1 0 0 1 0 0 0 0
$x^6 + x^3 + x$:	0 1 0 0 1 0 1 0
$x^7 + x^5 + x^3 + x + 1$:	1 0 1 0 1 0 1 1
	1 0 1 0 0 1 1 0

$(10100110)_2 = (A6)_{16}$

- $(03 \times 97) \oplus (01 \times EC) \oplus (01 \times C3) \oplus (02 \times 95)$

$03 \times 97 : (x+1)(x^7 + x^4 + x^2 + x + 1)$

$x^8 + x^5 + x^3 + x^2 + x + x^7 + x^4 + x^2 + x + 1$

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

$= x^7 + x^5 + x$

$01 \times EC : 1(x^7 + x^6 + x^5 + x^3 + x^2)$

$= x^7 + x^6 + x^5 + x^3 + x^2$

$01 \times C3 : 1(x^7 + x^6 + x + 1)$

$= x^7 + x^6 + x + 1$

$02 \times 95 : x(x^7 + x^4 + x^2 + 1)$

$x^8 + x^5 + x^3 + x$

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

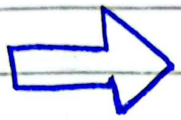
$= x^5 + x^4 + 1$

$x^7 + x^5 + x$:	1 0 1 0 0 0 1 0
$x^7 + x^6 + x^5 + x^3 + x^2$:	1 1 1 0 1 1 0 0
$x^7 + x^6 + x + 1$:	1 1 0 0 0 0 1 1
$x^5 + x^4 + 1$:	0 0 1 1 0 0 0 1
	1 0 1 1 1 1 0 0

$(10111100)_2 = (BC)_{16}$

Hence, we get :

87	F2	4D	97
6E	4C	90	EC
46	E7	4A	C3
A6	8C	D8	95



47	40	A3	4C
37	D4	70	9F
94	E4	3A	42
ED	A5	A6	BC