Assignment: 1

Hamza Mehmood
SP-21-110

Submit to:

Subject: Info Security

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

×

87	F2	4D	97
6E	4C	A0	EC
46	E7	40	C3
A6	8C	D8	95

$(02 \times 87) \oplus (03 \times 6E) \oplus (01 \times 46) \oplus (01 \times A6)$

$02 = 00000010 = u$

$87 = 10000111 = u^7 + u^2 + u + 1$

$(02 \times 87) = u(u^7 + u^2 + u + 1) = u^8 + u^3 + u^2 + u$

$= u^4 + u^3 + u^2 + u + u^3 + u^2 + u$

$= u^4 + u^2 + 1$

$= 00010101$

$03 = 00000011$, $6E = 01101110$

$46 = 01000110$, $01 = 00000001$

$03 \times 6E = (u+1) \times (u^6 + u^5 + u^3 + u^2 + u)$

$= u^7 + u^6 + u^4 + u^3 + u^2 + u^6 + u^5 + u^3 + u^2 + u$

$= u^7 + u^5 + u^4 + u$

$= 10110010$

$01 \times 46 = 1 \times (u^6 + u^2 + u)$

$= u^6 + u^2 + u$

$= 01001110$

$= 01000110$

01 x A6

01 = 00000001 = 1

A6 = 10100110 = $u^7+u^5+u^2+u$

01 x A6 = 1 0 1 0 0 1 1 0

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

47

02 = 00000010 = u

F2 = 11110010 = $u^7+u^6+u^5+u^4+u$

02 x F2 = $u(u^7+u^6+u^5+u^4+u)$

= $u^8+u^7+u^6+u^5+u^2$

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

= 11111111

03 = 00000011 = $u+1$

4C = 01001100 = $u^6+u^3+u^2$

03 x 4C = 01001100

01 = 00000001 = 1

E7 = 11100111 = $u^7+u^6+u^5+u^2+u+1$

01 x E7 = 11100111

01 = 00000001

8C = 10001100

01 x 8C = 10001100

1 1 1 1 1 1 1 1
1 1 0 1 0 1 0 0
1 1 1 0 0 1 1 1
1 0 0 0 1 1 0 0
0 1 0 0 0 0 0 0
40

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

$02 = 00000010 = x$

$4D = 01001101 = x^6 + x^3 + x^2 + 1$

$02 \times 4D = x^7 + x^4 + x^3 + x$

$= 10011010$

$03 = 00000011 = x + 1$

$90 = 10010000 = x^7 + x^4$

$03 \times 90 = x^8 + x^5 + x^7 + x^4$

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

$= 10101011$

$01 = 00000001 = 1$

$4A = 01001010 = x^6 + x^3 + x$

$01 \times 4A = 01001010 = x$

$01 = 00000001$

$D8 = 11011000$

$01 \times D8 = 11011000$

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

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

A3

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

02 = 00000010 = x

97 = 10010111 → $x^7 + x^4 + x^2 + x + 1$

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

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

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

$= 00110101$

01 = 00000001

03 = 11000011

$01 \times C3 = 11000011$

01 = 00000001

95 = 10010101

$01 \times 95 = 10010101$

00110101
00010111
10100011
10000101
01001100

$(01 \times 87) \oplus (02 \times 6E) \oplus (03 \times 46) \oplus (01 \times A6)$

__/__/202 Day:_____

$8.7 = 10000111$

$02 = 00000010$
$6E = 01101110$

$02 \times 6E = (x)(x^6+x^5+x^3+x^2+x)$
$= x^7+x^6+x^4+x^3+x^2$
$= 11011100$

$03 = 00000011$
$46 = 01000110$

$(03 \times 46) = (x+1)(x^6+x^2+x)$
$= x^7+x^3+x^2+x^6+x^2+x$
$= 11001010$

$A6 = 10100110$

10000111
11011100
11001010
10100110
00111011

3

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

$4D = 01001101$

$02 = 00000010 = x$
$90 = 10010000 = x^7+x^4$
$20 \times 90 = x^8+x^5$
$20 \times 90 = x^4+x^3+x+1+x^5$
$= 00111011$

Day:

__/__/202

$08 = 11011000$

$$
\begin{array}{r}
0\ 1\ 0\ 0\ 1\ 1\ 0\ 1 \\
0\ 0\ 1\ 1\ 1\ 0\ 1\ 1 \\
1\ 1\ 0\ 1\ 1\ 1\ 1\ 0 \\
1\ 1\ 0\ 1\ 1\ 0\ 0\ 0 \\
\hline
0\ 1\ 1\ 1\ 1\ 0\ 0\ 0 \\
7 \qquad\qquad 0
\end{array}
$$

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

$97 = 10010111$

$02 = x$

$EC = 11101100 = x^7 + x^6 + x^5 + x^3 + x^2$

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

$= x \cdot x^7 + x \cdot x^6 + x + 1 + x \cdot x^6 + x^4 + x^3$

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

$= 11000011$

$03 = x + 1$

$C3 = 11000011 = x^7 + x^6 + x + 1$

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

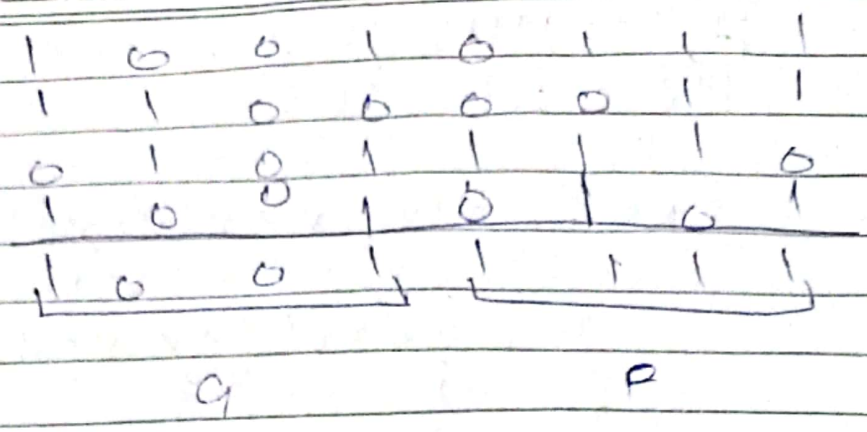
$03 \times C3 = x^8 + x^6 + x^2 + 1$

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

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

$= 01011110$

$95 = 10010101$



q p

$(01 \times 87) \oplus (01 \times 6E) \oplus (02 \times 46) \oplus (03 \times A6)$

87 = 10000111

6E = 01101110

02 = x

46 = 01000110 = $x^6 + x^2 + x$

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

= 10100100

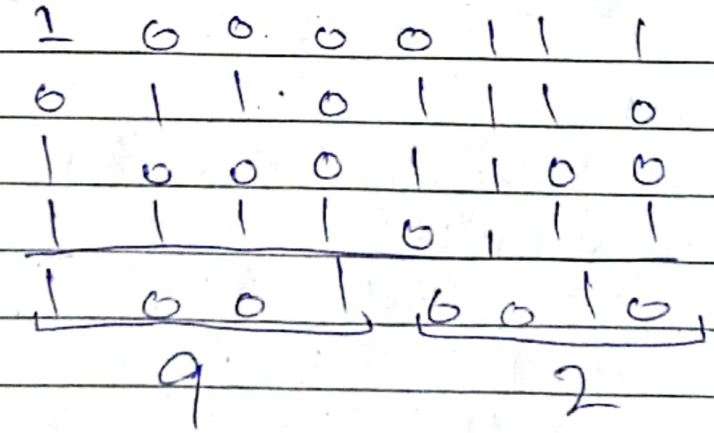
03 = x + 1

A6 = 10100110 = $x^7 + x^5 + x^2 + x^1$

$03 \times A6 = x^8 + x^6 + x^3 + x + x^7 + x^5 + x^2 + x$

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

F2 = 11110111



q 2

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

Day:

__/__/202

F2 = 11110010

4C = 01001100

02 x E7 = $u(u^7+u^6+u^5+u^2+u+1)$

$= u^8+u^7+u^6+u^3+u^2+u$

$= u^4+u^3+u+1+u^7+u^6+u^3+u^2+u$

= 11010101

03 = u+1

8C = 10001100 = $u^7+u^3+u^2$

(03 x 8C) = $(u+1)(u^7+u^3+u^2)$

$= u^4+u^3+u+1+u^7+u^6+u^3+u^2$

= 10001111

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

E4

(01 x 4D) ⊕ (01 x 90) ⊕ (02 x 4A) ⊕ (03 x D8)

4D = 01001101

90 = 10010000

02 = u

4A = 01001010 = u^6+u^3+u

$= u^7+u^4+u^2$

D = 10010100

03 = u+1

D8 = 11011000

$= u^8+u^7+u^5+u^4+u^4+u^6+u^4+u^3$

$(03 \times 87) \oplus (01 \times 6E) \oplus (01 + 46) \oplus (02 \times 46)$

$03 = u+1$

$87 = 10000111 = u^7+u^2+u+1$

$= u^8+u^3+u^2+u+u^7+u^2+u+1$

$= u^4+u^3+u+1+u^3+u+1$

$= u^7+u^4+u$

$= 10010010$

$02 = u$

$A6 = 10100110 = u^7+u^5+u^2+u$

$= u^8+u^6+u^3+u^2$

$= u^4+u^3+u+1+u^6+u^3+u^2$

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

$= 01010111$

$46 = 01000110$

$A6 = 10100110$

$$\begin{array}{cccccccc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ \hline 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{array}$$

2 5

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

$03 = u+1$

$F2 = 11110010 \rightarrow u^7+u^6+u^5+u^4+u$

$= u^8+u^7+u^6+u^5+u^2+u^7+u^6+u^5+u^4+u$

$= u^4+u^3+u+1+u^2+u^4+u$

$= u^3+u^2+1$

$= 00001101$

Day:

__/__/202

02 = 00000010

BC = 10000100 = $x^7 + x^3 + x^2$

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

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

$= x + 1$

= 00000011

14C = 01001100

E7 = 11100111

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

A S

(03 x 4D) ⊕ (01 x 90) ⊕ (01 x 4A) ⊕ (02 x D8)

03 = x + 1

4D = 01001101 = $x^6 + x^3 + x^2 + 1$

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

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

= 11010111

02 = x

DB = 11011000 → $x^7 + x^6 + x^4 + x^3$

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

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

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

= 10101011

Day:

__/__/202

$9D = 10011000$

$4A = 01001010$

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

F 4

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

$03 = x+1$

$97 = 10010111 = x^7 + x^4 + x^2 + x + 1$

$= x^8 + x^5 + x^3 + x^2 + x + x^5 + x^3 + x + x^2 + x + 1$

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

$= 10100010$

$02 = x$

$95 = 10010101 = x^7 + x^4 + x^2 + 1$

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

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

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

$= 00110001$

$C3 = 11000011$

$EC = 11101100$

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

B C

___/___/202 Day: _____

47	40	A3	4C
37	D4	70.	9F
92	E4	3A	42
25	A5	F4	BC