# Assignment - 02

CSE 447

Section - 01

Mohammad Shafkat Hasan

ID - 19101077

Submit : July 11, 2023

# Ans to the Q. No. 1

Element of $GF(2^4) = \{0, 1, x, x^2, x^3, x+1, x^2+1, x^3+1, x+x^2, x^2+x^3, x+x^3+1+x+x^2, 1+x+x^3, x+x^2+x^3, x+x^2+x^3, 1+x+x^2+x^3\}$

Here,
$A(x) = x^3+x^2+1$
$B(x) = x^2+x+1$

Addition:

$A(x) + B(x)$

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

$= x^3+x^2+x^2+x+1+1 \quad [\because (1+1) \bmod 2 = 0]$

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

$= x^3 + x$

Multiplication

$A(x) * B(x) = (x^3+x^2+1)(x^2+x+1)$

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

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

$= x^5+x+1$

$A \cdot B$

$x^5+x+1$

$x^5+x^2+x$

$x^2+1$

$x^4+x+1$

$x^4+x^2+x$

$P(x)$

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

$\therefore A(x) \cdot B(x) = x^4+x^2+x$

# Ans. To The Q. No. 2

Here,

Initial key: 4A CC 9E 45

Round constant: 00 01 10 11

$(W[0]\ W[1]\ W[2]\ W[3]) = 4A\ CC\ 9E\ 45$

$g(W[3]) = g(45)$

Rotate $W[3] = 45 \rightleftharpoons 54$

Sbox $(54) = 20$

$20 \oplus Rc$

$= 00100000 \oplus 00011011$

$= 00111011 = g(W[3])$

$W[4] = W[0] \oplus g(W[3])$

$= 4A \oplus g(W[3]) = 01001010 \oplus 00111011$

$= 01110001 = 71$

$W[5] = W[1] \oplus W[4] = CC \oplus W[4]$

$= 11001110 \oplus 01110001$

$= 10111111 = BF$

$W[6] = W[2] \oplus W[5] = 9E \oplus W[5]$

$= 10011110 \oplus 10111111$

$= 00100001$

$W[7] = W[3] \oplus W[6]$

$= 45 \oplus W[6]$

$= 01000101 \oplus 00100001$

$= 01100100$

# Ans. To The Q. No.3

Here,

$m = 31$ $\quad$ $SIk = \{2, 3, 6, 13, 27, 52\}$

$n = 105$

Encrypt $= 100100$

$m^{-1} \bmod = 31^{-1} \bmod 105 = 61$

Now,

$2 * 31 \bmod 105 = 62$

$3 * 31 \bmod 105 = 93$

$6 * 31 \bmod 105 = 81$

$13 * 31 \bmod 105 = 88$

$27 * 31 \bmod 105 = 102$

$52 * 31 \bmod 105 = 37$

Public key $= \{62, 93, 81, 88, 102, 37\}$

$\therefore$ Encrypt $= 62 + 88$

$= 150$

Decrypt:

$150 \times 61 = 9150 \bmod 105$

$= 15$

$15 = 2 + 13$

Obtain plaintext : 100100

[shown]

# Ans. To The Q. No. 4

Here,

$p = 31$

$q = 37$

$e = 17$

$m = 2$

$N = p * q$

$N = 31 \times 37$

$= 1147$

$\phi(n)$ = Relatively prime to $(p-1)(q-1)$

$= (31-1)(37-1)$

$= 1080$

$(d * e) \bmod \phi(n) = 1$

$\Rightarrow d * 17 \bmod 1080 = 1$

$\Rightarrow 17^{-1} \bmod 1080 = d$

| q | $r_1$ | $r_2$ | r | $t_1$ | $t_2$ | t |
|---|---|---|---|---|---|---|
| 63 | 1080 | 17 | 9 | 0 | 1 | -63 |
| 1 | 17 | 9 | 8 | 1 | -63 | 64 |
| 1 | 9 | 8 | 1 | -63 | 64 | -127 |
| 8 | 8 | 1 | 0 | 64 | -127 | 1080 |

$t = t_1 - q t_2$

$= 0 - 63 = -63$

$= 1 + 63 = 64$

$= -63 - 64 = -127$

$= 64 + (127 \times 8)$

$= 1080$

$17^{-1} \bmod 1080 = -127$

$= -127 + 1080$

$= 953$

$\therefore d = 953$

∴ Public key : (N, e) = (1147, 17)

Privat key : d = 953

$M = 2$

$C = M^e \bmod N = 2^{953} \bmod 1147 = 721$

~~$C = 2^{953} \bmod 1147 = 327721$~~

~~$C = 2^{17} \bmod 1147 = 324$~~

∴ Decrypt :

$M = C^{ed} \bmod N = 721^{17} \bmod 1147$

$= 2$

~~$= 324^{953} \bmod 1147$~~

$= 327^{953} \bmod 1147$

$= 2$

So after decryption we got same value.