Final Assignment

Tasnim Sakib Apon
ID : 20241068
CSE 490

Tasnim Sakib Apon
20241068

1. ∴ $P = (16, 8)$.

Given $\Rightarrow y^2 = x^3 - 2x + 2 \mod 23$

So $x = 16$
$y = 8$

So. L.H.S $\Rightarrow 8^2 \mod 23$
$= 64 \mod 23 \Rightarrow 18$

R.H.S $\Rightarrow 16^3 - 2.16 + 2 \mod 23$

$\Rightarrow 4096 - 32 + 2 \mod 23$

$\Rightarrow 4066 \mod 23$

$\Rightarrow 18$

$\therefore$ L.H.S = R.H.S.

$\therefore$ The point (16, 8) is on E.

2. $P = (16, 8)$.

$2P$:

$2P \Rightarrow P + P$

$\Rightarrow (16,8) + (16,8)$

$x_1\ y_1 \quad x_2\ y_2$

$y^2 = x^3 - 2x + 2 \bmod 23$

So, $a = -2$

$b = 2$.

$P = Q$.

So, $S \Rightarrow \frac{3x_1^2 + a}{2y_1} \bmod p$

$\Rightarrow \frac{3(16)^2 + (-2)}{2 \times 8} \bmod 23$

$\Rightarrow \frac{766}{16} \bmod 23$

$\Rightarrow 22$

$\therefore x_3 = S^2 - x_1 - x_2 \bmod p$

$= 22^2 - 16 - 16 \bmod 23$

$= 15$

20241068

$y_3 = s(x_1 - x_3) \text{ Mod } P$

$\Rightarrow 22(16-15) \text{ Mod } 23$

$\Rightarrow 22 \text{ Mod } 23$

$y_3 = s(x_1 - x_3) - y_1 \text{ Mod } P$

$= 22(16-15) - 8 \text{ Mod } 23$

$= 22.1 - 8 \text{ Mod } 23$

$= 14 \text{ Mod } 23$

$= 14$

$\therefore 2P \Rightarrow (15, 14)$ [Ans]

Now,

$3P \Rightarrow$ $3P \Rightarrow P + 2P$

$\Rightarrow (16, 8) + (15, 14)$

Here $x_1 = 16$

$x_2 = 15$

$y_1 = 8$

$y_2 = 14$

20241068

~~$y_3 \Rightarrow S(x_1 - x_3)$~~

$$S \Rightarrow \frac{y_2 - y_1}{x_2 - x_1} \text{ Mod } 23$$

$$= \frac{14-8}{15-16} \text{ Mod } 23$$

$$= -6 \text{ Mod } 23$$

$$= 17$$

$\therefore x_3 \Rightarrow S^2 - x_1 - x_2 \text{ Mod } 23$

$\Rightarrow 17^2 - 16 - 15 \text{ Mod } 23$

$\Rightarrow 258 \text{ Mod } 23$

$\Rightarrow 5$

$y_3 \Rightarrow S(x_1 - x_3) - y_1 \text{ Mod } 23$

$\Rightarrow 17(16-5) - 8 \text{ Mod } 23$

$\Rightarrow 179 \text{ Mod } 23$

$\Rightarrow 18$

$\therefore 3P \Rightarrow (5, 18)$ [Ans]

20241068

3. $P = (16, 8)$

a, Alice's shared key = 3

b, Bob's shared key = 6

Alice to Bob $\Rightarrow A = a.P$

$= 3(16, 8)$

$= (5, 18)$ [Ans]

Bob sends to Alice $B = b.P$

$= 6(16, 8)$

$= (15, 9)$ [Ans]

So, $a.B = 3.(15, 9)$

$= (15, 14)$

Now, $b.A = 6(5, 18)$

$= (15, 14)$

$\therefore$ Shared key $\Rightarrow$ ~~(15, 14)~~ 15

[Ans]

20241068

2. (a) Here,

$N = 51$

$S = 19$

$V = S^V \text{ Mod } (N)$

$= 19^V \text{ Mod } 51$

$= 361 \text{ Mod } 51$

$= 4$ [Ans]

(b) $r = 13$

∴ first message $\Rightarrow$ ~~r mod~~ $r^V \text{ Mod } (N)$

$\rightarrow 13^V \text{ Mod } (N)$

$\Rightarrow 169 \text{ Mod } 51$

$\Rightarrow 16$ [Ans]

(c) $e = 0$

so, $r \times S^e \text{ Mod } (N)$

$\rightarrow 13 \times 19^0 \text{ Mod } (51)$

$\Rightarrow 13 \text{ mod } (51)$

$\Rightarrow 13$ [Ans]

(d) $e=1$,

so,

$$r * s^e \bmod (N)$$

$$\Rightarrow 13 \times 19^1 \bmod (51)$$

$$\Rightarrow 43 \quad \text{[Ans]}$$

20241068

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
X	0	1	1	0	0	0	1	1	0	0	1	0	1	0	0	1	0	1	1					
Y	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1			
Z	1	0	0	1	1	1	0	1	1	0	1	1	1	1	1	0	0	1	0	0	1	1	1	

Here $m = maj(x_8, y_{10}, z_{10})$

$\Rightarrow maj(0, 0, 1)$

$\Rightarrow 0$

For $x_1 \Rightarrow x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$

$\Rightarrow 0 \oplus 0 \oplus 1 \oplus 1$

$\Rightarrow 0$

∴ After Right shifting $\Rightarrow$ 0011000110010100101

For $y \Rightarrow y_{20} \oplus y_{21}$

$\Rightarrow 0 \oplus 1$

$\Rightarrow 1$

∴ After Right shifting $\Rightarrow$ 10011000000000000011101

20241068

∴ First bit of key $\Rightarrow (1 \oplus 0 \oplus 1)$

$\Rightarrow 0$ [Ans]

Now again,

$m = maj(x_8 \oplus y_{10} \oplus z_{10})$

$= maj(1, 0, 0)$

Now,

again,

$m = maj(x_8, y_{10}, z_{10})$

$\Rightarrow (1, 0, 1)$

$= 1$

For, x,

$\Rightarrow x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$

$\Rightarrow 1 \oplus 1 \oplus 0 \oplus 1$

$\Rightarrow 1$

∴ x = 1001100011001010010

For z,

$\Rightarrow z_{21} \oplus z_{20} \oplus z_{21} \oplus z_{22}$

$\Rightarrow 1 \oplus 1 \oplus 1 \oplus 1$

$\Rightarrow 0$

∴ z → 0 | 00 | 1 | 01 | 01111 | 001 | 0011

20241068.

∴ 2nd bit → 0 ⊕ 0 ⊕ 1

→ 1 [Ans]

R0291068

4 ⇒ Let {1, 3, 7, 13, 26, 65, 119, 267} be the SIK.

m = 523

n = 467

so,

1 × 523 Mod 467 ⇒ 56

3 × 523 Mod 467 ⇒ 168

7 × 523 Mod 467 ⇒ 392

13 × 523 Mod 467 ⇒ 261

26 × 523 Mod 467 ⇒ 55

65 × 523 Mod 467 ⇒ 371

119 × 523 Mod 467 ⇒ 126

267 × 523 Mod 467 ⇒ 8

∴ General knapsack = {56, 168, 392, 261, 55, 371, 126, 8}

Encryption:

01001011

⇒ 168 + 55 + 126 + 8

⇒ 357.

Decryption:

m^{-1} Mod n

⇒ 523^{-1} Mod 467

⇒ 442

20241068

Now,

$35^{2} \times 442 \bmod 462$

$\Rightarrow 157^{2} \times 9 \bmod 462$

$\Rightarrow 415$

So, $415 \Rightarrow 3 + 26 + 119 + 26^{2}$

Obtained Plaintext $\Rightarrow$ 01001011.

[Decrypted]