Answer to the Question - 1

1. Given,

$$y^2 = x^3 - 2x + 2 \pmod{23}$$

If $x = 10$

$y = 19$,

$$19^2 = 10^3 - 2 \cdot 10 + 2 \pmod{23}$$

$$\Rightarrow 361 = 982 \pmod{23}$$

$$\Rightarrow 361 = 23 \times 27 + 361 \pmod{23}$$

So, if we mod both sides we get,

$$\Rightarrow 16 = 0 + 16$$

$$\therefore 16 = 16$$

So, the points (10, 19) are on E.

Given,

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

$$P(1,22) = Q(1,22)$$

$$\therefore s = \frac{3x_1^2 + a}{2y_1} \mod 23 \quad [\text{as } P = Q]$$

$$= \frac{3 \times 1 - 2}{22 \times 2} \mod 23$$

$$= \frac{1}{44} \mod 23$$

$$= 1 \times 44^{-1} \mod 23$$

$$= 11 \mod 23$$

$$x_3 = 11^2 - 1 - 1 \mod 23 \quad [x_3 = s^2 - x_1 - x_2 \mod p]$$

$$= 119 \mod 23$$

$$= 4 \mod 23$$

$$y_3 = 11(1-4) - 22 \mod 23 \quad [y_3 = s(x_1 - x_3) - y_1 \mod p]$$

$$= -55 \mod 23$$

$$= 14 \mod 23$$

$$\therefore 2P = (4, 14)$$

Again:

$3P = P + 2P$

$P = (1, 22)$

$Q = 2P = (4, 14)$

$$S = \frac{y_2 - y_1}{x_2 - x_1} \bmod p \; ; \; P \neq Q$$

$$= \frac{14 - 22}{4 - 1} \bmod 23$$

$$= -8 \times 3^{-1} \bmod 23$$

$$= 15 \times 8 \bmod 23$$

$$= 5$$

In this case,

$$x_3 = S^2 - x_1 - x_2 \bmod 23$$

$$= (5^2 - 1 - 4) \bmod 23$$

$$= 20 \bmod 23$$

$y_3 = s(x_1 - x_3) - y_1 \mod 23$

$= 5(1 - 20) - 22 \mod 23$

$= -117 \mod 23$

$= 21 \mod 23$

$\therefore 3P = (20, 21)$

Answer: $2P = (4, 14)$

$3P = (20, 21)$

3 Given,

$a = 10$

$b = 9$

$P = (10, 19)$

Alice		Bob
$a = K_{prA} = 10$		$b = K_{prB} = 9$
$a \cdot P = 10 \cdot (10, 19)$		$b \cdot P = 9 \cdot (10, 19)$
$= (4, 9)$	A (4,9) →	$= (18, 18)$
$= A$	← B (18,18)	$= B$

Here,

Alice send to Bob (4, 9)

Bob send to Alice (18, 18)

$a \cdot B = 10 \cdot (18, 18)$

$= (4, 9)$

$b \cdot A = 9 \cdot (4, 9)$

$= (4, 9)$

Here, the shared secret key is the value of K which is 4.

Answer to the Question-2

We know,

$$V = s^2 \bmod N$$

$$= 19^2 \bmod 51$$

$$= 4$$

Given,

$s = 19$

$N = 51$

Alice's first message if $r = 13$:

$$x = r^2 \bmod N$$

$$= 13^2 \bmod 51$$

$$= 16$$

If $r = 13$, $e = 0$, Alice's third message :

$$y = r \bmod N$$

$$= 13 \bmod 51$$

$$= 13$$

If r = 13, e = 1, Alice's third message:

$$y = r * s \bmod N$$

$$= 13 * 19 \bmod 51$$

$$= 43$$

Ans to the Question -3

Given,

$X = [0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 1]$

$Y = [0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0]$

$Z = [1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1]$

Here,

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

$= maj(0, 0, 1)$

$= 0$

Since $x_8 = m = 0$,

$t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$

$= 0 \oplus 0 \oplus 1 \oplus 1$

$= 0 \oplus 0$

$= 0$

$\therefore x_9 = 0$

again,

$y_{10} = m = 0,$

$t = y_{20} \oplus y_{21}$

$= 0 \oplus 1$

$= 1$

$\therefore y_0 = 1$

as $z_{10} \neq m$, nothing will change for z.

After shifting,

$X = [0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1]$

$Y = [1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0]$

$Z = [1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1]$

1st key stream bit is $= x_{18} \oplus y_{21} \oplus z_{22}$

$= 1 \oplus 0 \oplus 1$

$= 1 \oplus 1$

$= 0$

again, Here,

$$m = maj(0, 0, 1)$$

$$= 0$$

since,

$$h_8 = m = 0$$

$$t = h_{13} \oplus h_{16} \oplus h_{17} \oplus h_{18}$$

$$= 1 \oplus 1 \oplus 0 \oplus 1$$

$$= 0 \oplus 1$$

$$= 1$$

$$\therefore h_0 = 1$$

again,

$$y_{10} = m = 0$$

$$1 = y_{20} \oplus y_{21}$$

$$= 1 \oplus 0$$

$$= 1$$

$$y_0 = 1$$

as, $z_{10} \neq m$ ⊕ nothing will change.

After shifting,

end keystream bit = $0 \oplus 1 \oplus 1$

$= 1 \oplus 1$

$= 0$

---

x

Answer to the Question-4

Given,

{1, 3, 7, 13, 26, 65, 119, 267} be SIK.

$m = 523$

$n = 467$

To compute General knapsack:

$1 \cdot 523 \bmod 467 = 56$

$3 \cdot 523 \bmod 467 = 168$

$7 \cdot 523 \bmod 467 = 392$

$13 \cdot 523 \bmod 467 = 261$

$26 \cdot 523 \bmod 467 = 55$

$65 \cdot 523 \bmod 467 = 371$

$119 \cdot 523 \bmod 467 = 126$

$267 \cdot 523 \bmod 467 = 8$

GK: (56, 168, 392, 261, 55, 371, 126, 8)

To Encrypt 01 001011 :

$0 + 168 + 0 + 0 + 55 + 0 + 126 + 8 = 357$

Here,

$m^{-1} \bmod n = 523^{-1} \bmod 467$

$= 442$

To decrypt :

$357 \cdot 442 \bmod 467 = S$

$\therefore S = 415$

$415 = 267 + 119 + 26 + 3$

Obtained plaintext = 01 001011

Hence, we obtained the given plain text.

x