106118036

CT-1 CSPE-18

2) Curve: $y^2 = x^3 + x + 6$

$p = 11$

(i) $Z_p = \{0, 1, 2, \ldots, 10\}$

Trial and error:

$x = 1$		$x = 2$
$y^2 = 8$	X	$y^2 = 8 + 8 = 16 \therefore y = 4$

So, $\boxed{P(2,4)} \rightarrow$ (i)

Now, $x = 3$

$y^2 = 27 + 9 = 36$

$\therefore y = 6$

$\boxed{Q(3,6)} \rightarrow$ (ii)

ii) Now, we need to find $P+Q$ & $2P$

a) $P+Q$:-

Slope :- $S = (y_1 - y_2)/(x_1 - x_2)$

$S = (4-6)/(2-3)$

$\boxed{S = 2} \rightarrow$ (iii)

So,

$R = P+Q = (x_3, y_3)$

$x_3 = S^2 - x_1 - x_2$

$x_3 = 4 - 2 - 3 = -1 \mod 11$

$\boxed{x_3 = 10} \rightarrow$ (iv)

~~$y_3 = S(x_1 - x_2) - y_1 = 2(-1) - 4 = -6 \mod 11 \equiv 5$~~

So, $y_3^2 = x_3^3 + x_3 + 6$

$= (1000 + 10 + 6) \bmod 11$

$= (1016) \bmod 11$

$\boxed{y_3^2 = 4}$

$\therefore \boxed{y_3 = 2}$

$\therefore \boxed{P + Q = R\{10, 2\}}$ ⇒ Answer

(iii)

b) $2P$:-

$P + P \qquad P\{2, 4\}$

we find tangent and use formula

So, $s = \dfrac{3 * x_p^2 + a}{2 * y_p}$

$= \dfrac{3 * 4 + 1}{8} = \boxed{\dfrac{13}{8} = 5}$

$s = 13 \bmod 11 * 8^{-1} \bmod 11$

$= 2 * 7 = 14 \bmod 11 = \boxed{3}$

~~$x_3 = s^2 + 5$~~

$x_3 = \left(x_p^2 + \dfrac{6}{x_p^2}\right) \bmod 11$

$= (4 + 6 * 4^{-1} \bmod 11) \bmod 11$

$= (4 + 6 * 3) \bmod 11$

$= 9 - 2 - 2 = 5$

$y_3 = (3(2-5) - 4) \bmod 11$

$y_3 = 9$

$\therefore 2P \{5, 9\}$

iii) Finding P, Q, 2P sum.

Now, $P + Q = R = \{10, 2\} \rightarrow (a)$

$R + 2P = \{10, 2\} + \{5, 9\}$

So, $S = y_2 - y_1 / x_2 - x_1$

$= 7/-5 = 7 * 6^{-1} \bmod 11$

$= (7 * 2) \bmod 11$

$\boxed{S = 3}$

So, $x_3 = S^2 - x_1 - x_2$

$= (9 - 10 - 5) \% 11$

$\boxed{x_3 = 5}$

~~$y_3 = 3(10 - 5) -$~~

$y_3^2 = (125 + 5 + 6) \bmod 11$

$y_3^2 = 4$

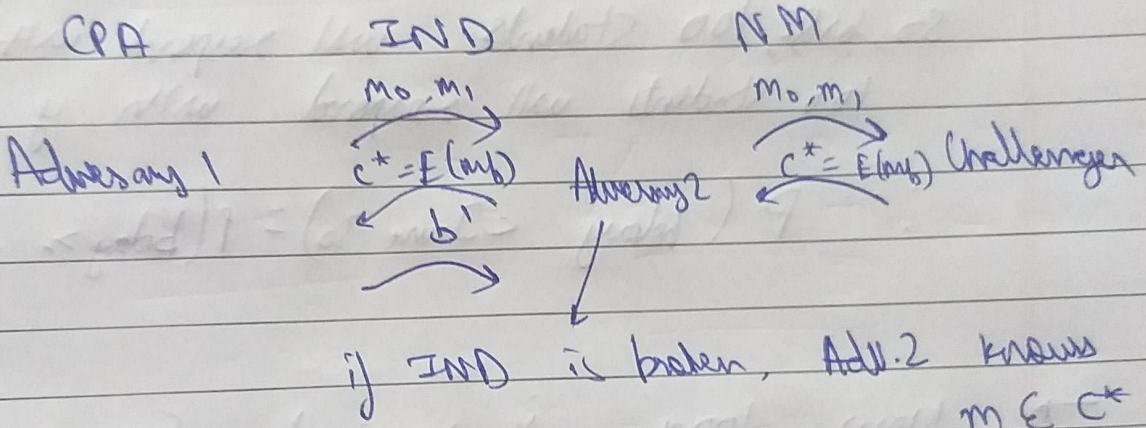
$\boxed{y_3 = 2}$

$\therefore \boxed{S (5, 2)} \Rightarrow$ Ans

1) We need to prove that
NM - CPA → IND - CPA secure

So, taking contrapositive (for (A → B, we will instead ¬B → ¬A)
if adversary can break, IND - CPA, then NM - CPA can also be broken by another adversary.

→ CPA



if IND is broken, Adv.2 knows $m \in c^*$.

Thus, Adv. 2 can encrypt same rm and give with the

$$R(d(c'), d(c)) \text{ as } d(c') = r_d(c^*)$$

3> Total population = 400
Number of students Ans Q_1 = P(heads) * 400
= 0.5 * 400 = 200

Number of student Ans Q_2 = P(tails) * 400 = 200

→ Since students will have a uniform b'day, considering June 30th as middle of year,

So, for 200 students will respond with x and 100 students will respond with y.

$\therefore P(\text{bday} < \text{June } 30) = P(\text{bday} > \text{June } 30) = 1/2$.

→ Now, 100x is received from here, i.e. Q_2.
So, Q_1 will respond with y because total x responses is 100.

∴ Number of students taking drugs is 0.

4) Given (g, g^k) which is generated by g of prime order 'q', schnorr group.

Now assuming that c_1, c_2 such that

$$c_2 = c_1^x \longrightarrow (i)$$

Taking random number 'k', we get

$$c_1 = g^k$$
$$c_2 = (g^x)^k \quad [\because (g, g^x)]$$

Hence,

$$c_2 = (g^x)^k = (g^k)^x = c_1^x$$

Thus, we can say that both (c_1, c_2) will belong to the Schnorr group G.

5) RSA (t', ϵ') → secure.
M_R (declared msg) → forge this in full domain hash sig. scheme

(i) $t = t' - (q_{hash} + q_{sig} + 1) \cdot O(k^3)$
(ii) $\epsilon = \epsilon'$.

(i) → Now, we need to apply the logic that for the rest of messages ~~inverter~~ will give trivial hash and signature.
→ For the declared msg, adversary will give a RSA-hard problem.
→ ~~$\epsilon = \epsilon'$~~ Now, the adversary has to forge because he won't ~~##~~ ask for both hash & sign.
→ Same as original time complexity $\therefore O(k^3)$.

(ii) Now, $\epsilon = \epsilon'$ because there is no probability element, hence, no random element.