Name :- SHREY Mavani
ID :- 20190224

1) Given $\alpha \in Z_p^*$ is a primitive element. Using the theorem given in question find the smallest primitive element module 97.

$2^{48} \bmod 97 = 1$
$3^{48} \bmod 97 = 1$
$4^{48} \bmod 97 = 1$
$5^{58} \bmod 97 = 96$ & $5^{32} \bmod 97 = 35$

$\Rightarrow$ Therefore the smallest primitive root module 97 is 5.

2)

a) Denote $d = gcd(p-1, q-1)$, $p-1 = p'd$ & $q-1 = q'd$
Then,

$\lambda(n) = p'q'd = (p-1)q' = p'(q-1)$ we have that $ab \equiv 1 \pmod{\lambda(n)}$, So

$ab = k\lambda(n) + 1 = k(p-1)q' + 1$ for some positive integer $k$.

Then, $X^{ab} \equiv X^{k(p-1)q'+1} \pmod{p} \equiv X \pmod{p}$

Similarly, $X^{ab} \equiv X^{k(q-1)p'+1} \pmod{q} \equiv X \pmod{q}$

Page No.
Date

Since $x^{ab} \equiv x \pmod{p}$ mod $x^{ab} \equiv \pmod{q}$, it follows immediately that $x^{ab} \equiv x \pmod{n}$

b) $d = 6$, $\lambda(n) = 468$ & $\phi(n) = 2808$

$b^{-1} \bmod (\lambda(n)) = 67$ & $b^{-1} \bmod \phi(n) = 2407$

3)

$$28702 = (2)^1 (113)^1 (127)^1$$

we find that,

$$\log_5 8563 \equiv 1 \pmod{2},$$

$$\log_5 8563 \equiv 67 \pmod{113}$$

$$\log_5 8563 \equiv 99 \pmod{127}$$

Using the chinese remainder theorem, $\log_5 8563 \equiv 3903$.

$$\Rightarrow 31152 = (2)^4 (11)^1 (3)^1 (59)^1$$

$\log_{10} 12611 \equiv 14 \pmod{16}$, $\log_{10} 12611 \equiv 2 \pmod{3}$
$\log_{10} 12611 \equiv 8 \pmod{11}$, $\log_{10} 12611 \equiv 51 \pmod{59}$

Using the chinese remainder theorem, $\log_{10} 12611 = 17102$

4]

a) Points on the ecliptic curve $y^2 = x^3 + x + 28$ over $Z_{11}$ are ~~made~~ make a table of x, $x^3 + x + 28 \bmod Z_{11}$, quadratic residue & y pts.

By doing this, we get 72 no. of pts.

b) If E were cyclic, there would be pts having order 72, but there are no such pts.

c) The maximum order of a points is 36, (4, 5) is one point having order 36.

[E is isomorphic to $Z_{36} \times Z_2$.]

5]

First, we compute, $k = (x_1 - x_2)(\delta_1 - \delta_2)^{-1} \bmod (P-1)$

$= -22425 \times (10915)^{-1} \bmod 31846$

$= 1165$

To determine a, we will solve the congruence

$$ya \equiv x_1 - k\delta_1 \pmod{P-1}$$ for a.

This congruence simplifies to $23472a \equiv 23764 \pmod{31846}$

We have that gcd(23972, 31846) = 2 &

2 | 23704, So the congruence is equivalent to

$$11986a \equiv 11852 \times 11986^{-1} \pmod{15923}$$
$$\equiv 7459 \pmod{15923}$$

Therefore, $a = 7459$ or $a = 7459 + (P-1)/2$
$= 23382$

By computing $x^{7459} \bmod P = 25703 = B$

& $x^{23382} \bmod P = 6144 \neq B$, we see that $x = 7459$

6)

a) Signature (20679, 11082) on the msg $x = 20543$

$5^{20543} \bmod 31847 = 20688$
$= 26379^{20679} \; 20679^{11082} \bmod 31847$

b) by solving an instance of discrete logarithm

$a = \log_5 26379 = 7973$

c) To determine k, we will solve the congruence

$k\delta \equiv x - a\gamma \pmod{P-1}$

for $k$. This congruence simplifies to

$$11082k \equiv 13618 \pmod{31846}$$

$g.c.d(11082, 31846) = 2$ & $2 \mid 13618$.
So the congruence is equivalent to

$$5541k \equiv 6809 \pmod{15923}$$

This congruence has the solution,

$$k \equiv 6809 \times 5541^{-1} \pmod{15923} \equiv 3464 \pmod{15923}$$

Therefore, $k = 3464$ or $k = 7459 + (p-1)/2 = 19387$
By computing $\alpha^{3464} \bmod p \equiv 11168 \neq \gamma$ &
$\alpha^{19387} \bmod p \equiv 20679 = \gamma$, we can see that

$$\boxed{k = 19387}$$