Problem 2 :

a) A digital certificate from certificate authority can be validated by anyone prior to using a public key to encrypt and send message to recipient. Without it, its difficult to verify the authenticity of someone's public key due to MITM vulnerability.

b) Use extended euclidean algorithm

c) Quorum is required because their solutions are required to solve series of equations to "unlock" the key. Without quorum, there are not enough solutions to solve equations / get secret.

D) So that square root can be taken easily.

E) Prime factorization
Discrete logarithm problem
Elliptic curve discrete logarithm problem

F) Discrete logarithm problem
$$g^x \equiv a \bmod p$$

G) The point of infinity is important to satisfy the "identity" property of elliptic curves, given elliptic curves under modulus form a group, and groups must satisfy the "identity" property. More specifically, the point of infinity acts as the point O (zero), which allows for the elliptic curve addition example P (some point) $\oplus$ $O = P$. Without point of infinity, elliptic curve arithmetic is not mathematically consistent.

Problem 3 :

a) Find sqrts of 400 (mod 19) :

(1) Check proposition 2.26 (Hoffstein) :

$400 \bmod 19 \equiv 1 \bmod 19 \not\equiv 3 \bmod 4$

(2) Use brute force method to find sqrts:

$1^2 = 1 \bmod 19$ -> yes
$2^2 = 4 \bmod 19$
$3^2 = 9 \bmod 19$
$4^2 = 16 \bmod 19$
$5^2 = 25 = 6 \bmod 19$
$6^2 = 36 = 17 \bmod 19$
$7^2 = 49 = 11 \bmod 19$
$8^2 = 64 = 7 \bmod 19$
$9^2 = 81 = 5 \bmod 19$
$10^2 = 100 = 5 \bmod 19$
$11^2 = 121 = 7 \bmod 19$
$12^2 = 144 = 11 \bmod 19$
$13^2 = 169 = 17 \bmod 19$
$14^2 = 196 = 6 \bmod 19$
$15^2 = 225 = 16 \bmod 19$
$16^2 = 256 = 9 \bmod 19$
$17^2 = 289 = 4 \bmod 19$
$18^2 = 324 = 1 \bmod 19$ -> yes

Answer: Sqrts are
$1 \bmod 19$
$18 \bmod 19$
or
$\pm 1 \bmod 19$

b) Find sqrts 400 mod 23

(1) Check Proposition 2.26 (Hoffstein):

$400 \bmod 23 \equiv 9 \bmod 23$

$23 \equiv 3 \bmod 4$ (yes)

(2) Find sqrts using equation:

$b = a^{(p+1)/4} \bmod p$

$b = 9^{(23+1)/4} \bmod 23$

$b = 9^{6} \bmod 23$

$b = \pm 3 \bmod 23$

used wolfram for calculation

Answer: Sqrts are

$3 \bmod 23$

$20 \bmod 23$

or

$\pm 3 \bmod 23$

c) Find first root:

① From 3a, 3b, we have equations:

$\pm 1 \bmod 19$; $\pm 3 \bmod 23$

combinations: $1 \bmod 19$, $3 \bmod 23$

$1 \bmod 19$, $-3 \bmod 23$

$-1 \bmod 19$, $3 \bmod 23$

$-1 \bmod 19$, $-3 \bmod 23$

② Select one combination and use CRT to find root:

$x \equiv 1 \bmod 19$

$x \equiv 3 \bmod 23$

③ Equation:

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$$

$\underset{a_1}{1} \bmod \underset{m_1}{19}$; $\underset{a_2}{3} \bmod \underset{m_2}{23}$

$M = m_1 \cdot m_2$; $M_1 = \frac{M}{m_1}$; $M_2 = \frac{M}{m_2}$

(next page)

(4) $M = m_1 \cdot m_2$

$M = 19 \cdot 23$

$M = 437$

(5) $M_1 = \frac{M}{m_1} = \frac{437}{19} = 23$

$M_2 = \frac{M}{m_2} = \frac{437}{23} = 19$

(6) $M_1^{-1} = M_1 \cdot M_1^{-1} \equiv 1 \bmod m_1$

$= 23 \cdot M_1^{-1} \equiv 1 \bmod 19$

$23x + 19y = 1$

$23 = 19(1) + 4$

$19 = 4(4) + 3$

$4 = 3(1) + 1$

$3 = 1(3) + 0$

$1 = 4 + 3(-1)$

$1 = (23 + 19(-1)) + (19 + 4(-4))(-1)$

$1 = 23 + 19(-1) + 19(-1) + 4(4)$

$1 = 23 + 19(-2) + (23 + 19(-1))(4)$

$1 = 23 + 19(-2) + 23(4) + 19(-4)$

$1 = 23(5) + 19(-6)$

(next page)

$1 = 23(5) + 19(-6)$

$M_1^{-1} = 5$

$M_2^{-1} = -6$

7 solve with input:

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$

$x = (1 \cdot 23 \cdot 5 + 3 \cdot 19 \cdot (-6)) \bmod 437$

$x = (115 + (-342)) \bmod 437$

$x = (-227) \bmod 437$

$\underline{\underline{x = 210}}$

$\boxed{\text{Answer: A root is } 210 \bmod 437}$

$210 \equiv 1 \bmod 19$ ✓

$210 \equiv 3 \bmod 23$ ✓

D) Find second root :

① Select one combination and use CRT to find root :

$x \equiv 1 \mod 19$

$x \equiv -3 \mod 23 \equiv 20 \mod 23$

② Equation :

$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \mod M$

$\underset{a_1}{1} \mod \underset{m_1}{19}$; $\underset{a_2}{20} \mod \underset{m_2}{23}$

$M = m_1 \cdot m_2$; $M_1 = \frac{M}{m_1}$; $M_2 = \frac{M}{m_2}$

③ $M = m_1 \cdot m_2$

$M = 19 \cdot 23$

$M = \underline{\underline{437}}$

④ $M_1 = \frac{M}{m_1} = \frac{437}{19} = \underline{\underline{23}}$

$M_2 = \frac{M}{m_2} = \frac{437}{23} = \underline{\underline{19}}$

⑤ $M_1^{-1} = M_1 \cdot M_1^{-1} \equiv 1 \bmod m_1$

$= 23 \cdot M_1^{-1} \equiv 1 \bmod 19$

$23x + 19y = 1$

$23 = 19(1) + 4$
$19 = 4(4) + 3$
$4 = 3(1) + 1$
$3 = 1(3) + 0$

$1 = 4 + 3(-1)$
$1 = (23 + 19(-1)) + (19 + 4(-4))(-1)$
$1 = 23 + 19(-1) + 19(-1) + 4(4)$
$1 = 23 + 19(-2) + (23 + 19(-1))(4)$
$1 = 23 + 19(-2) + 23(4) + 19(-4)$
$1 = 23(5) + 19(-6)$

$M_1^{-1} = 5$

$M_2^{-1} = -6$

⑥ $x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$

$x = (1 \cdot 23 \cdot 5 + 20 \cdot 19 \cdot (-6)) \bmod 437$

$x = (115 + (-2280)) \bmod 437$

$x = (-2165) \bmod 437$

$x = \underline{\underline{20}}$

$\boxed{\text{Answer: Another root is } 20 \bmod 437}$

Problem 4:

a) Discrete logarithm problem

$$g^x \equiv a \mod p$$

$$\boxed{5^x \equiv 1 \mod 10223}$$

b) 317 is not a generator mod 10223 because when taking 317 to every power up to modulus 10223 (i.e. $317^1, 317^2, 317^3$, etc.) it does not produce unique values between 1 - 10223. It contains repeating # or does not contain full set.

c) Discrete log base 5 of 3529

$$\log_5 3529 = x$$

$$\left.\begin{aligned} &\rightarrow 5^x = 3529 \\ &\rightarrow x = 5.075542\ldots \end{aligned}\right\} \text{used wolfram}$$