



1. Does the elliptic curve $y^2 \equiv x^3 + 2x + 5 \pmod{7}$ is non-singular? Justify your answer.
2. Let E be an elliptic curve $y^2 \equiv x^3 + 3x + 2 \pmod{7}$.
 - a. Compute all points on E over Z_7
 - b. $|E|$
 - c. Given the element $P = (1, 2)$, determine the order of P . Is P a primitive element? Justify your answer.
3. Given the elliptic curve $y^2 \equiv x^3 + x + 2 \pmod{3}$ with the points:

$$\{(1, \pm 1), (2, 0), \varphi\}$$

Verify that $G = (1, 2)$ is a generator point. Justify your answer.

4. Given the elliptic curve $y^2 \equiv x^3 + x + 1 \pmod{5}$.

Compute the following operations :

- a. Compute all points on E
 - b. if $P = (0, 4)$ and $Q = (4, 3)$, calculate $P + Q$.
 - c. Calculate $2P$.
 - d. If $R = (2, -1)$, find $-R$.
5. Compute a session key between two entities Alice and Bob, in a ECDH protocol. Your secret value is $a = 5$. You receive from Bob $B = (3, 2)$. The elliptic curve being used is defined by

$$y^2 \equiv x^3 + x + 4 \pmod{5}$$

6. Consider the public key $K_{pb} = (p, a, b, q, A, B) = (7, 1, 1, 5, (2, 5), (0, 6))$ for ECDSA, if $h(x) = 4$, verify the signature $(r, s) = (0, 3)$.
7. Consider ECDSA, show why the signature (r, s) satisfies the condition $r = x_p \pmod{q}$ where x_p is the x coordinate of $P = u_1A + u_2B$, A is generator and B is the public key.



8. What is the purpose of RSA-PSS? Please list the differences between schoolbook RSA and RSA-PSS?
9. Considering EdDSA answer the following questions:
 - a. Which cryptographic service provide EdDSA?
 - b. Why is this cryptographic algorithm secure? Please describe the intractable mathematical problem that provide security to EdDSA.
 - c. List the differences between the parameters (elliptic curve, finite field, etc.) used for ECDSA and the parameters used for EdDSA.
10. Answer the following questions about AES-GCM:
 - a. List the cryptographic services provided by this combination of block cipher and mode of operation. Explain what operations provide each cryptographic service.
 - b. What is the finite field used in AES-GCM?
 - c. Draw a diagram to show how AES-GCM do deciphering and verification.
11. The protocol TLS 1.3 provides security over a computer network. To do this it uses several cryptographic algorithms.
 - a. List the cryptographic algorithms used in this protocol to provide integrity.
 - b. Why TLS 1.3 provide perfect forward secrecy (PFS)? Which cryptographic mechanism provide PFS and why?
 - c. Which cryptographic algorithms are used for key exchange in TLS 1.3?
 - d. What would happen if we do not use digital certificates in TLS?
 - e. What is the purpose of a certificate authority?