Due Aug 25, 2025

MATH 173B: Cryptology II
Homework 3: Encryption Algorithms on EC

Instructions: I appreciate clarity and rigorous logic. Show all your work to receive full credit. Write your answers clearly and justify each step. If you use Python, attach **PEP 8–compliant code** with **clear comments**.

1 EC Diffie-Hellman (40 pts)

Alice and Bob agree to use elliptic Diffie–Hellman key exchange with prime, curve, and base point

$$p = 2671, \qquad E:\ Y^2 = X^3 + 171X + 853, \qquad P = (1980, 431) \in E(\mathbb{F}_{2671}).$$

1. Alice sends Bob the point $Q_A = (2110, 543)$. Bob uses the secret multiplier $n_B = 1943$. What point should Bob send to Alice?
2. What is their secret shared value?
3. How difficult is it for Eve to figure out Alice's secret multiplier n_A? How many steps of calculation would it require?
4. Alice and Bob decide to exchange a new piece of secret information using the same p, E, and P. This time Alice sends only the x-coordinate $x_A = 2$ of her point Q_A. Bob uses the secret multiplier $n_B = 875$. What single number modulo p should Bob send to Alice, and what is their secret shared value?

2 Elliptic Curve ElGamal (20 pts)

Assume Alice wants to turn the previous elliptic curve into an ElGamal scheme. She will use the number n_A as her secret number.

1. What is the public key?
2. What is the private key?
3. Suppose Bob intends to send a message m to Alice. Bob chooses his secret number n_B (i.e. Bob's random number used in encryption is n_B). If Eve can solve the Elliptic Curve Diffie–Hellman problem, can she retrieve the secret message m? If so, explain how Eve can compute m. If not, point out which value/points is hard to compute for Eve.

3 ECDSA (30 pts)

$$E:\ y^2 = x^3 + 231x + 473, \qquad p = 17389, \qquad q = 1321, \qquad G = (11259, 11278) \in E(\mathbb{F}_p).$$

Verify that G has order q. Then answer:

1. With private key $s = 542$, find the signer Samantha's public key and her signature on $d = 644$ using $e = 847$.
2. With public key $V = (11017, 14637)$, is $(s_1, s_2) = (907, 296)$ a valid signature on $d = 993$?
3. With public key $V = (14594, 308)$, find Umberto's private key and forge a signature on $d = 516$ using $e = 365$.

4 Lattice (10pts)

State the definition of a lattice in $\mathbb{R}^n$ correctly and precisely.