1. Consider the elliptic curve $y^2 \equiv x^3 + 4x + 4 \pmod{11}$.
   a. Add the points $(1, 3) + (2, 3)$.
   b. Add the points $(1, 8) + (2, 3)$.
   c. Double the point $(1, 3)$.
   d. Find the order of the point $(1, 8)$.
   e. Find the number of points on the elliptic curve.
   
   Be sure to check that the given points and your answers all lie on the curve.

2. Use Shanks’ baby-step-giant-step method to solve the discrete logarithm problem $2^x \equiv 82 \pmod{107}$.

3. Alice and Bob use the Massey-Omura cipher with common modulus $p = 2591$. Alice’s secret enciphering exponent is $e_A = 107$; Bob’s is $e_B = 257$. Compute the deciphering exponents and show the numbers passed between them when Alice sends Bob the plaintext $M = 1234$.

4. Alice and Bob use the elliptic curve Massey-Omura cipher with the elliptic curve $y^2 \equiv x^3 + 1441x + 611 \pmod{2591}$. Alice’s secret enciphering multiplier is $e_A = 107$; Bob’s is $e_B = 257$.
   a. Find the number of points on the elliptic curve.
   b. Compute the deciphering multipliers $d_A$ and $d_B$.
   c. Show the numbers in the messages passed between them when Alice sends Bob the plaintext $P = (1619, 2103)$.

5. Alice and Bob use the elliptic curve ElGamal public key cipher for their secret communication. One day, Bob tosses a coin and sends Alice the enciphered result. Knowing only public data and that the plaintext is either “Heads” or “Tails,” can Eve the Eavesdropper tell which plaintext it is from the ciphertext she has intercepted?

6. Alice and Bob use the elliptic curve Diffie-Hellman key exchange protocol to choose random AES keys. The elliptic curve group is public and has order $N$ near $2^{160}$. Because of a defect in her random number generator, the low-order 100 bits of Alice’s random $x_A$ are always one, but the high-order 60 bits are really random. Eve is aware of this defect because she has studied the source code of Alice’s random number generator. Eve records all messages passing between Alice and Bob. Eve has a computer powerful enough to perform about $2^{80}$ elliptic curve group additions in a reasonable time. Explain how Eve can compute, with high probability, the AES keys chosen by Alice and Bob. (Eve knows which bits of the point Alice and Bob use for the AES key.)