HOMEWORK

For this week, please answer the following questions from the text. I've copied the problem itself below and the question numbers for your convenience.

(1) (6.14) Alice and Bob agree to use elliptic curve Diffie-Hellman key exchange with the prime, elliptic curve, and point

$$p = 2671,\ E : y^2 = x^3 + 171x + 853,\ P = (1980, 431) \in E(\mathbb{F}_p)$$

  (a) Alice sends Bob the point $Q_A = (2110, 543)$. Bob decides to use the secret multiplier $n_B = 1943$. What point should Bob send to Alice?
  (b) What is their secret shared value?
  (c) How difficult is it for Eve to figure out Alice's secret multiplier n_A? Use a computer to find n_A.
  (d) Alice and Bob decide to exchange a new piece of secret information using the same prime, curve, and point. This time Alice sends Bob only the x- coordinate $x_A = 2$ of her point Q_A. Bob decides to use the secret multiplier $n_B = 875$. What single number modulo p should Bob send to Alice, and what is their shared secret value?

(2) (6.17) The Menezes-Vanstone variant of the ellipic Elgamal public key cryptosystem improves the message expansion while avoiding the difficulty of directly attaching plaintext to points in $E(\mathbb{F}_p)$. The MV-Elgamal cryptosystem is described in Figure 1.
  (a) The last line of the table claims that $m_1' = m_1$ and $m_2' = m_2$. Prove that this is true, so the decryption process does work.
  (b) What is the message expansion of MV-Elgamal?
  (c) Alice and Bob agree to use

$$p = 1201,\ E : y^2 = x^3 + 19x + 17,\ P = (278, 285) \in E(\mathbb{F}_p)$$

  for MV-Elgamal. Alice's secret value is $n_A = 595$. What is her public key? Bob sends Alice the encrypted message $((1147, 640), 279, 1189)$. What is the plaintext?

(3) (6.20) This exercise asks you to compute some numerical instances of the elliptic curve digital signature algorithm described in Table 6.7 for the public parameters

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

You should begin by verifying that G is a point of order q in $E(\mathbb{F}_q)$.
  (a) Samantha's private signing key is $s = 542$. What is her public verification key? What is her digital signature on the document $d = 644$ using the random element $e = 847$?
  (b) Tabitha's public verification key is $V = (11017, 14637)$. Is $(s_1, s_2) = (907, 296)$ a valid signature on the document $d = 993$?
  (c) Umberto's public verification key is $V = (14594, 308)$. Use any method you want to find Umberto's private signing key, and then use the private key to forge his signature on the document $d = 516$ using the random element $e = 365$.

FIGURE 1. MV-Elgamal

Public Parameter Creation	
A trusted party chooses and publishes a (large) prime p, an elliptic curve E over $\mathbb{F}_p$, and a point P in $E(\mathbb{F}_p)$.	
Alice	**Bob**
Key Creation	
Chooses a secret multiplier n_A. Computes $Q_A = n_A P$. Publishes the public key Q_A.	
Encryption	
	Chooses plaintext values m_1 and m_2 modulo p. Chooses a random number k. Computes $R = kP$. Computes $S = kQ_A$ and writes it as $S = (x_S, y_S)$. Sets $c_1 \equiv x_S m_1 \pmod{p}$ and $c_2 \equiv y_S m_2 \pmod{p}$. Sends ciphertext (R, c_1, c_2) to Alice.
Decryption	
Computes $T = n_A R$ and writes it as $T = (x_T, y_T)$. Sets $m_1' \equiv x_T^{-1} c_1 \pmod{p}$ and $m_2' \equiv y_T^{-1} c_2 \pmod{p}$. Then $m_1' = m_1$ and $m_2' = m_2$.	

Table 6.13: Menezes–Vanstone variant of Elgamal (Exercises 6.17, 6.18)