EECE 455/632 – Cryptography and Network Security

Assignment

CHAPTER 10

Question #1

Alice and Bob use the Diffie-Hellman key exchange technique with a common prime: $q = 23$ and a primitive root $a = 5$.

a) If Bob has a public key $Y_B = 10$, what is Bob's private key X_B?

b) If Alice has a public key $Y_A = 8$, what is the shared key K with Bob?

c) Show that 5 is a primitive root of 23.

Question #2

Consider ElGamal scheme with a common prime $q = 71$ and a primitive root $\alpha = 7$.

a. If B has public key $Y_B = 3$ and A chose the random integer $k = 2$, what is the ciphertext of $M = 30$?

b. If A now chooses a different value of k so that the encoding of $M = 30$ is $C = (59, C_2)$, what is the integer C_2?

Question #3

Consider the elliptic curve $E_7(2,1)$; that is, the curve is defined by y2 = x 3 + 2 x + 1, with a modulus of $p = 7$. Determine all the points in $E_7(2, 1)$.

Question #4

The cryptosystem parameters of ECC scheme are E11(1, 6) and G = (2, 7). B's secret key is $n_B = 3$.

a. Find B's public key P_B.

b. A wishes to encrypt the message $P_m = (10, 9)$ and choose a random value $k = 4$. Determine the ciphertext Cm.

c. Show how to recover P_m from C_m.