UEE4611 Assignment #8, 2020 due June 9

---

1. Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q = 23$ and a primitive root $\alpha = 5$.
   (a) If Bob has a public key $Y_B = 10$, what is Bob's private key X_B? (5%)
   (b) If Alice has a public key $Y_A = 8$, what is the shared key K with Bob? (5%)
   (c) Show that 5 is a primitive root of 23. (5%)
2. Suppose Alice and Bob use an Elgamal scheme with a common prime $q = 157$ and a primitive root $\alpha = 5$.
   (a) If Bob has public key $Y_B = 10$ and Alice chose the random integer $k = 3$, what is the ciphertext of $M = 9$? (5%)
   (b) If Alice now chooses a different value of k so that the encoding of $M = 9$ is $C = (25, C_2)$, what is the integer C_2? (5%)
3. Given 5 as a primitive root of 23, solve the following congruence:
$$7x^{10} + 1 \equiv 0 \pmod{23}.$$
   (10%)
4. This problem performs elliptic curve encryption/decryption using the scheme outlined in Section 10.4. The cryptosystem parameters are $E_{11}(1, 7)$ and $G = (3, 2)$. B's private key is $n_B = 7$.
   (a) Find B's public key P_B. (5%)
   (b) A wishes to encrypt the message $P_m = (10, 7)$ and chooses the random value $k = 5$. Determine the ciphertext C_m. (5%)
   (c) Show the calculation by which B recovers P_m from C_m. (5%)