Assignment 3

Deadline 30th May

1. Check whether 5 is primitive root of 23 or not. Justify with the reason.
2. Encrypt the text ‘2’ using RSA algorithm with p=3 q=11 and also decrypt the resulting cipher.
3. Callie wants to send the message M = 13 to Alice. Using Alice’s public and private keys, calculate the ciphertext C, and the value for R when Alice recovers the message.
4. Dexter wants to set up his own public and private keys. He chooses p = 23 and q = 19 with e = 283. Find d so that ed has a remainder of 1 when divided by (p − 1)(q − 1).
5. For given p=11, g=2, x_A = 9, x_B = 4. Find the session key by Diffie Helman Algorithm.
6. Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. What will be their common session key.
7. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice’s secret key is 4 and Bob’s secret key is 6, what is the secret key they exchanged?
8. Alice uses the prime p = 467 and the primitive root g = 2. She chooses a = 153 to be her private key .Compute A’s public key. Bob decides to send Alice the message m = 331. He chooses an ephemeral key at random, say he chooses k = 197. Find ciphertext pair (c1, c2). Finally decrypt the cipher text.(use ElGamal public key cryptosystem).