Tutorial

Day 3

Practice Problems:

1. What is the cipher message if the plain text is encrypt using ceaser cipher: a. Alice b. Hacker c. transformation
2. What is the cipher text if the plain text is shifted the letters of the message by obtaining 8 places down:

   a. National Institute Of Technology b. Silchar

3. Given two prime numbers P =7, Q = 17 , find out N, E and D in an RSA encryption process. Assume Plain text as 10
4. Given two prime numbers P =3, Q = 11 , find out N, E and D in an RSA encryption process. Assume original message as 31
5. In RSA , given N= 187 and the encryption key (E) as 17, find out the corresponding private key (D). Let M = 5
6. Consider a plain text(G) CSE (ASCII code 67, 83. 69). Using the RSA algorithm and the values as E = 3 , D = 11 and N = 15, find out what this plain text alphabet encrypts to and verify that upon decryption, it transform back to G

7. Alice and Bob want to establish a secret key using the Diffie-hellman key exchange protocol. Assuming the values as n= 11, g = 7, x = 3 and y = 6, Find out the values of A, B and the secret key (k_1 or k_2)

8. 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 D-H key ?

9. 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?