1. Explain RSA algorithm, perform encryption and decryption to the system with p=7, q=11, e=17, M=8.

2. Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root a=7. If user A has private key XA=5, what is A’s public key YA?

3. Alice wants to generate a pair of RSA public and private keys. She starts by selecting two primes p = 5 and q = 7.

(a) Compute n, 1(n)?

(b) In selecting a decryption (private) key d, Alice decides d = 3 is not good. Why? She selects d = 11 instead. Which is correct encryption (public) key, e1 = 11 or e2 = 13?

(c) Suppose Bob wants to send a message M = 33 to Alice, Which key should he use? What’s the cipher text he sends to Alice?

(d) After Alice receives the cipher text, how does she decrypt?

(e) If Alice wants to send B a signed message, given M’ = 6, what would Alice send?

(f) How does Bob verify the message sent by Alice?

4. State Chinese Remainder theorem and find X for the given set of congruent equations

Using CRT.

X = 2(mod 3)

X = 3(mod 5)

X = 2(mod 7).

5. State Chinese Remainder theorem and find X for the given set of congruent equations

Using CRT.

X = 1(mod 5)

X = 2(mod 7)

X = 3(mod 9)

X = 4(mod 11)

6. Perform encryption and decryption using RSA algorithm for the following:

p = 7, q = 11, e = 7, M = 9

7. Perform encryption/decryption using RSA algorithm for the following:

p=3, q=11, e=7, m=5

8. Explain the RSA algorithm in detail. For the given values, trace the sequence of calculation in

RSA. p=7, q=13, e= 5 and m=10.

9. Perform encryption and decryption using RSA algorithm for

p = 17, q = 11, e = 7 and M = 88

10. Explain RSA algorithm, perform encryption and decryption to the system with

p = 7; q = 11; e = 17; M= 8.

11. Users A and B use the Diffie Hellman key exchange technique a common prime q=11 and a primitive root alpha=7**.**

(i) If user A has private key XA =3 what is A’s public key YA?

(ii) If user B has private key XB =6 what is B’s public key YB?

12.User A & B use the Diffie-Hellman key exchange algorithm with a common prime q=71, and a primitive root a=7. If user A has a private key Xa =5. What is A’s public key Ya

13. Users Alice and Bob use the Diffie Hellman key exchange technique a common prime q=83 and a primitive root alpha=5**.**

(i) If Alice has private key XA =6 what is Alice’s public key YA?

(ii) If Bob has private key XB =10 what is Bob’s public key YB?

(iii) What is the shared secret key?

13. Find the secret key shared between user A and user B using Diffie Hellman algorithm for the following:

q = 353; α (primitive root) = 3, XA = 45 and XB = 50