Assignment IV - B.Tech VIth*Semester*

Cryptography

last date for submission - will be announced in class

five students can submit one assignment

1. (i) Prove formally that hardness of CDH problem relative to cyclic group G implies hardness of discrete logarithm problem relative to G.
   (ii) Prove formally that hardness of DDH problem relative to G implies hardness of CDH problem relative to G.

2. Prove that text-ElGamal is not semantically secure (IND-CPA).

3. Prove that modified ElGamal is semantically secure (IND-CPA) if the DDH assumption holds. But modified ElGamal is not IND-CCA secure.

4. Explain RSA signature scheme. In RSA digital signature,suppose signatures of Alice for the messages 5 and 9 are respectively 6 and 24. Given the public keys, can you find the signature of Alice for message 405. Explain.

5. Define existential forgery. Show that RSA signature scheme is vulnerable for existential forgery under known message attack.Write two method to prevent existential forgery.

6. Define selective forgery. Show that RSA signature scheme is vulnerable for selective forgery under chosen message attack.

7. Suppose Alice wants to sign a message x. She first constructs the message digest z = h(x), and then computes the signature on z,namely, $y = sig_K(z)$. Then she transmits the ordered pair(x,y) over the channel.Suppose hash function is not secondary image resistant.Then show that Adversary can make selective forgery using chosen message attack.

8. Suppose Alice wants to sign a message x. She first constructs the message digest z = h(x),and then computes the signature on z,namely, $y = sig_K(z)$. Then she transmits the ordered pair(x,y) over the channel. Suppose hash function is not secondary image resistant. Then show that Adversary can make existential forgery using known message attack.

9. Suppose Alice wants to sign a message x. She first constructs the message digest z = h(x), and then computes the signature on z,namely, $y = sig_K(z)$. Then she transmits the ordered pair(x,y) over the channel. Suppose hash function is not collision resistant. Then show that Adversary can make existential forgery using chosen message attack.

10. Suppose RSA is (t', ϵ')-secure. Assume that challenge to the adversary is to make forgery on message M_c(Declared Message) in Full Domain Hash signature scheme. Then the Full Domain Hash signature scheme is (t, ϵ)-secure where
$t = t' - (q_{hash} + q_{sig} + 1)O(k^3)$
$\epsilon = \epsilon'$.

11. Show that the ElGamal signature scheme is existentially forgeable.

12. Show that Schnore Signature Algorithm is existentially unforgeable under known message attack.

13. Users Alice and Bob use the Diffie-Hellman key exchange protocol with common prime p = 23 and a primitive root g = 7. Alice has private key 3 and Bob has private key 5. Find the shared symmetric key. Can you make man in middle attack on Diffie- Hellman key exchange protocol with one private key and the corresponding public key.