Principles of Information Security

Assignment- 4

1. Suppose there is only one public channel between Alice and Bob and it has been given that no "active" adversary (there may be passive adversaries) is "active" over this channel. Alice want to send a message securely to Bob at time t So that Bob can get the message content after time t + t_1 where t_1 can be significantly large. Assuming that the channel have no transmission delay, Can you give a simple protocol for a successful communication between Alice and bob using the concepts of Private and Public key cryptography. If the adversary were active, can you tell that an active adversary is available, provided some message disruption have been made?

2. Group Theory

   (a) What do you understand by order of a group? Suppose, G is a multiplicative group of order n and g ϵ G. Then Prove that order of g devides n.

   (b) What do you understand by cyclic group. Suppose p is a prime then prove that Z_p^* is a cyclic group where Z_p^* is the set $Z_p - \{0\}$.

   (c) Explain Isomorphism, Homomorphism and Direct Product in the context of group?

3. (a) Using Extended Euclid Algorithms, Compute the following.
      i. 17^{-1} mod 101.
      ii. 357^{-1} mod 1234.
      iii. 3125^{-1} mod 9987.

   (b) Solve these relations.

   - x $\equiv$ 12 mod (25)
     x $\equiv$ 9 mod (26)
     x $\equiv$ 23 mod (27)

   - 13x $\equiv$ 4 mod (99)
     15x $\equiv$ 56 mod (101)

4. Primality Testing

   (a) Explain Solovay Strassen Primality Test Algorithm.

   (b) Explain Miller-Robin Primality Test Algorithm. How it is different from the Solovay Strassen Primality test Algorithm?

   (c) Assume that you have a computer performing 1 million bit operations per second. You want to spend only 2 hours on primality testing. What is larger number you can test using the following primality testing methods?

i. Trivial division method
ii. AKS algorithm
iii. Miller-Robin test

5. RSA

   (a) Suppose n= 84773093. The adversary somehow has learned the value of $\phi(n) =$ 84754668. Explain How can he learn the two factors p and q ? Here, Is there any need to learn the values of p and q if adversary only want to decrypt the message encrypted by and arbitrary e (co- prime to $\phi(n)$) and n?

   (b) Consider the RSA cryptosystem and an encryption exponent e =3. show that plaintext message m can be recovered if it is enciphered (encrypted) and sent to three different entities having the pairwise relatively prime moduli n_1, n_2, n_3.

6. Users A and B use the Diffie-Hellman key exchange techniques with a common prime q = 71 and a primitive root $\alpha = 7$.

   (a) If the user A has private key $X_A = 69$, what is the As public key Y_A ?

   (b) If the user B has private key $X_B = 15$, what is the Bs public key Y_B ?

   (c) What is the shared secret key between A and B?

7. It is well known that there is an active attack on the Diffie-Hellman Key exchange Techniques which is known as the "Man in the Middle attack"? Explain this attack in detail. The station to station key agreement method on the Diffie-Hellman uses authentication to thwart this serious attack. Explain this method.

8. Let G be a finite cyclic group (e.g. G=Z_p) with generator g. Suppose the Diffie-Hellman function $DH_g(g^x, g^y) = g^{\{xy\}}$ is difficult to compute in G. Which of the following functions is also difficult to compute: As usual, identify the f below for which the contra-positive holds: if f(,) is easy to compute then so is $DH_g(,)$. If you can show that then it will follow that if DH_g is hard to compute in G then so must be f.

   (a) $f(g^x, g^y)=(g^2)^{\{x+y\}}$

   (b) $f(g^x, g^y)=g^{\{xy\}^{0.5}}$

   (c) $f(g^x, g^y)=(g^{0.5})^{\{x+y\}}$

   (d) $f(g^x, g^y)=g^{\{xy+x+y+1\}}$

9. (a) Explain The ElGamal scheme in detail. Consider an ElGamal scheme with a common prime number q = 71 and a primitive root $\alpha = 7$. If the recipient B has the public key $Y_B = 3$ and the sender A chooses the random integer $X_A =$ 2, what is the ciphertext of the plaintext message M = 30?

   (b) What is the discrete logrithm of a prime number p.Define formally the elliptic curve discrete logrithm problem (ECDLP) with the adversary A's advantage.

10. Let two parties A and B agree on the following digital signature scheme. Entity A signs a binary message m of arbitrary length. Entity B can verify this signature by using the public key of A.
Entity A perform the following step for key generation:

    (a) select two prime p and q such that q | (p-1).

    (b) select random integer g with 1< g <p-1, such that $\alpha = g^{\{(p-1)/q\}} (\text{mod p})$ and $\alpha > 1$.

    (c) Select a private key a (integer), 0 < a < q.

    (d) Compute y = α^a (mod p).

    Public key of A is (p, q, α, y).
    After key generation, A generates a signature on m as follows:

    (a) Select a random secret integer k, 1 < k < q.

    (b) Compute r = α^k mod p, e = H(m‖r), and s = (ae + k) mod q.

    (c) Select two random secret integers u and v, 0 < u < q and 0 <v < q, and compute r' =r$\alpha^{-u} y^v$ mod p.

    (d) Compute e' = H(m‖r') such that e'= e-v and s'= s-u. A then sends the signed message (m,(e',s')) to the verifier B. Here H is a hash function.

    Devise a verification algorithm for the party B.Prove the verification equation mathematically.