NSS Homework - 1

Kaustav Vats (2016048)

Question 1

Describe how DHK Exchange can work for more than two parties?

Diffie-Hellman Algorithm is usually used for exchanging key between two peoples. Any number of users can use Diffie-Hellman Algorithm to exchange keys. Let say there are 3 users, A, B, C.

1. All group members agree on the Prime P, and G
2. All group members generate there private keys a, b and c
3. Let say a user A computes $\mathbf{G^a}$ and sends it to another user B.
4. Now B computes $\mathbf{G^{ab}}$ and sends it to user C.
5. Now C computes $\mathbf{G^{abc}}$ and used it as a secret key for encrypting and decrypting messages.
6. Now B computes $\mathbf{G^b}$ and sends it to user C
7. C computes $\mathbf{G^{bc}}$ and sends it to user A
8. Now user A computes $\mathbf{G^{bca}}$ and used it as a secret key for communication.
9. Now C computes $\mathbf{G^c}$ and sends it to user A
10. A computes $\mathbf{G^{ca}}$ and sends it to user B
11. Now user B computes $\mathbf{G^{cab}}$ and used it as a secret key for communication.

Note-

1. All users have computed the same secret key
2. $G^{abc} = G^{bca} = G^{cab}$
3. Eavesdropper won't be able to generate key using available values like, G^a, G^b, G^c, G^{ab}, G^{bc}, G^{ca}

This can be further extended to be used for N users in a group.

- Main idea is that everyone knows P and Q. Now each user need to compute the secret key. The secret is raised to power of every user private key and final raised power is further raised by user private key to compute secret key. Order of raise doesn’t matter.

- This problem can be further simplified by visualizing that keys are rotated clockwise in a circle.

Question 2

MITM attacks are possible in above algorithm. It depends on the strength of the numbers chosen and also on the number of group members.

- If P and Q are not large prime factor
- If Group size is small
- If generated keys of all user are not random
- Discrete logarithm algorithm can be used to generate private keys of each user making whole system insecure
- Since there’s not authentication method in Diffie-Hellman Algorithm, then it's possible that attacker is sitting in between and exchanging his own keys and computed numbers with users. Basically spoofing identity.
  Ex - Users A and B, Attacker T
  A<-------------------->T<------------------>B
  In the above step, both parties won’t know that key they are receiving is from the actual user or not

To prevent MITM attacks

- P and Q used should be large prime factor
- Group size should be large (Makes more difficult for attacker to compute keys)
- Private keys generated by each user should be large random numbers.
- One way is to have a public and private key pair for each user. Where public key would be known to everyone. Lets say there are user A and B. User(A) can first encrypt message with other users(B) public key then send the encrypted text. The Receiving user(B) can Decrypt and

check the message. (Note- Data encrypted with public key can only be seen by decrypting with private keys). But authentication is again not ensured, so a user(A) can also sign the encrypted text with his own private key and receiver can validate using A's public key. This ensures that document that is received by the user B was actually send by the user A. This further ensures that MITM attacks won't be possible if using Public private key pair.

- One more way is to compare hash. Each user will have a Key and IV which is common and shared by completely secure method(Offline or online). Now while sending encrypted text to another user, let say A is sending encrypted text to user B. Then A can generate Hash of encrypted text using and attach it with the message. Whereas user B can also generate hash of received encrypted text and compare both the hash. If same then it means that document was sent by the actual user A.