Feedback on Topic 8 Ex

Exercise Question – E8.1

Assuming that Alice is to send a message, *M*, to Bob. *M* is encrypted with a shared key established using the DH protocol. Explain whether Eve could access this message *M.* If so, explain how, and propose a solution to address this vulnerability.

Exercise Question – E8.1 – A(1)

How:

This is an active attack. The attacker intercepts and substitutes Ya and Yb with Ye. So at the end of the message exchanges, Eve will have Kae, Kbe, Alice will have Kae and Bob will have Kbe. Any messages encrypted with Kae will be decrypted and read by Eve and then re-encrypted with Kbe and vice versa without the knowledge of Alice and Bob.

Exercise Question – E8.1 – A(2)

There are two solutions as detailed below:

(1) Fixed DH

Server’s and client’s public key certificates contain their respective DH public key parameters. In other words, the DH public keys are certified by a CA. But there has to be a way that Alice and Bob could prove to each other that they are the rightful owners of the corresponding certificates (unless the identity of one entity is already known to the other). With this method, the established symmetric key is not really a session-valid key. So the security level is not as high as the second method.

Exercise Question – E8.1 – A(3)

(2) Ephemeral DH

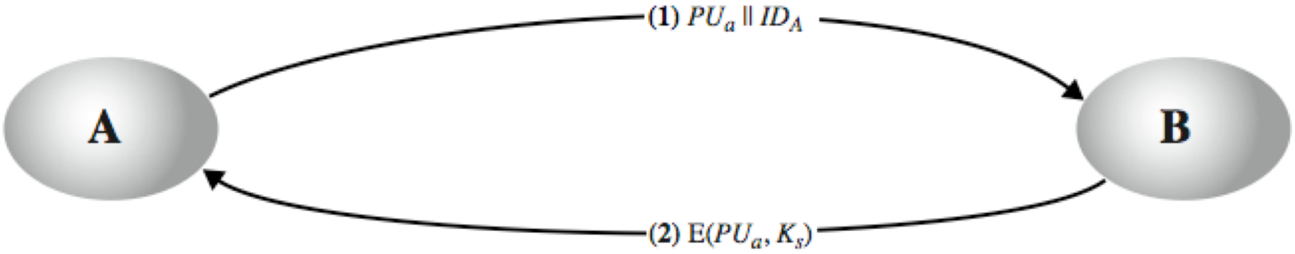
DH public keys are exchanged, signed using the sender’s private DSA key; the receiver uses the corresponding public keys (certified in the certificates) to verify the signatures. The certificates are used to certify the DSA keys, and DH shares are signed using DSA by the respective signers. This is the so called DH-DSA method, used to create a temporary, one-time session key.

Exercise Question – E8.2

The following is an extremely simple protocol proposed for symmetric key distribution. It is assumed that A and B has never met before (or there is no key established prior to this communication).

i. Identify as many problems/flaws as you can.

ii. Modify the protocol to fix the problems/flaws you have identified.



Exercise Question – E8.2(i) - A

- This simply protocol does not provide mutual authentication: it does not show that the public key has been certified and that the demonstration of private key associated to the public key in the certificate is missing.

Eve can intercept the message, creates its own public/private key pair {PUe, PRe} and transmits PUe||IDA to Bob.

Bob generates a secret key, Ks, and transmits E(PUe, Ks).

Eve intercepts the message and learns Ks by computing D(PRe, E(PUe, Ks)).

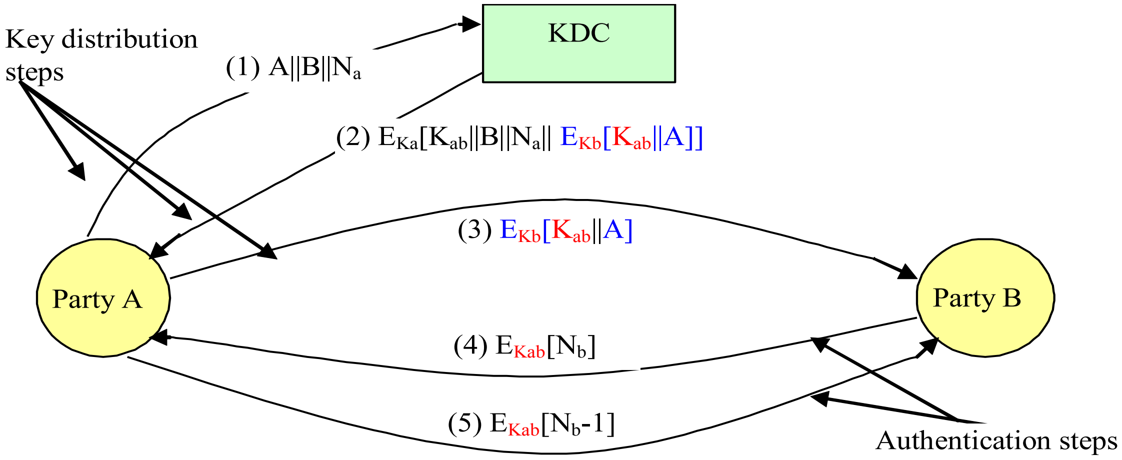
Eve transmits E(PUa, Ks) to Alice.

The result is that both Alice and Bob know *Ks* and are unaware that *Ks* has also been revealed to Eve. Alice and Bob can now exchange messages using *Ks*. Eve no longer actively interferes with the communications channel but simply eavesdrops. Knowing *Ks*, Eve can decrypt all messages, and both A and B are unaware of the problem.

Exercise Question – E8.2(ii) - A

- Both A and B need to authenticate to each other by demonstrating they are indeed A and B; this requires each of the parties to use their certified public keys AND demonstrating that they each know the corresponding private keys associated to the public keys.

Exercise Question – E8.3



Key distribution steps

KDC

(1) $A||B||N_a$

(2) $E_{Ka}[K_{ab}||B||N_a|| E_{Kb}[K_{ab}||A]]$

(3) $E_{Kb}[K_{ab}||A]$

Party A

Party B

(4) $E_{Kab}[N_b]$

(5) $E_{Kab}[N_b-1]$

Authentication steps

This is the Needham-Schroeder protocol. Answer the following questions:

i. What are the benefits for A to forward the session key to B (i.e. step 3), rather than letting KDC to directly send the session key to B?

ii. TRY to identify two application areas of the Needham-Schroeder protocol and to elaborate the benefits of using the Needham-Schroeder protocol in these application areas.

Exercise Question – E8.3(i) - A

Benefits:

- reduced involvement of KDC, thus less overhead not just for KDC also for B;
- This protocol (designed in this way) can also be used for authentication purpose, in addition to confidential communication between A and B.

Exercise Question – E8.3(ii) - A

- **Two applications**: one is establishing a secure communication channel; and the other is for authentication service.
- **Benefits:**
  - Party A (i.e. user) does not need to remember many keys while being able to use a different key for a different correspondent;
  - When used for authentication, the protocol supports single sign-on, i.e. a user only need to remember a single password, but is able to use different short-term secrets for different servers and the users' master secrets (i.e. long-term passwords) are only managed by one entity, i.e. KDC.