A summary of symmetric key (session key, secret key) establishment protocols

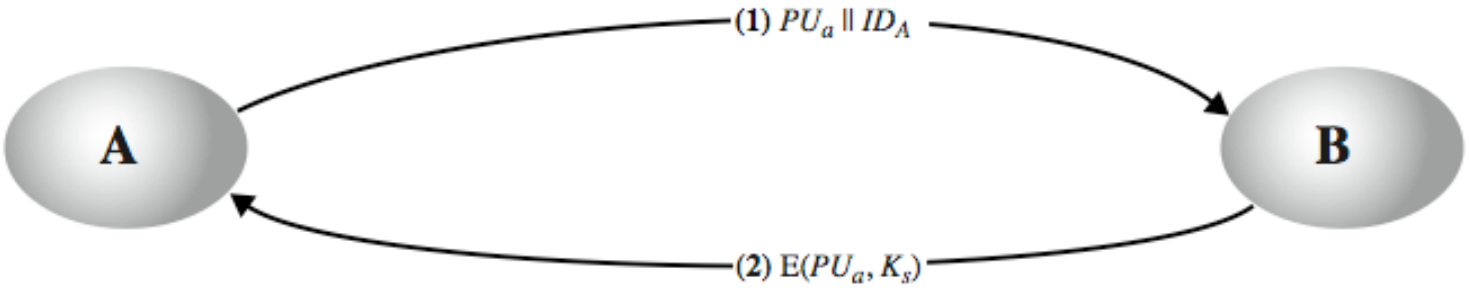
Protocols	ThirdParty	Timestamps	EntityAuth	messages
Diffie-Hellman	No	No	None	2
Needham-Schroeder protocol	KDC (online)	No	Symmetric encryption	5
X.509 (2 pass)	CA (offline)	Yes	mutual	2
X.509 (3 pass)	CA (offline)	No, but with nonce	mutual	3

Exercise Question – E6.1

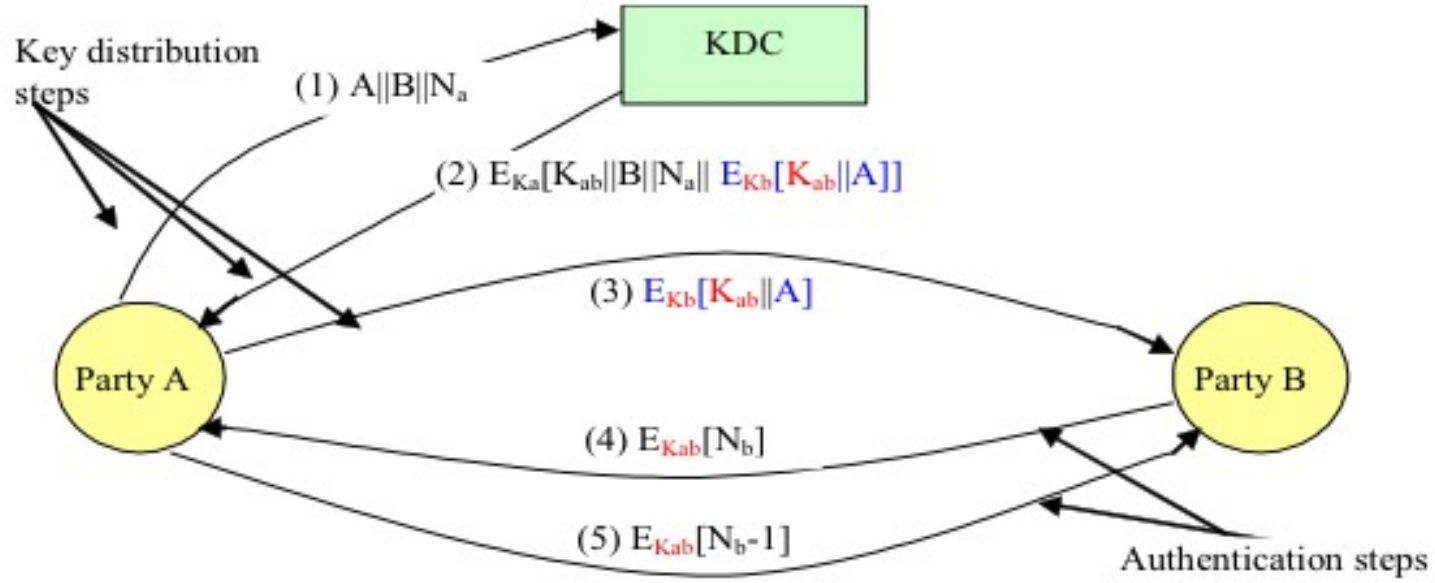
Assuming that Alice is to send a message, *M*, to Bob. *M* is encrypted with a shared key established using the DH protocol. Explain whether Eve could access this message *M*. If so, explain how, and propose a solution to address this vulnerability.

Exercise Question – E6.2

- 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).
  - Identify as many problems/flaws as you can.
  - Modify the protocol to fix the problems/flaws you have identified.



Exercise Question – E6.3



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.

Conclusions

- Key management encompasses a number of critical issues to the effective use of cryptosystems.
- A number of protocols exist to support symmetrical key distribution and agreement.
  - Key transport protocols
    - One party creates or otherwise obtains a secret value, and securely transfers it to the other party.
  - Key agreement protocols
    - A shared secret is derived by the parties using information contributed by each, such that no party can predetermine the resulting value.
- Key agreement/distribution protocols can be vulnerable to security attacks, such as the man-in-the-middle and replay attacks, so they should be used with care.