COMP90043 Cryptography and Security
Semester 2, 2020, Workshop Week 9

Symmetric Key Distribution Protocol

1. Consider a variation of the symmetric key distribution protocol discussed in the lecture involving n users and a KDC. Here every user decides to generate random number themselves for the communication they seek to start. All users share a master key with the KDC, all communications can be observed by all users.
   The steps are as follows:

   (a) A generates a random session key K_s and sends to the KDC his identity ID_A, destination ID_B, and $E(K_A, K_s)$.

   (b) KDC responds by sending $E(K_B, K_s)$ to A.

   (c) A sends $E(K_s, M)$ together with $E(K_B, K_s)$ to B.

   (d) B knows K_B, thus decrypts $E(K_B, K_s)$, to get K_s and will subsequently use K_s to decrypt $E(K_s, M)$ to get M.

   Is this secure?

2. Consider the following protocol, designed to let A and B decide on a fresh, shared session key K_s. We assume that they already share a long-term key K_{AB}.

$$
\begin{aligned}
A \rightarrow B &: ID_A, N_A \\
B \rightarrow A &: E(K_{AB}, [N_A, K_s]) \\
A \rightarrow B &: E(K_s, N_A)
\end{aligned}
$$

   (a) Why would A and B believe after the protocol ran that they share K_s with each other?
   A believes that she shares K_s with B since ...
   B believes that he shares K_s with A since ...

   (b) Why would they believe that this shared key K_s is fresh?
   A believes that K_s is fresh since ...
   B believes that K_s is fresh since ...

   (c) Assume now that A starts a run of this protocol with B. However, the connection is intercepted by the adversary C. Show how C can start a new run of the protocol using reflection, causing A to believe that she has agreed on a fresh key with B (in spite of the fact that he has only been communicating with C). Thus, in particular, the belief in (a) is false.

   (d) Propose a modification of the protocol that prevents this attack.

Key Management and Distribution

1. Discuss four methods which are used in distributing public keys.

2. What are the essential ingredients of a public-key directory?

3. What is a chain of certificates? What are forward and reverse certificates?

4. For the following hierarchy, what is the chain of certificates that user "Udaya" needs to obtain in order to establish a certificate path to "Ram"? You can use X.509 conventions for the certificate chain, for example the certificate for "Udaya" by CA "CIS" is represented as CIS«Udaya».