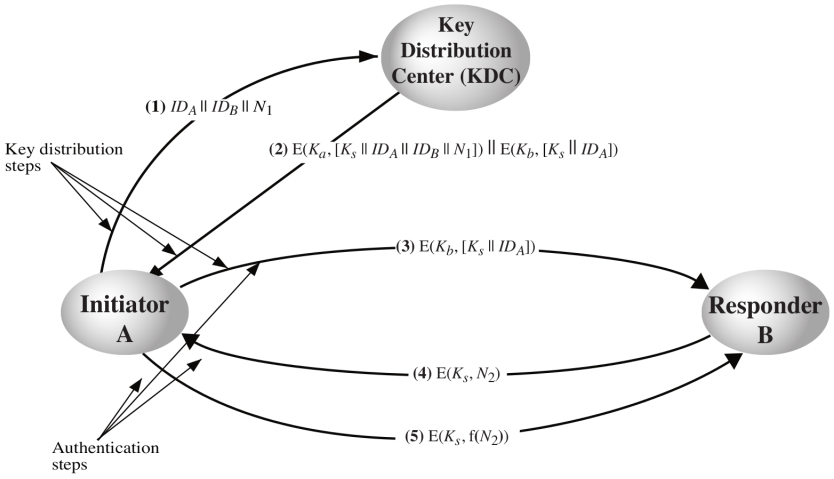
CSS322 – Quiz 6

Security and Cryptography, Semester 2, 2010

Prepared by Steven Gordon on 4 February 2011
CSS322Y10S2Q06, Steve/Courses/CSS322/Assessment/Quiz5.tex, r1651

Question 1 [4 marks]

Consider the mechanism below. Assume the number of users in the network is the last two digits of your ID (A and B are two of the users).



(a) Excluding session keys, how many keys must the KDC know for this mechanism to work?

Answer. *If there are n users, then the KDC must know the master keys of each user. That is, the KDC must know n keys (excluding session keys).*

(b) If user A has applied this mechanism to communicate with all other users in the network, then how many keys does user A know?

Answer. *User A has its own master key, K_a, as well as session keys with each other user. There is a session key shared between A and B ($K_{s_{ab}}$), a separate session key shared between A and C ($K_{s_{ac}}$), and so on. With $n-1$ other users, A must know 1 master key and $n-1$ session keys. That is, a total of n keys.*

(c) What is a disadvantage of this mechanism compared to the decentralised key distribution (in previous quiz)?

Answer. *1. Performance. Requests go to the KDC; if the KDC is slow (i.e. a bottleneck) then each user will be delayed in obtaining a session key, subsequently delaying communications with the other user. 2. Trust. All users must trust the KDC; this is not possible in some cases. 3. Security. The KDC must be secure; if it is compromised, all master keys and sessions keys can be obtained by attacker.*

(d) If an attacker replayed message (3), then explain how this attack will be detected.

Answer. *B will respond with message (4), choosing a new (random) value of N_2. If A receives message (4) it will detect an attack, since A did not sent message (3) and hence its not expecting a response. If the attacker intercepts message (4) before it arrives at A, and then the attacker tries to send message (5), then B will detect an attack. This is because the attacker cannot create the correct message (5) (because they don't know N_2 or K_s). Also, if message (5) was not sent, then B will eventually realise, again detecting an attack.*