ΕΠΛ 674: Εργαστήριο 7

Ασκήσεις από τα Κεφάλαια 14, 15, 19 (5th Edition)

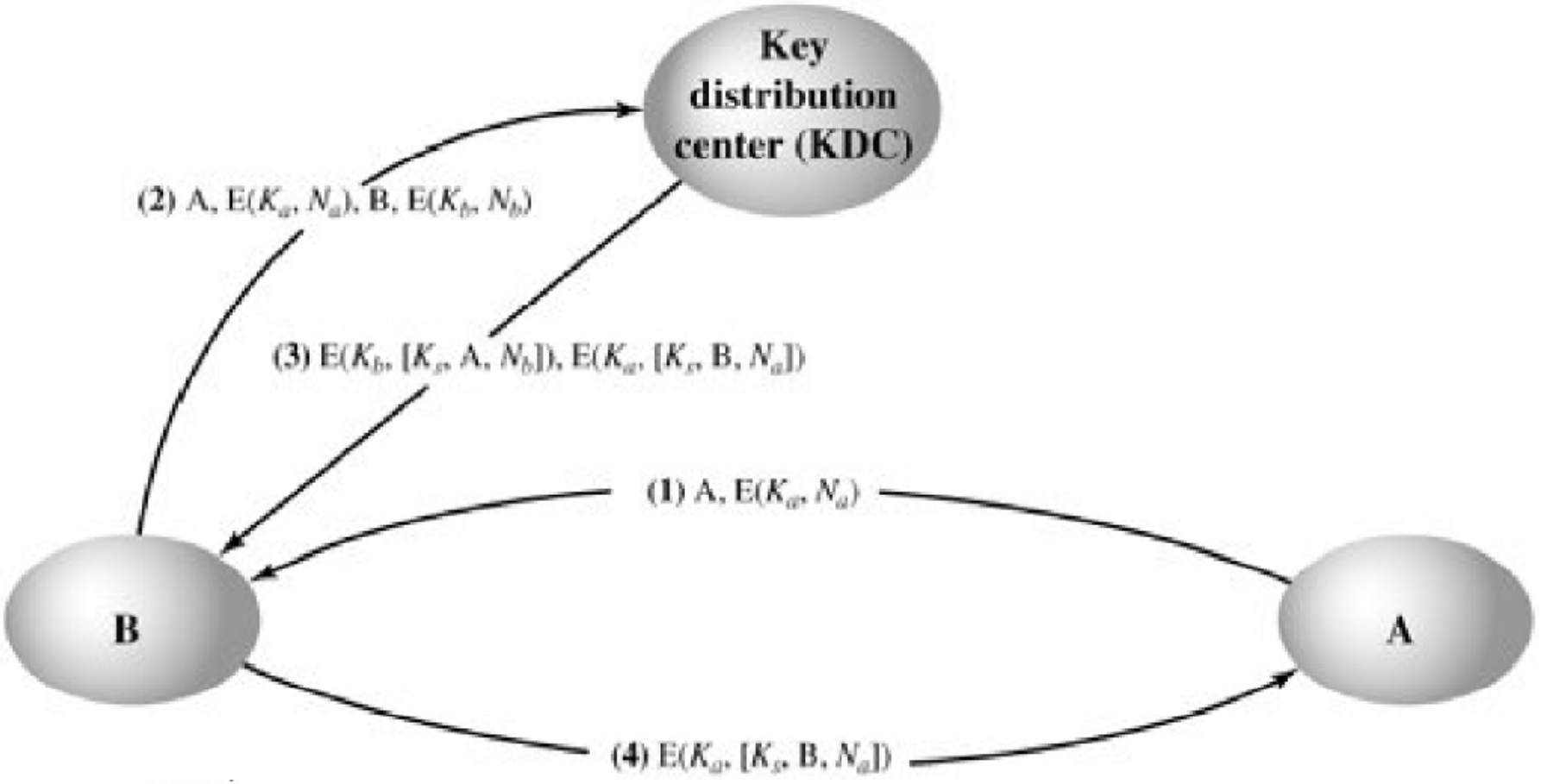
University of Cyprus
Department of Computer Science

Παύλος Αντωνίου

NETworks Research Laboratory

Problem 14.1

- One local area network vendor provides a key distribution facility
  - Q: Describe the scheme.



Problem 14.1

- A: A sends a connection request to B, with an event marker or nonce (Na) encrypted with the key that A shares with the KDC. If B is prepared to accept the connection, it sends a request to the KDC for a session key, including A's encrypted nonce plus a nonce generated by B (Nb) and encrypted with the key that B shares with the KDC. The KDC returns two encrypted blocks to B. One block is intended for B and includes the session key, A's identifier, and B's nonce. A similar block is prepared for A and passed from the KDC to B and then to A. A and B have now securely obtained the session key and, because of the nonces, are assured that the other is authentic.

Problem 14.1

University of Cyprus

– Q: Compare this scheme (slide 4) to that of Figure 14.3. What are the pros and cons?

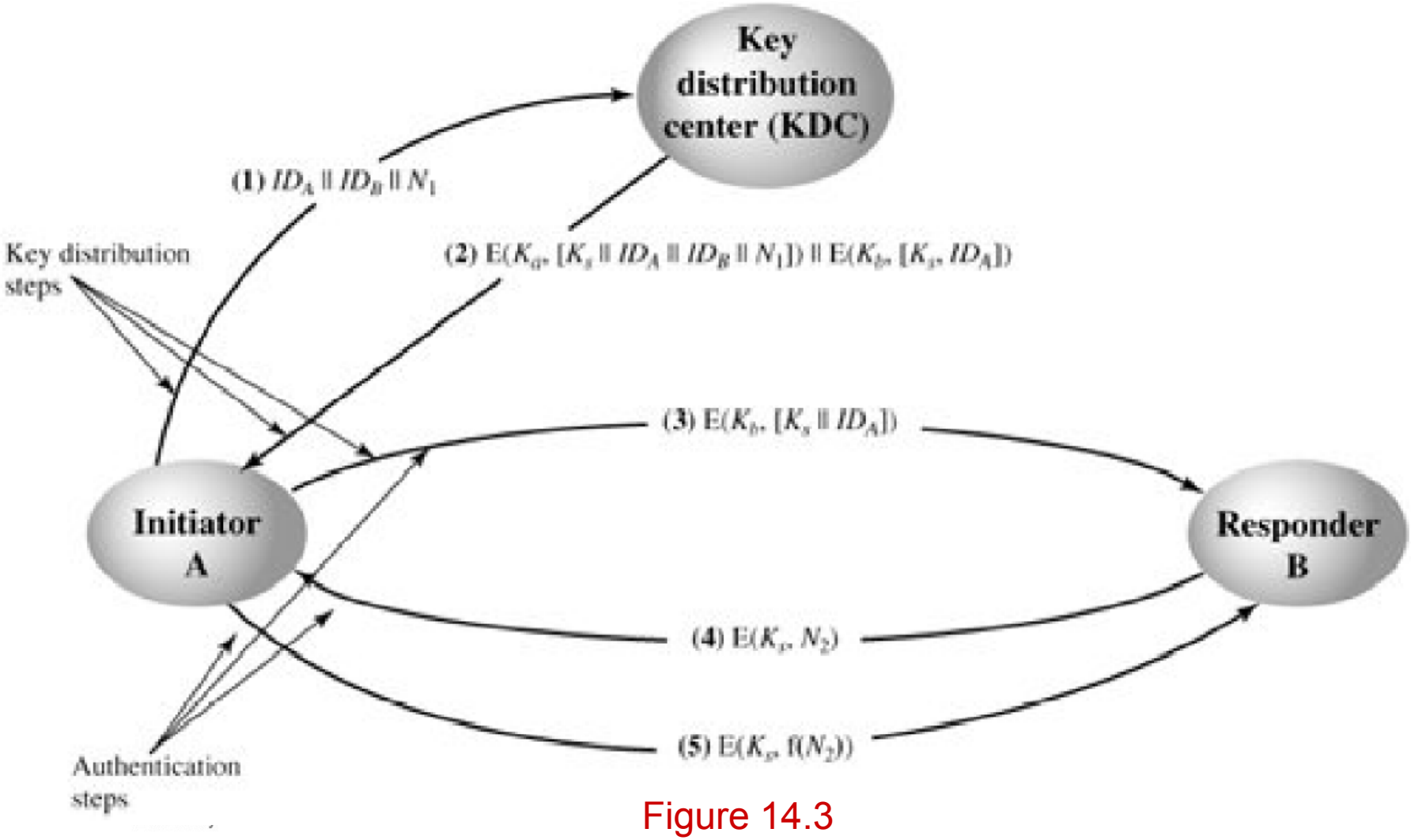


Figure 14.3

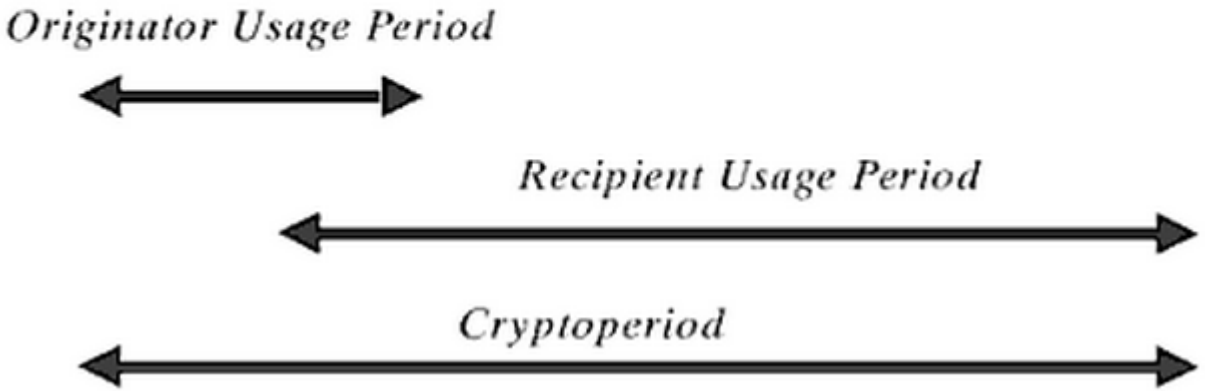
Problem 14.1

University of Cyprus

- A: The proposed scheme appears to provide the same degree of security as that of Figure 14.3. One advantage of the proposed scheme is that the, in the event that B rejects a connection, the overhead of an interaction with the KDC is avoided.

Problem 14.5 (Question)

NIST defines the term cryptoperiod as the time span during which a specific key is authorized for use or in which the keys for a given system or application may remain in effect. One document on key management uses the following time diagram for a shared secret key.



Explain the overlap by giving an example application in which the originator's usage period for the shared secret key begins before the recipient's usage period and also ends before the recipients usage period.

Problem 14.5 (Answer)

University of Cyprus

- When a symmetric key is used to protect stored information, the recipient usage period may start after the beginning of the originator usage period as shown in the figure. For example, information may be encrypted before being stored on a compact disk. At some later time, the key may be distributed in order to decrypt and recover the information.

Problem 14.6 (Question)

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

1. $A \rightarrow B: A, N_A$.
2. $B \rightarrow A: E(K_{AB}, [N_A, K'_{AB}])$
3. $A \rightarrow B: E(K'_{AB}, N_A)$

a. We first try to understand the protocol designer's reasoning:

—Why would A and B believe after the protocol ran that they share K'_{AB} with the other party?

—Why would they believe that this shared key is fresh?

In both cases, you should explain both the reasons of both A and B, so your answer should complete the sentences

A believes that she shares K'_{AB} with B since...

B believes that he shares K'_{AB} with A since...

A believes that K'_{AB} is fresh since...

B believes that K'_{AB} is fresh since...

b. 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 she has only been communicating with C). Thus, in particular, the belief in (a) is false.

c. Propose a modification of the protocol that prevents this attack.

Problem 14.6 (Answer)

University of Cyprus

- **a.** A believes that she shares K'_{AB} with B since her nonce came back in message 2 encrypted with a key known only to B (and A).

  B believes that he shares K'_{AB} with A since N_A was encrypted with K'_{AB}, which could only be retrieved from message 2 by someone who knows K'_{AB} (and this is known only by A and B). A believes that K'_{AB} is fresh since it is included in message 2 together with N_A (and hence message 2 must have been constructed after message 1 was sent). B believes (indeed, knows) that K'_{AB} is fresh since he chose it himself.

Problem 14.6 (Answer)

University of Cyprus

- **b.** We consider the following interleaved runs of the protocol:

$$
\begin{array}{lll}
1. & \mathrm{A} \rightarrow \mathrm{C(B)}: & \mathrm{A}, N_A \\
1`. & \mathrm{C(B)} \rightarrow \mathrm{A}: & \mathrm{B}, N_A \\
2`. & \mathrm{A} \rightarrow \mathrm{C(B)}: & \mathrm{E}(K_{AB}, [N_A, K'_{AB}]) \\
2. & \mathrm{C(B)} \rightarrow \mathrm{A}: & \mathrm{E}(K_{AB}, [N_A, K'_{AB}]) \\
3. & \mathrm{A} \rightarrow \mathrm{C(B)}: & \mathrm{E}(K'_{AB}, N_A)
\end{array}
$$

  C cannot encrypt A's nonce, so he needs to get help with message 2. He therefore starts a new run with A, letting A do the encryption and reflecting the reply back. A will accept the unprimed protocol run and believe that B is present.

- **c.** To prevent the attack, we need to be more explicit in the messages, e.g. By changing message 2 to include the sender and receiver (in this order), i.e. to be $\mathrm{E}(K_{AB}, [\mathrm{A}, \mathrm{B}, N_A, K'_{AB}])$.

Problem 15.8

University of Cyprus

- Q: Consider a one-way authentication technique based on asymmetric encryption:
  - A→B: ID_A
  - B→A: R_1
  - A→B: $E(PR_a, R_1)$
  - a. Explain the protocol
  - b. What type of attack is this protocol susceptible to?
- A:
  - **a.** This is a means of authenticating A to B. R_1 serves as a challenge, and only A is able to encrypt R_1 so that it can be decrypted with A's public key.
  - **b.** Someone (e.g., C) can use this mechanism to get A to sign a message. Then, C will present this signature to D along with the message, claiming it was sent by A. This is a problem if A uses its public/private key for both authentication, signatures, etc.

Problem 15.9

University of Cyprus

- Q: Consider a one-way authentication technique based on asymmetric encryption:
  - A→B: ID_A
  - B→A: $E(PU_a, R_2)$
  - A→B: R_2
  - a. Explain the protocol
  - b. What type of attack is this protocol susceptible to?
- A:
  - **a.** This is a means of authenticating A to B. Only A can decrypt the second message, to recover R_2.
  - **b.** Someone (e.g. C) can use this mechanism to get A to decrypt a message (i.e., send that message as R_2) that it has eavesdropped from the network (originally sent to A).

Problem 19.5 (Question)

University of Cyprus

- Suppose that the current replay window spans from 60 to 124 (default window size in IPsec: 64).
  - If the next incoming authenticated packet has sequence number 100, what will the receiver do with the packet, and what will the parameters of the window be after that?
  - If the next incoming authenticated packet has sequence number 150, what will the receiver do with the packet, and what will the parameters of the window be after that?
  - If the next incoming authenticated packet has sequence number 50, what will the receiver do with the packet, and what will the parameters of the window be after that?

Problem 19.5 (Answer)

- **a.** The received packet falls within the window. If it is new, the MAC is checked. If the packet is authenticated, the corresponding slot in the window is marked. If it is not new, the packet is discarded. In either case, no change is made to window parameters.
- **b.** The received packet is to the right of the window and is new, so the MAC is checked. If the packet is authenticated, the window is advanced so that this sequence number is the right edge of the window, and the corresponding slot in the window is marked. In this case, the window now spans from 86 to 150.
- **c.** The received packet is to the left of the window, so the packet is discarded; this is an auditable event. No change is made to window parameters.