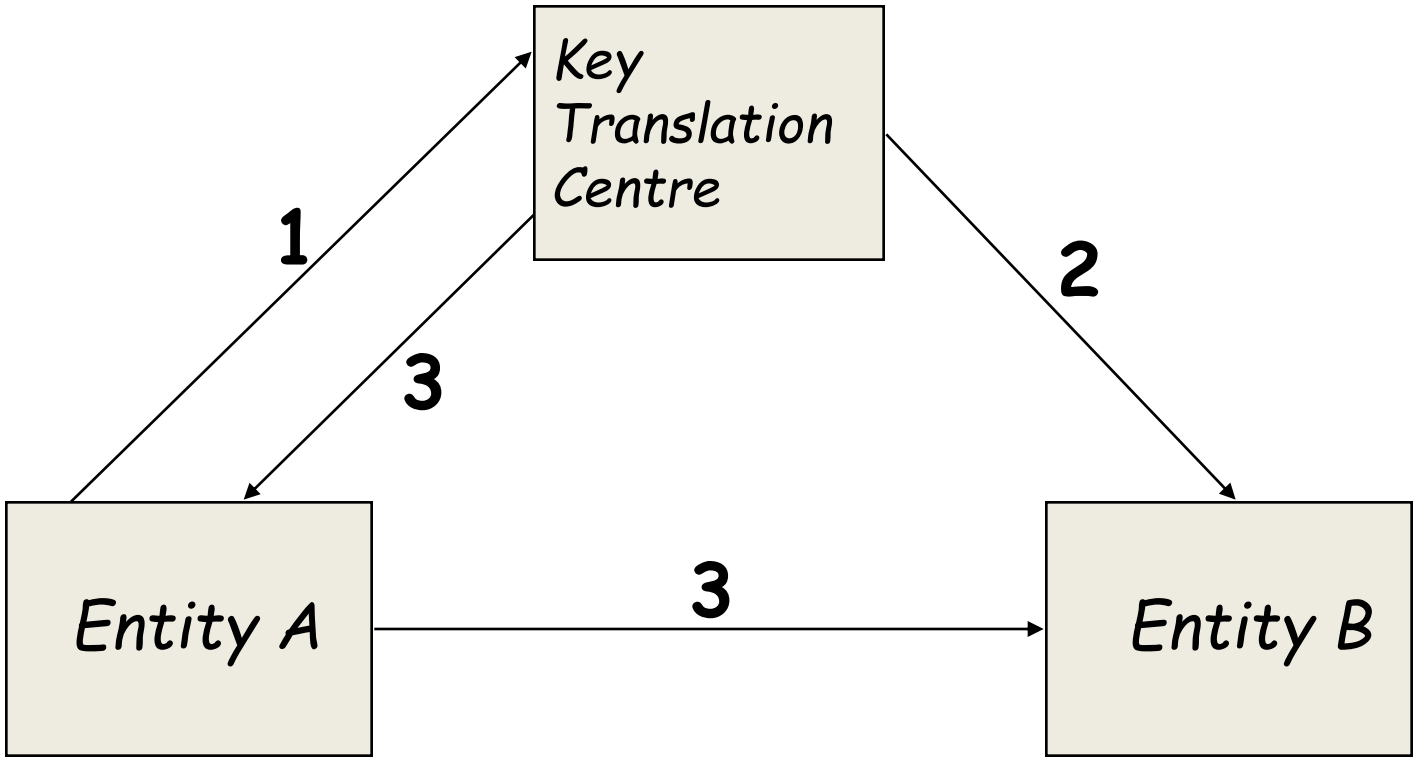
Tutorial 7 Solutions

CS5285

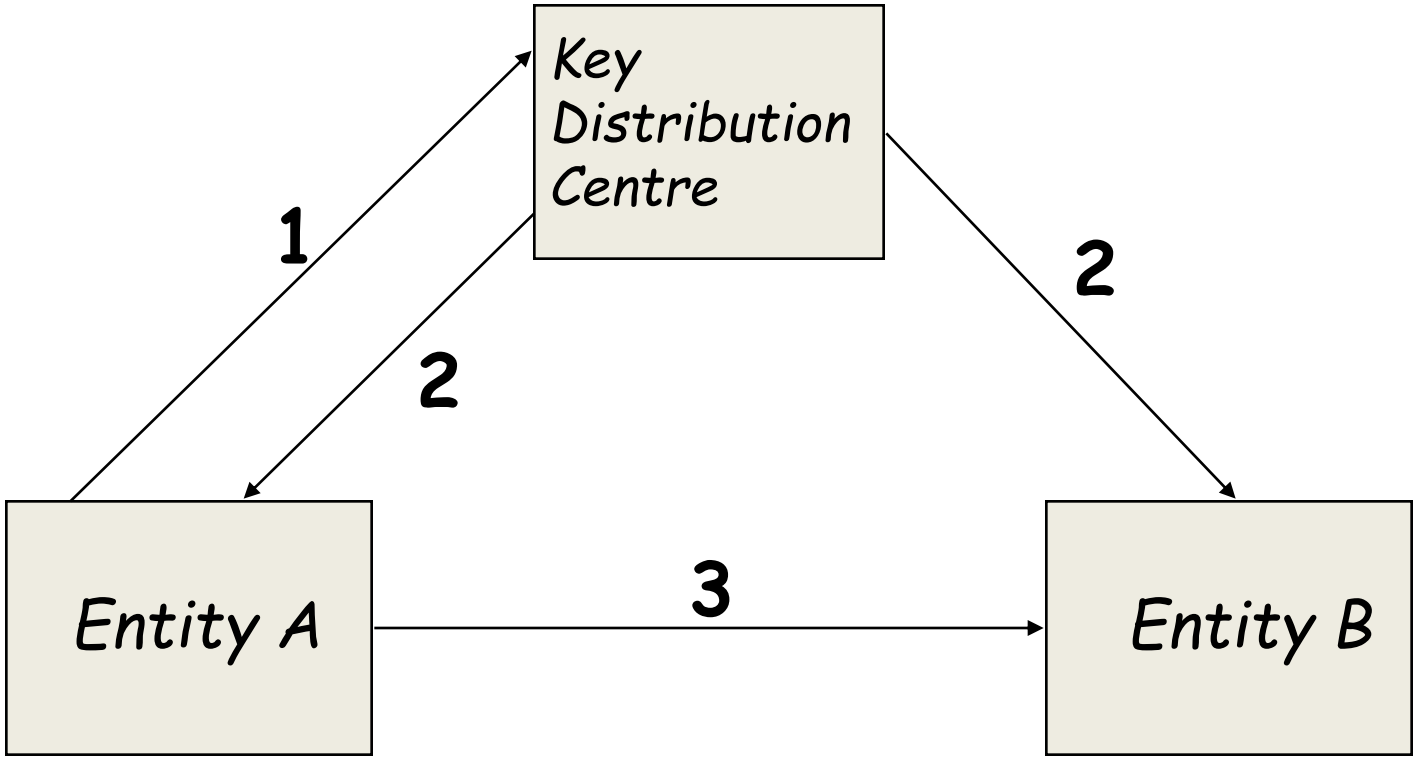
Terms for key management

- *Key establishment*: Process of making a secret key available to multiple entities.
- *Key control*: Ability to a choose a key's value.
- *Key agreement*: Process of establishing a key in such a way that neither entity has key control.
- *Key transport*: Process of securely transferring a key from one entity to another.
- *Key confirmation*: Assurance that another entity has a particular key.

Key Translation Centre



Key Distribution Centre



Question 1

The following protocol establishes a new key KAB between A and B using a trusted third party S. What type of key establishment is this and what is S called?

A > S: E_KAS(KAB,B)
S > B: E_KBS(KAB,A)

This is key transport (A has key control).
This makes S a Key Translation Centre

Question 2

- Consider the following protocol, where E is a symmetric key encryption scheme and K is a long-term symmetric key shared between A and B.

$$\begin{array}{lcll} A & \rightarrow & B & : \quad \text{“Alice”}, R_1 \\ A & \leftarrow & B & : \quad R_2, E_K(R_1) \\ A & \rightarrow & B & : \quad E_K(R_2) \end{array}$$

Does the scheme support session key establishment? If not, modify the protocol so that it does.

Question 2

- Solution

The protocol does not support session key establishment, because all random numbers (R_1, R_2) are public. Neither of them can be used as a session key. We modify the protocol as follows:

$$\begin{array}{lcll} A & \rightarrow & B & : \quad \text{“Alice”}, R_1 \\ A & \leftarrow & B & : \quad R_2, E_K(R_1, R_2, K') \\ A & \rightarrow & B & : \quad E_K(R_2, K') \end{array}$$

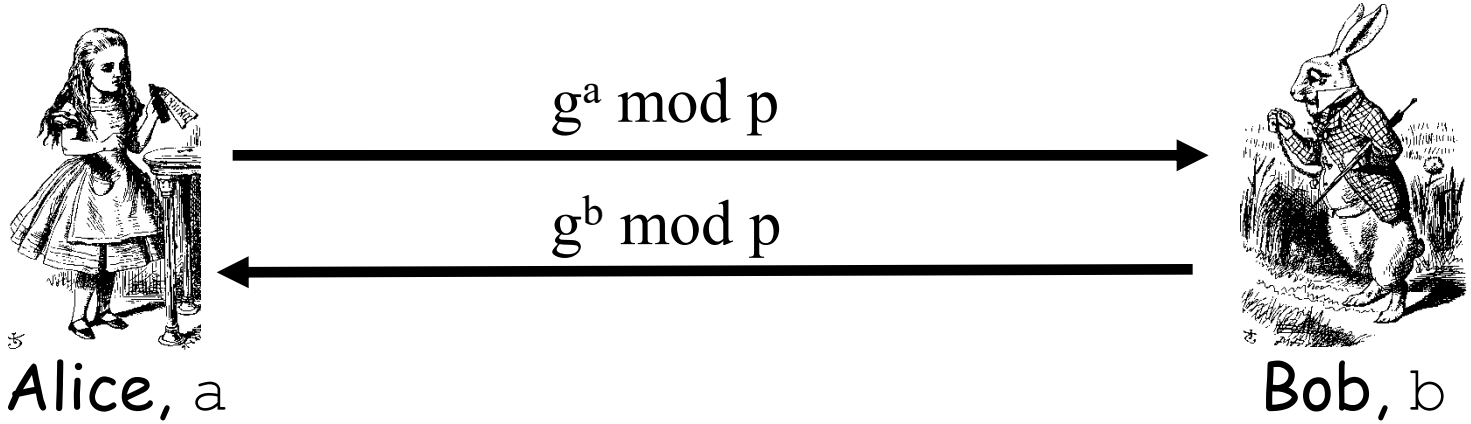
Bob chooses a random session key K', which is encrypted together with R_1 and R_2 and sent to Alice. Because K' is encrypted, an eavesdropper cannot learn K'.

Question 3

- Consider the following protocol, where E is a symmetric key encryption scheme, and K is computed as $K = g^{ab} \bmod p$. $[message]_{name}$ means $message$ signed by $name$. What is the long-term secret of this scheme?

$$
\begin{array}{lcll}
A & \rightarrow & B & : \quad \text{“I'm Alice”}, g^a \ mod \ p \\
A & \leftarrow & B & : \quad \text{“Bob”}, g^b \ mod \ p, E_K([g^a \ mod \ p, g^b \ mod \ p]_{\text{Bob}}) \\
A & \rightarrow & B & : \quad \text{“Alice”}, E_K([g^a \ mod \ p, g^b \ mod \ p]_{\text{Alice}})
\end{array}
$$

Diffie-Hellman Key Exchange



- Alice computes $(g^b)^a = g^{ba} = g^{ab} \bmod p$
- Bob computes $(g^a)^b = g^{ab} \bmod p$
- Could use $K = g^{ab} \bmod p$ as symmetric key

- This key exchange scheme is secure against eavesdroppers if Diffie-Hellman Problem is assumed to be hard to solve.
- However, it is insecure if the attacker in the network is active: man-in-the-middle attack. "Active" means that the attacker can intercept, modify, remove or insert messages into the network.

Question 3

- Solution
- a and b are random, K is the session key
- g and p are public
- Session key established via DH
- The only long-term secrets in this scheme are the private signing keys of Alice and Bob.

Question 4

- Design a protocol that will use a *key distribution centre* to set up a shared key K between Alice and Bob. You should use *timestamps for freshness and assume that Bob cannot talk directly to the KDC*. Alice and Bob does not need to be authenticated to each other and there is no need for explicit key authentication. State all your assumptions about the system.

Question 4.i

- Solution
- Key distribution means what for Alice and Bob?

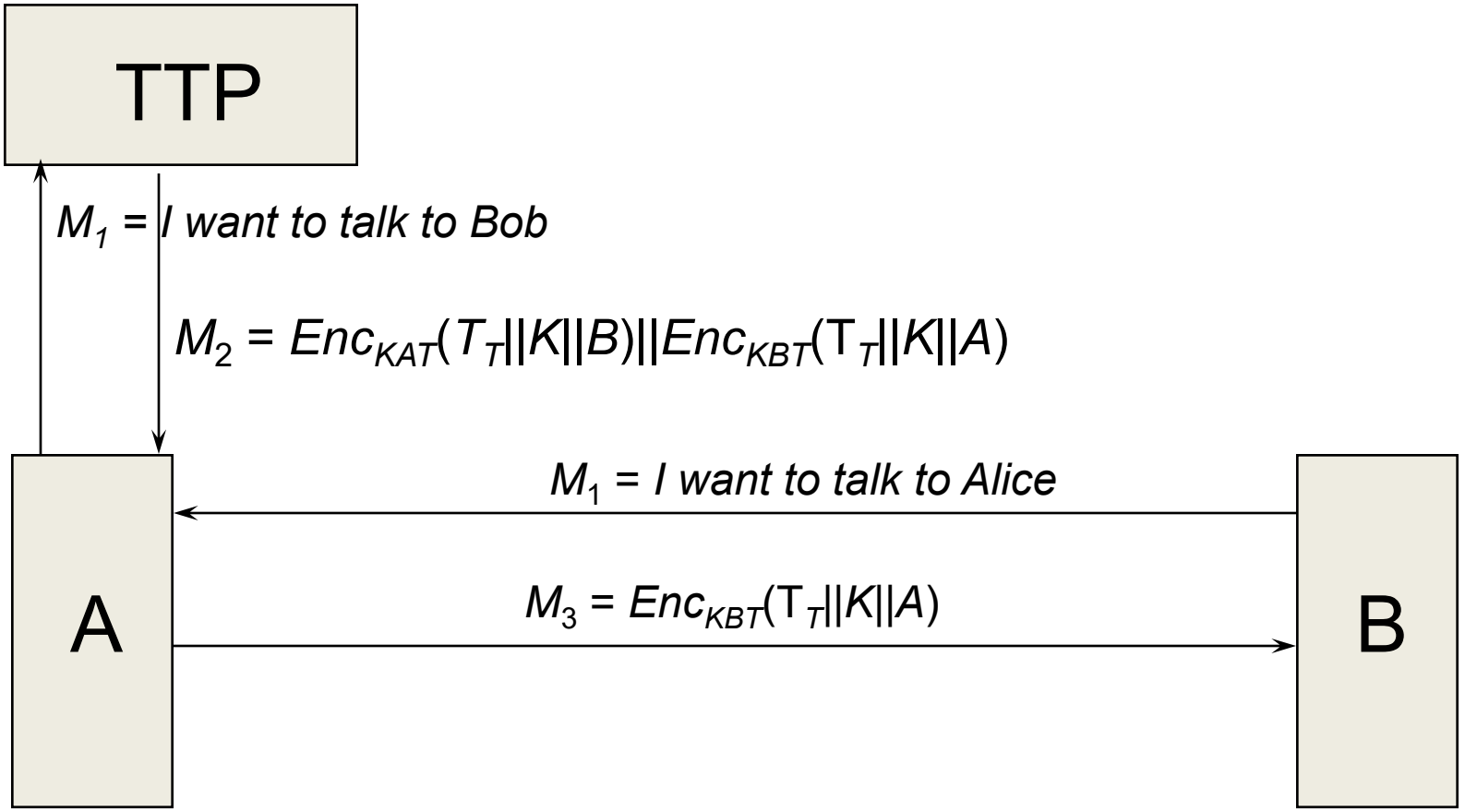
  Alice and Bob has no key control.
- Alice and Bob does not need to be authenticated but who should be?

  The KDC
- Do you need to use key K in the protocol?

  No, only implicit key authentication required.
- What assumptions are there for this to work?

  Alice and Bob shares keys with KDC

Question 4.i


TTP
M_1 = I want to talk to Bob
$M_2 = Enc_{KAT}(T_T||K||B)||Enc_{KBT}(T_T||K||A)$
A
M_1 = I want to talk to Alice
$M_3 = Enc_{KBT}(T_T||K||A)$
B

Question 4.ii

- ii) What is the key hierarchy in this protocol?

  There are two levels. Top level is K_{AT} and K_{BT}, and bottom level is K.

- iii) If K_{AT} and K_{BT} are 56-bit DES keys and K is a 256-bit AES key what is the effective security of key K?

  It can only be as secure as the key that is being used to distribute it so 2^55