Computer Security

Cunsheng DING, HKUST

COMP4631

Lecture 12: Several Key Distribution Protocols

Outline of this Lecture

1. Passive and active attacks
2. Merkel's protocol.
3. The Needham-Schröder protocol.
4. Shamir's three-pass protocol.

Passive and active attacks

Passive attacks: Any attack on a security system under the assumption that the attacker can only intercept messages exchanged over a communication channel is called a **passive attack**.

Active attacks: Any attack on a security system under the assumption that the attacker can stop, intercept, delete, modify, and replay messages exchanged over a communication channel or insert his/her messages into the channel is called a **passive attack**.

In such a scenario, we say that the attacker has **full control** over the communication channel.

Secret Key Distribution with a PKC

Comments:

Public key cryptosystems are usually not used for real encryption, as they are very slow. They are used for distributing secret keys of one-key ciphers and/or for signing messages.

Question: How to use a PKC for distributing a secret key?

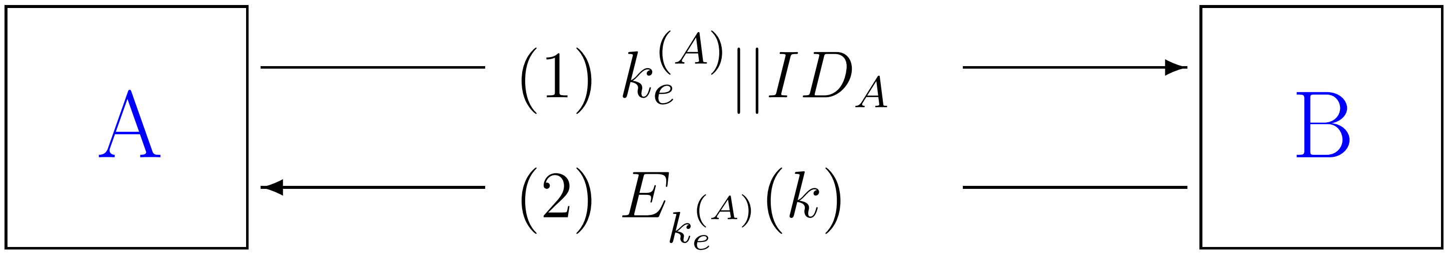
Merkel's Key Distribution Protocol

Scenario: A and B want to establish a session key.

1. A generates a key pair $\left(k_e^{(A)}, k_d^{(A)}\right)$, and sends $k_e^{(A)} || ID_A$ to B, where ID_A is an identifier of A.
2. B generates a secret key k, and sends $E_{k_e^{(A)}}(k)$ to A.
3. A computes $D_{k_d^{(A)}}\left[E_{k_e^{(A)}}(k)\right] = k$.
4. A discards $\left(k_e^{(A)}, k_d^{(A)}\right)$, and B discards $k_e^{(A)}$.

Remark: This is a variant of the **digital envelop protocol**.

Merkel Key Distribution Protocol: Pictorial



Remark: This is a variant of the **digital envelop protocol**, here we assume that A and B did not exchange their public keys before.

Comments: This protocol is vulnerable to an active attack. If an enemy E has control of the **intervening** communication channel, then E can **"compromise"** the communication without being detected.

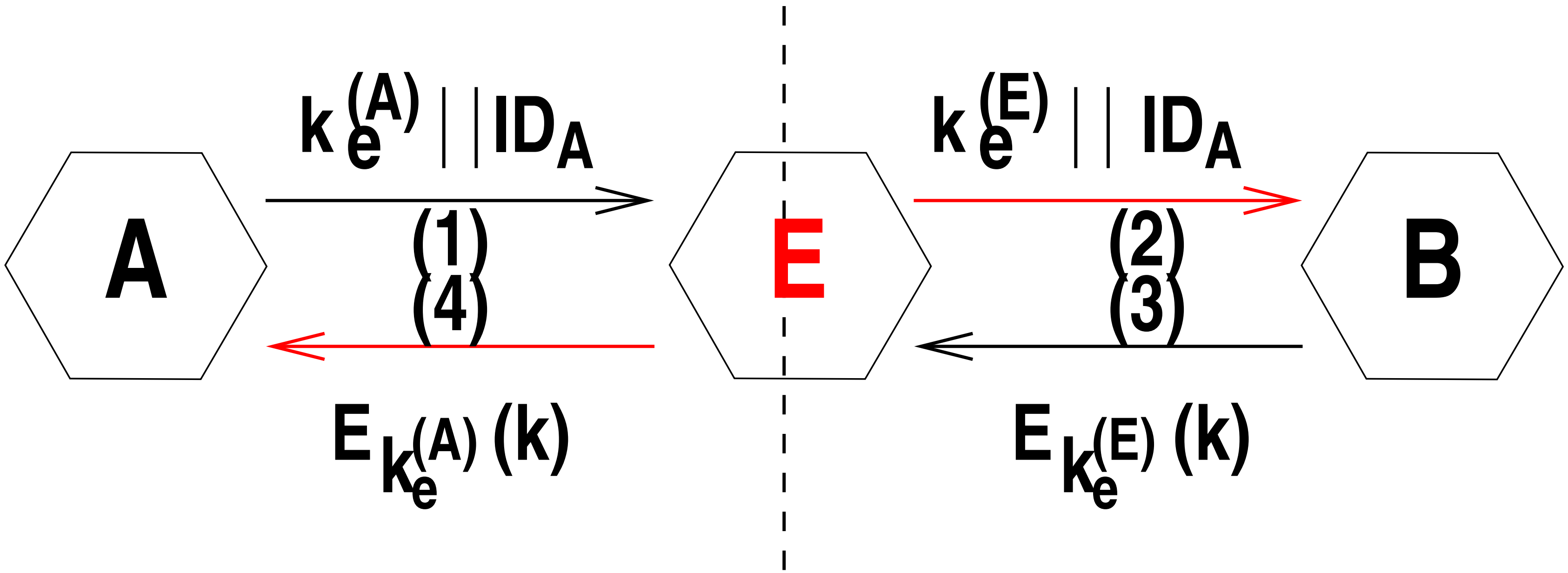
Question: What is the **active** attack?

Active Attack on the Merkel Protocol

1. A generates a key pair $\left(k_e^{(A)}, k_d^{(A)}\right)$, and sends $k_e^{(A)} || ID_A$ intended for B, where ID_A is an identifier of A.
2. E intercepts the message, creates its own key pair $\left(k_e^{(E)}, k_d^{(E)}\right)$, and sends $k_e^{(E)} || ID_A$ to B.
3. B generates a secret key k, and sends $E_{k_e^{(E)}}(k)$ (intended for A).
4. E intercepts the message, decrypts it to get k; then he computes and sends $E_{k_e^{(A)}}(k)$ to A.

Comment: A and B are unaware that E has got k.

The Intruder-in-the-Middle Attack: Pictorial



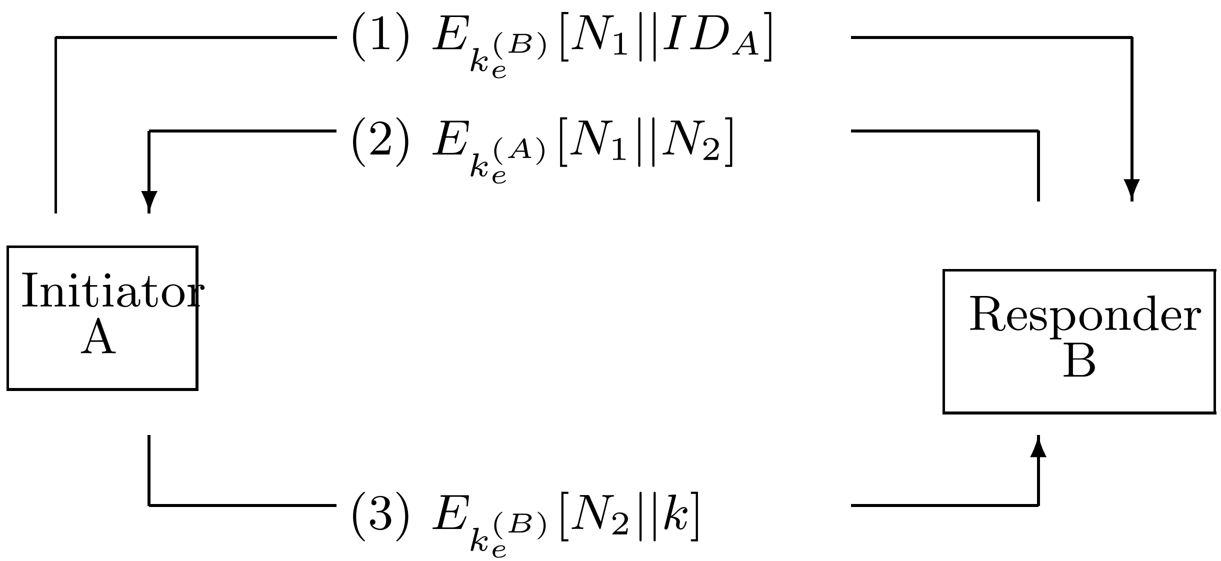
attacker in the middle

Active attack on the Merkel Protocol

The Modified Needham-Schröder Protocol

For both confidentiality and authentication:

Assume that A and B have exchanged their public keys with some method.



Remarks: Nonce N_1 is to identify this transaction uniquely.

The Modified Needham-Schröder Protocol

1. A sends $E_{k_e^{(B)}}[N_1||ID_A]$ to B, where N_1 is a nonce used to identify this transaction uniquely, and is generated by A.

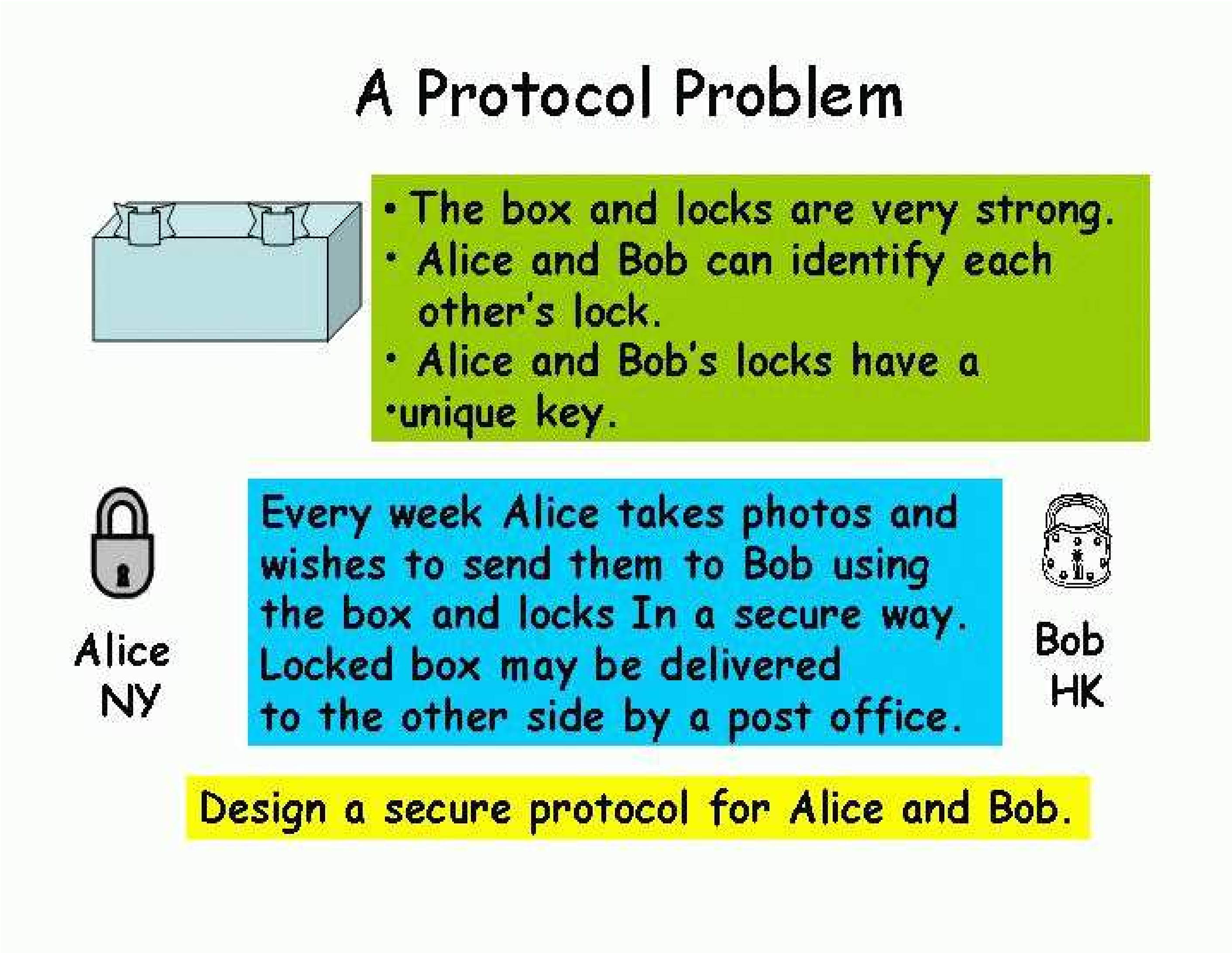
2. B generates a new nonce N_2, and sends $E_{k_e^{(A)}}[N_1||N_2]$ to A. After decryption A gets N_1, and is sure that the responder is B.

3. A selects a secret key k and sends $E_{k_e^{(B)}}[N_2||k]$ to B.

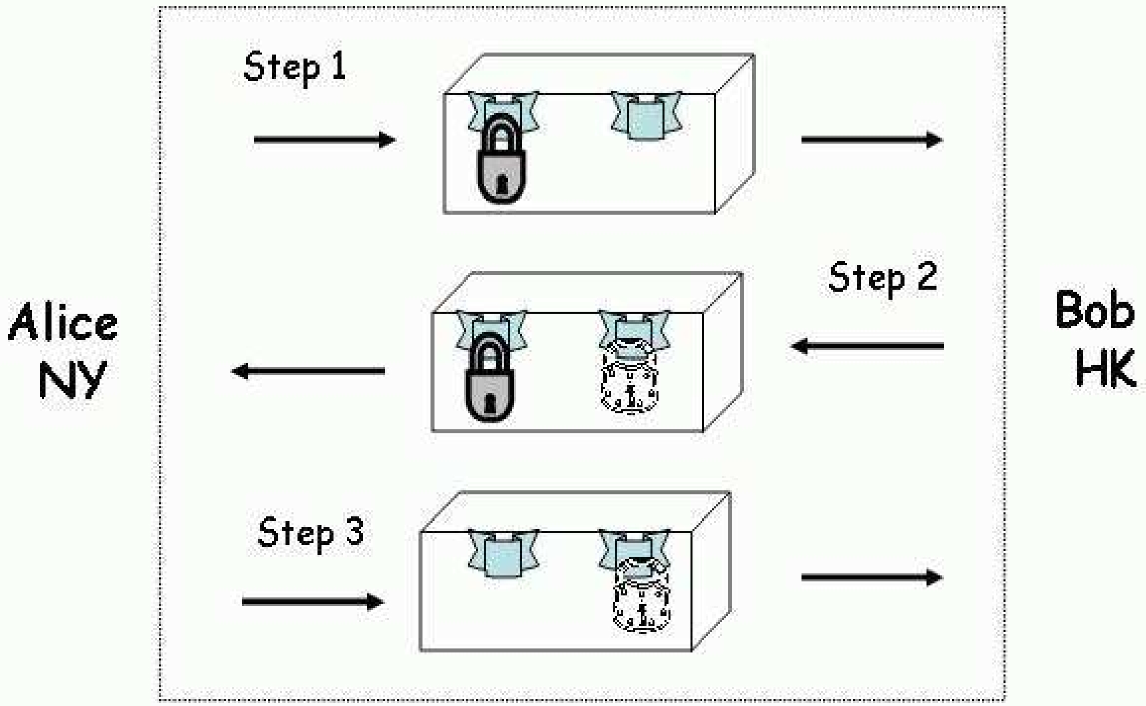
   (Encryption with B's public key ensures confidentiality)

4. After decryption B gets N_2 and k, and is sure that its correspondent is A.

Question: How does this protocol ensure both confidentiality and authenticity?


A Protocol Problem
• The box and locks are very strong.
• Alice and Bob can identify each other's lock.
• Alice and Bob's locks have a
•unique key.
Alice
NY
Every week Alice takes photos and wishes to send them to Bob using the box and locks In a secure way. Locked box may be delivered to the other side by a post office.
Bob
HK
Design a secure protocol for Alice and Bob.

A Protocol Problem: Solution



Secure w.r.t. active and passive attacks?

Shamir's Three-Pass Protocol

Objective: Alice wants to transfer a secret key k to Bob via a public communication channel.

System Parameters:

- A prime p is chosen so that the discrete logarithm problem mod p is hard. p is a public knowledge.
- Alice selects a random number a with $\gcd(a, p-1) = 1$. a^{-1} denotes the inverse of a mod $p-1$.
- Bob selects a random number b with $\gcd(b, p-1) = 1$. b^{-1} denotes the inverse of b mod $p-1$.

Shamir's Three-Pass Protocol

First of all, Alice computes $k_1 = k^a \bmod p$.

1. Alice sends $k_1 = k^a \bmod p$ to Bob.
2. Bob sends $k_2 = k_1^b \bmod p$ to Alice.
3. Alice sends $k_3 = k_2^{a^{-1}} \bmod p$ to Bob.

Finally, Bob computes $k = k_3^{b^{-1}} \bmod p$.

Question: Why $k = k_3^{b^{-1}} \bmod p$?

Why $k = k_3^{b^{-1}} \bmod p$

By the definition of multiplicative inverse,

$$a \cdot a^{-1} = u_1(p-1)+1, \quad b \cdot b^{-1} = u_2(p-1)+1$$

If $k = 0$, it is obvious. If $k \neq 0$, by Fermat's theorem

$$\begin{aligned}
k_3^{b^{-1}} \bmod p &= k^{aa^{-1}bb^{-1}} \bmod p \\
&= k^{[u_1u_2(p-1)+u_1+u_2](p-1)+1} \bmod p \\
&= \left((k^{[u_1u_2(p-1)+u_1+u_2]})^{p-1} \bmod p \right) k \bmod p \\
&= k \bmod p \\
&= k.
\end{aligned}$$

The Security of the Protocol

1. Alice sends $k_1 = k^a \bmod p$ to Bob.
2. Bob sends $k_2 = k_1^b \bmod p$ to Alice.
3. Alice sends $k_3 = k_2^{a^{-1}} \bmod p$ to Bob.

Security: security w.r.t. to passive attacks depends on the difficulty of solving the discrete logarithm problem.

Not secure with respect to an active attack (the so-called intruder-in-the-middle attack).