Week 7

An Introduction to Cyber Security – CS 573

Instructor: Dr. Edward G. Amoroso
eamoroso@tag-cyber.com

Week 7

Required Week Seven Readings

1. "THE POSSIBILITY OF SECURE NON-SECRET DIGITAL ENCRYPTION
by J. H. Ellis, January 1970
https://cryptocellar.org/cesg/possnse.pdf

2. **Finish Reading "*From CIA to APT: An Introduction*"**
to Cyber Security**, E. Amoroso & M. Amoroso**

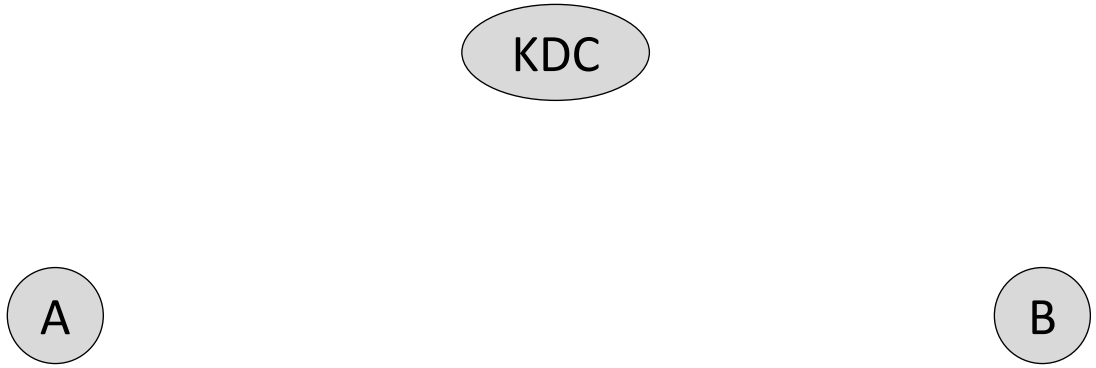
Twitter: @hashtag_cyber
LinkedIn: Edward Amoroso

Week 7: Public Key Cryptography

What Properties of Conventional Cryptography Must Be Maintained?

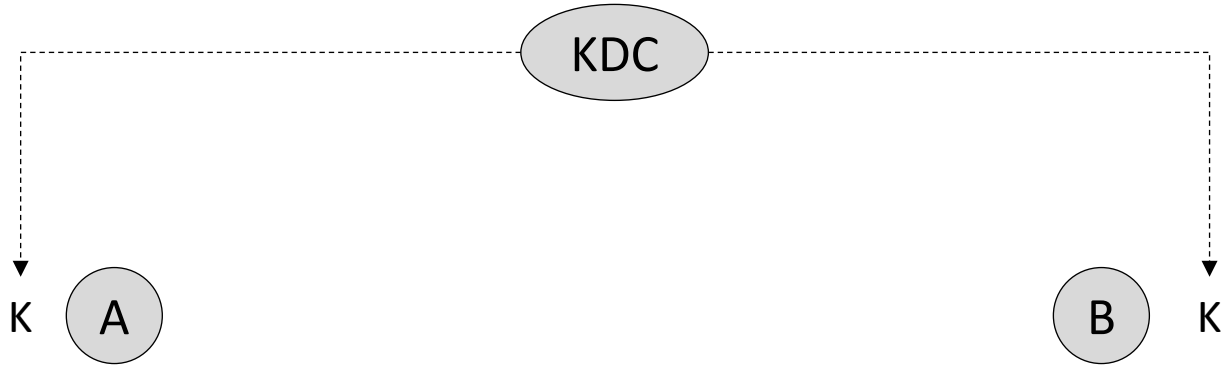
Week 7

Conventional Cryptography



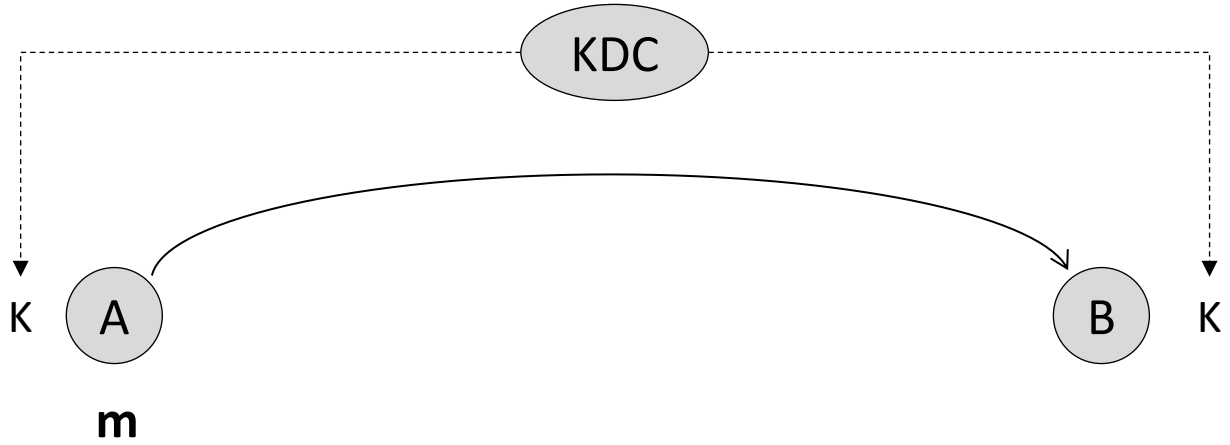
Week 7

Conventional Cryptography



Week 7

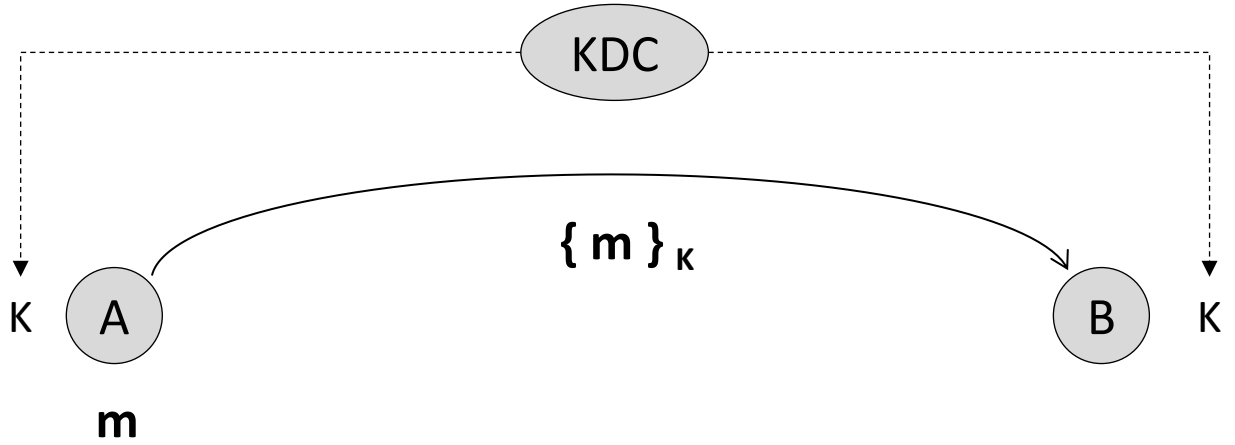
Conventional Cryptography



Alice creates message m . . .

Week 7

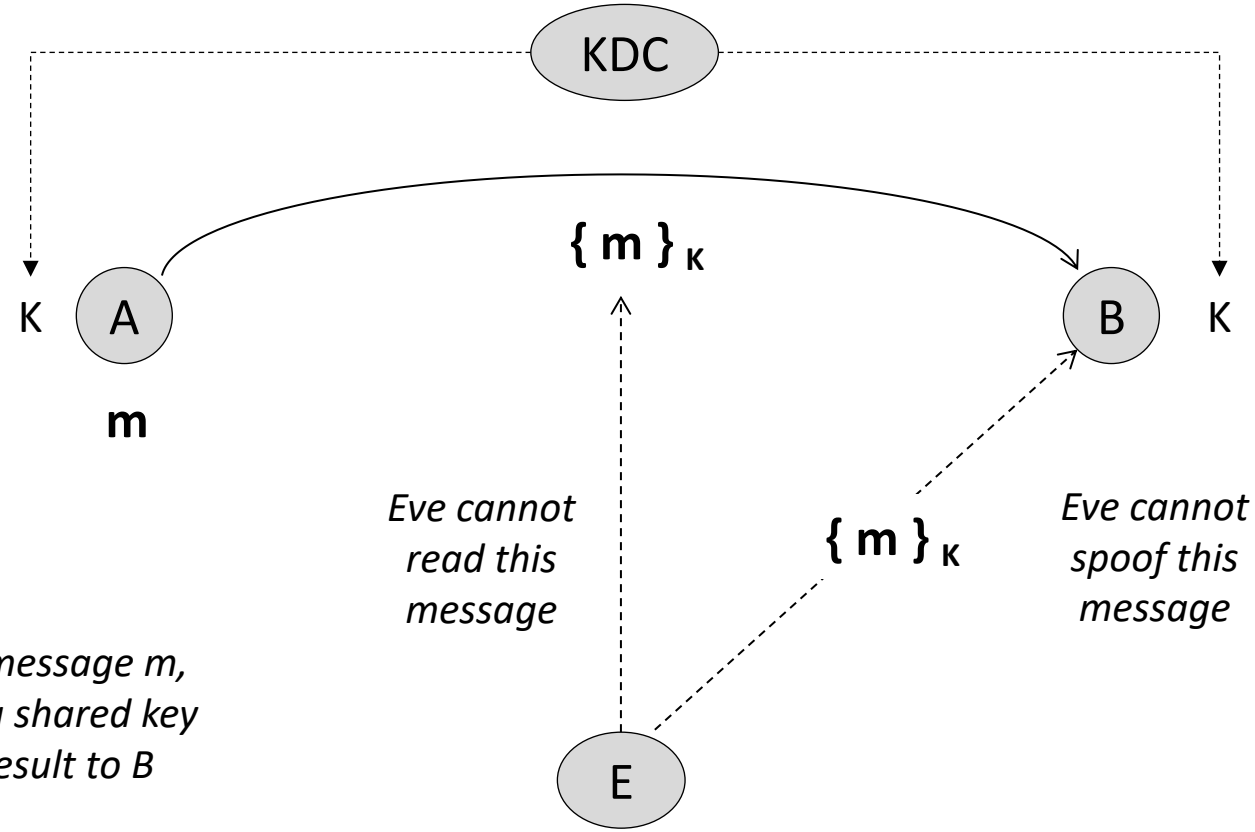
Conventional Cryptography



Alice creates message m, encrypts using shared key k, and sends result to B

Week 7

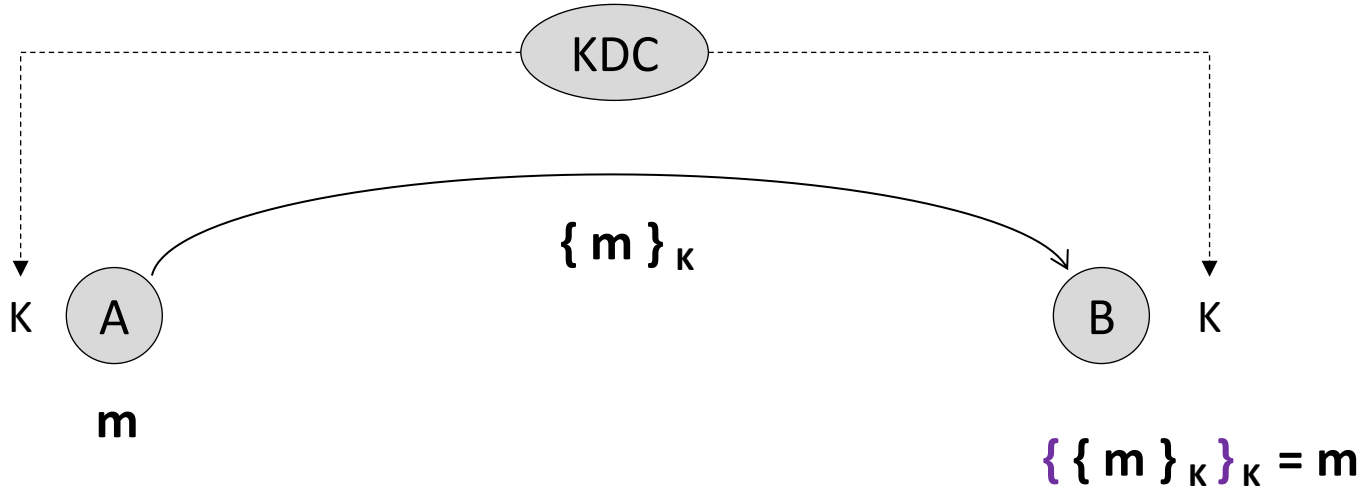
Conventional Cryptography



Alice creates message m, encrypts using shared key k, and sends result to B

Week 7

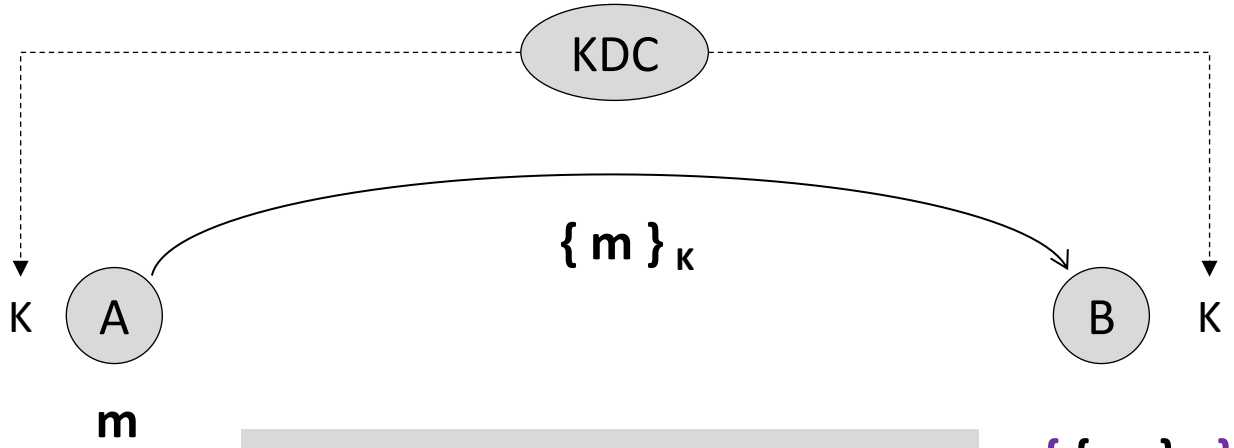
Conventional Cryptography



Bob receives encrypted message, and decrypts using shared key k, and obtains message m

Week 7

Conventional Cryptography

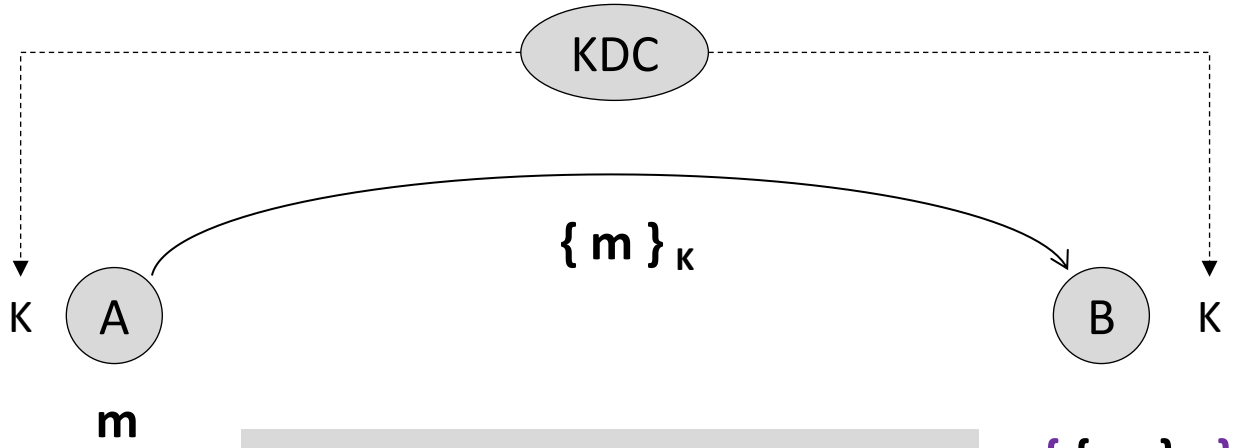


Secrecy Between A and B? **YES**
Authentication of A by B? **YES**

$\{\{ m \}_K\}_K = m$

Week 7

Conventional Cryptography



Secrecy Between A and B? **YES**
Authentication of A by B? **YES**

$\{\{ m \}_K\}_K = m$

Does this approach scale? **NO**

What are the Basic Properties of Public Key Cryptography?

Week 7

Public Key Cryptography Basics

Two Communicants: A and B

1. A generates pair of keys PA and SA
2. B generates pair of keys PB and SB

Week 7

Public Key Cryptography Basics

Two Communicants: A and B

1. A generates pair of keys PA and SA
2. B generates pair of keys PB and SB
3. Properties:

$$\{\{ m \}_{PA} \}_{SA} = m$$
$$\{\{ m \}_{SA} \}_{PA} = m$$
$$\{\{ m \}_{PA} \}_{X} = m \Rightarrow (X = SA)$$
$$\{\{ m \}_{SA} \}_{X} = m \Rightarrow (X = PA)$$

Concept proposed by Whit Diffie and Marty Hellman, Stanford and Ralph Merkle, UC Berkeley – circa 1976

Week 7

Public Key Cryptography Basics

Two Communicants: A and B

1. A generates pair of keys PA and SA
2. B generates pair of keys PB and SB
3. Properties:

$$\{\{ m \}_{PA} \}_{SA} = m$$
$$\{\{ m \}_{SA} \}_{PA} = m$$
$$\{\{ m \}_{PA} \}_{X} = m \Rightarrow (X = SA)$$
$$\{\{ m \}_{SA} \}_{X} = m \Rightarrow (X = PA)$$

Concept proposed by Whit Diffie and Marty Hellman, Stanford and Ralph Merkle, UC Berkeley – circa 1976

Requirements:

(i) Keep SA, SB secret to A, B
(ii) Make PA, PB public to all
(iii) No KDC required to generate keys

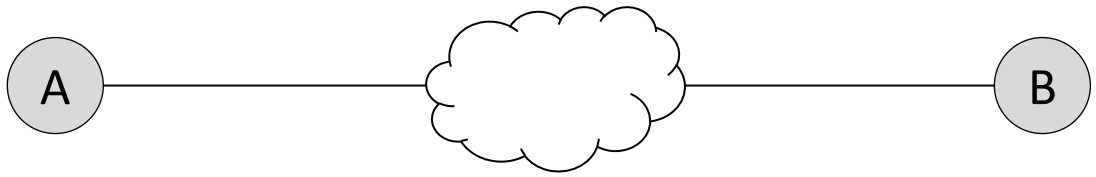
*"**Address Scaling Issue**"*

Week 7

Understanding Public Key Technology

"Assume A is a client"

"Assume B is a server"



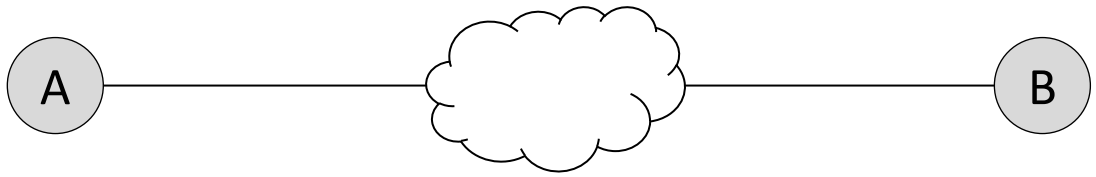
Week 7

Understanding Public Key Technology

No Key Distribution Center (KDC) Required

"Assume A is a client"

"Assume B is a server"



User A Locally Generates Key Pair:

PA: Public Key of A
SA: Secret Key of A

User B Locally Generates Key Pair:

PB: Public Key of B
SB: Secret Key of B

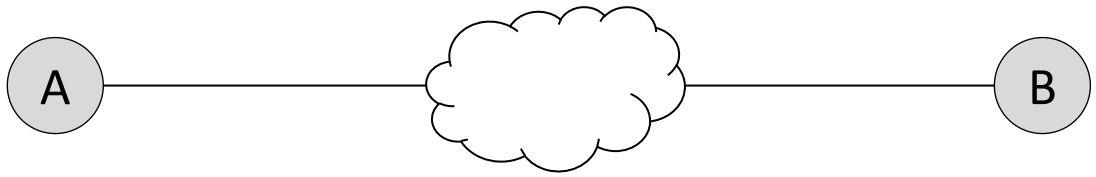
Week 7

Understanding Public Key Technology

No Key Distribution Center (KDC) Required

"Assume A is a client"

"Assume B is a server"



User A Locally Generates Key Pair:

PA: Public Key of A
SA: Secret Key of A

User B Locally Generates Key Pair:

PB: Public Key of B
SB: Secret Key of B

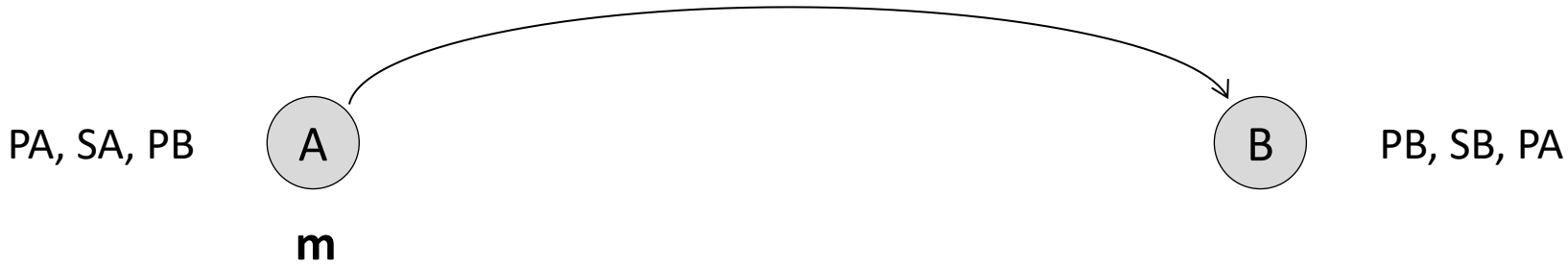
Common Key Generation Algorithm Required (e.g., RSA)

Public Key Infrastructure (PKI)

Week 7

Sending a Secret Message

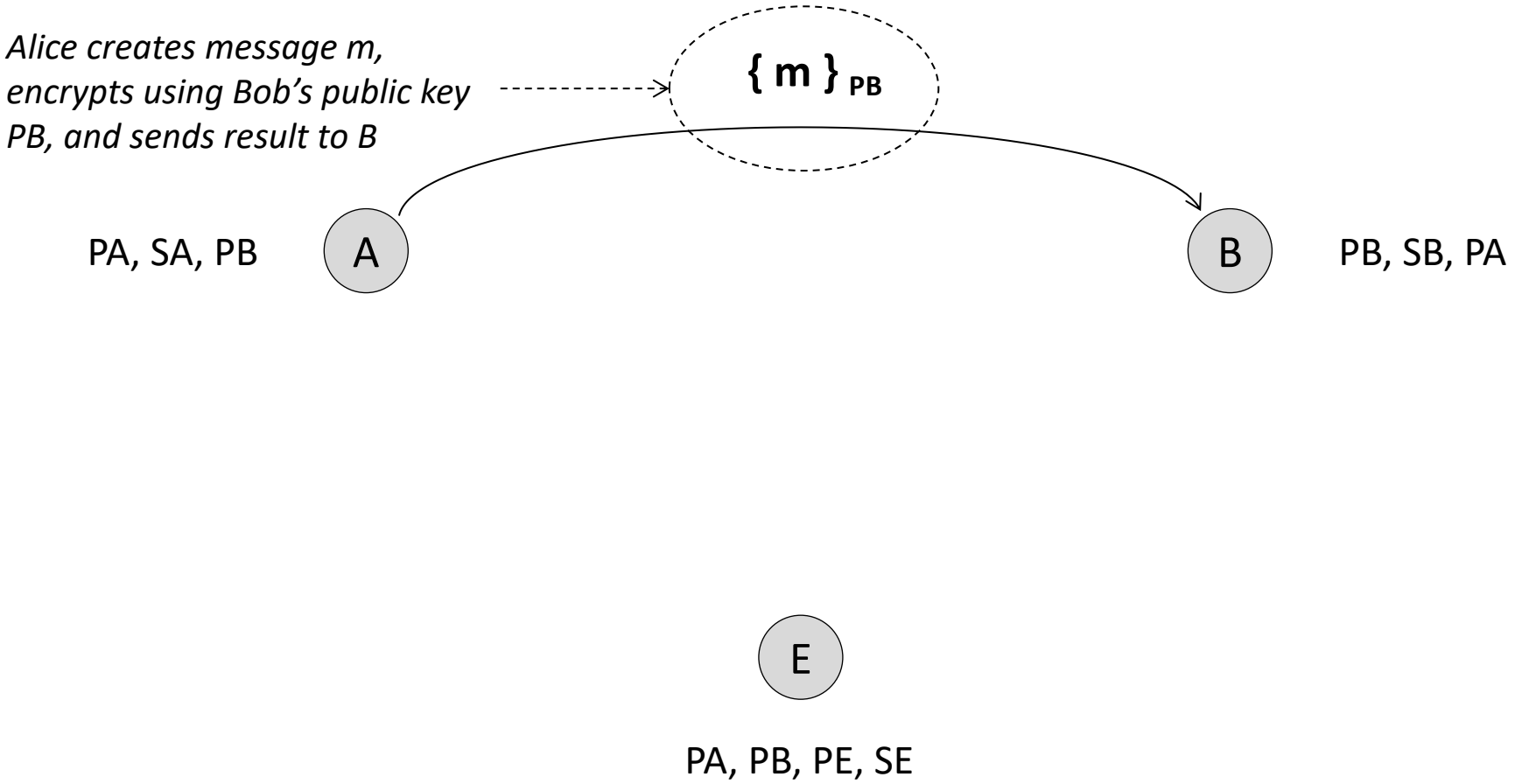
Alice creates message m . . .



PA, PB, PE, SE

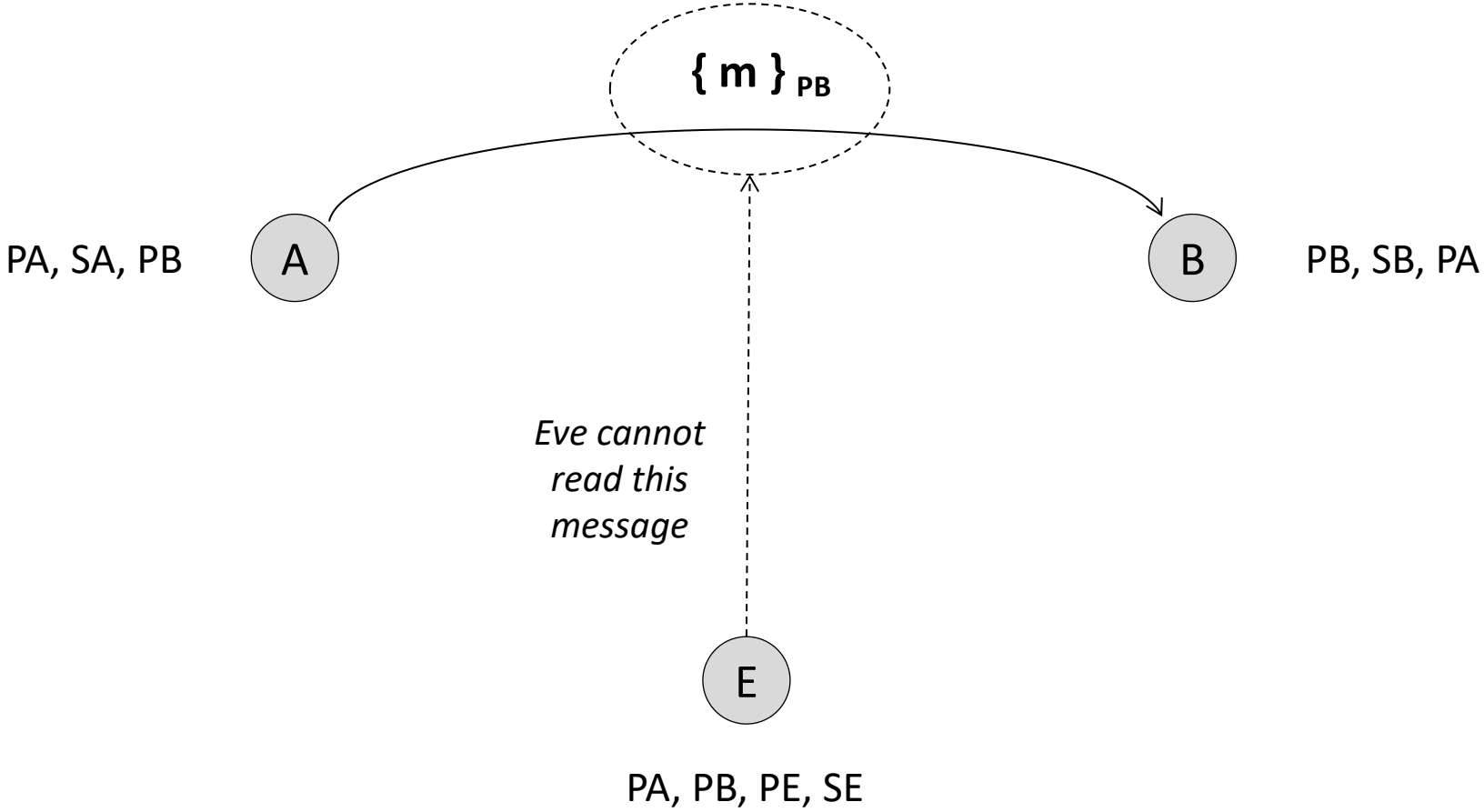
Week 7

Sending a Secret Message



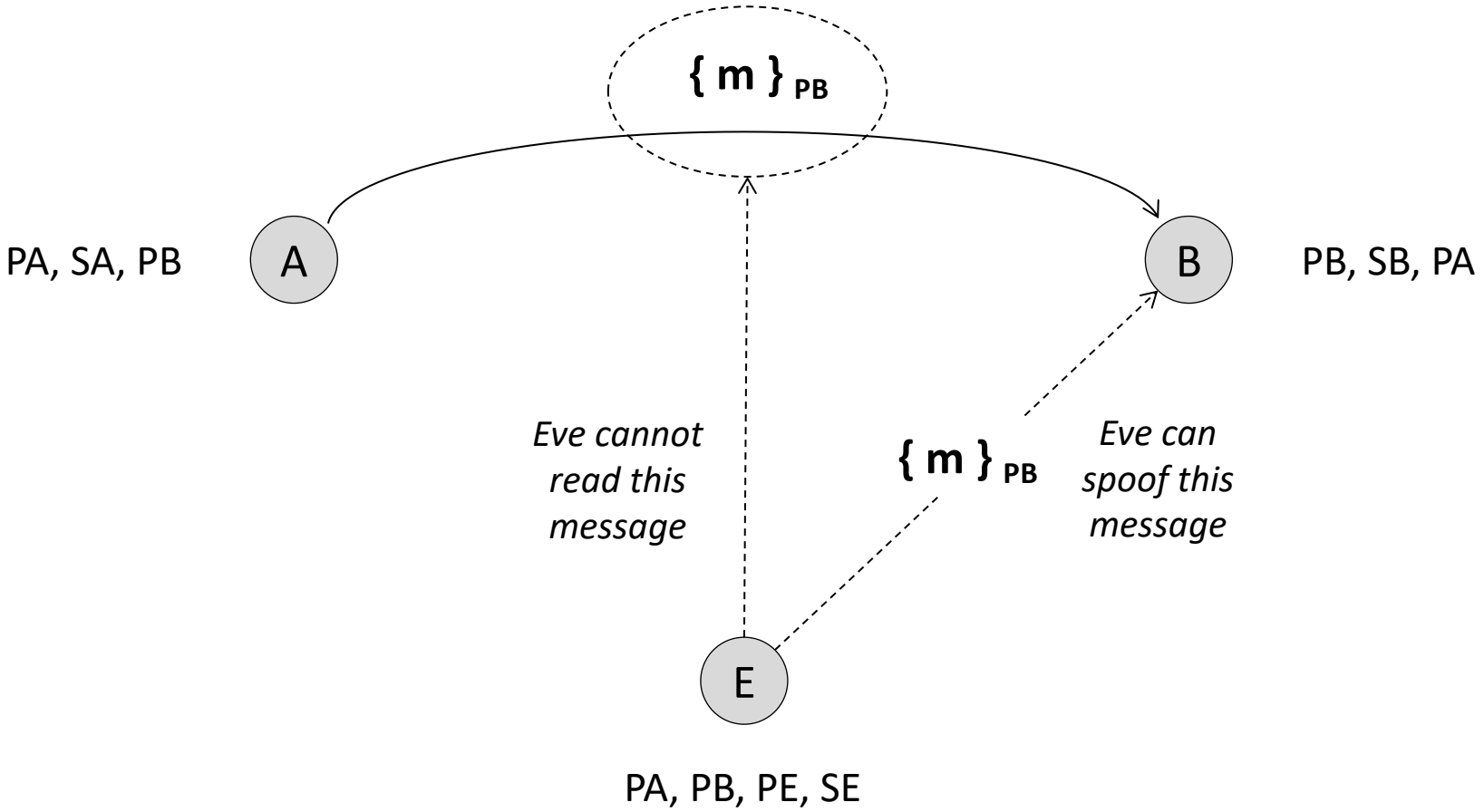
Week 7

Sending a Secret Message



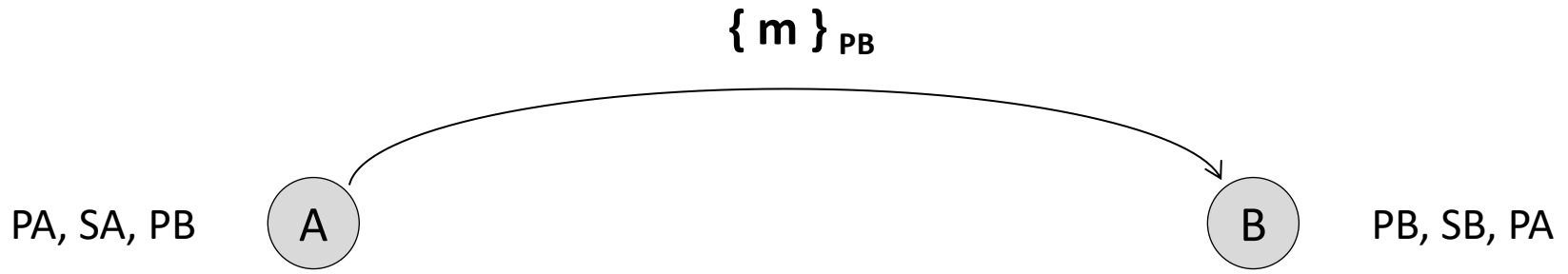
Week 7

Sending a Secret Message



Week 7

Sending a Secret Message



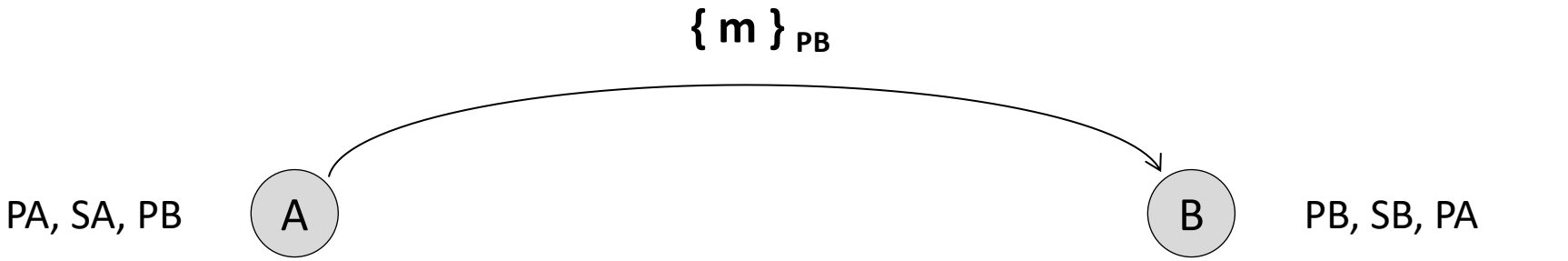
$\{ \{ m \}_{PB} \}_{SB} = m$

Bob receives the encrypted message, decrypts using Bob's secret key SB, and obtains message m

PA, PB, PE, SE

Week 7

Sending a Secret Message



Secrecy Between A and B? **YES**
Authentication of A by B? **NO**

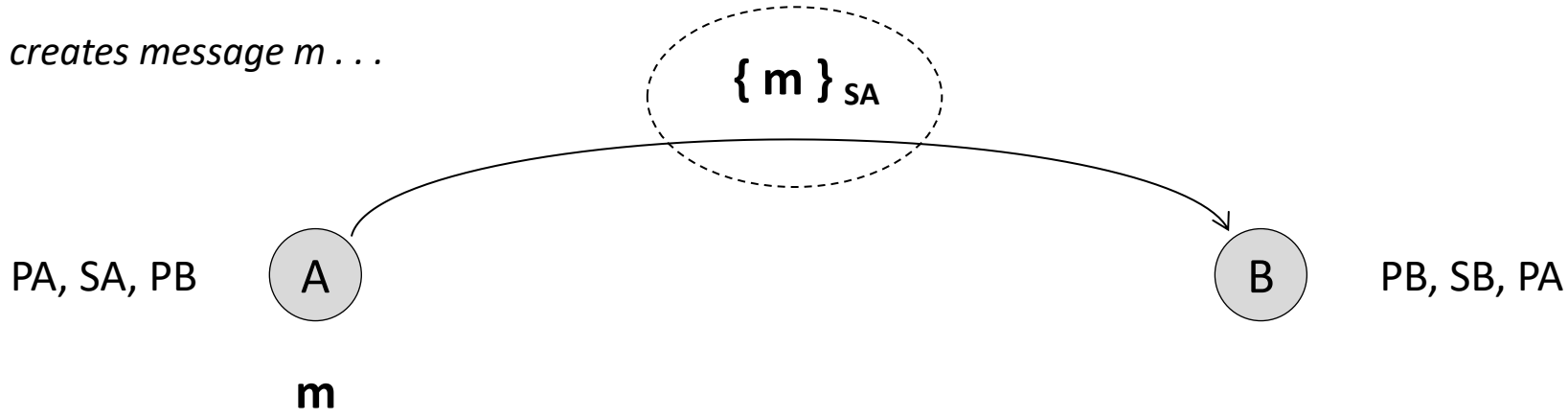
$\{ \{ m \}_{PB} \}_{SB} = m$

PA, PB, PE, SE

Week 7

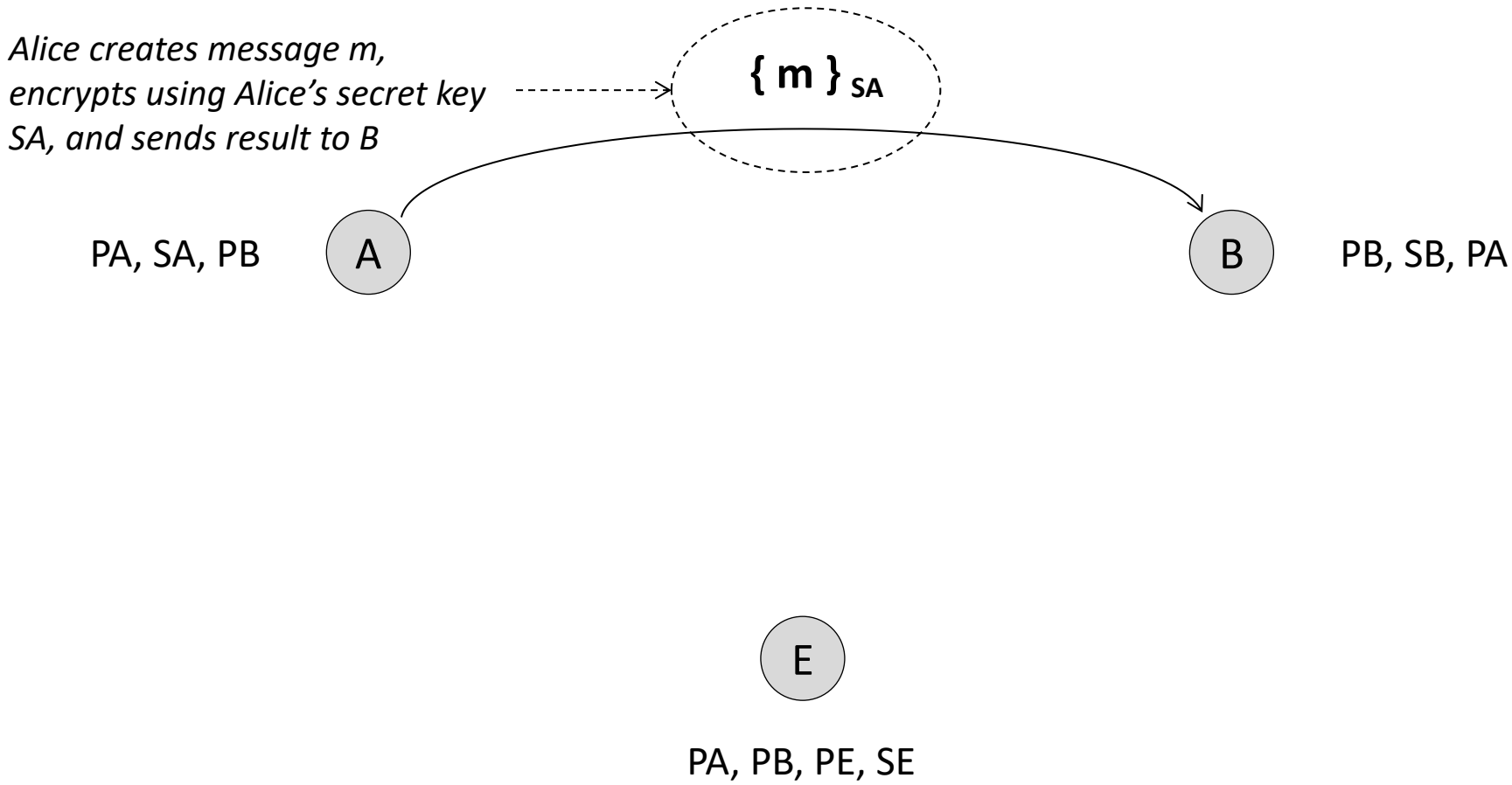
Sending a Signed Message

Alice creates message m . . .



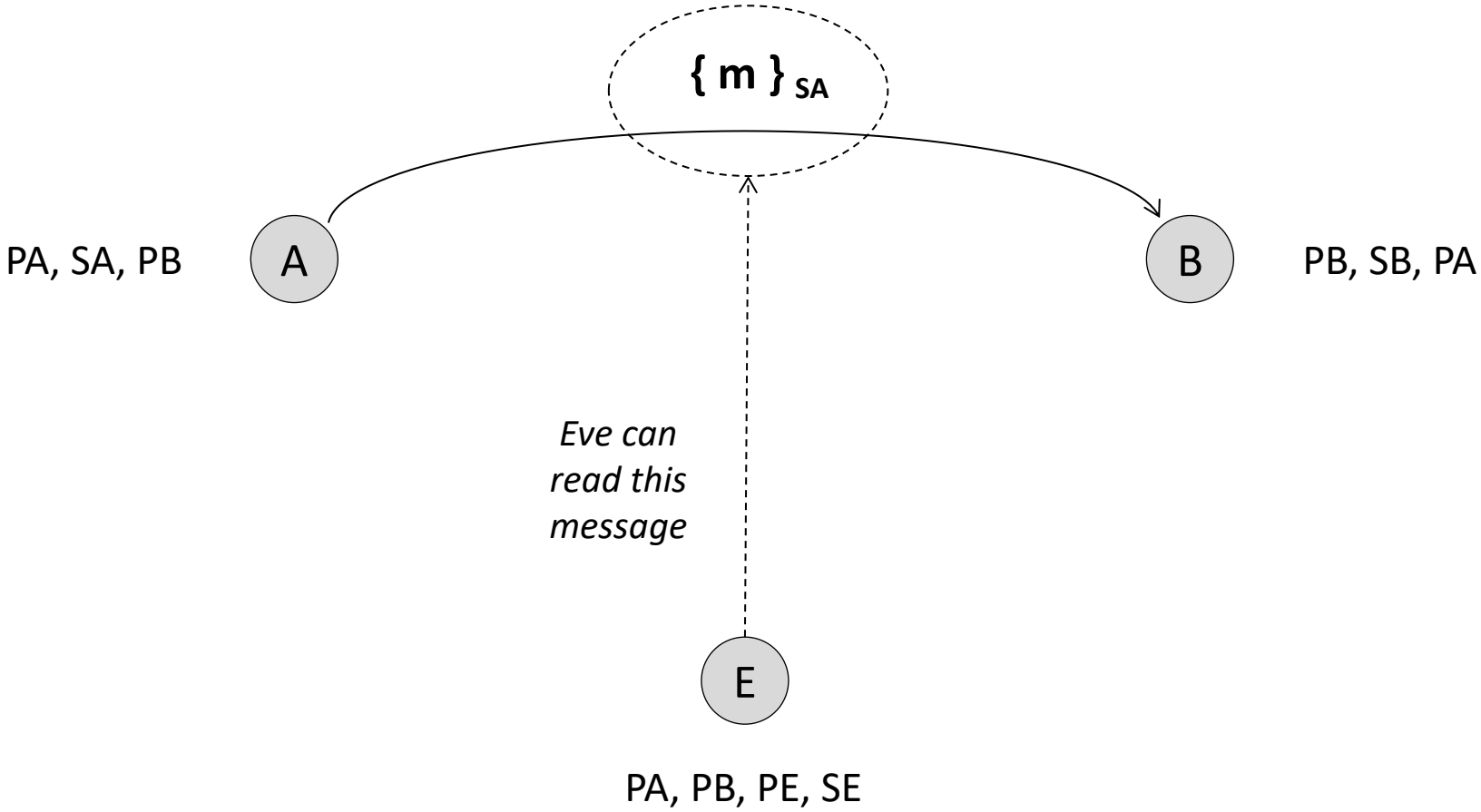
Week 7

Sending a Signed Message



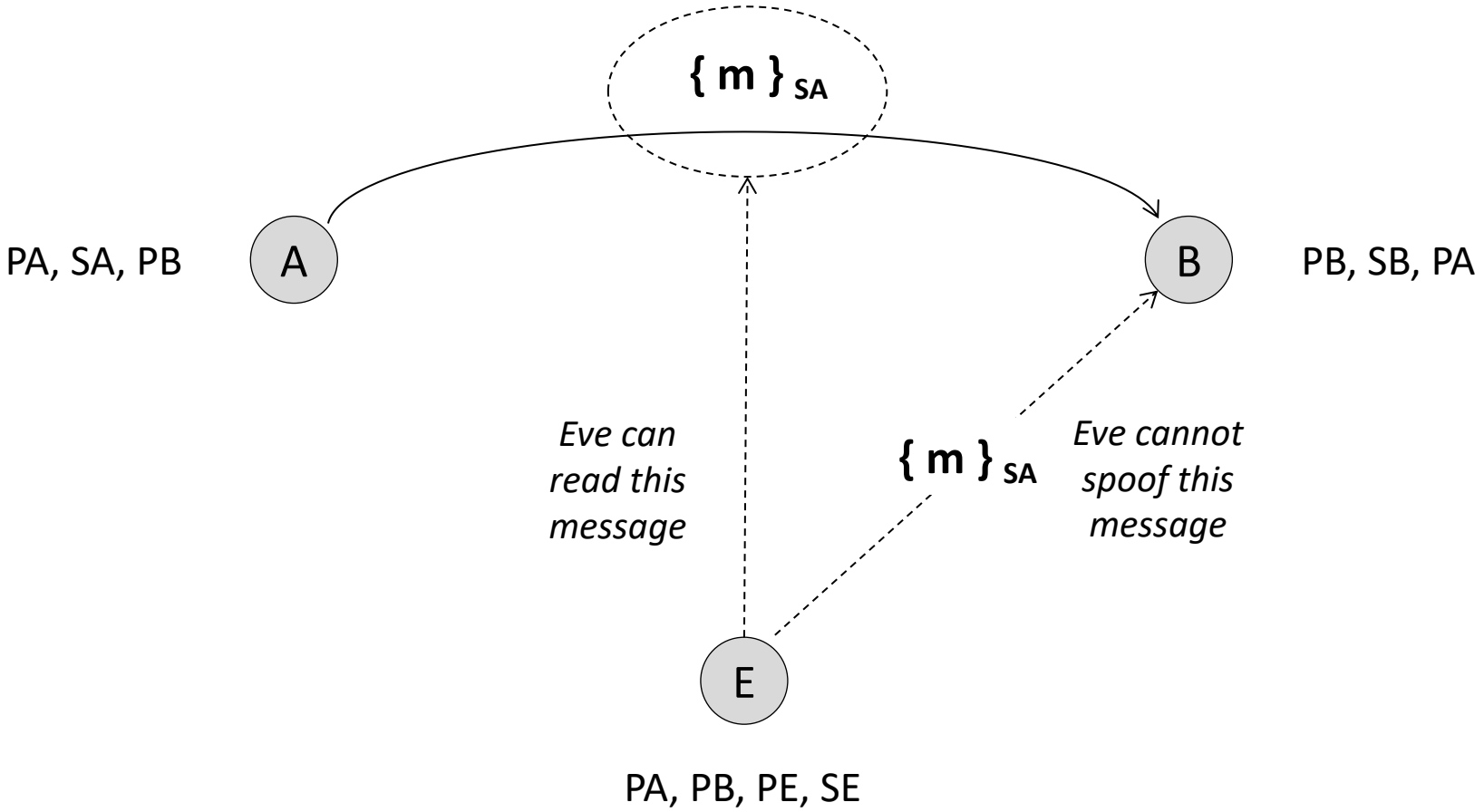
Week 7

Sending a Signed Message



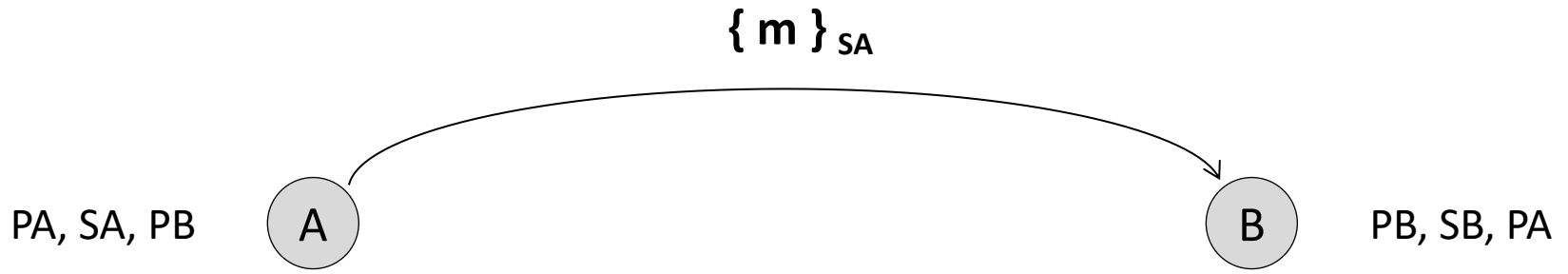
Week 7

Sending a Signed Message



Week 7

Sending a Signed Message



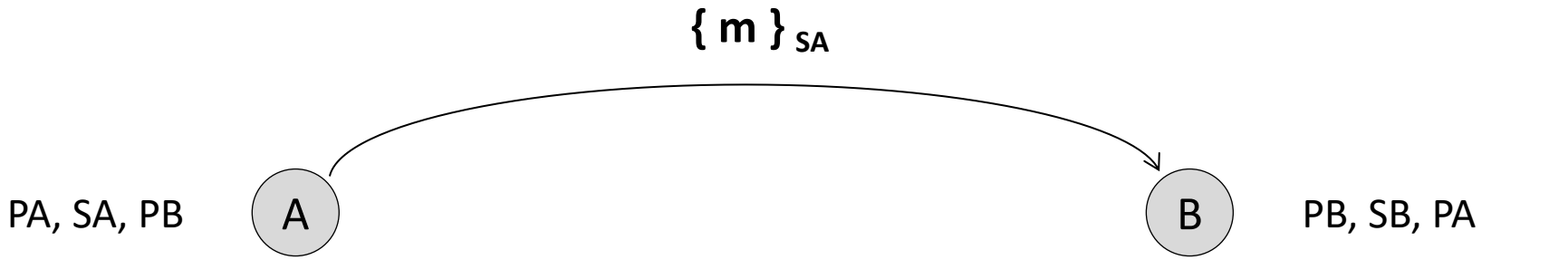
$\{\{ m \}_{SA}\}_{PA} = m$

Bob receives the encrypted message, decrypts using Alice's public key PA, and obtains message m

PA, PB, PE, SE

Week 7

Sending a Signed Message



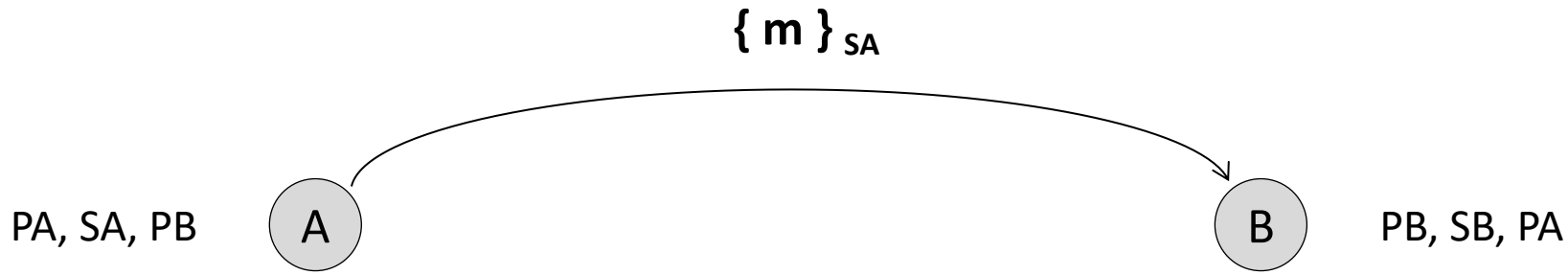
{ { m } SA }PA = m

Secrecy Between A and B? **NO**
Authentication of A by B? **YES**

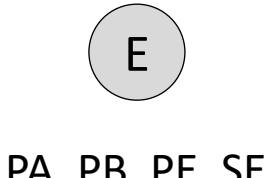
PA, PB, PE, SE

Week 7

Secure Message Exchange

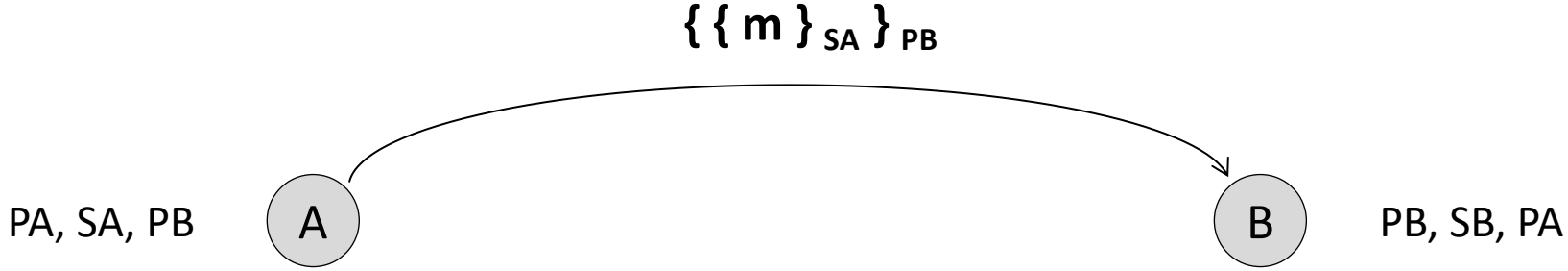


Alice creates a message m,
encrypts it with a public key algorithm
using her secret key SA . . .



Week 7

Secure Message Exchange

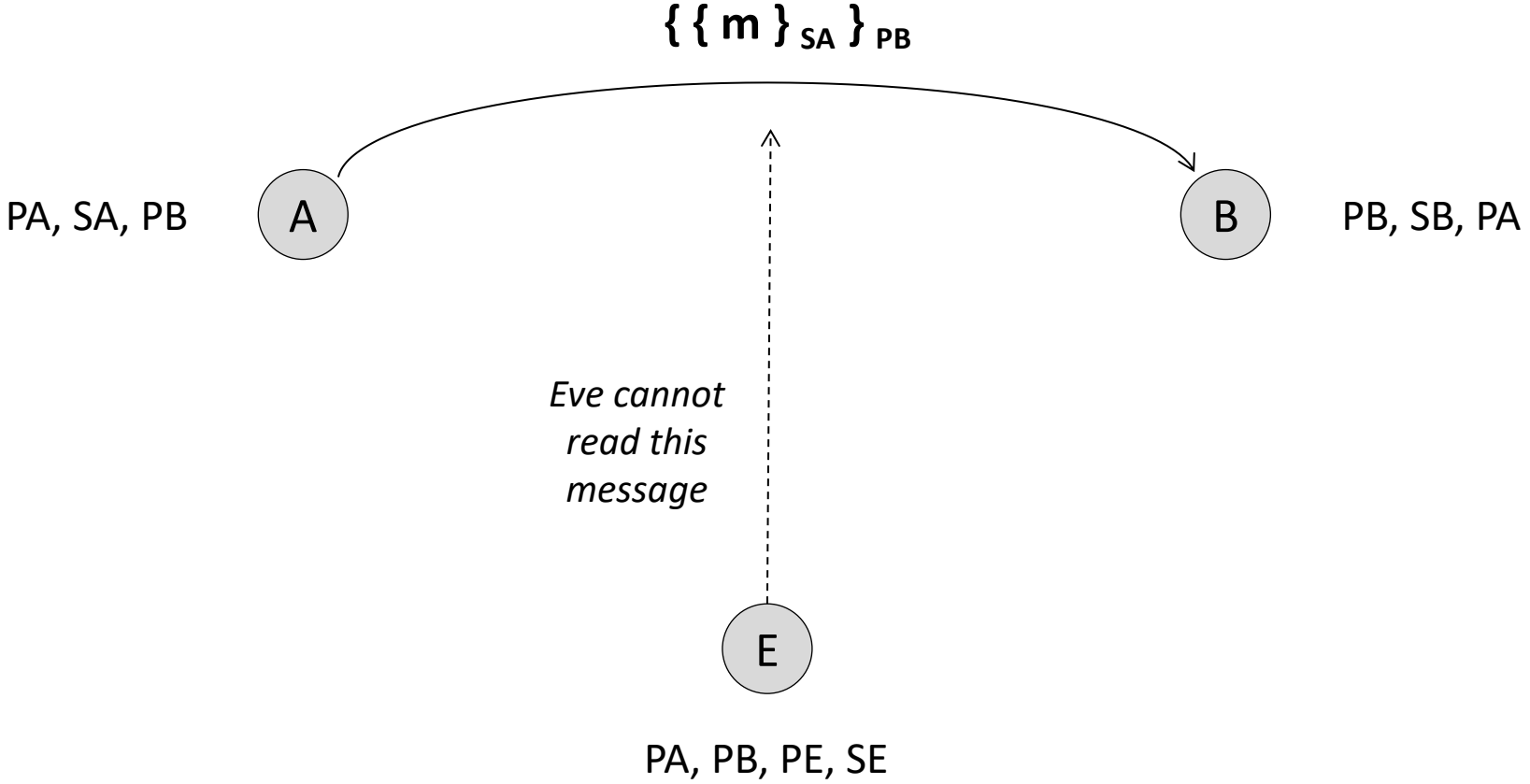


Alice creates a message m,
encrypts it with a public key algorithm
using her secret key SA, encrypts it again
using a public key algorithm with Bob's
public key PB, and sends the result to Bob

PA, PB, PE, SE

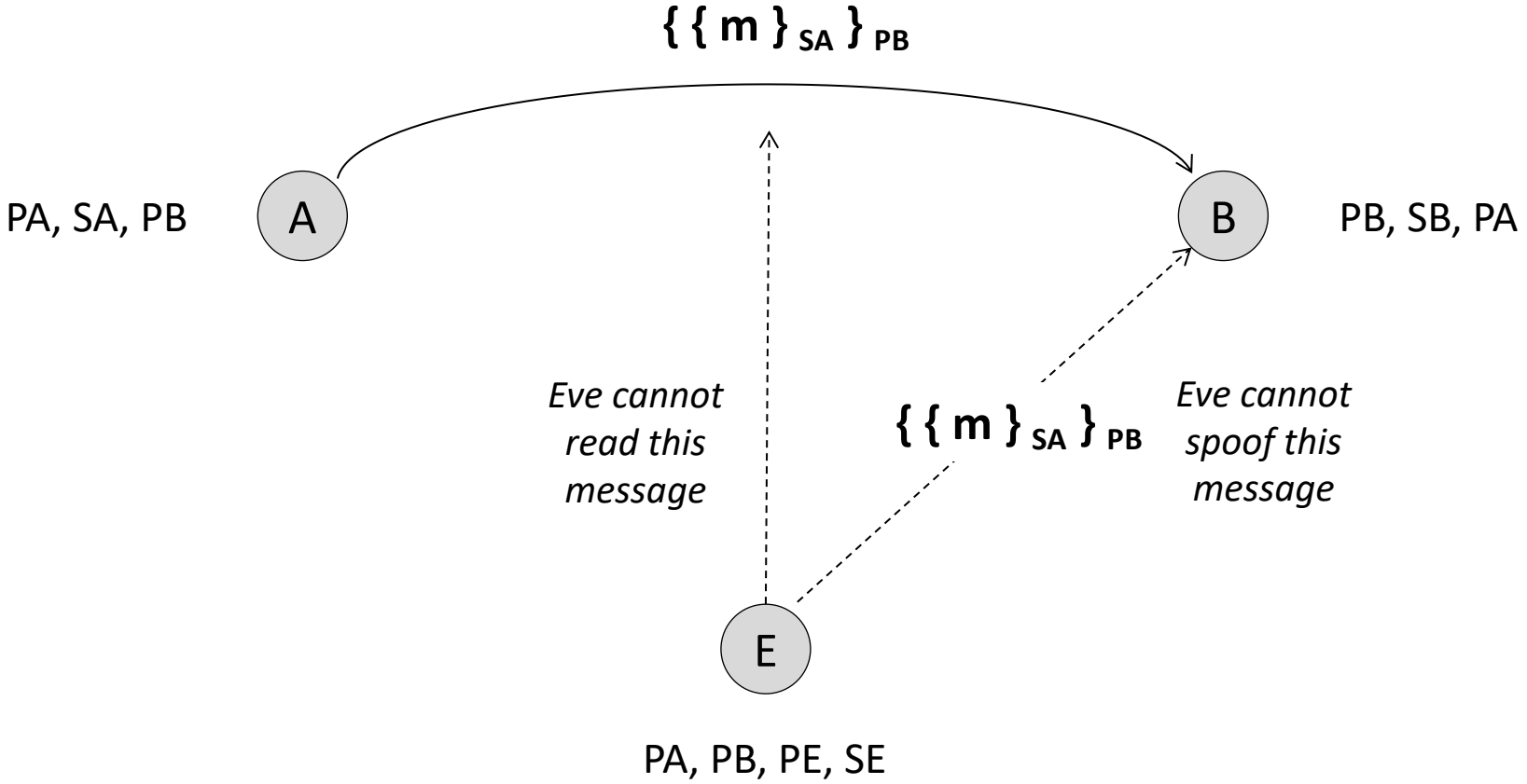
Week 7

Secure Message Exchange



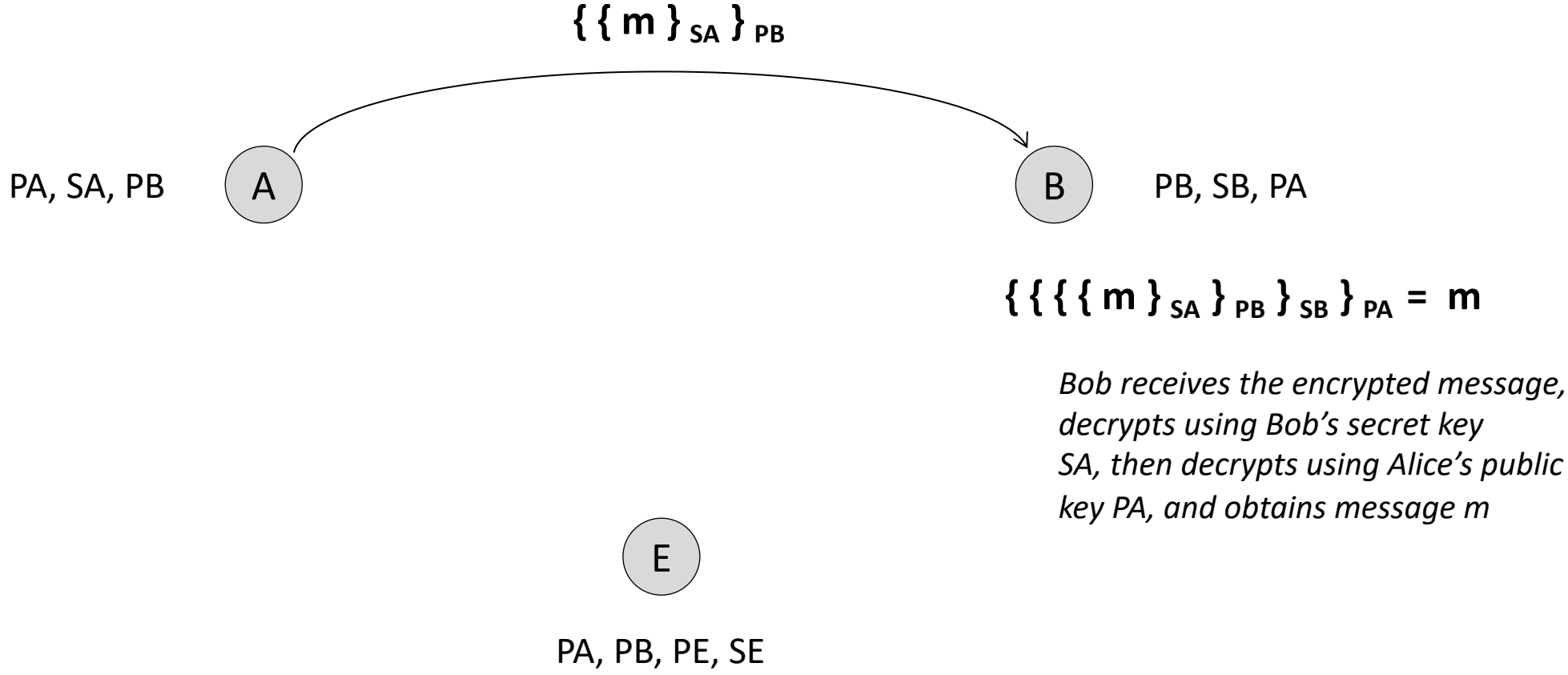
Week 7

Secure Message Exchange



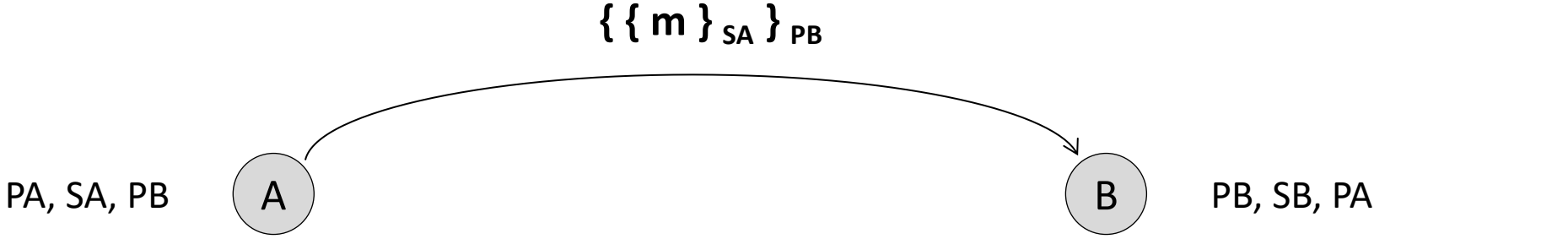
Week 7

Secure Message Exchange



Week 7

Secure Message Exchange

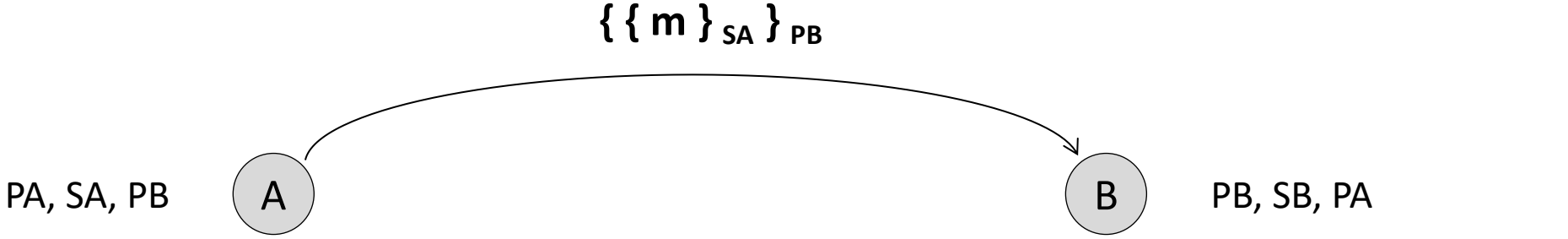


Secrecy Between A and B? **YES**
Authentication of A by B? **YES**

$\{\{\{\{m\}_{SA}\}_{PB}\}_{SB}\}_{PA} = m$

Week 7

Secure Message Exchange



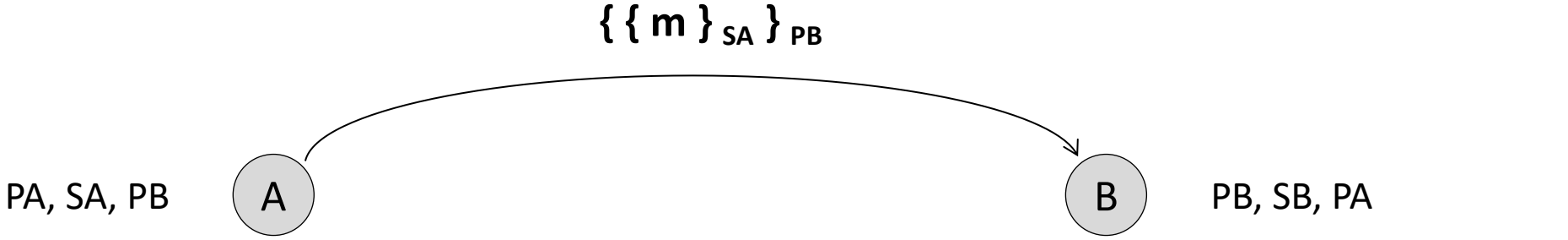
Secrecy Between A and B? **YES**
Authentication of A by B? **YES**

$\{\{\{\{m\}_{SA}\}_{PB}\}_{SB}\}_{PA} = m$

Does this approach scale? **YES**

Week 7

Secure Message Exchange



Secrecy Between A and B? **YES**
Authentication of A by B? **YES**

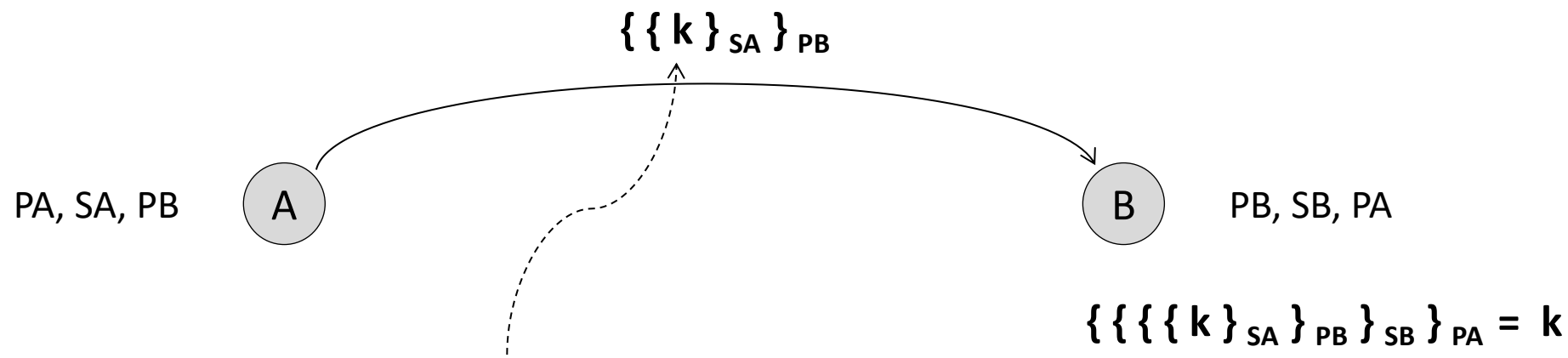
$\{\{\{\{m\}_{SA}\}_{PB}\}_{SB}\}_{PA} = m$

Does this approach scale? **YES**

Is this approach efficient (cryptographically)? **NO**

Week 7

Secure Key Exchange

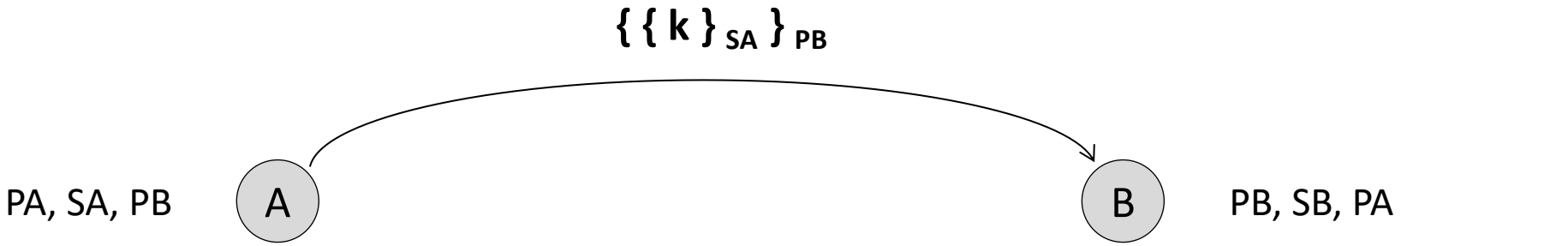


Alice generates a key k for some bulk encryption algorithm (like 3-DES) and provides this key to B using secure key exchange

- *Scalable*
- *Secret*
- *Authenticated*

Week 7

Secure Key Exchange



Secrecy Between A and B? **YES**
Authentication of A by B? **YES**

{ { { { k } SA } PB } SB } PA = k

Does this approach scale? **YES**

Is this approach efficient (cryptographically)? **YES**