

Week 7



STEVENS
INSTITUTE *of* TECHNOLOGY
THE INNOVATION UNIVERSITY®



An Introduction to Cyber Security – CS 573

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

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**

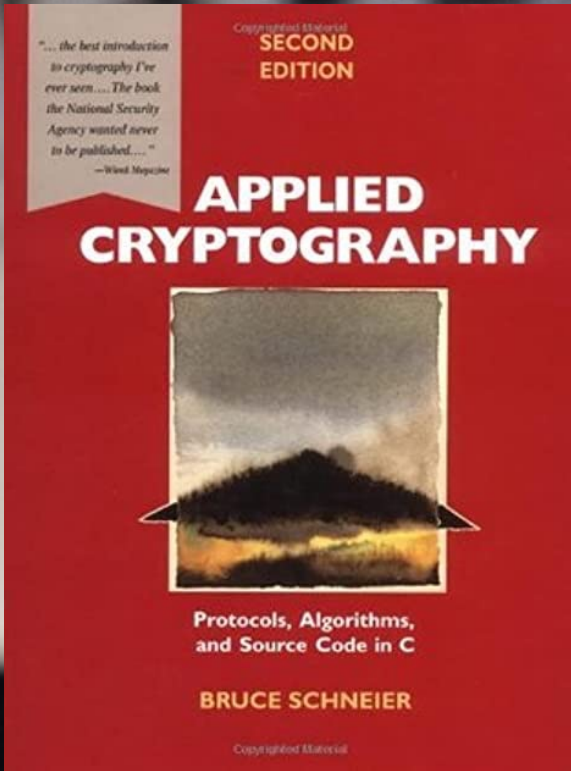
**Twitter: @hashtag_cyber
LinkedIn: Edward Amoroso**



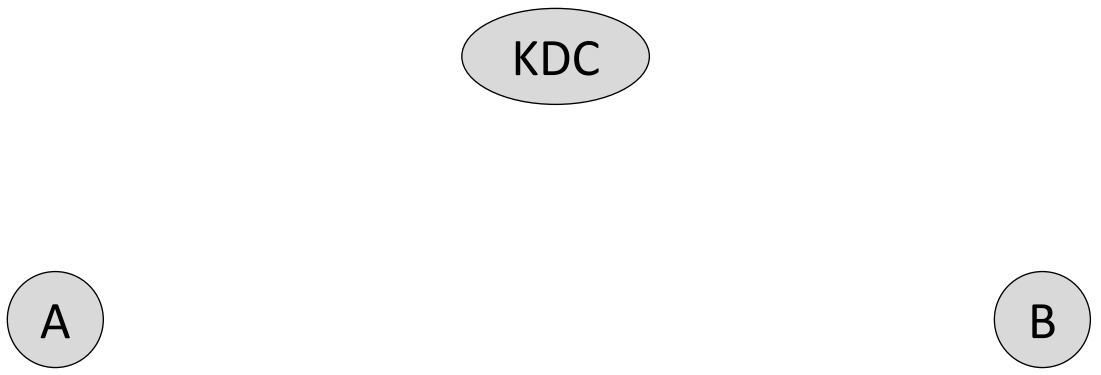
Week 7: Public Key Cryptography

What Properties of Conventional Cryptography
Must Be Maintained?

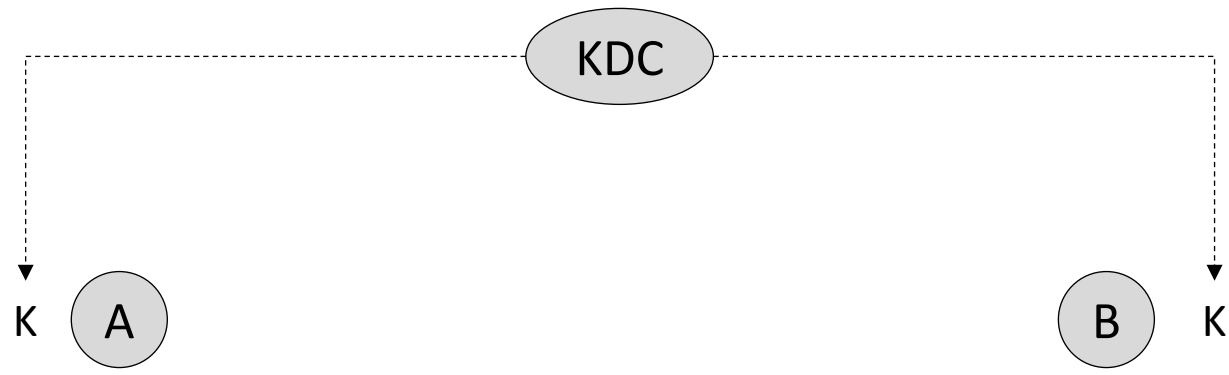
Week 7



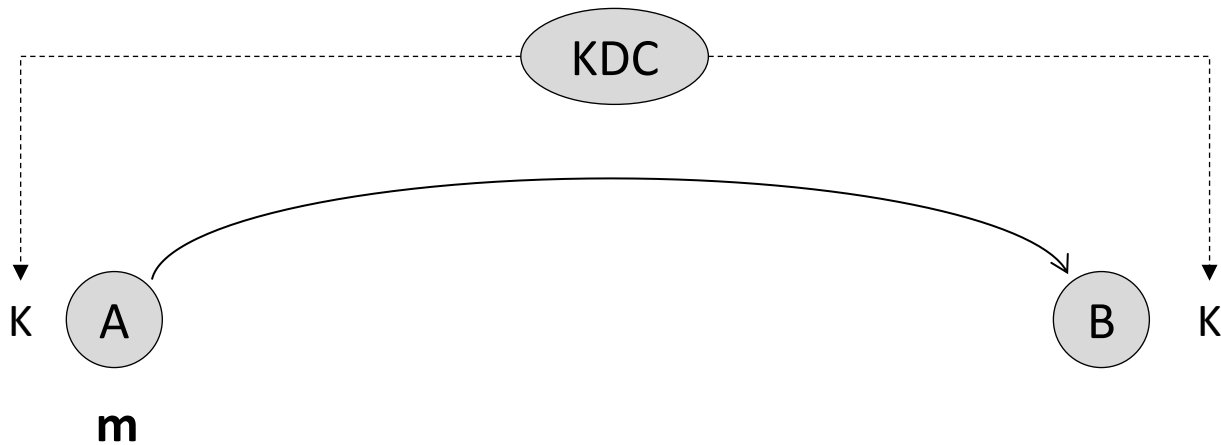
Conventional Cryptography



Conventional Cryptography

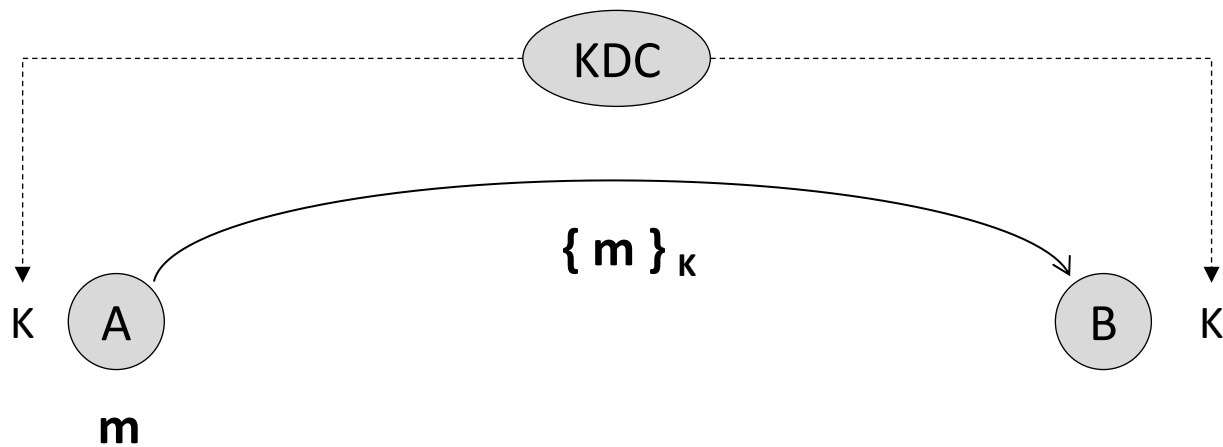


Conventional Cryptography



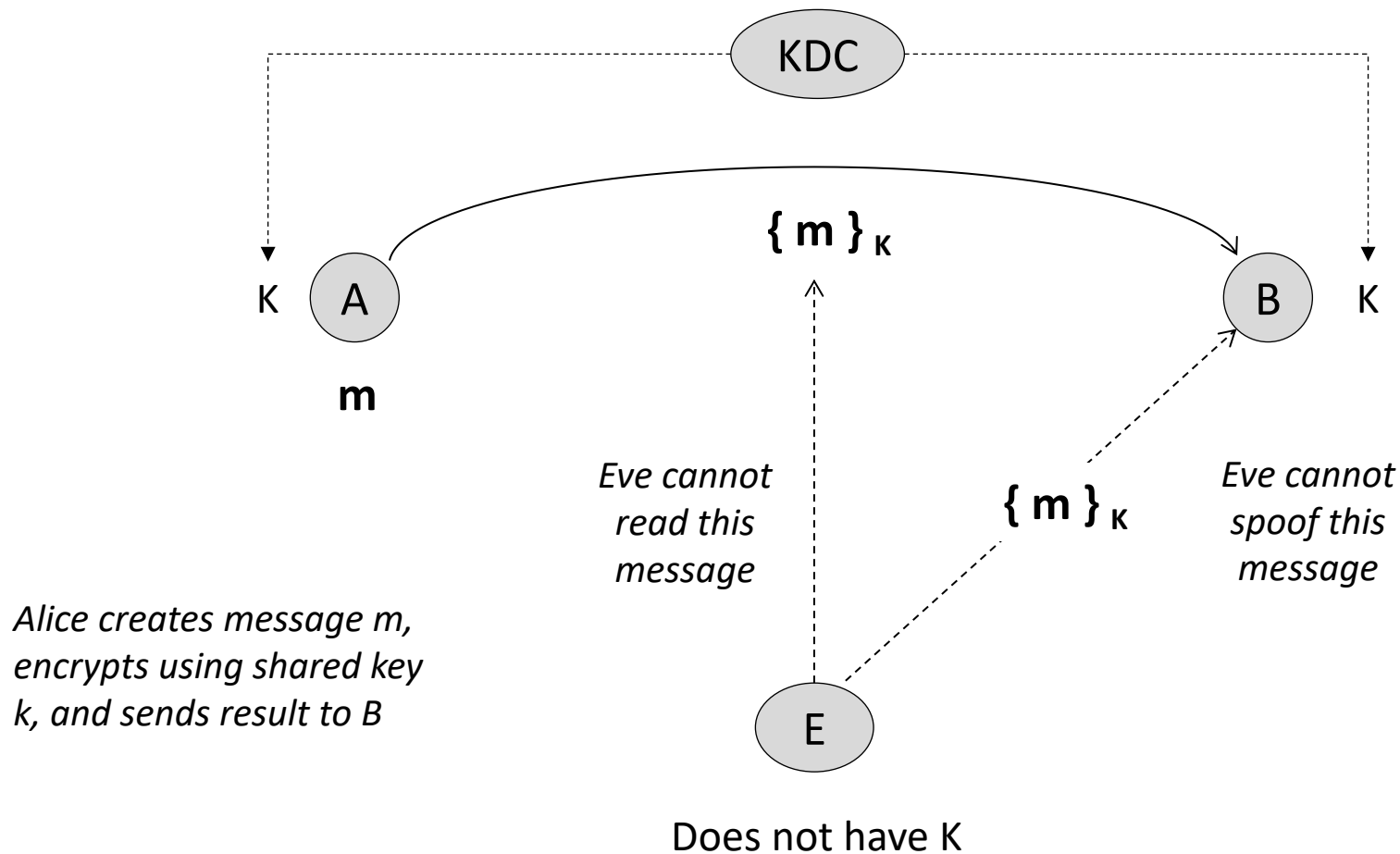
Alice creates message m . . .

Conventional Cryptography

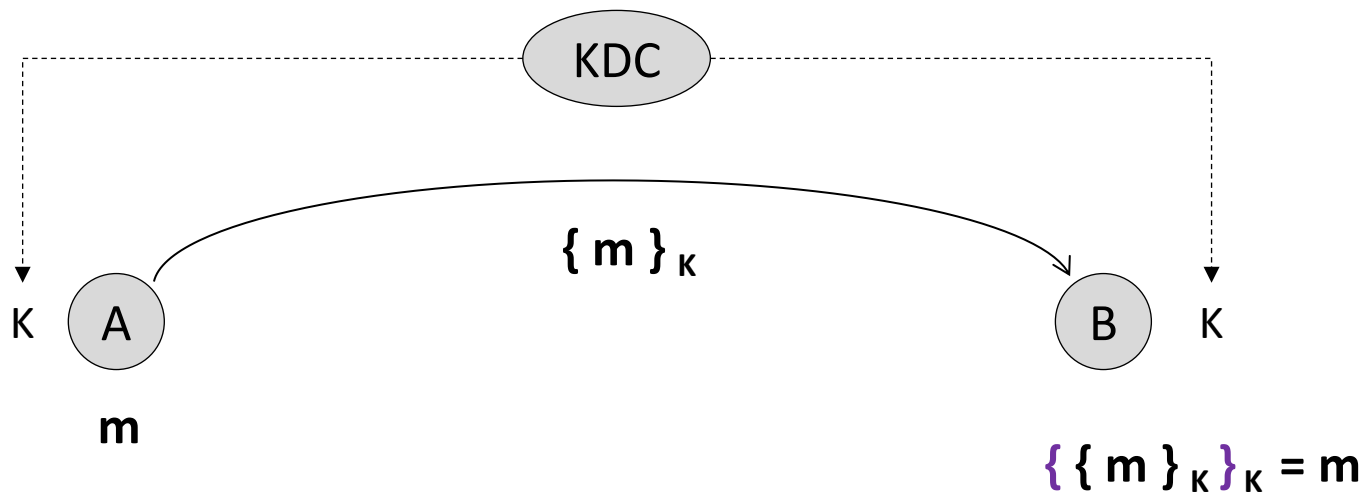


*Alice creates message m ,
encrypts using shared key
 k , and sends result to B*

Conventional Cryptography

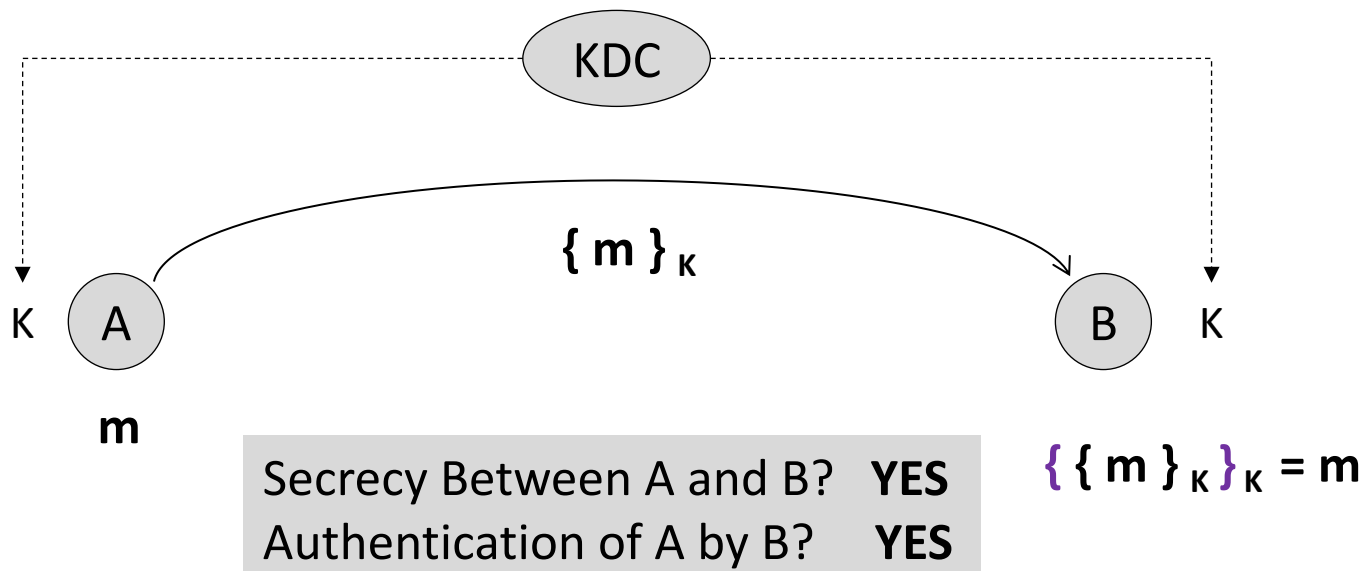


Conventional Cryptography

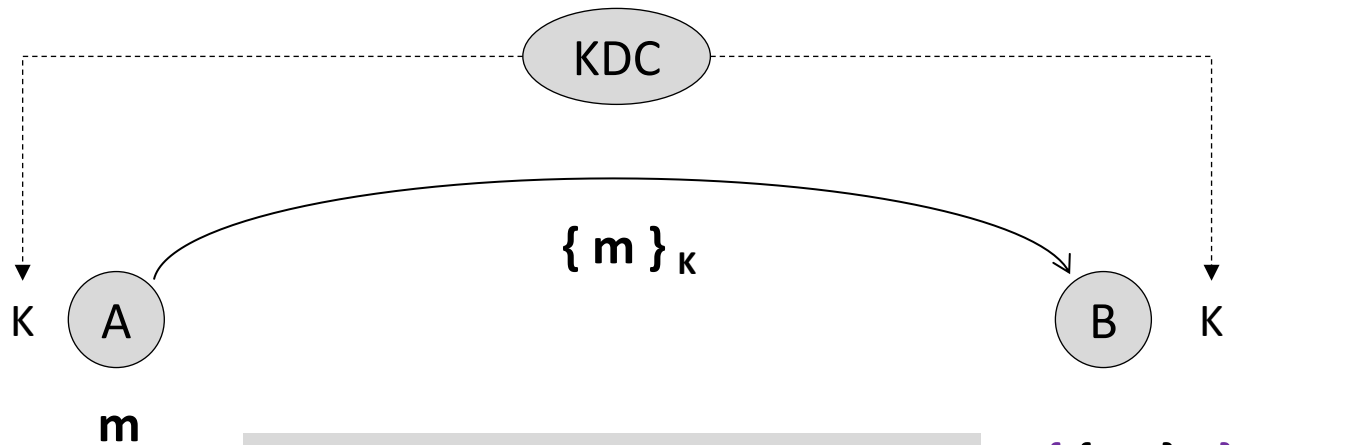


Bob receives encrypted message, and decrypts using shared key k , and obtains message m

Conventional Cryptography



Conventional Cryptography



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

Does this approach scale? **NO**

What are the Basic Properties of
Public Key Cryptography?

Public Key Cryptography Basics

Two Communicants: A and B

1. A generates pair of keys P_A and S_A
2. B generates pair of keys P_B and S_B

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*



Public Key Cryptography Basics

Two Communicants: A and B

1. A generates pair of keys P_A and S_A
2. B generates pair of keys P_B and S_B
3. Properties:

$$\{ \{ m \}_{P_A} \}_{S_A} = m$$

$$\{ \{ m \}_{S_A} \}_{P_A} = m$$

$$\{ \{ m \}_{P_A} \}_X = m \Rightarrow (X = S_A)$$

$$\{ \{ m \}_{S_A} \}_X = m \Rightarrow (X = P_A)$$

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

Requirements:

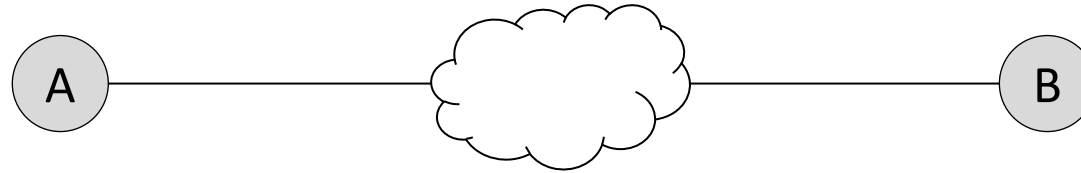
- (i) Keep S_A , S_B secret to A, B
- (ii) Make P_A , P_B public to all
- (iii) No KDC required to generate keys

“Address Scaling Issue”



Understanding Public Key Technology

*“Assume A
is a client”*



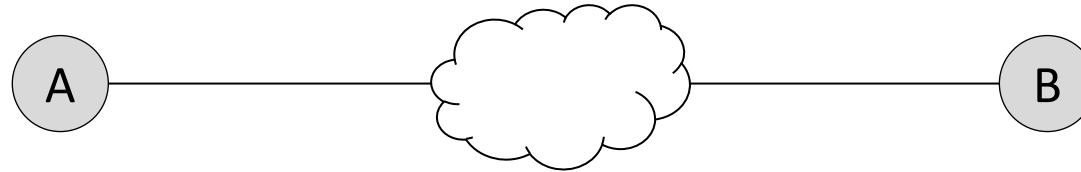
*“Assume B
is a server”*

Understanding Public Key Technology

*"Assume A
is a client"*

*No Key Distribution
Center (KDC) Required*

*"Assume B
is a server"*



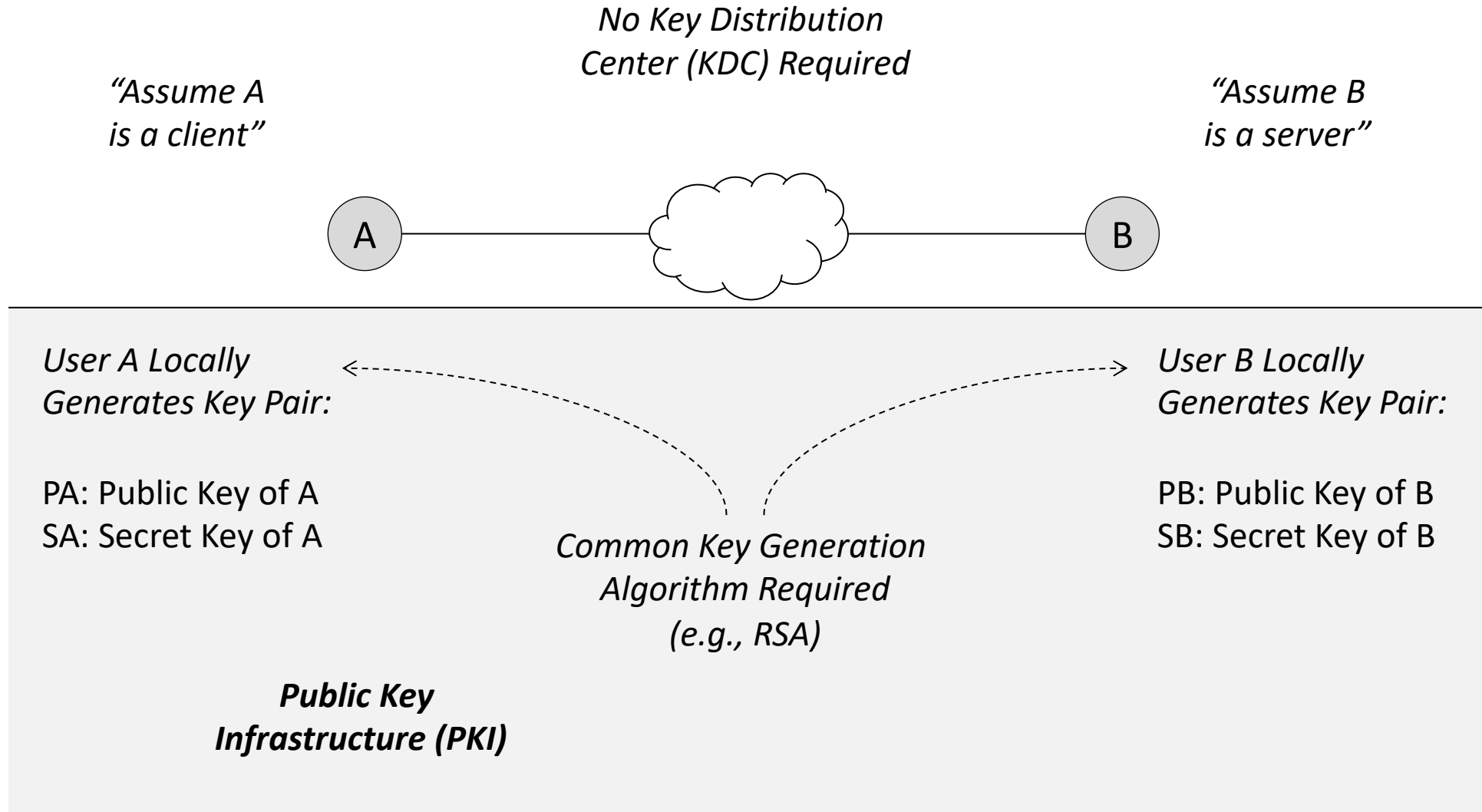
*User A Locally
Generates Key Pair:*

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

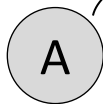
Understanding Public Key Technology



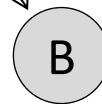
Sending a Secret Message

Alice creates message m . . .

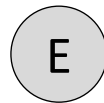
PA, SA, PB



m



PB, SB, PA

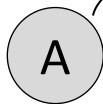


PA, PB, PE, SE

Sending a Secret Message

*Alice creates message m ,
encrypts using Bob's public key
 PB , and sends result to B*

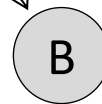
PA, SA, PB



$\{ m \}_{PB}$

B

PB, SB, PA

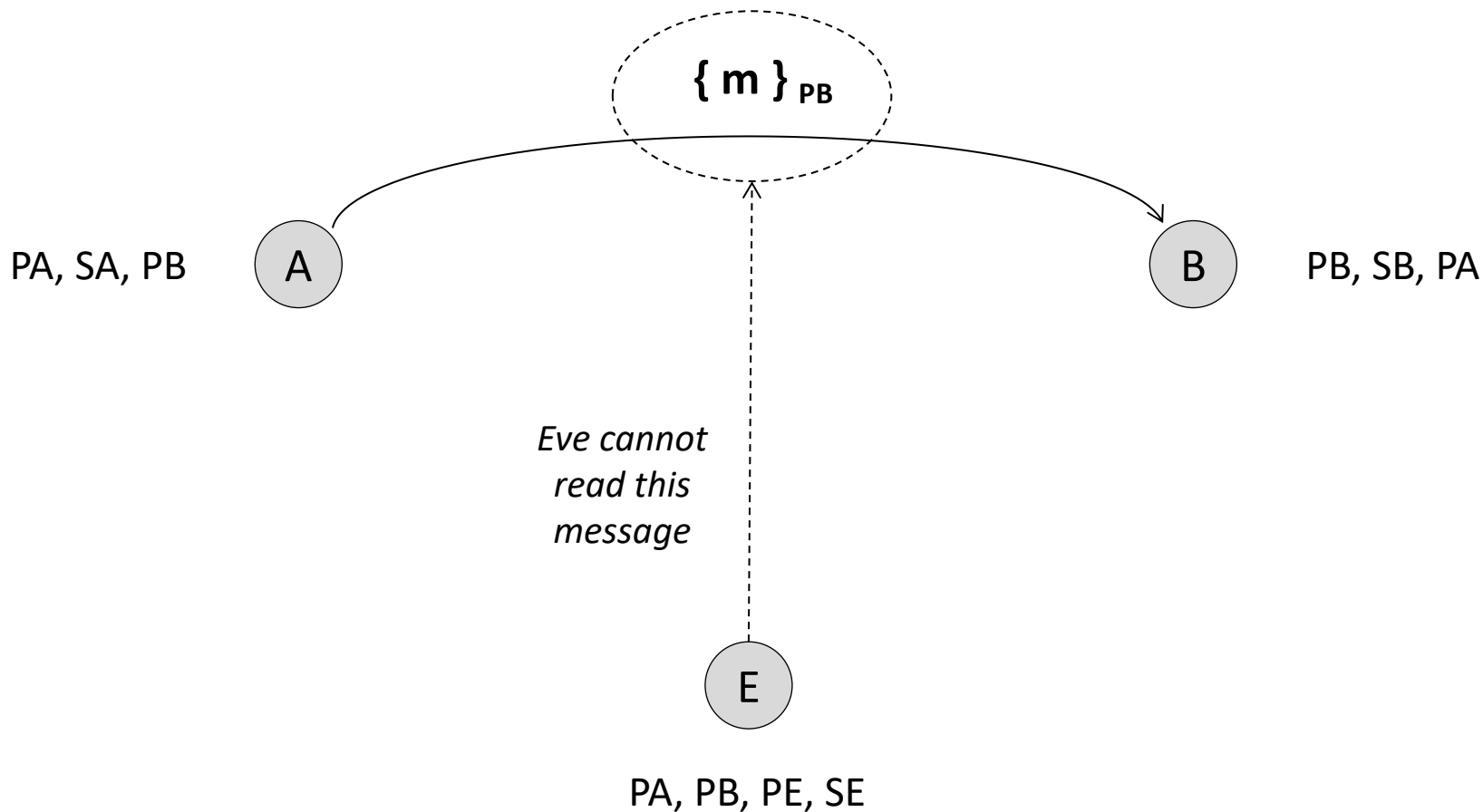


E

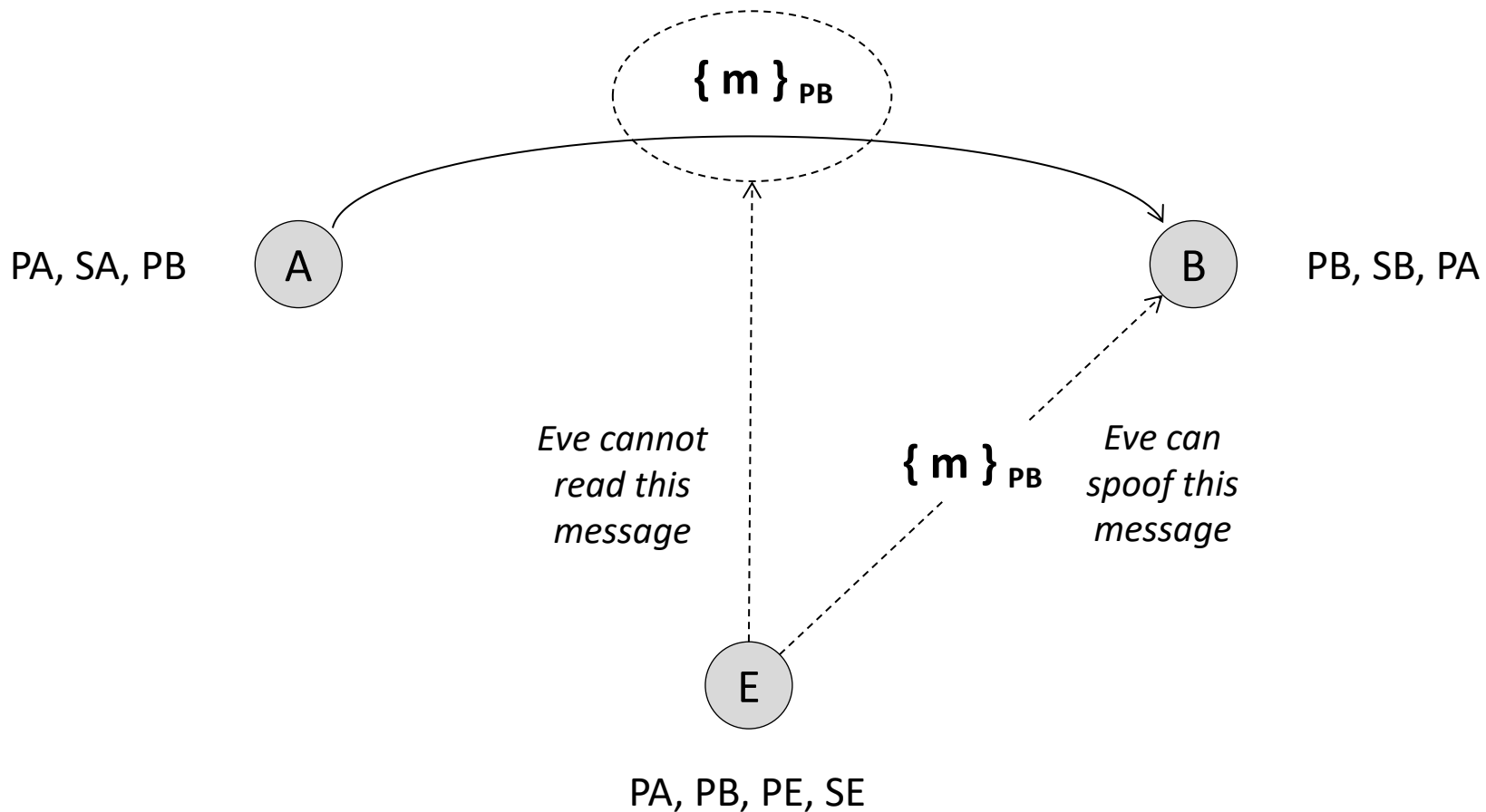
PA, PB, PE, SE



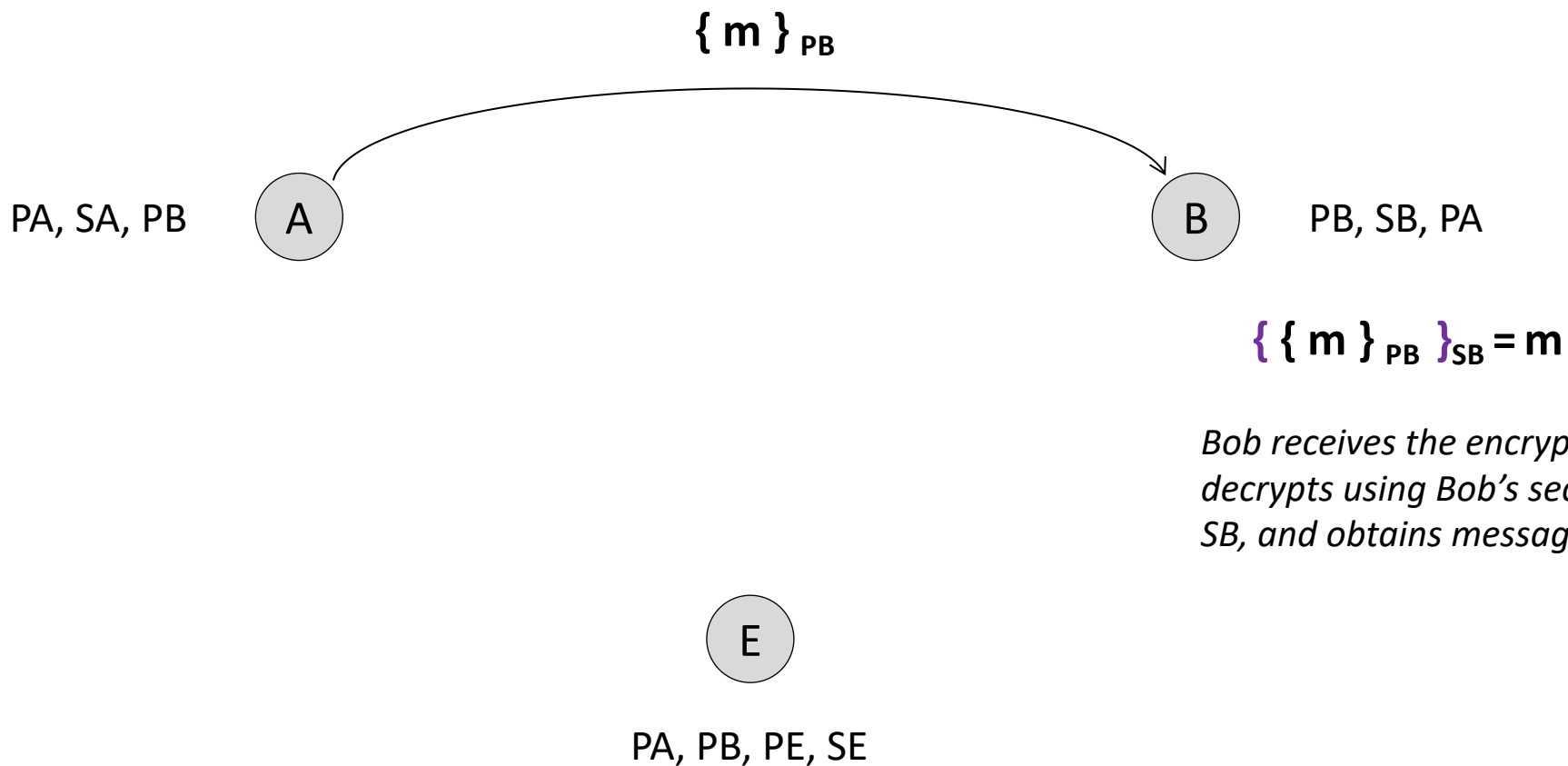
Sending a Secret Message



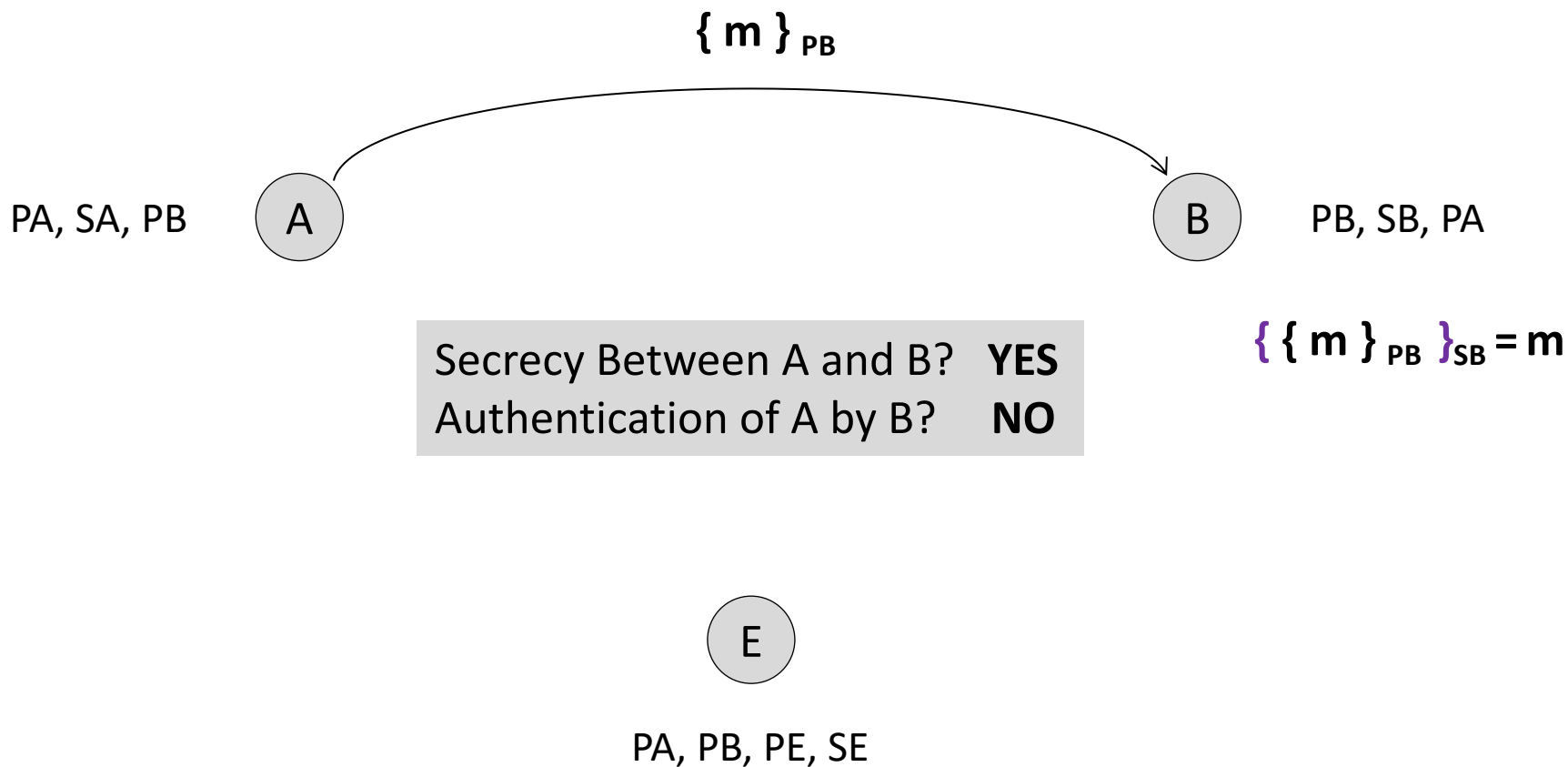
Sending a Secret Message



Sending a Secret Message

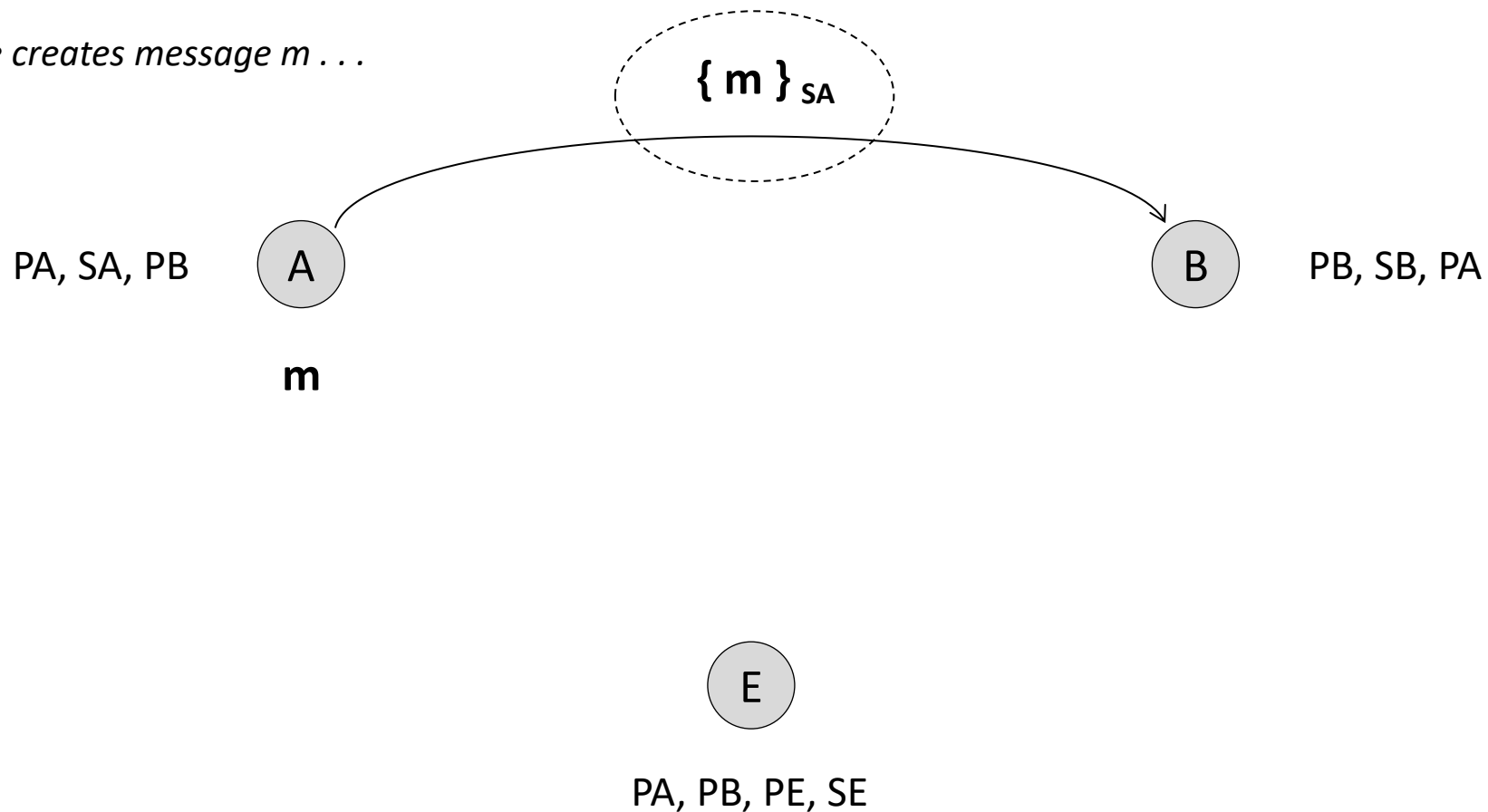


Sending a Secret Message



Sending a Signed Message

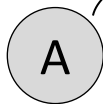
Alice creates message m . . .



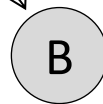
Sending a Signed Message

*Alice creates message m ,
encrypts using Alice's secret key
 SA , and sends result to B*

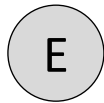
PA, SA, PB



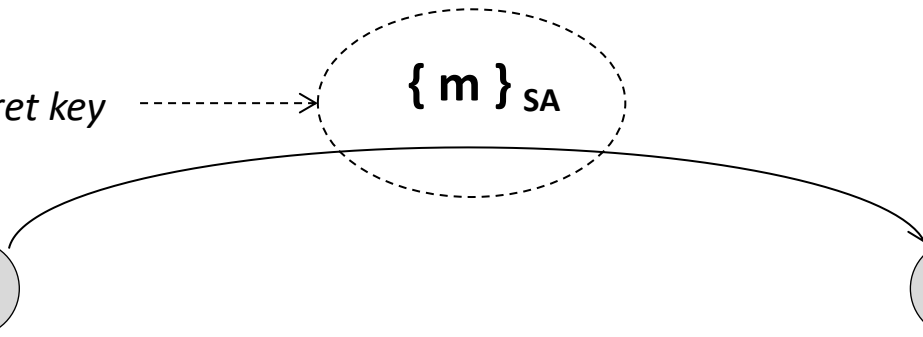
$\{ m \}_{SA}$



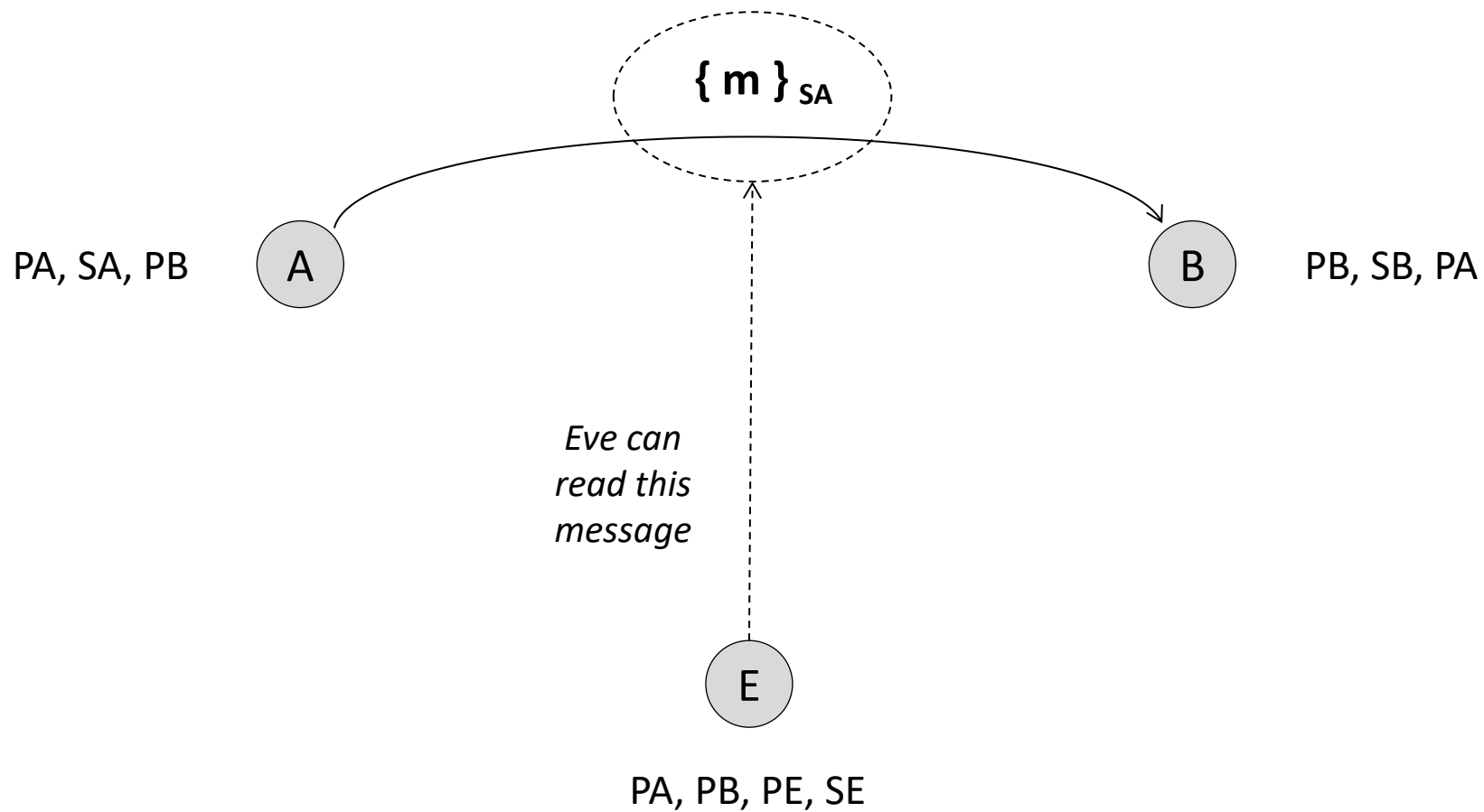
PB, SB, PA



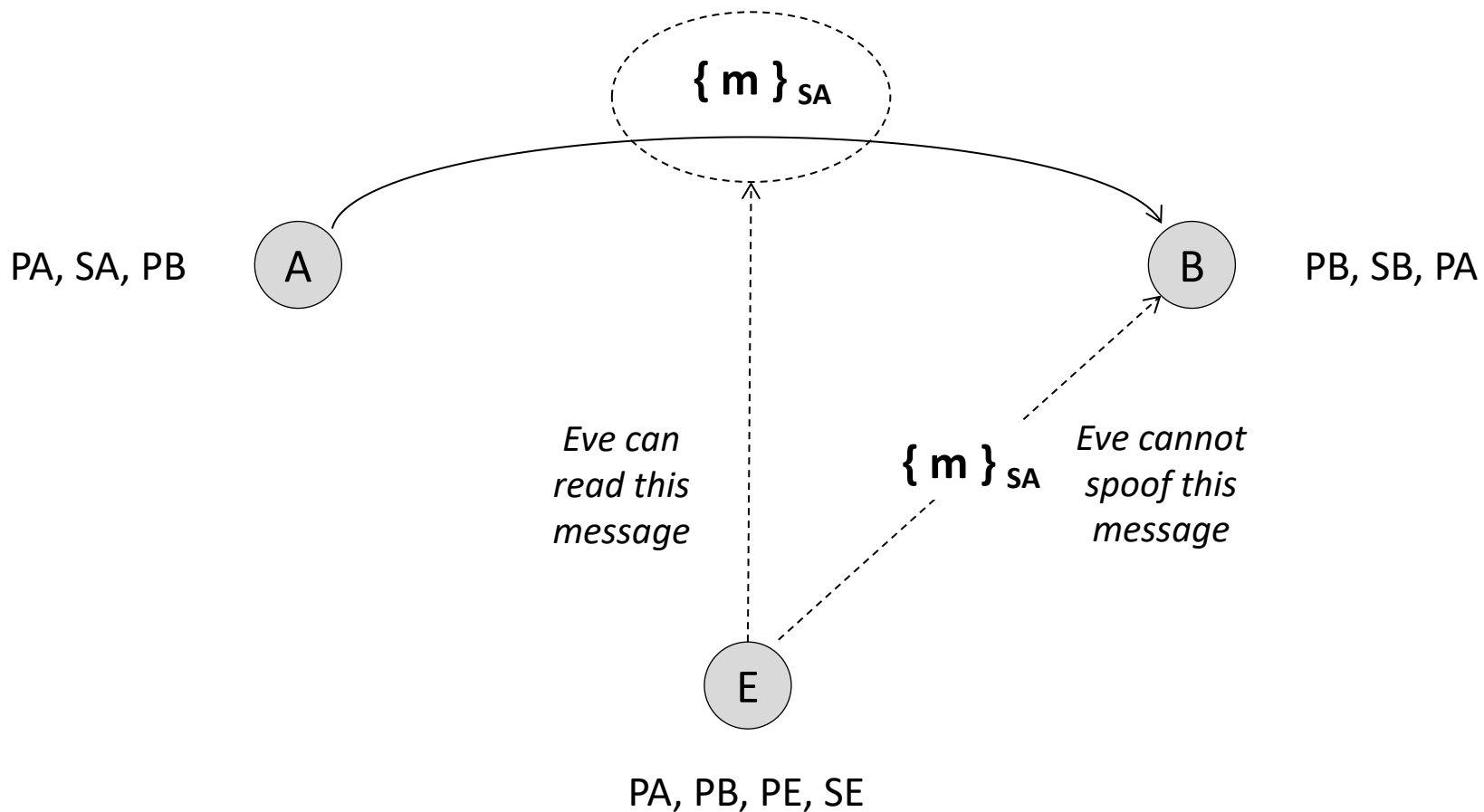
PA, PB, PE, SE



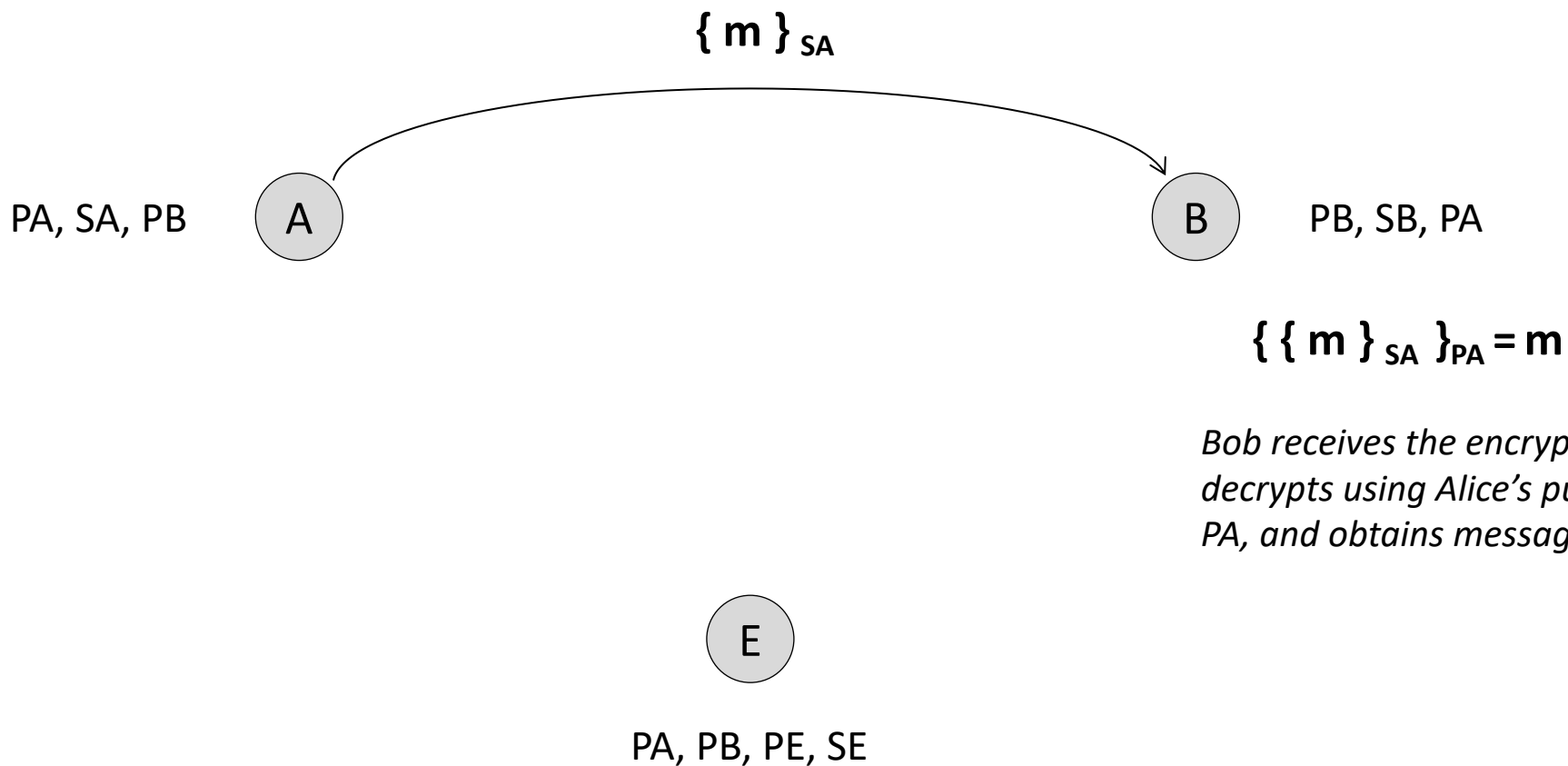
Sending a Signed Message



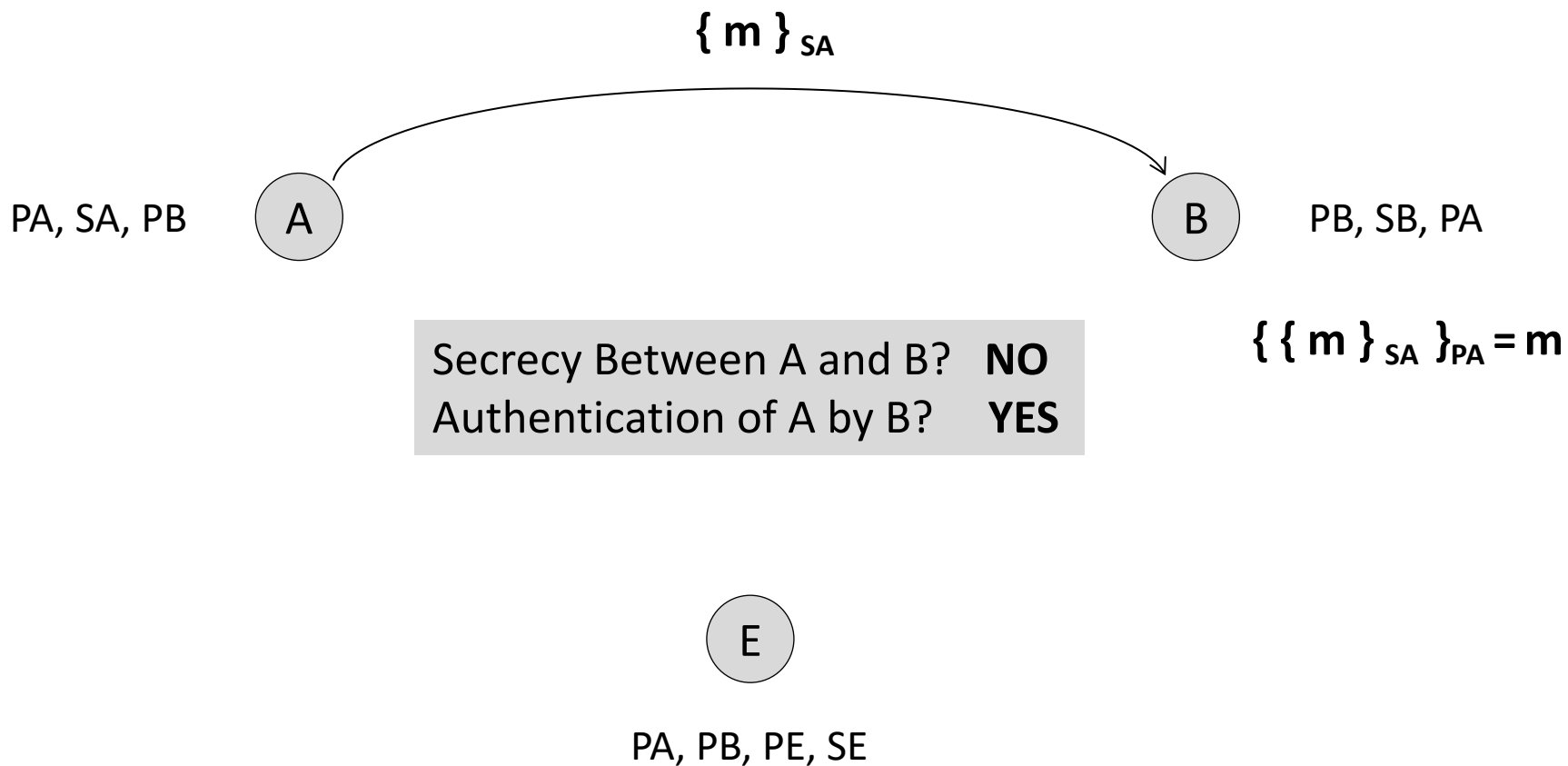
Sending a Signed Message



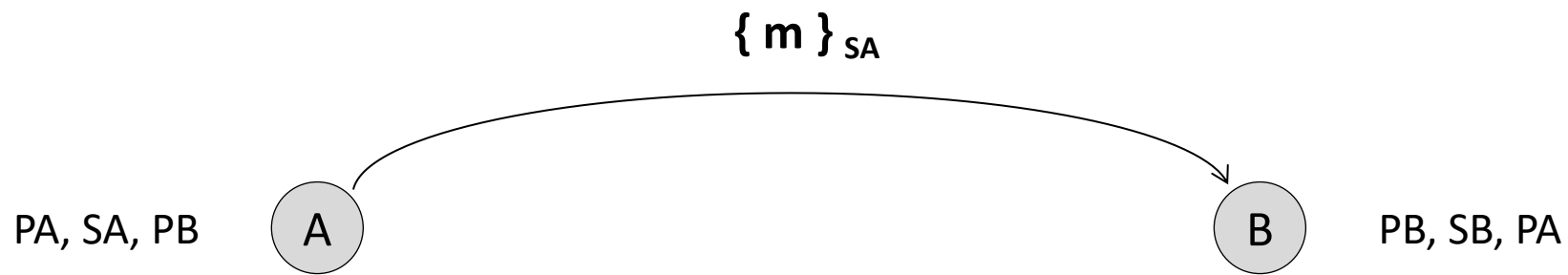
Sending a Signed Message



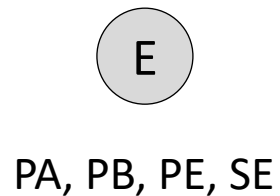
Sending a Signed Message



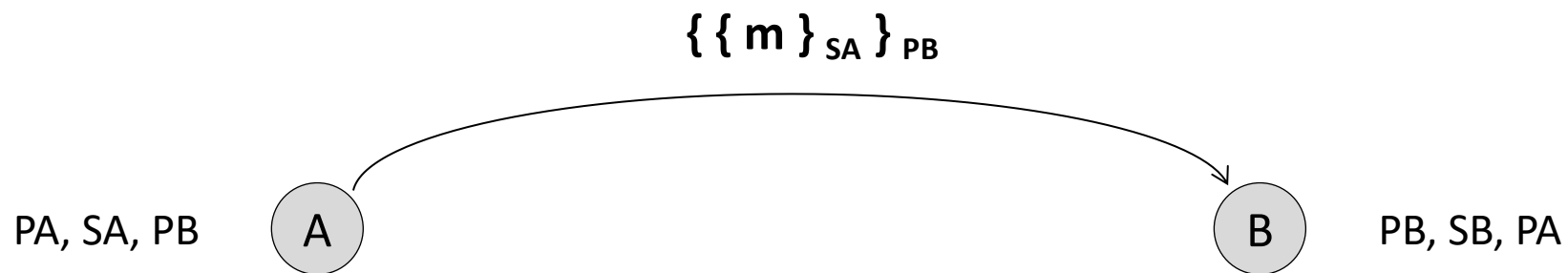
Secure Message Exchange



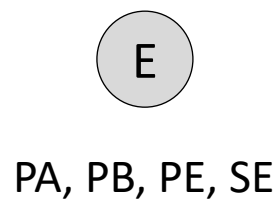
*Alice creates a message m ,
encrypts it with a public key algorithm
using her secret key SA . . .*



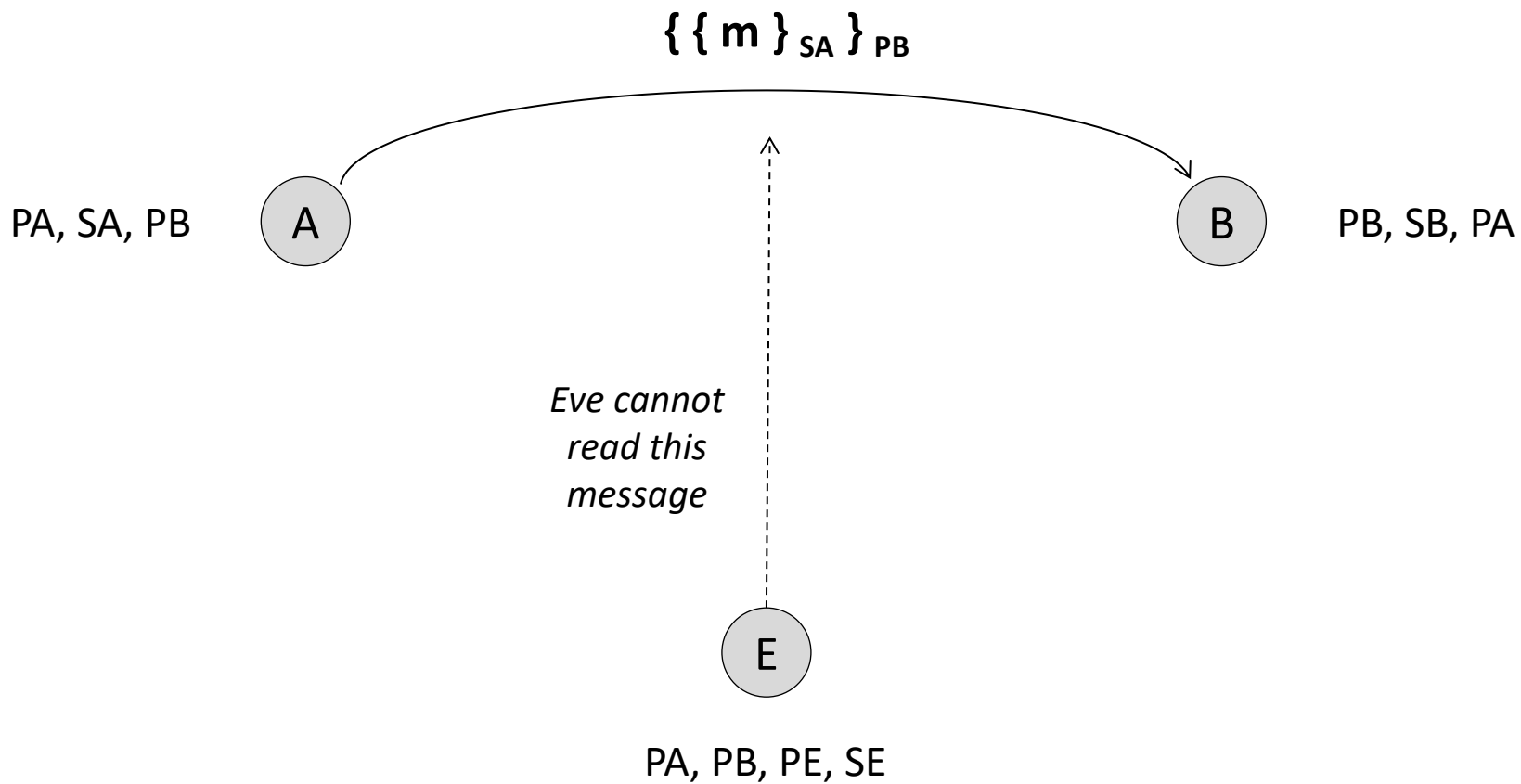
Secure Message Exchange



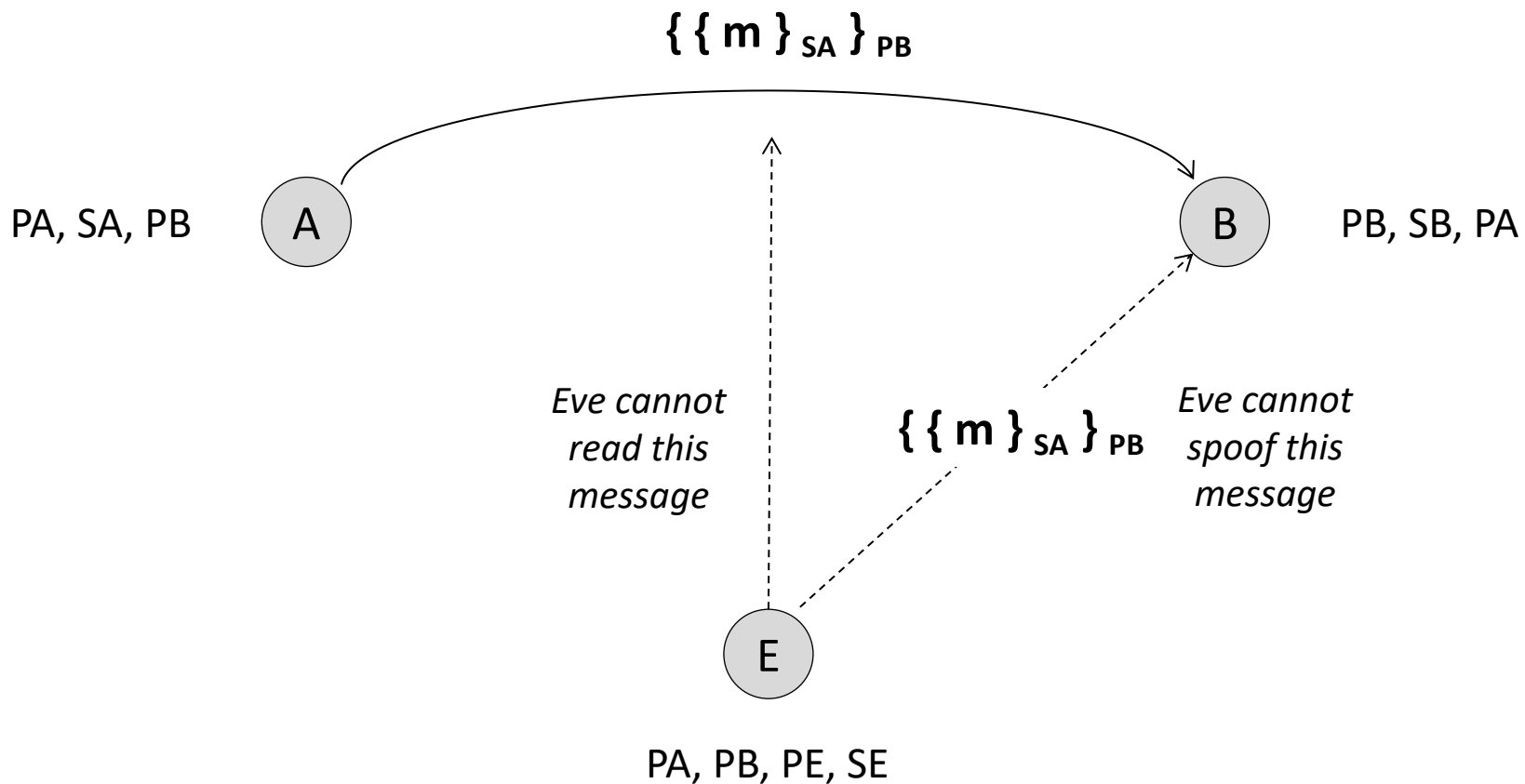
*Alice creates a message m ,
encrypts it with a public key algorithm
using her secret key SA , encrypts it again
using a public key algorithm with Bob's
public key PB , and sends the result to Bob*



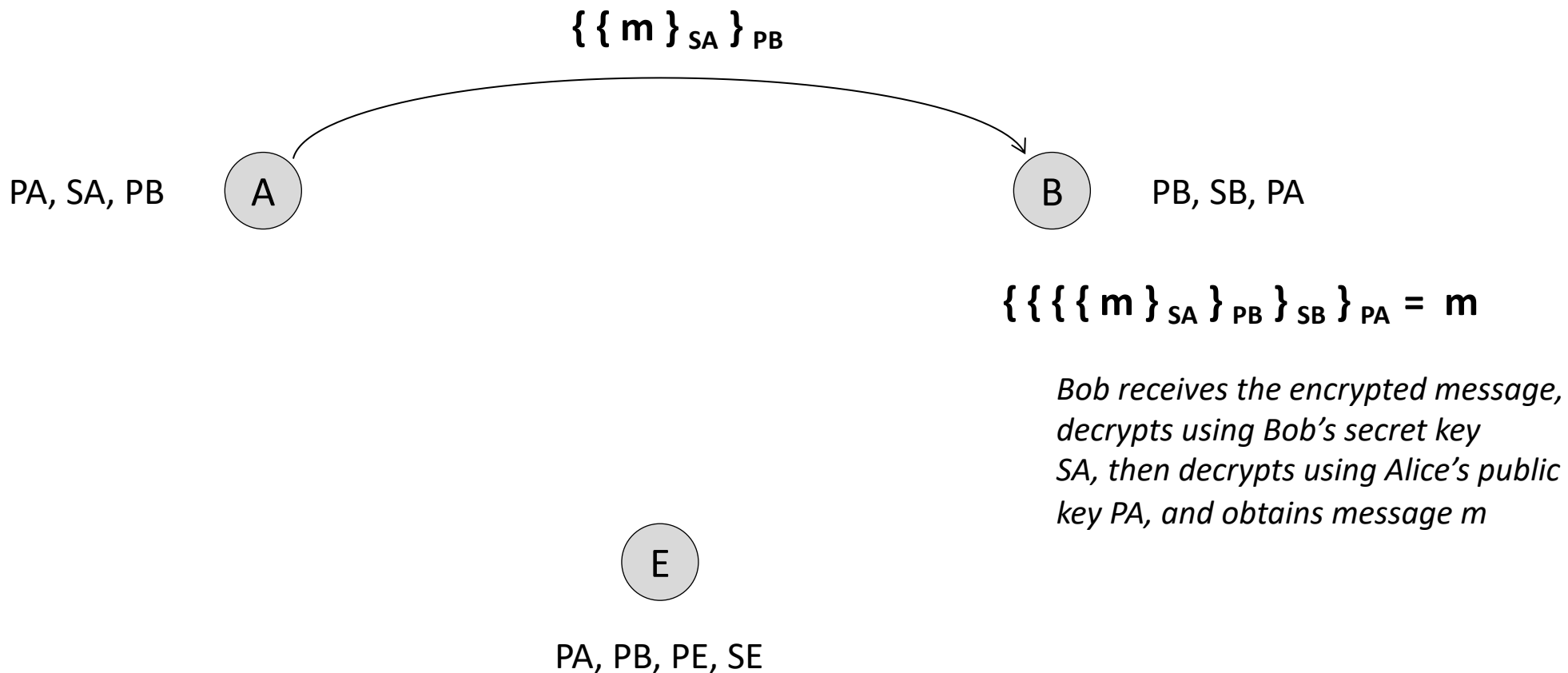
Secure Message Exchange



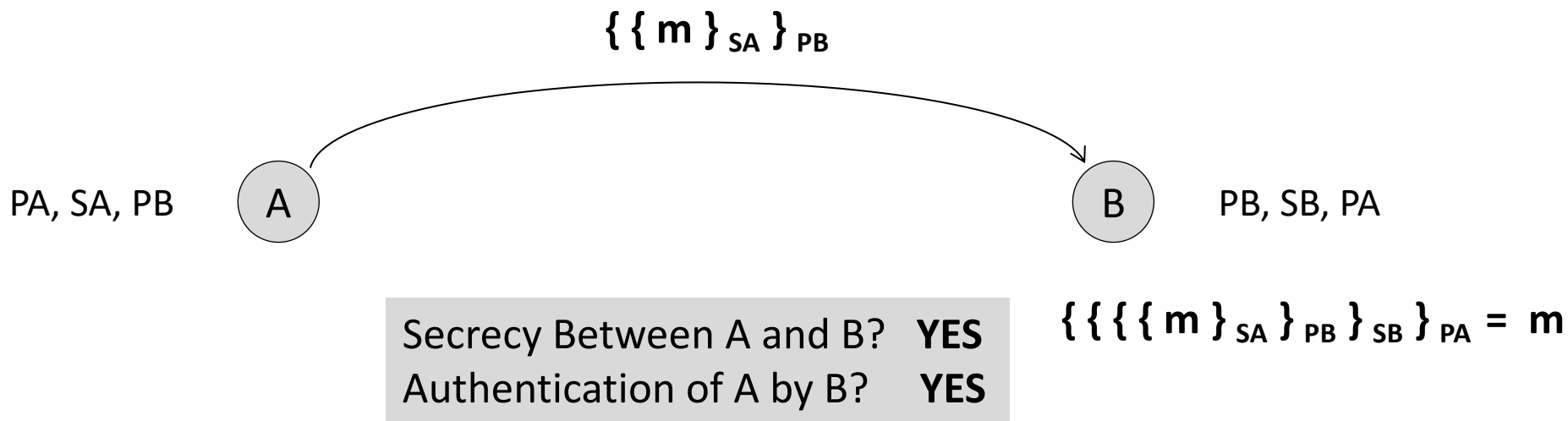
Secure Message Exchange



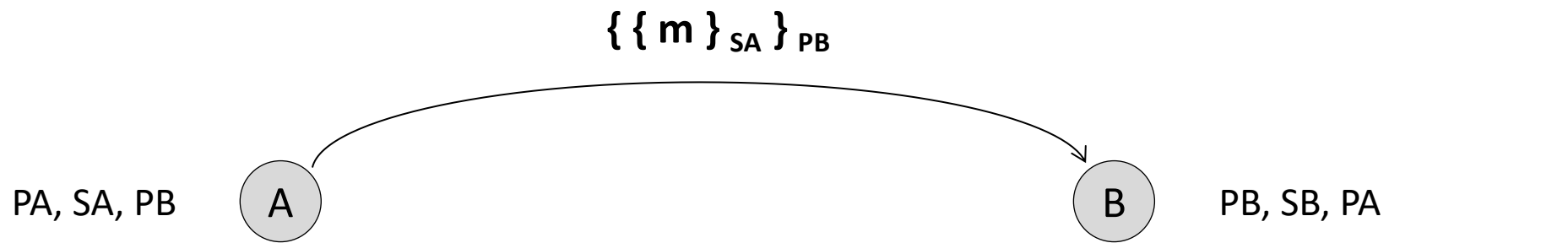
Secure Message Exchange



Secure Message Exchange



Secure Message Exchange

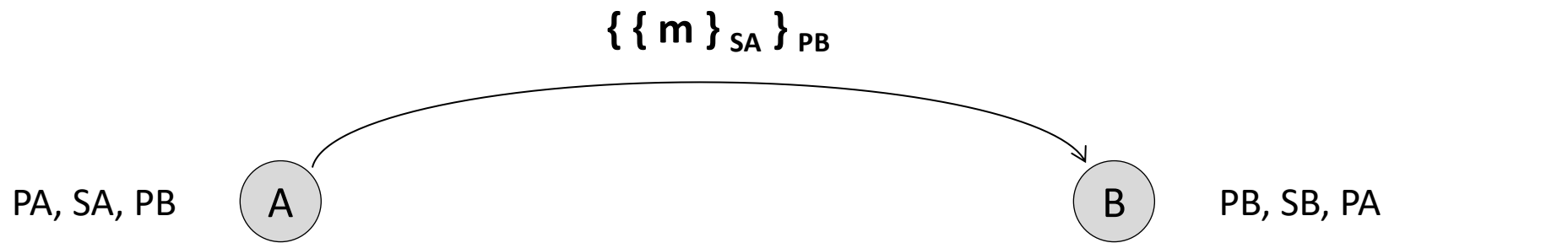


Secrecy Between A and B? **YES**
 Authentication of A by B? **YES**

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

Does this approach scale? **YES**

Secure Message Exchange



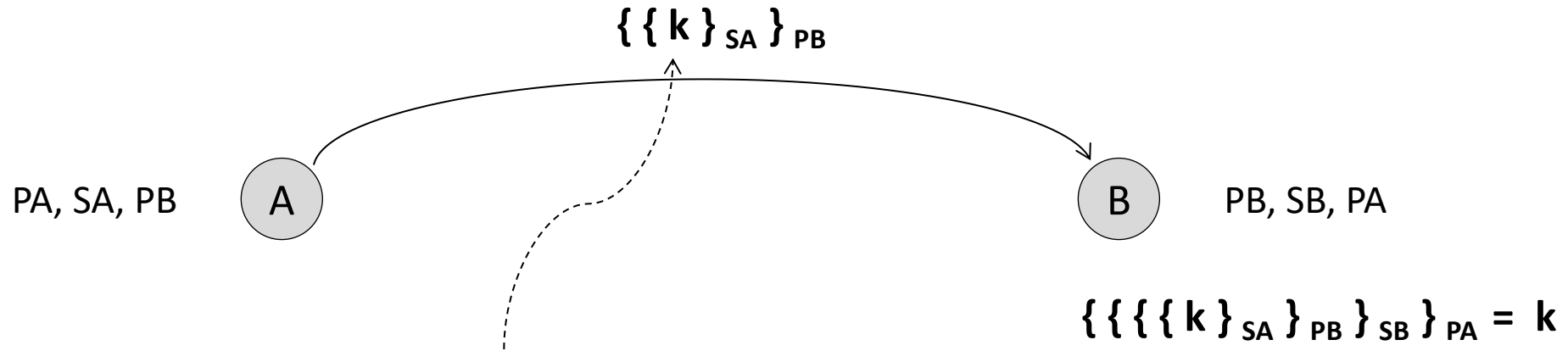
Secrecy Between A and B? **YES**
 Authentication of A by B? **YES**

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

Does this approach scale? **YES**

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

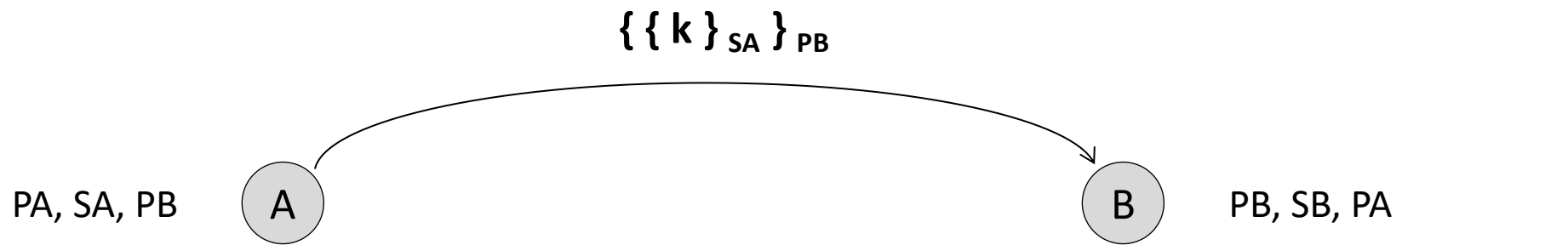
Secure Key Exchange



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

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**

How Does Diffie-Hellman Key Exchange Work?

Week 7

WHITFIELD DIFFIE & MARTIN HELLMAN

Invented public-key
cryptography



A.M.
TURING AWARD
2015

Diffie-Hellman Key Exchange

A

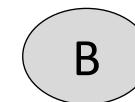
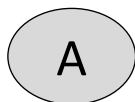
B

Goal:

*A and B share an encryption key k
with no KDC assistance*

Diffie-Hellman Key Exchange

p, g



p, g

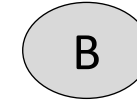
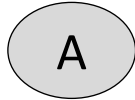
Assume Two Publicly Known Parameters:

p : Large Prime – Typically 1024 Bits

g : Primitive Element

Diffie-Hellman Key Exchange

p, g, a



p, g, b

Step 1:

*A and B each locally generate
private random values a and b*

Diffie-Hellman Key Exchange

p, g, a
 $g^a \bmod p$

A

B

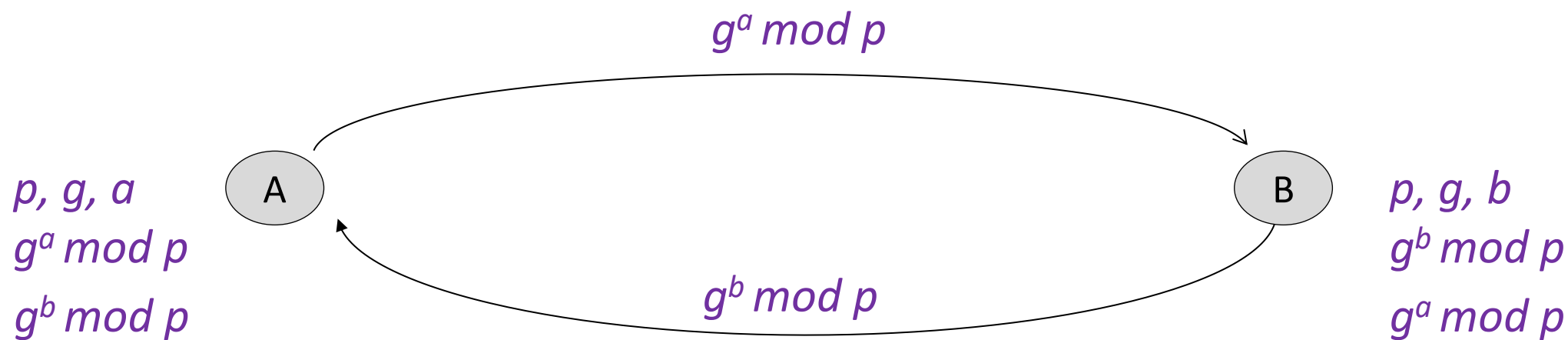
p, g, b
 $g^b \bmod p$

Step 2:

A calculates $g^a \bmod p$

B calculates $g^b \bmod p$

Diffie-Hellman Key Exchange

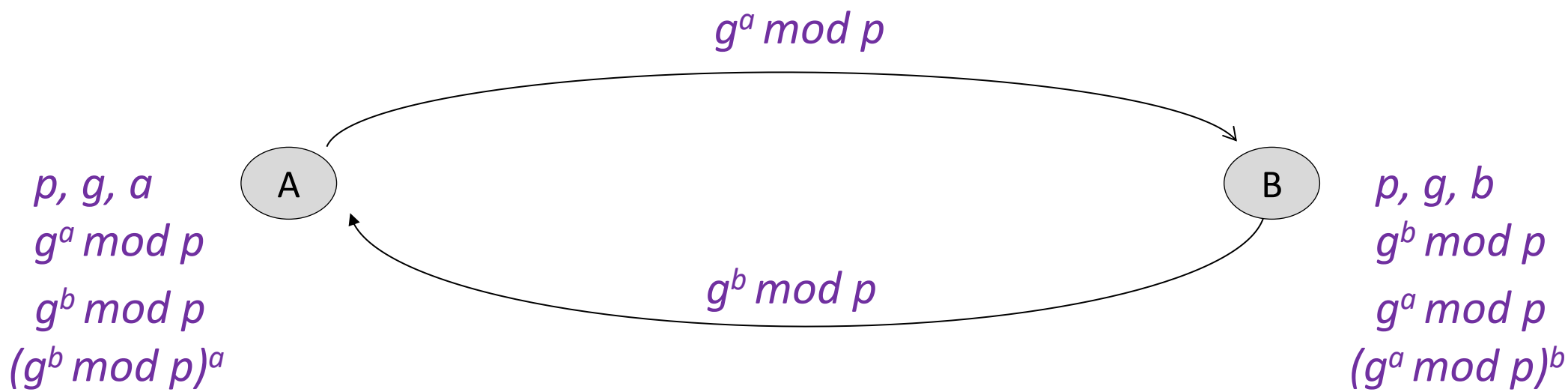


Step 3:

A sends $g^a \bmod p$ to B

B send $g^b \bmod p$ to A

Diffie-Hellman Key Exchange

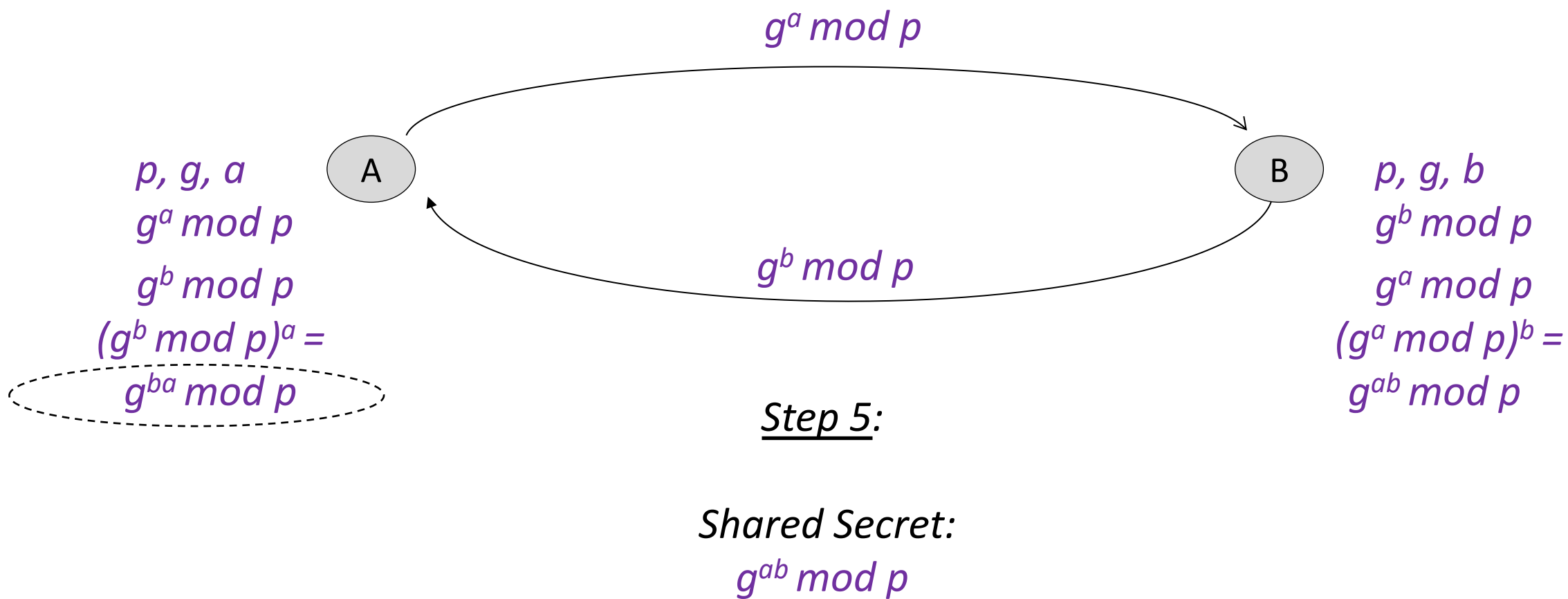


Step 4:

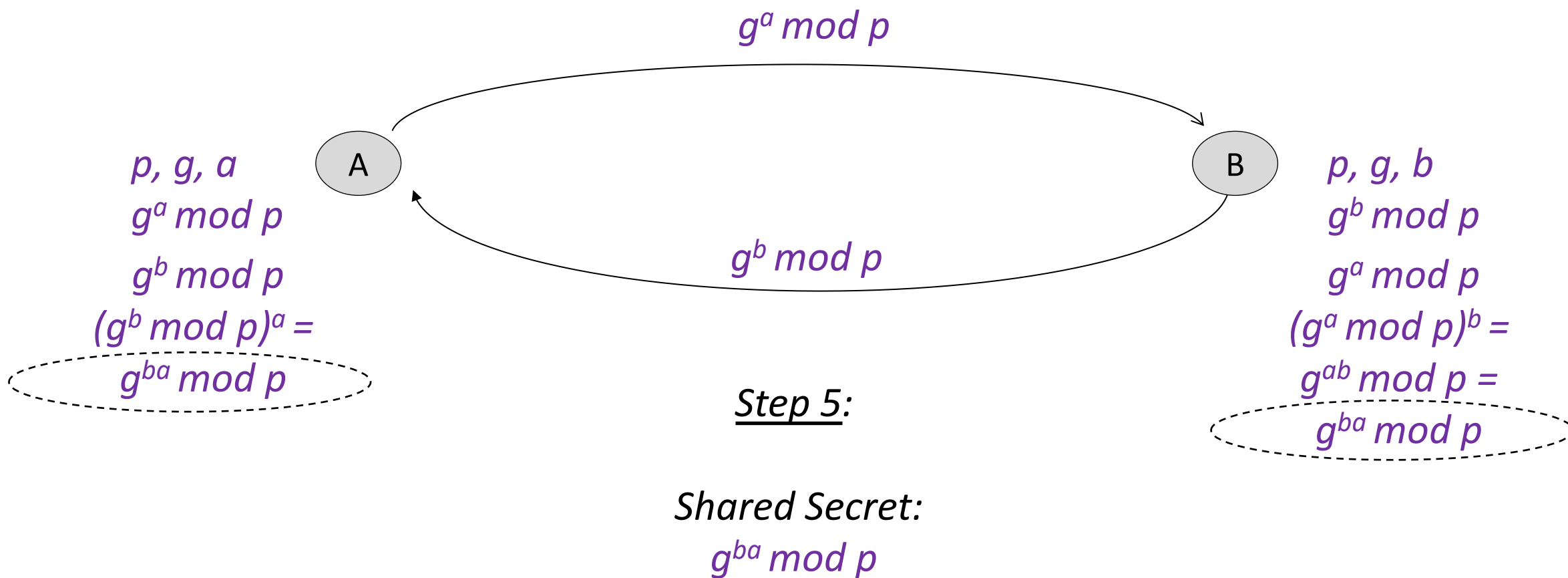
A computes $(g^b \bmod p)^a$ to B

B computes $(g^a \bmod p)^b$ to A

Diffie-Hellman Key Exchange



Diffie-Hellman Key Exchange



Public Key Cryptography – Original Paper By Diffie and Hellman

644

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channels without compromising the security of the system. In a *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D , such that computing D from E is computationally infeasible (e.g., requiring

How Does the Original RSA Algorithm Work?

Week 7

RON RIVEST, ADI SHAMIR & LEN ADLEMAN



A W A R D
2002

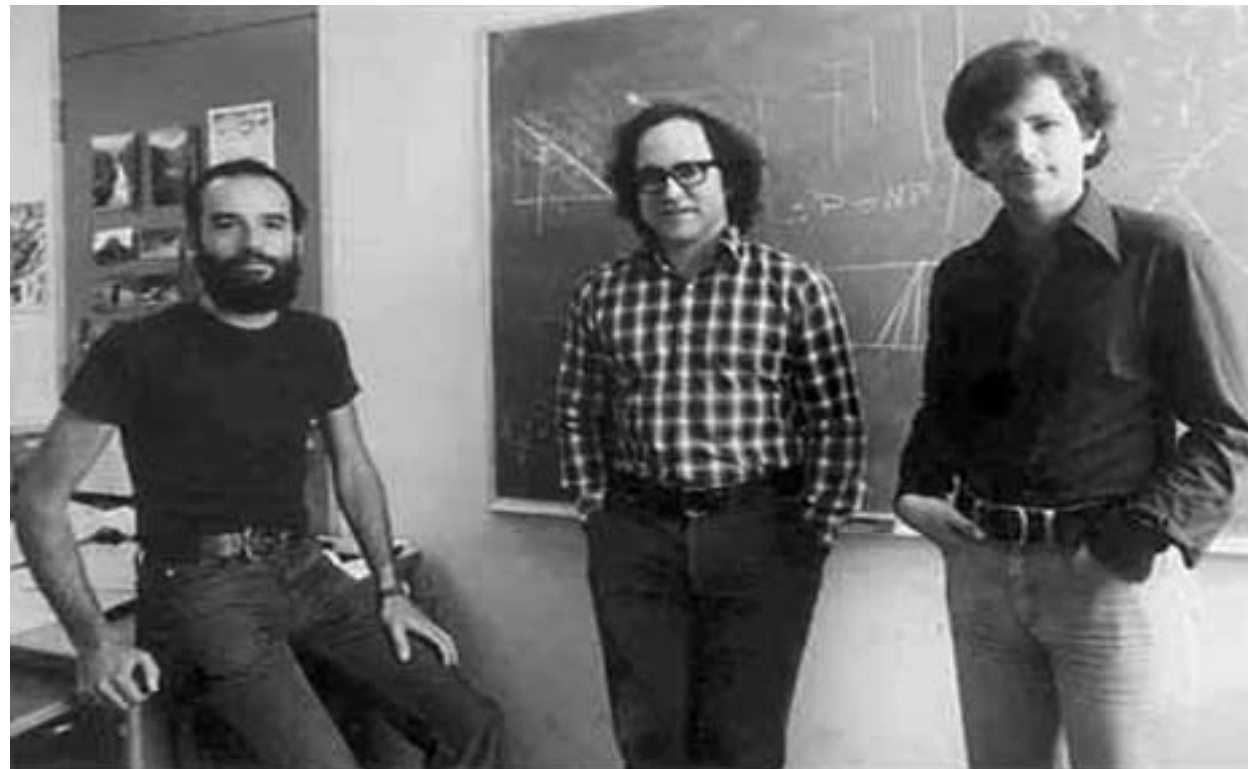


RSA public-key cryptography

A.M.
TURING

RSA Algorithm

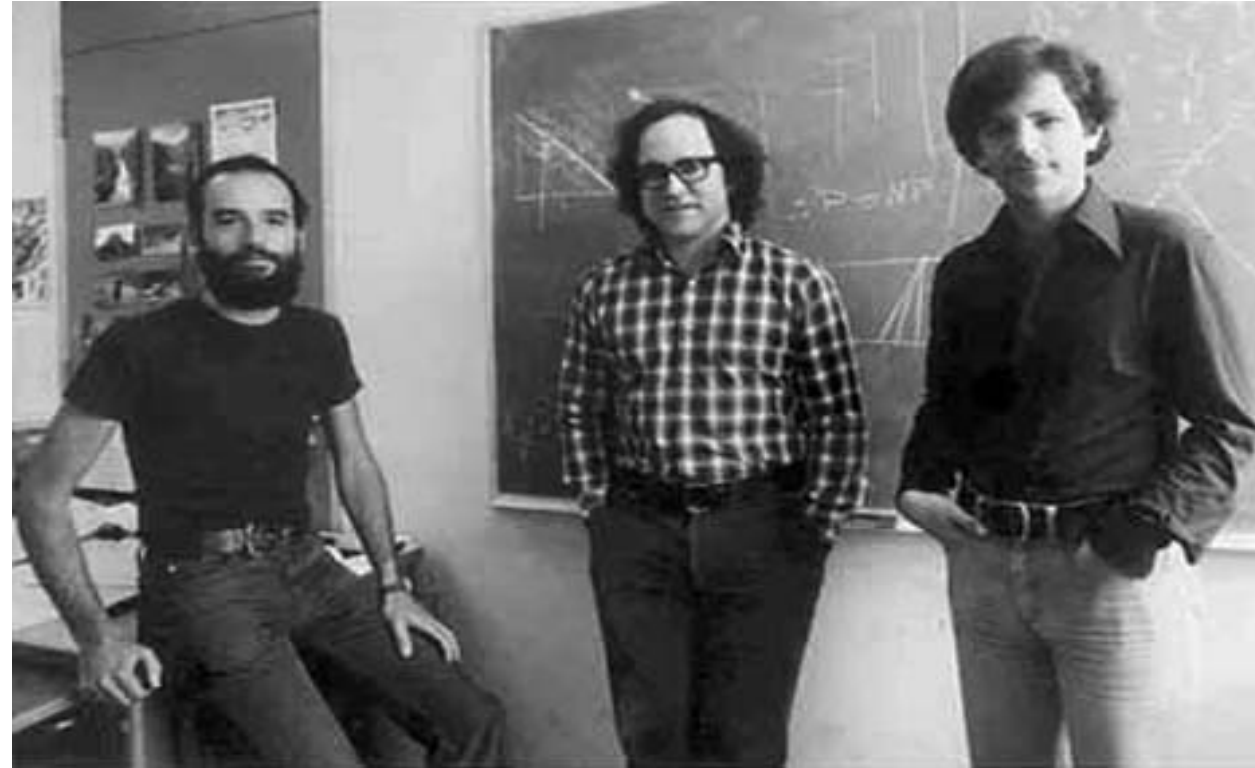
Step 1: Select two prime numbers p and q , each about 100 decimal digits in length



RSA Algorithm

Step 1: Select two prime numbers p and q , each about 100 decimal digits in length

Step 2: Calculate $n = pq$ and $\psi = (p - 1)(q - 1)$



RSA Algorithm

Step 1: Select two prime numbers p and q , each about 100 decimal digits in length

Step 2: Calculate $n = pq$ and $\Psi = (p - 1)(q - 1)$

Step 3: Select integer E between 3 and Ψ , which has no common factors with Ψ



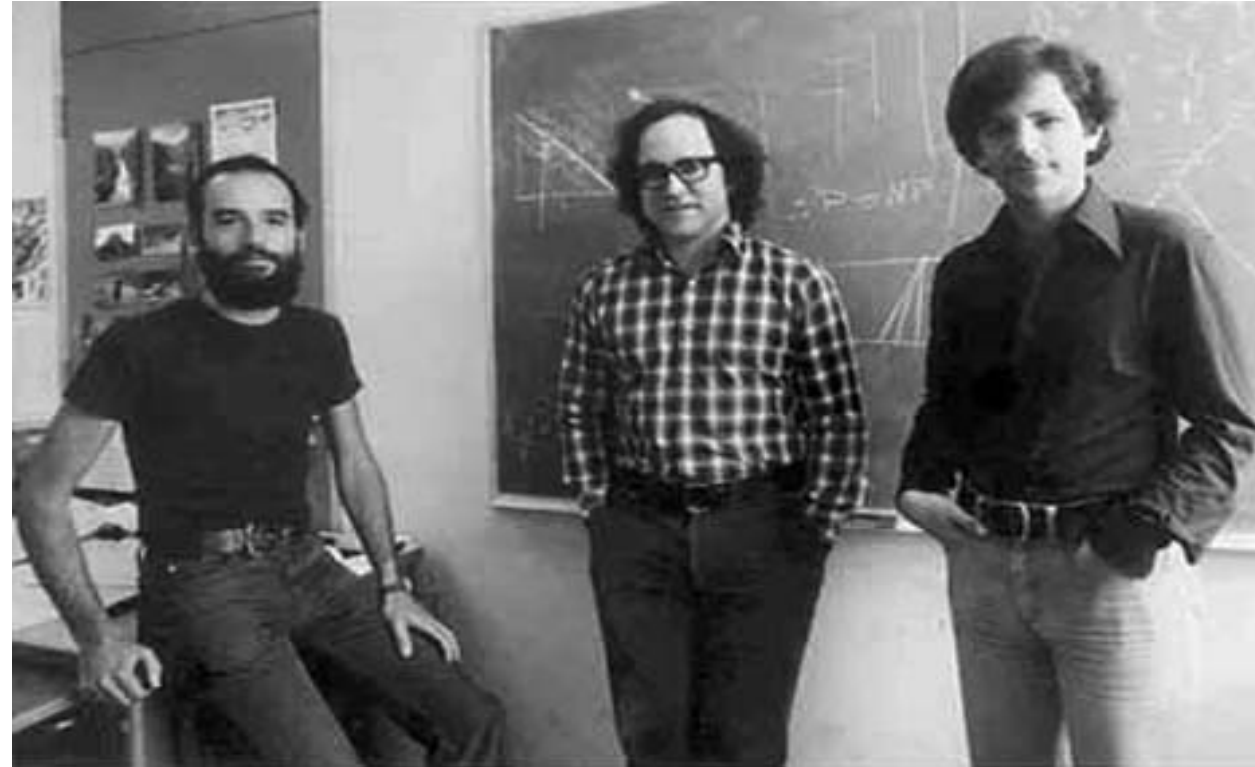
RSA Algorithm

Step 1: Select two prime numbers p and q , each about 100 decimal digits in length

Step 2: Calculate $n = pq$ and $\Psi = (p - 1)(q - 1)$

Step 3: Select integer E between 3 and Ψ , which has no common factors with Ψ

Step 4: Select integer D such that DE differs by 1 from a multiple of Ψ



RSA Algorithm

Step 1: Select two prime numbers p and q , each about 100 decimal digits in length

Step 2: Calculate $n = pq$ and $\Psi = (p - 1)(q - 1)$

Step 3: Select integer E between 3 and Ψ , which has no common factors with Ψ

Step 4: Select integer D such that DE differs by 1 from a multiple of Ψ

Step 5: Make E , n public, but keep p , q , D and Ψ secret



RSA Algorithm

Step 1: Select two prime numbers p and q , each about 100 decimal digits in length

Step 2: Calculate $n = pq$ and $\Psi = (p - 1)(q - 1)$

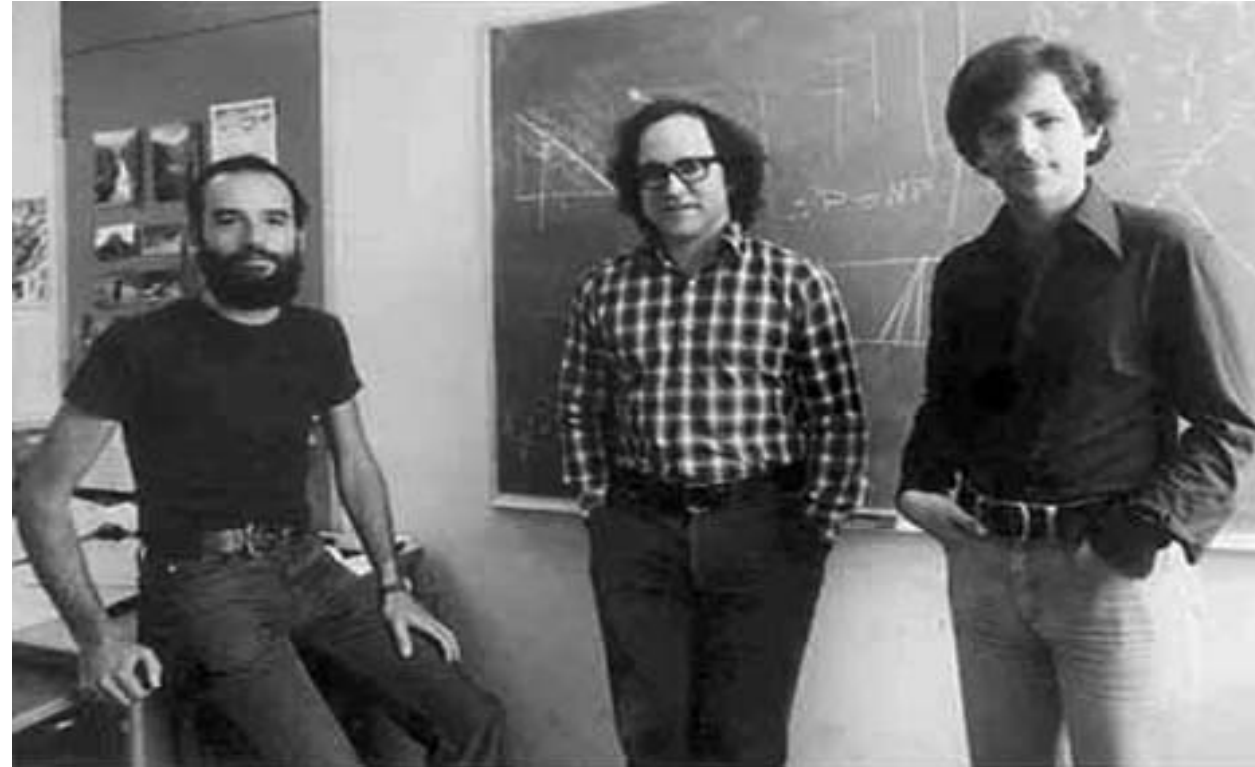
Step 3: Select integer E between 3 and Ψ , which has no common factors with Ψ

Step 4: Select integer D such that DE differs by 1 from a multiple of Ψ

Step 5: Make E , n public, but keep p , q , D and Ψ secret

Encryption: $C = P^E \bmod n$

Decryption: $P = C^D \bmod n$



RSA Algorithm

Step 1: Select two prime numbers p and q , each about 100 decimal digits in length

Step 2: Calculate $n = pq$ and $\Psi = (p - 1)(q - 1)$

Step 3: Select integer E between 3 and Ψ , which has no common factors with Ψ

Step 4: Select integer D such that DE differs by 1 from a multiple of Ψ

Step 5: Make E , n public, but keep p , q , D and Ψ secret

Encryption: $C = P^E \bmod n$

Decryption: $P = C^D \bmod n$



Example: $p = 3$, $q = 5$, $n = 15$, $\Psi = 8$ Select $E = 5$, $D = 5$

Encrypt "2": $2^5 \bmod 15 = 2$

Decrypt "2": $2^5 \bmod 15 = 2$

Who Really Invented Public Key Technology?
(Hint: UK)

James Ellis, Engineer at GCHQ – Circa 1969



Bell Labs – Project C43 (1944)

SECRET 054 450						ATI- 29345
TITLE: Final Report - Part I - Speech Privacy Systems - Interception, Diagnosis, Decoding, Evaluation						REVISION (None)
AUTHOR(S): Koenig, W.						ORIG. AGENCY NO. (None)
ORIGINATING AGENCY: Bell Telephone Labs., Inc., New York, N. Y.						PUBLISHING AGENCY NO. 4573A
PUBLISHED BY: Office of Scientific Research and Development, NDRC, Div. 13						
DATE Oct '44	DOC. CLASS. Secr.	COUNTRY U.S.	LANGUAGE Eng.	PAGES 111	ILLUSTRATIONS photos, tables, diagrs	
<p>ABSTRACT:</p> <p>The results of three years' experience in diagnosing, decoding, and evaluating speech privacy systems are summarized. Speech privacy systems may be used in connection with radio telephone systems or wire systems, but radio interception problems only are discussed. The decoding techniques described apply to wire as well as to radio communications. The sound spectrograph is described including its history, method of operation, and capabilities. It analyzes speech in terms of its three basic dimensions, frequency, amplitude, and time; and portrays the analysis in the form of spectrograms. Basic speech scrambling methods are also explained in which the original speech is transmitted with its parts modified, displaced, or interchanged. Cryptanalysis and cryptography, which apply to telegraph types of communication, are also described.</p>						
<p><i>NTIS SOP memo 2 Aug 60</i></p> <p>DISTRIBUTION: Copies of this report obtainable from the Communications Division, AT&T, MCDND</p>						
DIVISION: Electronics (6)				SUBJECT HEADINGS: Communication systems, Secret (23992.87); Decoders (28877)		
SECTION: Communications (1, 5, 6)						
AD-A800 206				CAL INDEX		
SECRET				Wright-Patterson Air Force Base Dayton, Ohio		

GCHQ – Original and New Headquarters in Cheltenham, UK



James Ellis' Paper 1970 – Classified for Three Decades

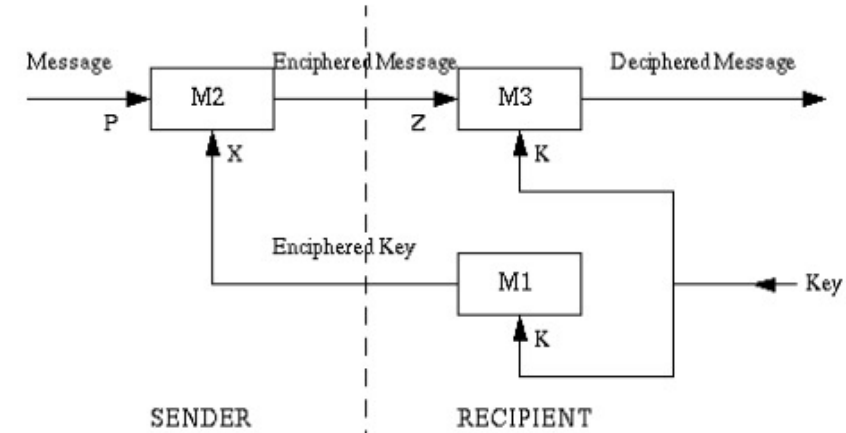
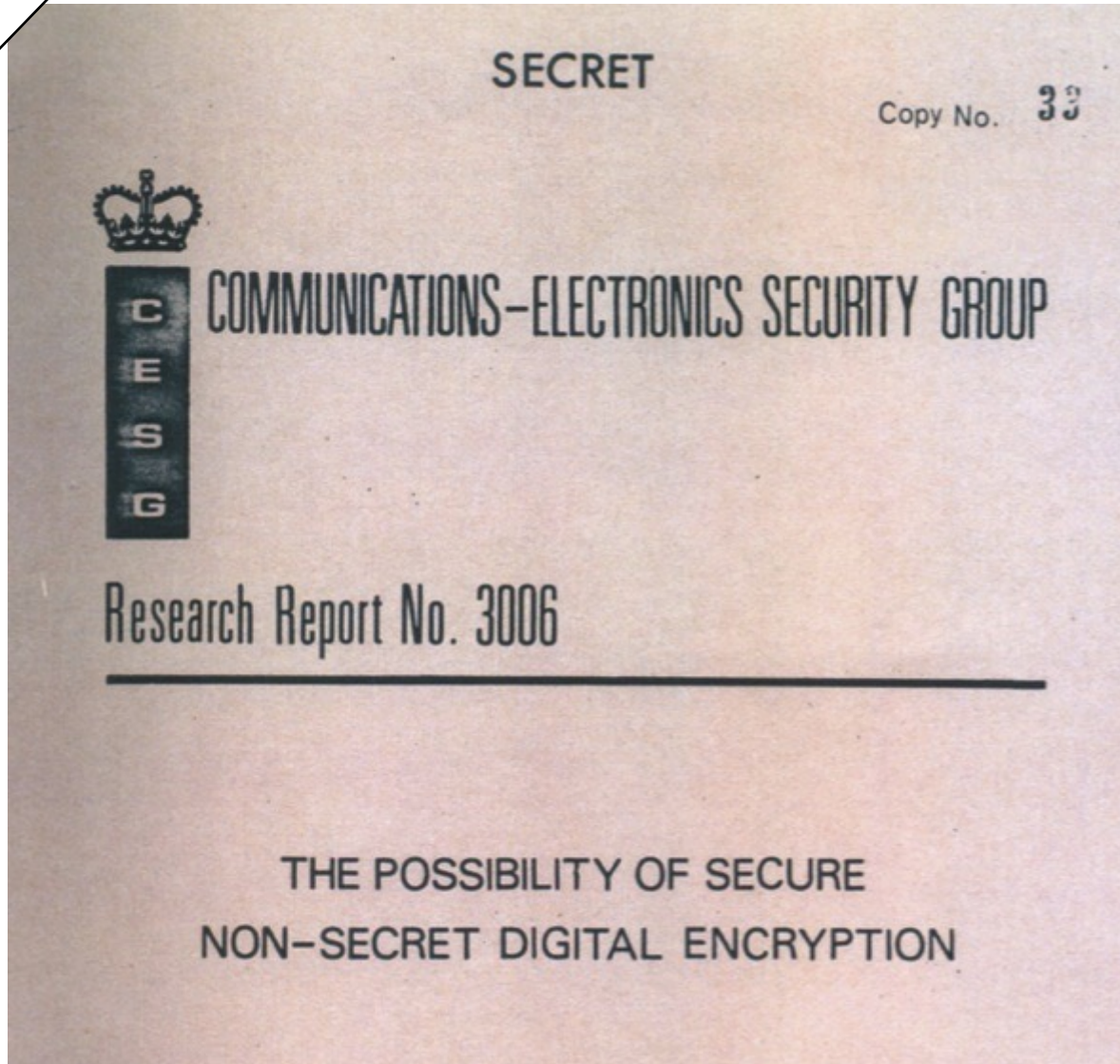


Fig. 1

13. The following properties are clearly essential. It must be impossible for the interceptor to obtain p from z without knowing k even though he knows x . Also, since a knowledge of k would enable him to decipher z , he must be unable to obtain k from x . Finally $M3$ must have the property of being able to decipher z . To obtain these properties we specify the look-up tables corresponding to $M1$, $M2$ and $M3$ in the following way: -

- Let k have n different possible values and p have m different possible values, for simplicity take them to be the integers 1 to n and 1 to m respectively. Let x have the same range of values as k , and z have the same range as p .
- $M1$ can be defined as a linear look-up table of n entries whose contents are the numbers 1 to n in a random order, where "random" implies that the output is sufficiently uncorrelated with the input so that the position of a particular entry in the table cannot be found in a simpler way than by searching through the table.
- $M2$ corresponds to an n by m rectangular table in which the entries for a fixed value of x consists of the numbers 1 to m in random order, and where the columns for the various values of x are suitable uncorrelated with one another.

Clifford Cocks and Malcolm Williamson



SECRET

- 1 -

Note on "Non-Secret Encryption"

In [1] J H Ellis describes a theoretical method of encryption which does not necessitate the sharing of secret information between the sender and receiver. The following describes a possible implementation of this.

a. The receiver picks 2 primes P, Q satisfying the conditions

i. P does not divide $Q-1$.

ii. Q does not divide $P-1$.

He then transmits $N = PQ$ to the sender.

b. The sender has a message, consisting of numbers

C_1, C_2, \dots, C_r with $0 < C_i < N$

He sends each, encoded as D_i where

$$D_i = C_i^N \text{ reduced modulo } N.$$

c. To decode, the receiver finds, by Euclids Algorithm, numbers P', Q'

satisfying $P P' \equiv 1 \pmod{Q-1}$

$Q Q' \equiv 1 \pmod{P-1}$

Then $C_i \equiv D_i^{P'} \pmod{Q}$

and $C_i \equiv D_i^{Q'} \pmod{P}$

Credit Where Credit is Due

