

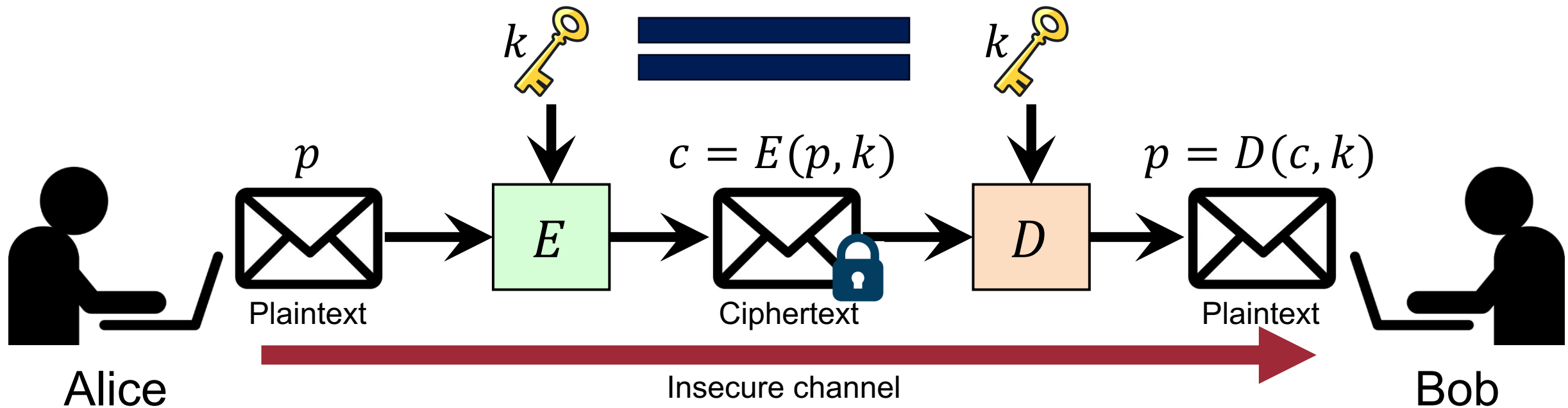
CSE467: Computer Security

5-2. Asymmetric-key Encryption

Seongil Wi

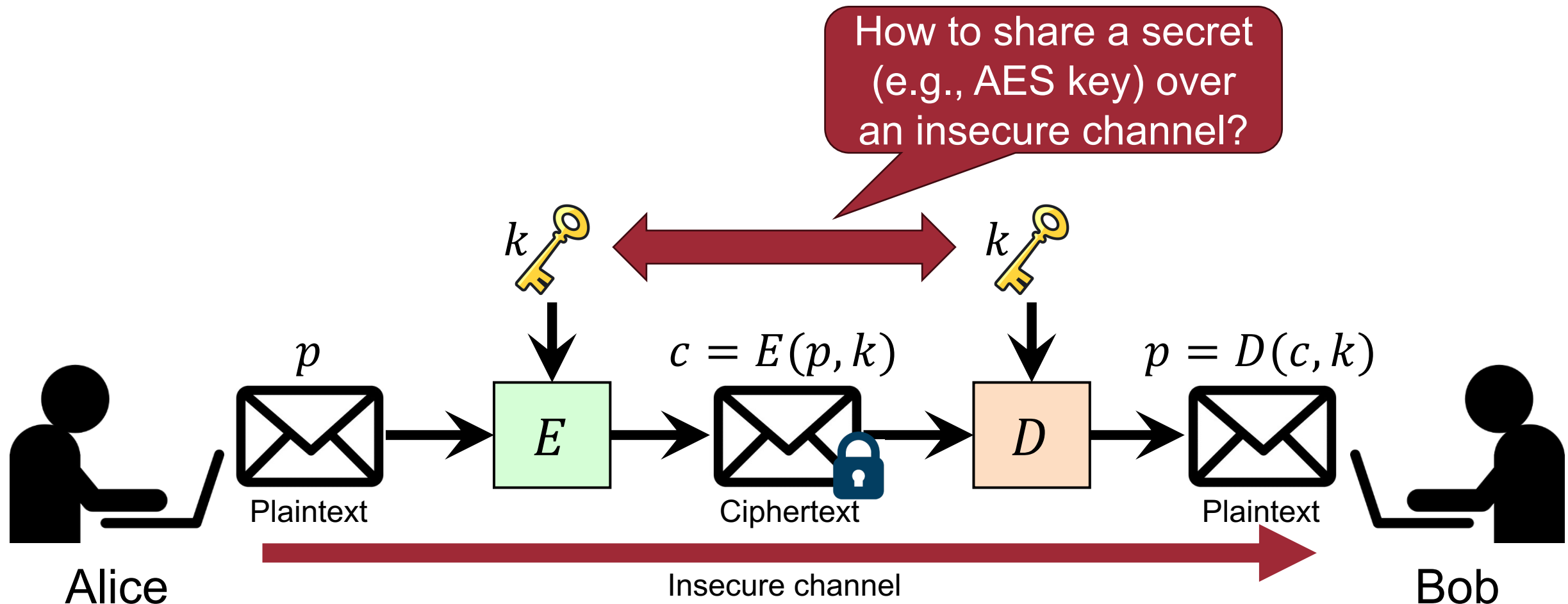
Recap: Symmetric-key Encryption

- **Symmetric:** the encryption and decryption keys *are the same*



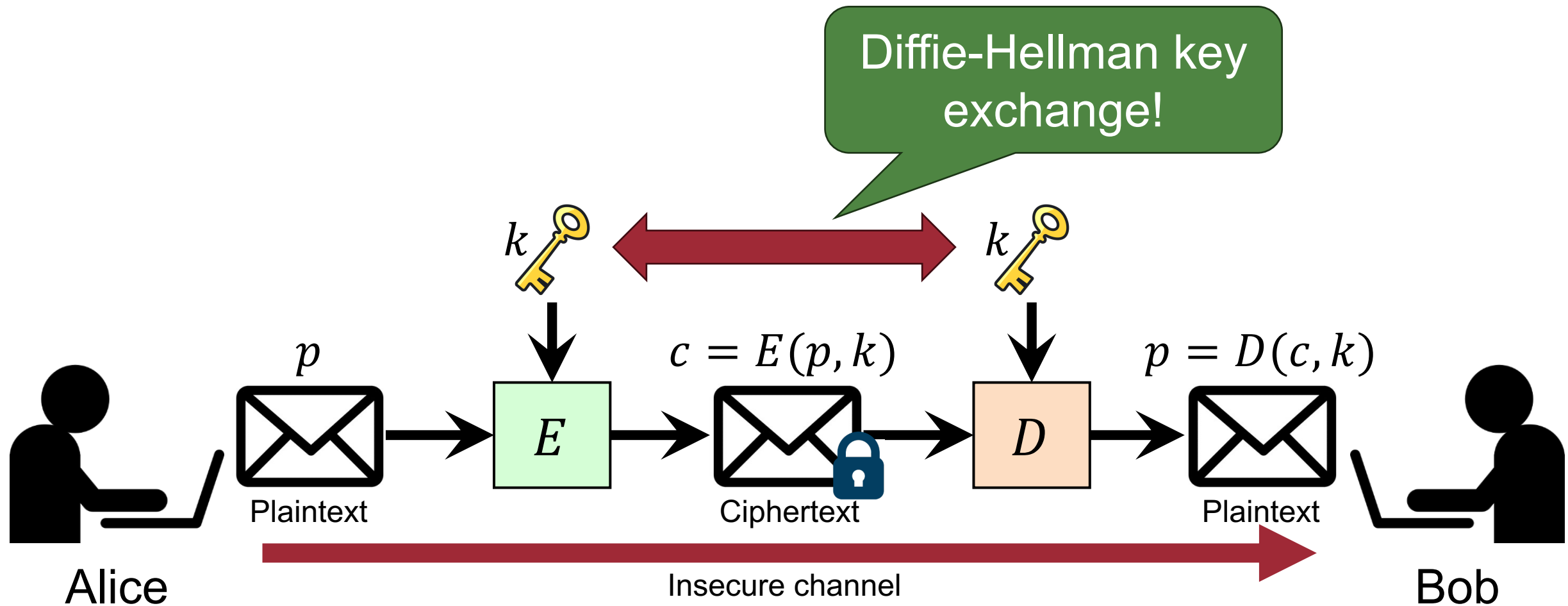
Recap: Symmetric-key Encryption

- **Symmetric:** the encryption and decryption keys *are the same*



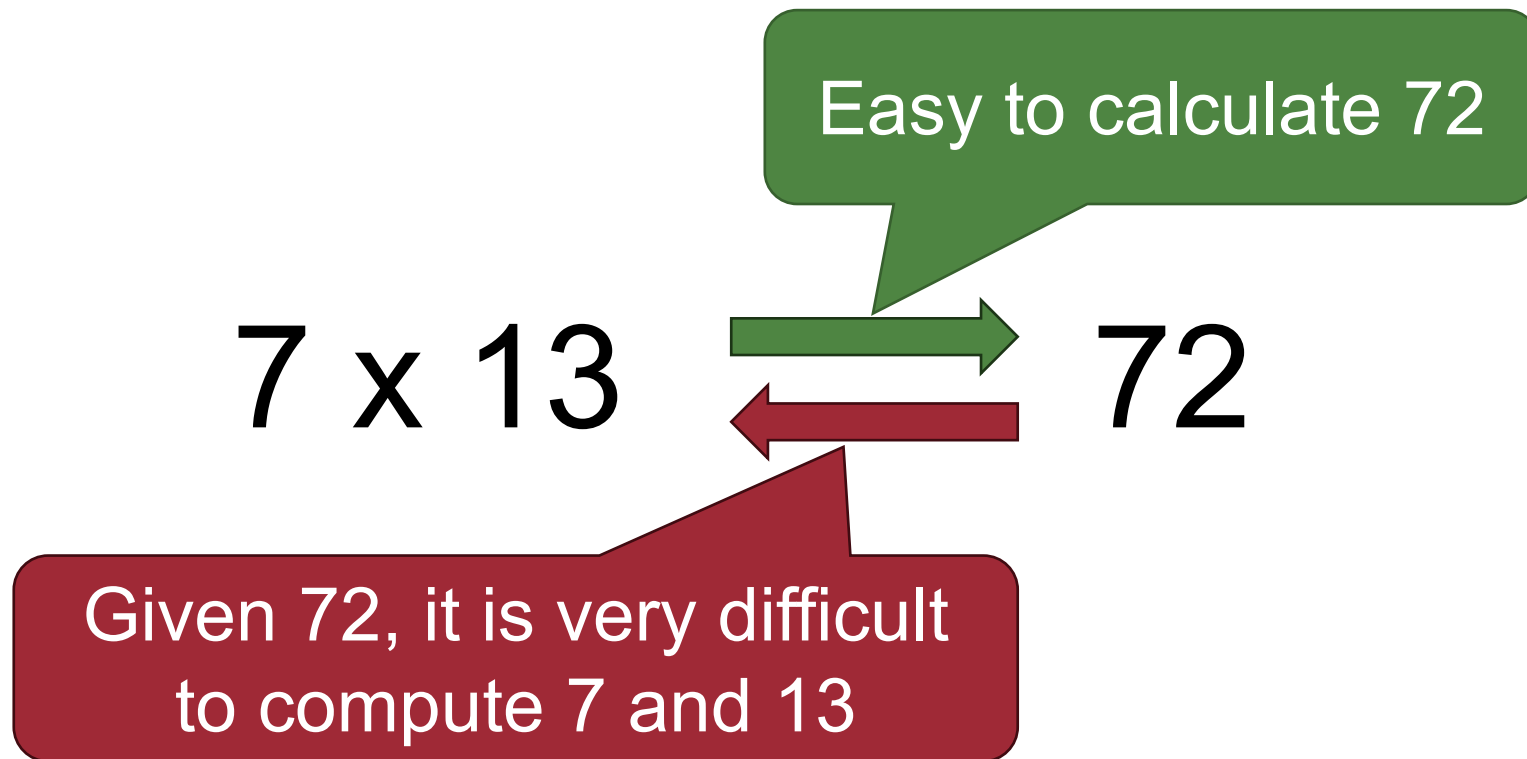
Motivation of the Diffie-Hellman Key Exchange ⁴

- **Symmetric:** the encryption and decryption keys *are the same*



Core Idea: One-way Function

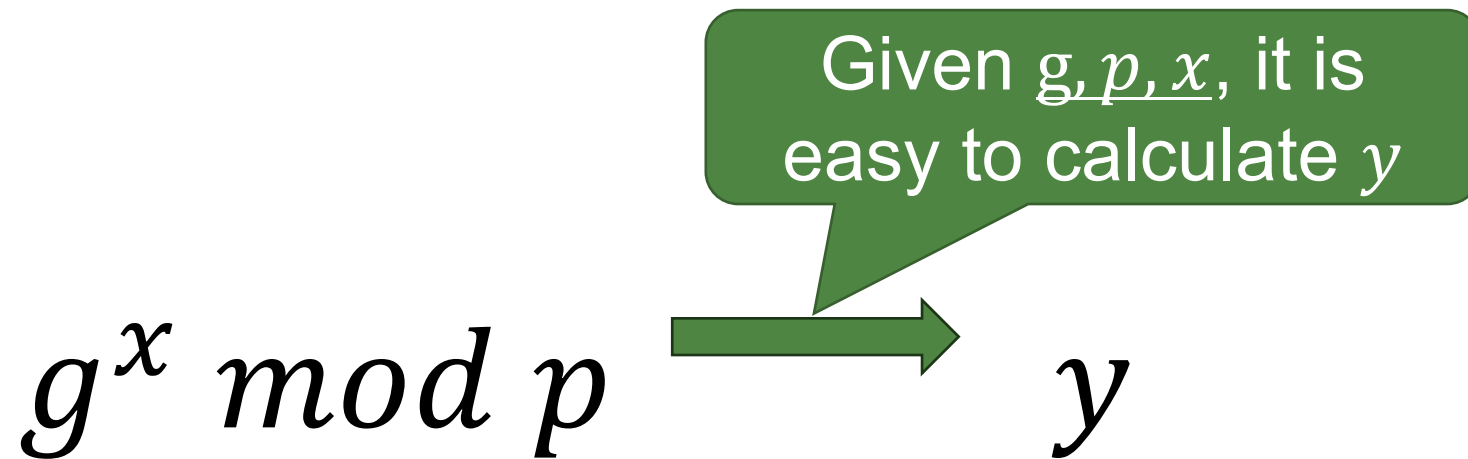
- Easy in one direction, but hard in the reverse direction
 - f is easy to compute, but f^{-1} is easy to compute



Integer Factorization Problem

Core Idea: One-way Function

- Easy in one direction, but hard in the reverse direction
 - f is easy to compute, but f^{-1} is easy to compute



Core Idea: One-way Function



- Easy in one direction, but hard in the reverse direction
 - f is easy to compute, but f^{-1} is easy to compute

$$g = 3$$

$$p = 5$$

$$x = 2$$

$$g^x \bmod p \longrightarrow y = ?$$

Core Idea: One-way Function

- Easy in one direction, but hard in the reverse direction
 - f is easy to compute, but f^{-1} is easy to compute

$$g = 3$$

$$p = 5$$

$$x = 2$$

$$g^x \bmod p$$

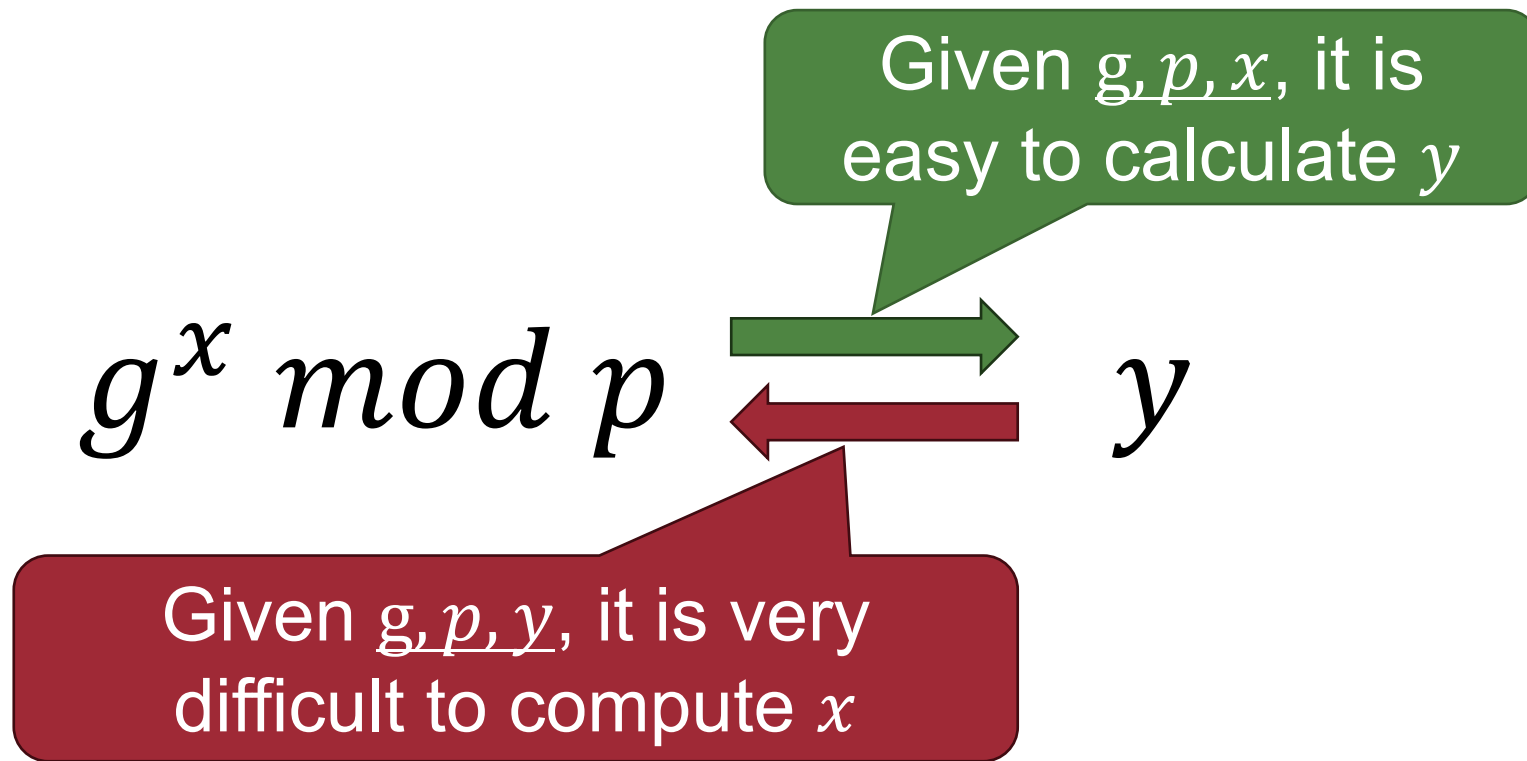


Given g, p, x , it is
easy to calculate y

$$y = 4$$

Core Idea: One-way Function

- Easy in one direction, but hard in the reverse direction
 - f is easy to compute, but f^{-1} is easy to compute



Core Idea: One-way Function

- Easy in one direction, but hard in the reverse direction
 - f is easy to compute, but f^{-1} is easy to compute

$$g = 3$$

$$p = 5$$

$$x = ?$$

$$g^x \bmod p \longleftarrow y = 4$$

Given g, p, y , it is very difficult to compute x

Discrete Logarithm Problem

Core Idea: One-way Function

- Easy in one direction, but hard in the reverse direction
 - f is easy to compute, but f^{-1} is easy to compute

$$g = 3$$

$$p = 5$$

$$x = ?$$

$$g^x \bmod p \longleftarrow y = 4$$

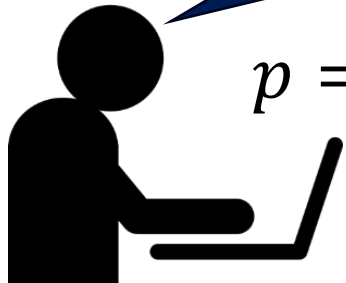
There is no efficient algorithm known for computing discrete logarithms in general

Diffie-Hellman Key Exchange (1)

$$g^x \bmod p \begin{matrix} \xrightarrow{\text{green}} \\ \xleftarrow{\text{red}} \end{matrix} y$$

Pick two value:
Large prime p and
integer g

$$p = 23, g = 9$$



Alice



Insecure channel



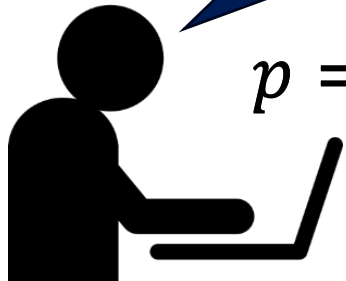
Bob

Diffie-Hellman Key Exchange (2)

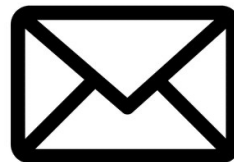
$$g^x \bmod p \xrightleftharpoons[\text{red arrow}]{\text{green arrow}} y$$

Publicly share
 p and g

$p = 23, g = 9$



Alice



Insecure channel

$p = 23, g = 9$



Bob

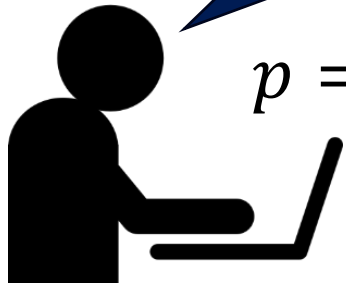
Diffie-Hellman Key Exchange (2)

$$g^x \bmod p \xrightleftharpoons[\text{red arrow}]{\text{green arrow}} y$$

$$p = 23, g = 9$$

Publicly share
 p and g

$$p = 23, g = 9$$



Alice



Insecure channel



$$p = 23, g = 9$$

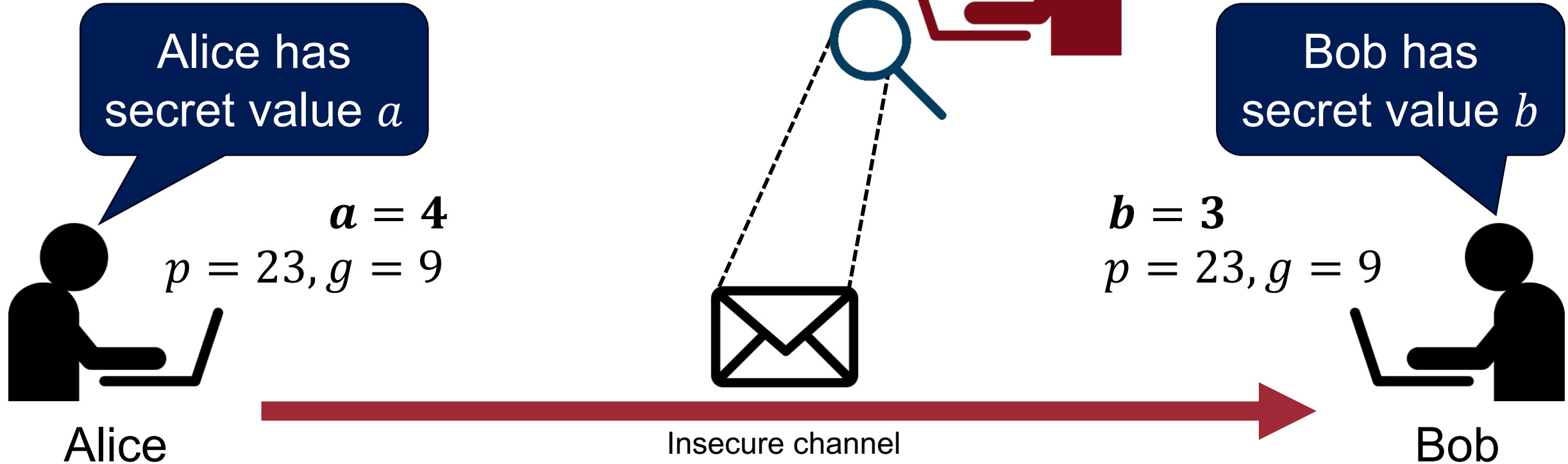


Bob

Diffie-Hellman Key Exchange (3)

$$g^x \bmod p \xrightleftharpoons[\text{red arrow}]{\text{green arrow}} y$$

$$p = 23, g = 9$$



Diffie-Hellman Key Exchange (4)

$$g^x \bmod p \xrightleftharpoons[\text{red arrow}]{\text{green arrow}} y$$

$$p = 23, g = 9$$

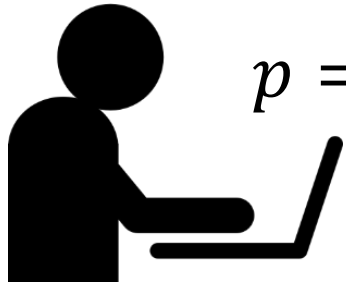


Send
 $A = g^a \bmod p$
to Bob

$$a = 4$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$



Alice

$$b = 3$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$



Bob

Insecure channel

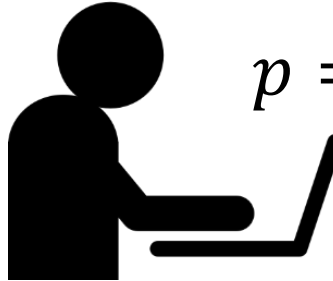
Diffie-Hellman Key Exchange (4)

17

$$g^x \bmod p \xrightleftharpoons[\text{red arrow}]{\text{green arrow}} y$$




$$p = 23, g = 9$$
$$A = (g^a \bmod p) = 6$$



$a = 4$
 $p = 23, g = 9$
 $A = (g^a \bmod p) = 6$

Alice

$b = 3$
 $p = 23, g = 9$
 $A = (g^a \bmod p) = 6$



Bob

Insecure channel

Diffie-Hellman Key Exchange (4)

18

$$g^x \bmod p \xleftrightarrow{\text{green}} y \xleftrightarrow{\text{red}}$$



$$p = 23, g = 9$$
$$A = (g^a \bmod p) = 6$$

Given g, p, y , it is very difficult to compute a

$$a = 4$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$



Alice

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$



Insecure channel

Discrete Logarithm Problem

Diffie-Hellman Key Exchange (4)

$$g^x \bmod p \xrightleftharpoons[\text{red arrow}]{\text{green arrow}} y$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$



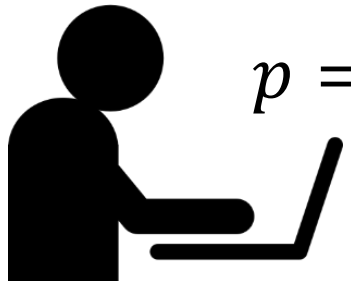
Send
 $B = g^b \bmod p$
 to Alice

$$a = 4$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$



Alice

$$b = 3$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$



Bob

Insecure channel

Diffie-Hellman Key Exchange (4)

20

$$g^x \bmod p \xrightleftharpoons[\text{red arrow}]{\text{green arrow}} y$$



$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

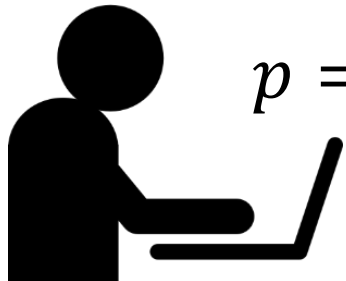
$$B = (g^b \bmod p) = 16$$

$$a = 4$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$



Alice

$$b = 3$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$



Bob

Insecure channel

Diffie-Hellman Key Exchange (5)

Symmetric key:



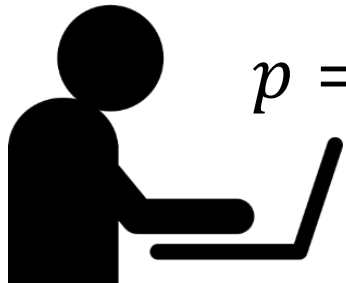
$$K = g^{ab} \bmod p$$



$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$



$$a = 4$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$

Alice

$$b = 3$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$



Bob

Insecure channel

Diffie-Hellman Key Exchange (5)

Symmetric key:

$$\text{key} \quad K = g^{ab} \bmod p$$



$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$

$$\begin{aligned} K &= (B^a \bmod p) = (g^{ab} \bmod p) \\ &= (16^4 \bmod 23) = 9 \end{aligned}$$

Theorem:

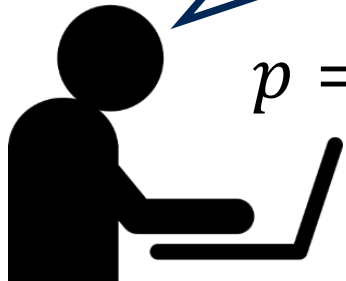
$$((X \bmod p)^k \bmod p) = (X^k \bmod p)$$

$$a = 4$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$



Alice

$$b = 3$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$



Bob

Insecure channel

Diffie-Hellman Key Exchange (5)

Symmetric key:

$$\text{key} \quad K = g^{ab} \bmod p$$



$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$

$$K = (B^a \bmod p) = (g^{ab} \bmod p) \\ = (16^4 \bmod 23) = 9 \quad \text{key}$$

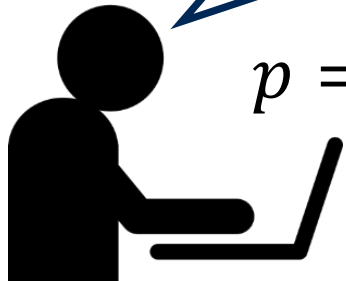
$$K = (A^b \bmod p) = (g^{ab} \bmod p) \\ = (6^3 \bmod 23) = 9 \quad \text{key}$$

$$a = 4$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$



Alice

$$b = 3$$

$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$



Bob

Insecure channel

Security of the Diffie-Hellman Key Exchange

24

Symmetric key:



$$K = g^{ab} \bmod p$$



$$p = 23, g = 9$$

$$A = (g^a \bmod p) = 6$$

$$B = (g^b \bmod p) = 16$$

The attacker cannot efficiently
compute $(g^{ab} \bmod p)$
without knowing a and b

Why should p be Prime?

Symmetric key:



$$K = g^{ab} \bmod p$$

$$g = 2$$

$$p = 11$$

- $2^0 \bmod 11 = 1$
- $2^1 \bmod 11 = 2$
- $2^2 \bmod 11 = 4$
- $2^3 \bmod 11 = 8$
- $2^4 \bmod 11 = 5$
- $2^5 \bmod 11 = 10$
- $2^6 \bmod 11 = 9$
- $2^7 \bmod 11 = 7$
- $2^8 \bmod 11 = 3$
- $2^9 \bmod 11 = 6$
- $2^{10} \bmod 11 = 1$

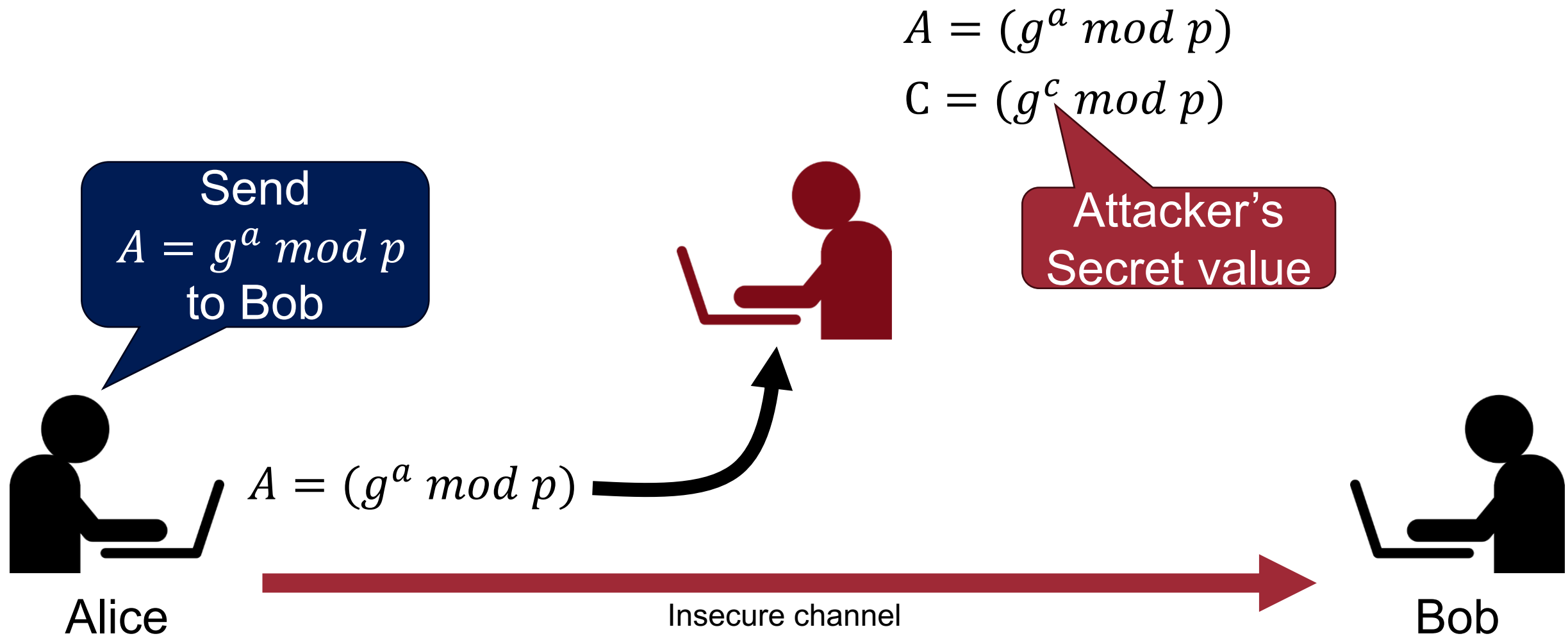
$$p = 12$$

- $2^0 \bmod 12 = 1$
- $2^1 \bmod 12 = 2$
- $2^2 \bmod 12 = 4$
- $2^3 \bmod 12 = 8$
- $2^4 \bmod 12 = 4$
- $2^5 \bmod 12 = 8$
- $2^6 \bmod 12 = 4$
- $2^7 \bmod 12 = 8$
- $2^8 \bmod 12 = 4$
- $2^9 \bmod 12 = 8$
- $2^{10} \bmod 12 = 4$

Too simple key pattern
that can be inferred

Man-in-the-Middle Attack in DH Key Exchange

26

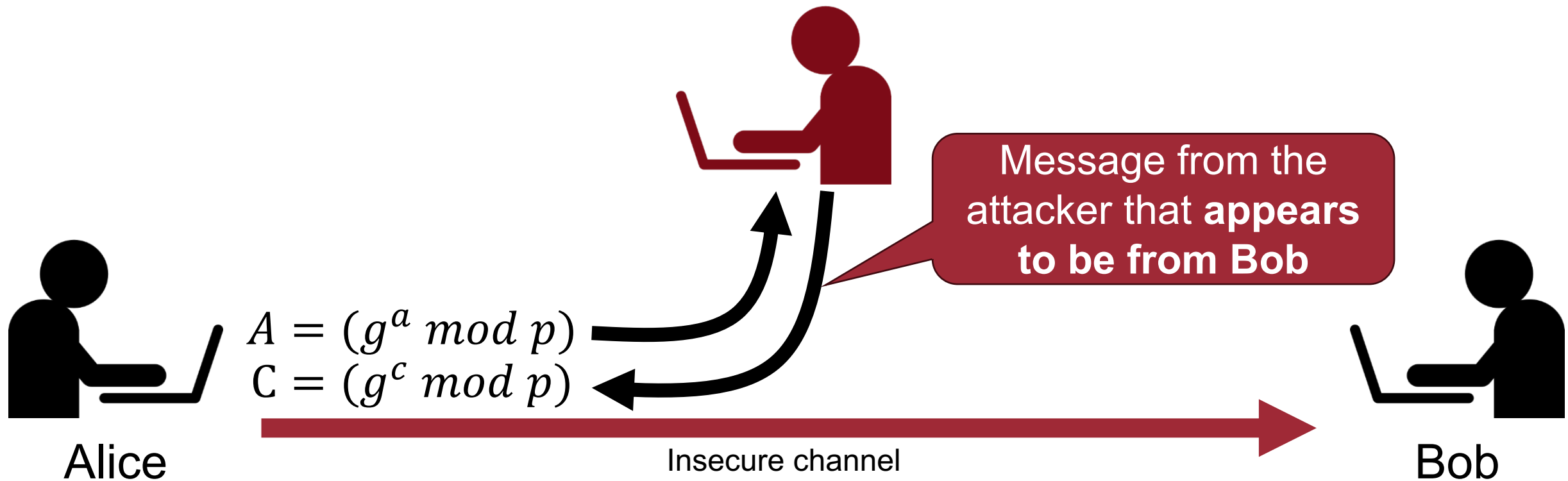


Man-in-the-Middle Attack in DH Key Exchange

27

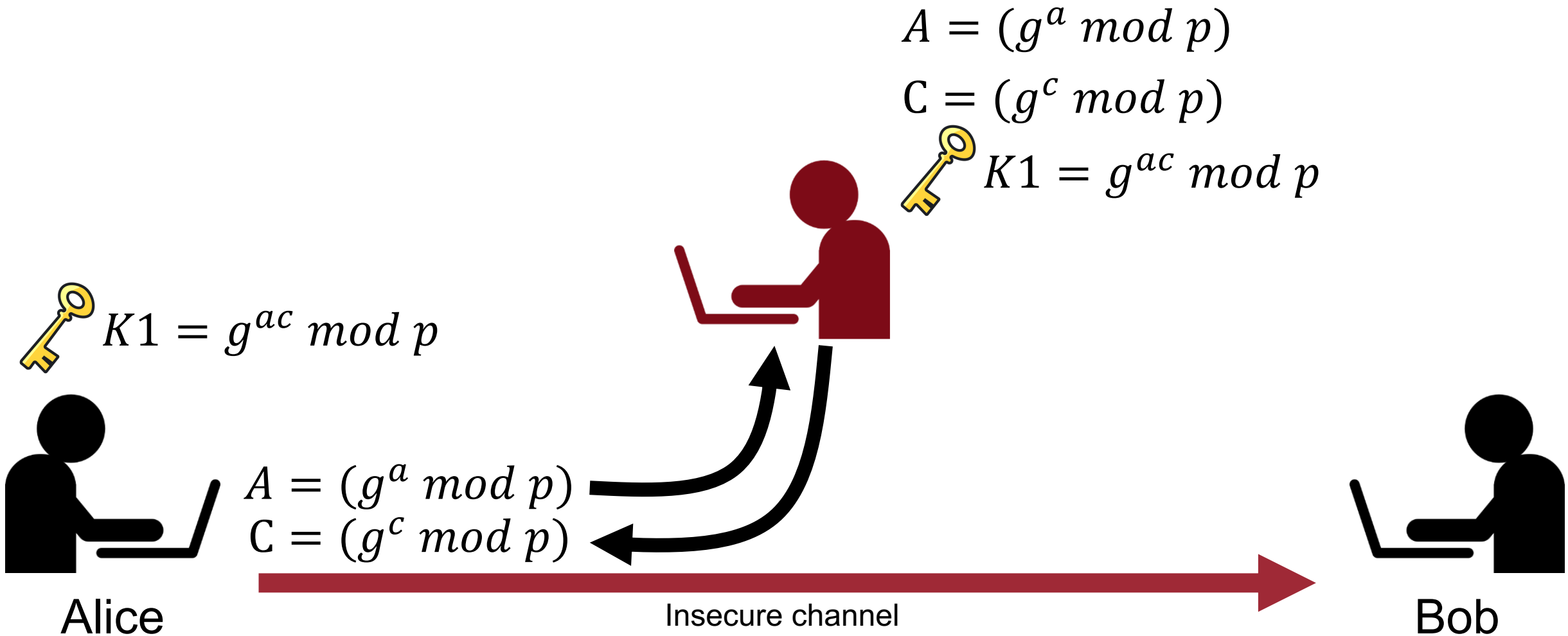
$$A = (g^a \bmod p)$$

$$C = (g^c \bmod p)$$



Man-in-the-Middle Attack in DH Key Exchange

28





Man-in-the-Middle Attack in DH Key Exchange


29


$$B = (g^b \bmod p)$$

$$C = (g^c \bmod p)$$


$$K2 = g^{bc} \bmod p$$


$$K1 = g^{ac} \bmod p$$


$$K1 = g^{ac} \bmod p$$


$$K2 = g^{bc} \bmod p$$



Alice



Insecure channel

$$B = (g^b \bmod p)$$

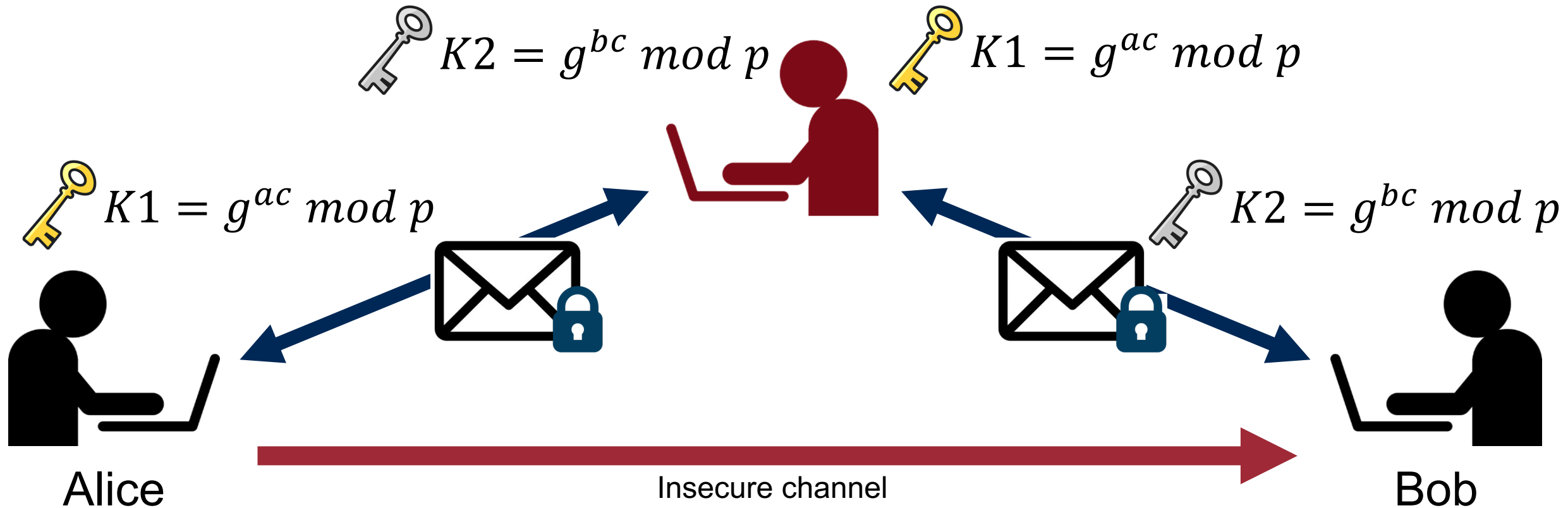
$$C = (g^c \bmod p)$$



Bob

Man-in-the-Middle Attack in DH Key Exchange

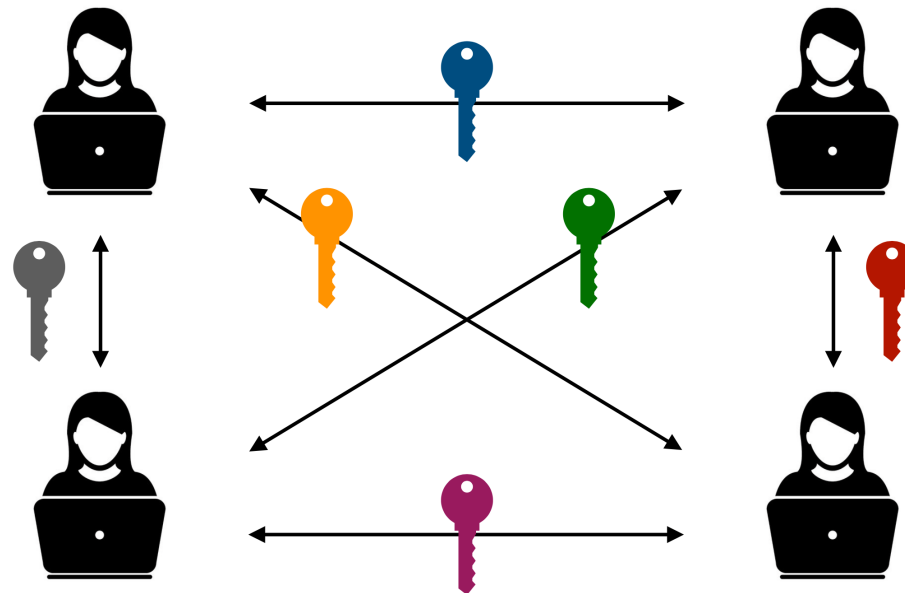
30



Symmetric-key Cryptography

- Recap: the same key shared between two parties
- What happens if there are many users?
 - n users: $\binom{n}{2} = n(n-1)/2$
 - Example: 100 users \rightarrow 4,950 keys
- Key distribution and maintenance problem

How to solve this issue?



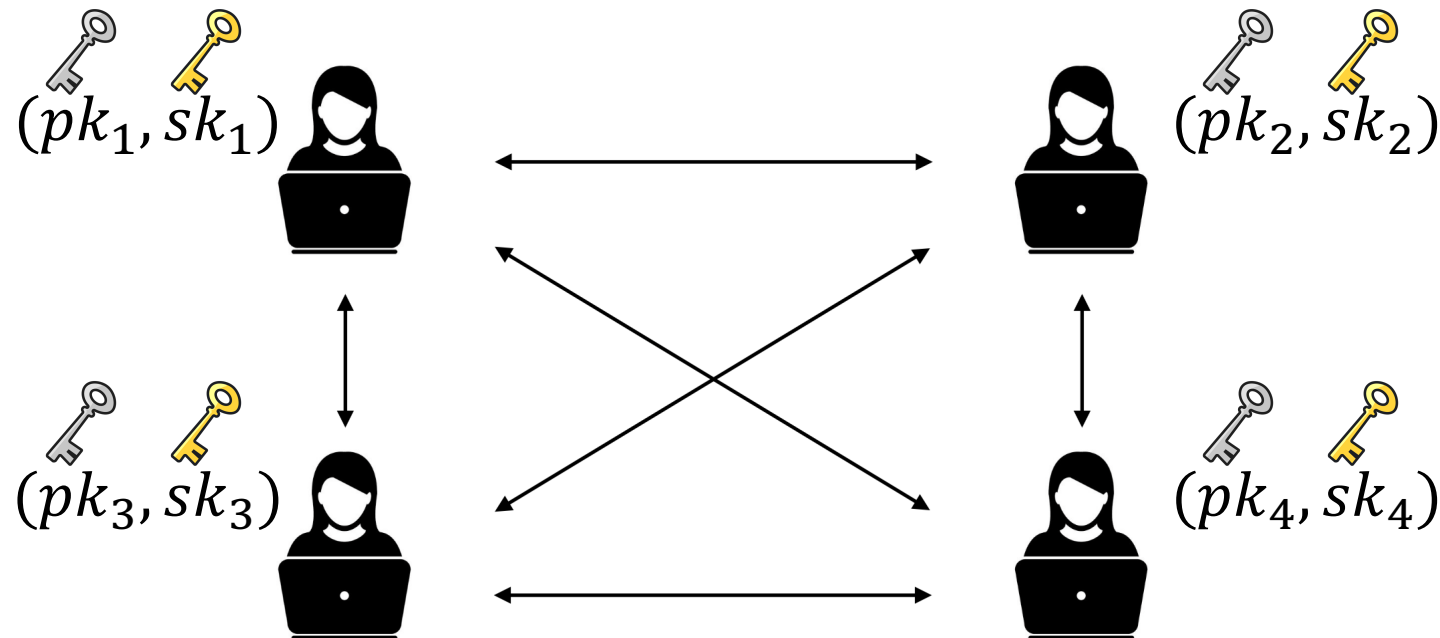
Asymmetric-key Cryptography



- Each party has two distinct keys: public key and private key
 - Also known as public-key algorithm
- Invented in 1976 by Diffie and Hellman (ACM Turing Award 2015)

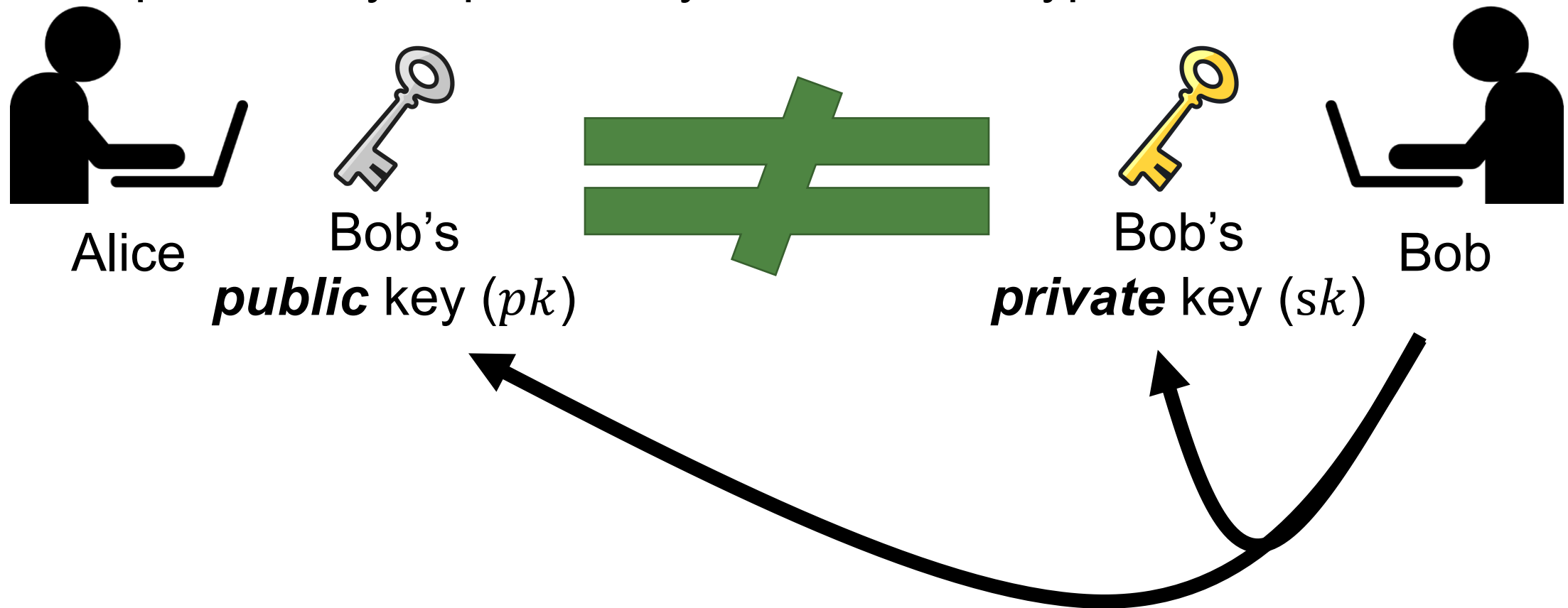
Asymmetric-key Cryptography

- pk : public key, widely disseminated, used for encryption
- sk : private key kept secretly, used for decryption
- n users: $2n$ keys



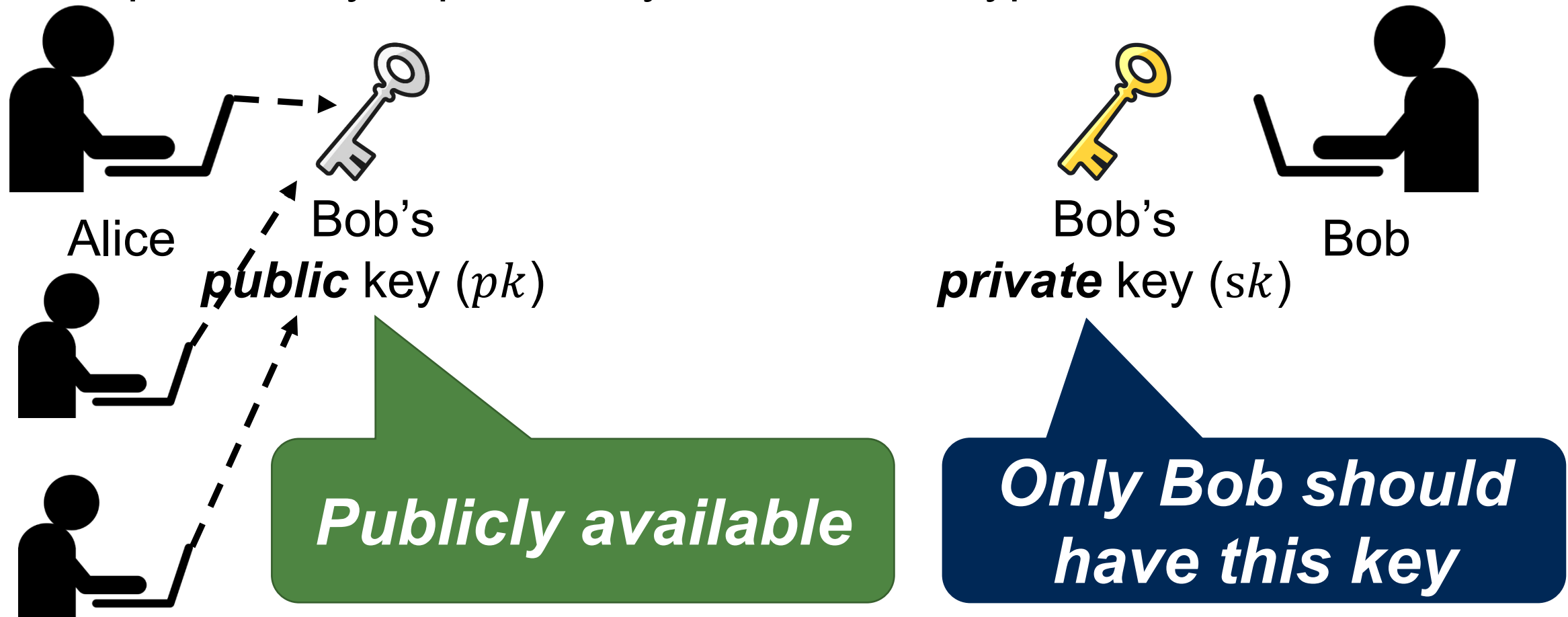
Asymmetric-key Cryptography

- pk : public key, widely disseminated, used for encryption
- sk : private key kept secretly, used for decryption



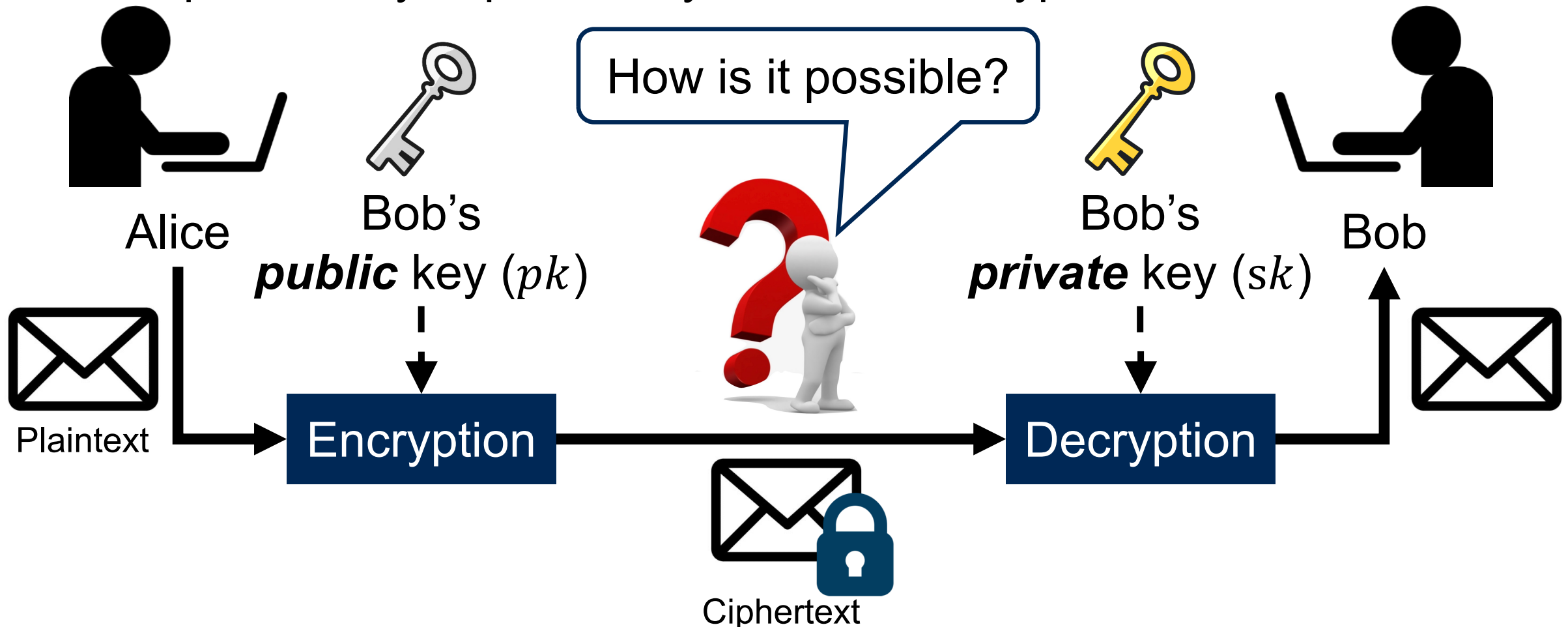
Asymmetric-key Cryptography

- pk : public key, widely disseminated, used for encryption
- sk : private key kept secretly, used for decryption



Asymmetric-key Cryptography

- pk : public key, widely disseminated, used for encryption
- sk : private key kept secretly, used for decryption

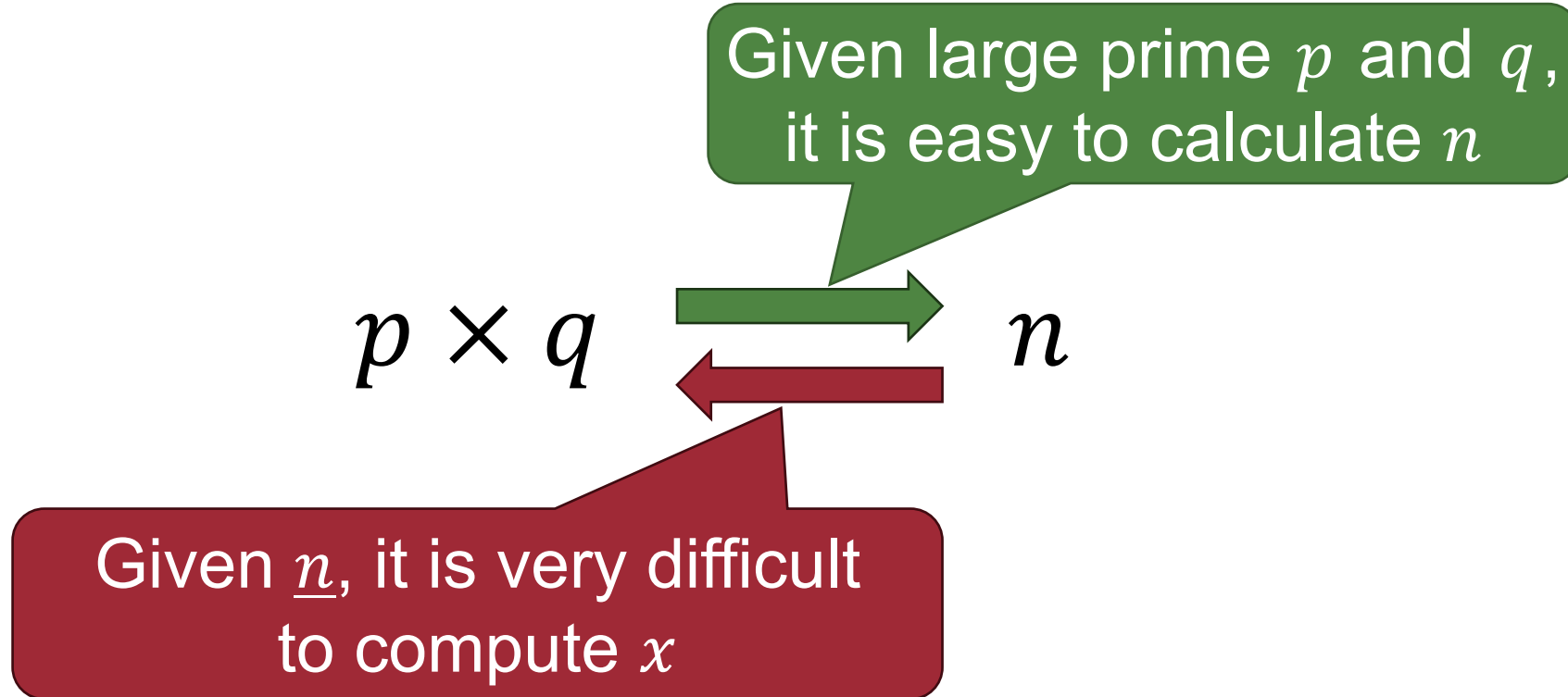


RSA Cryptosystem



- Invented by Rivest, Shamir, and Adleman (MIT) in 1977
 - ACM Turing award in 2002
- Rely on the practical difficulty of factoring the product of two large prime numbers
 - Security based on *Integer Factorization Problem*

Integer Factorization Problem



RSA Algorithm (1): Key Generation

39

Select two large
primes p and q

$$p = 7, q = 13$$

Public place



Alice

Insecure channel



Bob

RSA Algorithm (1): Key Generation

40

Compute $n = pq$ and
 $\phi(n) = (p - 1)(q - 1)$

$$p = 7, q = 13$$
$$n = 91, \phi(n) = 72$$

Public place



Alice

Insecure channel



Bob

RSA Algorithm (1): Key Generation

41

Choose e s.t.

- $1 < e < \phi(n)$ and
- $\gcd(\phi(n), e) = 1$

$$p = 7, q = 13$$

$$n = 91, \phi(n) = 72$$

$$e = 5$$

Public place



Alice

Insecure channel



Bob

RSA Algorithm (1): Key Generation

How to find d ?
→ Extended Euclidean Algorithm!

Choose d s.t.

- $1 < d < \phi(n)$ and
- $(ed \bmod \phi(n)) = 1$

Public place



Alice



$p = 7, q = 13$
 $n = 91, \phi(n) = 72$
 $e = 5$
 $d = 29$



Bob

Insecure channel

Euclidean Algorithm



Goal: Finding Greatest Common Divisor (GCD)

Fact 1: $\gcd(a, 0) = a$

Fact 2: $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b ($a > b$)

Example

$\gcd(72, 5)$

$$p = 7, q = 13$$
$$n = 91, \phi(n) = 72$$

$$e = 5$$
$$d = 29$$

Choose e s.t.

- $1 < e < \phi(n)$ and
- $\gcd(\phi(n), e) = 1$

Euclidean Algorithm



Goal: Finding Greatest Common Divisor (GCD)

Fact 1: $\gcd(a, 0) = a$

Fact 2: $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b ($a > b$)

Example

$$\gcd(72, 5) \quad 72 = (5 * 14) + 2$$

Euclidean Algorithm



Goal: Finding Greatest Common Divisor (GCD)

Fact 1: $\gcd(a, 0) = a$

Fact 2: $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b ($a > b$)

Example

$$\gcd(72, 5) \quad 72 = (5 * 14) + 2$$

$$\gcd(5, 2) \quad 5 = (2 * 2) + 1$$

Euclidean Algorithm



Goal: Finding Greatest Common Divisor (GCD)

Fact 1: $\gcd(a, 0) = a$

Fact 2: $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b ($a > b$)

Example

$$\gcd(72, 5) \quad 72 = (5 * 14) + 2$$

$$\gcd(5, 2) \quad 5 = (2 * 2) + 1$$

$$\gcd(2, 1) \quad 2 = (2 * 1) + 0$$



Euclidean Algorithm



Goal: Finding Greatest Common Divisor (GCD)

Fact 1: $\gcd(a, 0) = a$

Fact 2: $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b ($a > b$)

Example

$$\gcd(72, 5) \quad 72 = (5 * 14) + 2$$

$$\gcd(5, 2) \quad 5 = (2 * 2) + 1$$

$$\gcd(2, 1) \quad 2 = (2 * 1) + 0$$

$$\gcd(1, 0)$$



Euclidean Algorithm



Goal: Finding Greatest Common Divisor (GCD)

Fact 1: $\gcd(a, 0) = a$

Fact 2: $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b ($a > b$)

Example

$$\gcd(72, 5) \quad 72 = (5 * 14) + 2$$

$$\gcd(5, 2) \quad 5 = (2 * 2) + 1$$

$$\gcd(2, 1) \quad 2 = (2 * 1) + 0$$

$$\gcd(1, 0) = 1$$

Extended Euclidean Algorithm

- **Goal:** Computing integers x and y s.t.
$$ax + by = \gcd(a, b)$$

Choose e s.t.

- $1 < e < \phi(n)$ **and**
- $\gcd(\phi(n), e) = 1$

Choose d s.t.

- $1 < d < \phi(n)$ **and**
- $(ed \bmod \phi(n)) = 1$

$$p = 7, q = 13$$
$$n = 91, \phi(n) = 72$$

$$e = 5$$
$$d = 29$$

Extended Euclidean Algorithm

- **Goal:** Computing integers x and y s.t.

$$ax + by = \gcd(a, b)$$

$$ed + \phi(n)(-k) = \gcd(\phi(n), e) = 1$$

Choose e s.t.

- $1 < e < \phi(n)$ **and**
- $\gcd(\phi(n), e) = 1$

Choose d s.t.

- $1 < d < \phi(n)$ **and**
- $(ed \bmod \phi(n)) = 1$

$$p = 7, q = 13$$

$$n = 91, \phi(n) = 72$$

$$e = 5$$

$$d = 29$$

Extended Euclidean Algorithm

- **Goal:** Computing integers x and y s.t.

$$ax + by = \gcd(a, b)$$

$$ed + \phi(n)(-k) = \gcd(\phi(n), e) = 1$$

$(e = 5, \phi(n) = 72)$

We can find
the value d ! 😊

Extended Euclidean Algorithm

- **Goal:** Computing integers x and y s.t.

$$ax + by = \gcd(a, b)$$

$$ed + \phi(n)(-k) = \gcd(\phi(n), e) = 1$$

$(e = 5, \phi(n) = 72)$

Example

$$\gcd(72, 5) \quad 72 = (5 * 14) + 2$$

$$\gcd(5, 2) \quad 5 = (2 * 2) + 1 \quad \Rightarrow \quad 5 - (2 * 2) = 1$$

$$\gcd(2, 1) \quad 2 = (2 * 1) + 0$$

$$\gcd(1, 0) = 1$$

$$\begin{aligned} x &= 1 \\ y &= -2 \end{aligned}$$

Extended Euclidean Algorithm

- **Goal:** Computing integers x and y s.t.

$$ax + by = \gcd(a, b)$$

$$ed + \phi(n)(-k) = \gcd(\phi(n), e) = 1$$

$(e = 5, \phi(n) = 72)$

Example

$$\gcd(72, 5) \quad 72 = (5 * 14) + 2$$

$$\gcd(5, 2) \quad 5 = (2 * 2) + 1 \quad \Rightarrow \quad 5 - (2 * 2) = 1$$

$$\gcd(2, 1) \quad 2 = (2 * 1) + 0$$

$$\gcd(1, 0) = 1$$

$$2 = 72 - (5 * 14)$$

Extended Euclidean Algorithm

- **Goal:** Computing integers x and y s.t.

$$ax + by = \gcd(a, b)$$

$$ed + \phi(n)(-k) = \gcd(\phi(n), e) = 1$$

$(e = 5, \phi(n) = 72)$

Example

$$\gcd(72, 5) \quad 72 = (5 * 14) + 2 \longrightarrow 5 - ((72 - 5 * 14) * 2) = 1$$

$$\gcd(5, 2) \quad 5 = (2 * 2) + 1 \longrightarrow 5 - (2 * 2) = 1$$

$$\gcd(2, 1) \quad 2 = (2 * 1) + 0$$

$$\gcd(1, 0) = 1$$

Extended Euclidean Algorithm

- **Goal:** Computing integers x and y s.t.

$$ax + by = \gcd(a, b)$$

$$ed + \phi(n)(-k) = \gcd(\phi(n), e) = 1$$

$(e = 5, \phi(n) = 72)$

Example

$$\gcd(72, 5) \quad 72 = (5 * 14) + 2 \quad \Rightarrow \quad 5 * 29 + 72(-2) = 1$$

$$\gcd(5, 2) \quad 5 = (2 * 2) + 1 \quad \Rightarrow \quad 5 - (2 * 2) = 1$$

$$\gcd(2, 1) \quad 2 = (2 * 1) + 0$$

$$\gcd(1, 0) = 1$$

$$x = d = 29$$

$$y = -k = -2$$

Logic Flow

```

 $r_1 \leftarrow a; \quad r_2 \leftarrow b;$  (Initialization)
while ( $r_2 > 0$ )
{
   $q \leftarrow r_1 / r_2;$ 
   $r \leftarrow r_1 - q \times r_2;$ 
   $r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$ 
}
gcd( $a, b$ )  $\leftarrow r_1$ 

```

Euclidean Algorithm

```

 $r_1 \leftarrow a; \quad r_2 \leftarrow b;$ 
 $s_1 \leftarrow 1; \quad s_2 \leftarrow 0;$  (Initialization)
 $t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$ 
while ( $r_2 > 0$ )
{
   $q \leftarrow r_1 / r_2;$ 
   $r \leftarrow r_1 - q \times r_2;$  (Updating  $r$ 's)
   $r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$ 
   $s \leftarrow s_1 - q \times s_2;$  (Updating  $s$ 's)
   $s_1 \leftarrow s_2; \quad s_2 \leftarrow s;$ 
   $t \leftarrow t_1 - q \times t_2;$  (Updating  $t$ 's)
   $t_1 \leftarrow t_2; \quad t_2 \leftarrow t;$ 
}
gcd( $a, b$ )  $\leftarrow r_1; \quad s \leftarrow s_1; \quad t \leftarrow t_1$ 

```

Extended Euclidean Algorithm

Exercise



- Given $a = 161$ and $b = 28$, find $\gcd(a, b)$ and the values of x and y such that $ax + by = \gcd(a, b)$

RSA Algorithm (1): Key Generation

How to find d ?
→ Extended Euclidean Algorithm!

Choose d s.t.

- $1 < d < \phi(n)$ and
- $(ed \bmod \phi(n)) = 1$

Public place



Alice



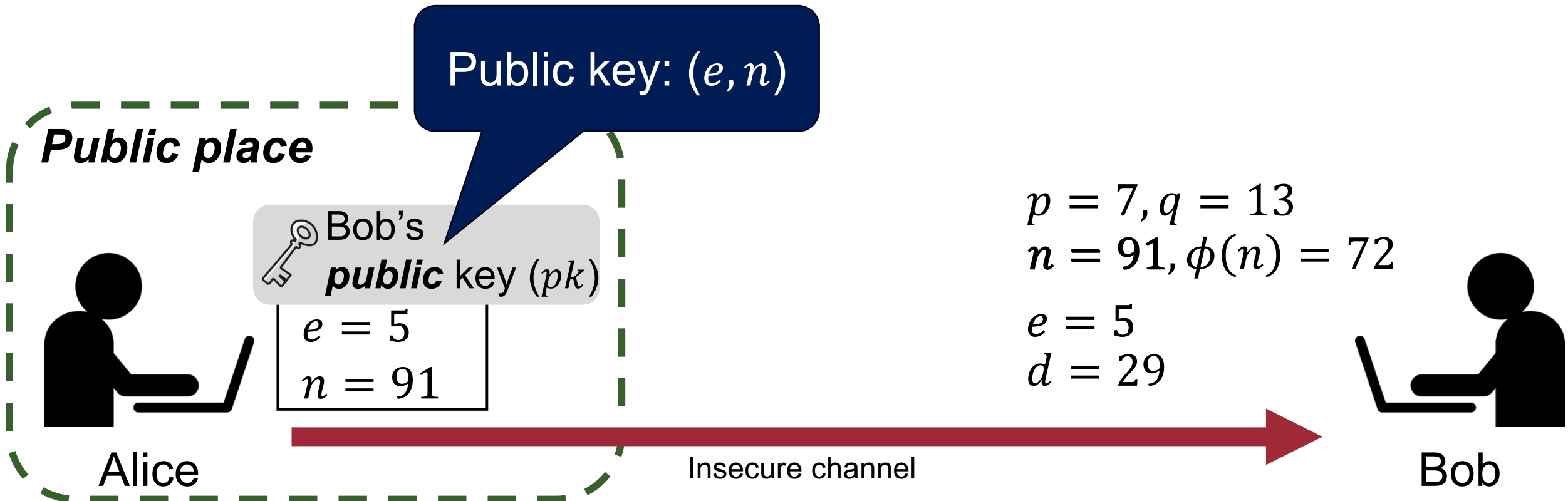
$p = 7, q = 13$
 $n = 91, \phi(n) = 72$
 $e = 5$
 $d = 29$



Bob

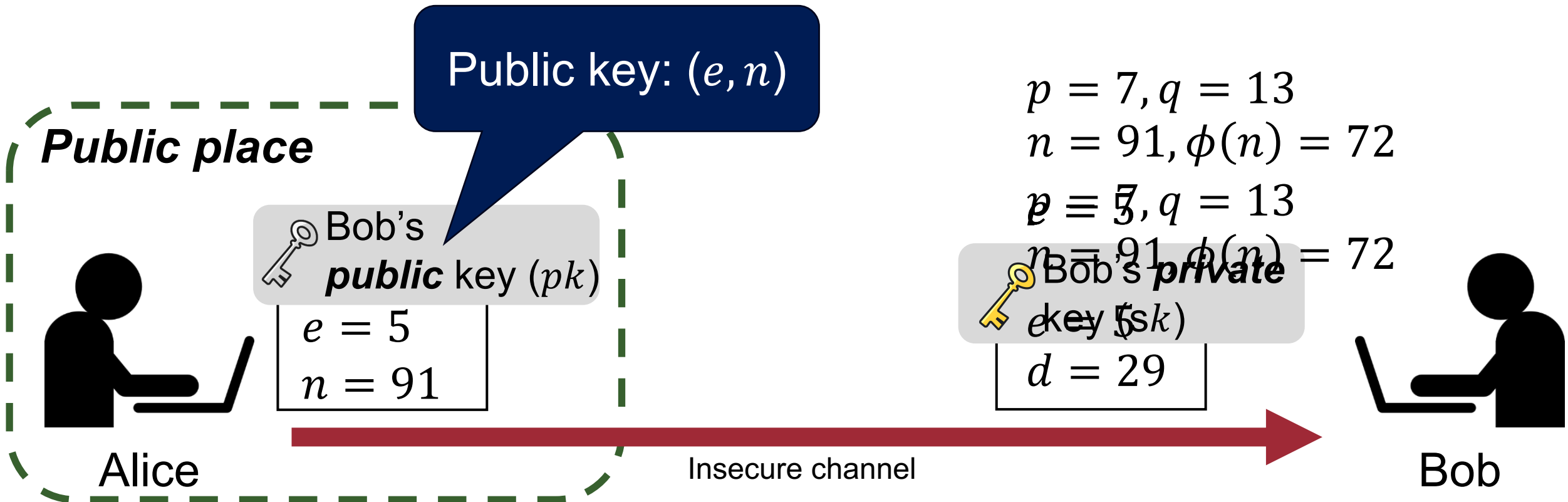
Insecure channel

RSA Algorithm (1): Key Generation



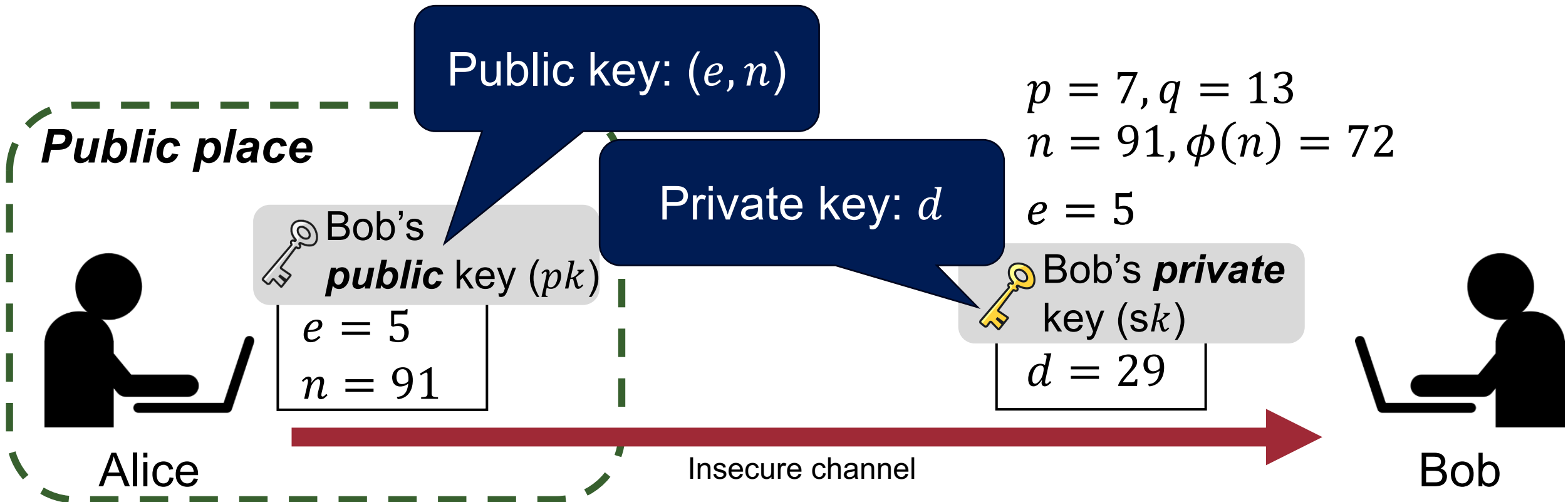
RSA Algorithm (1): Key Generation

60

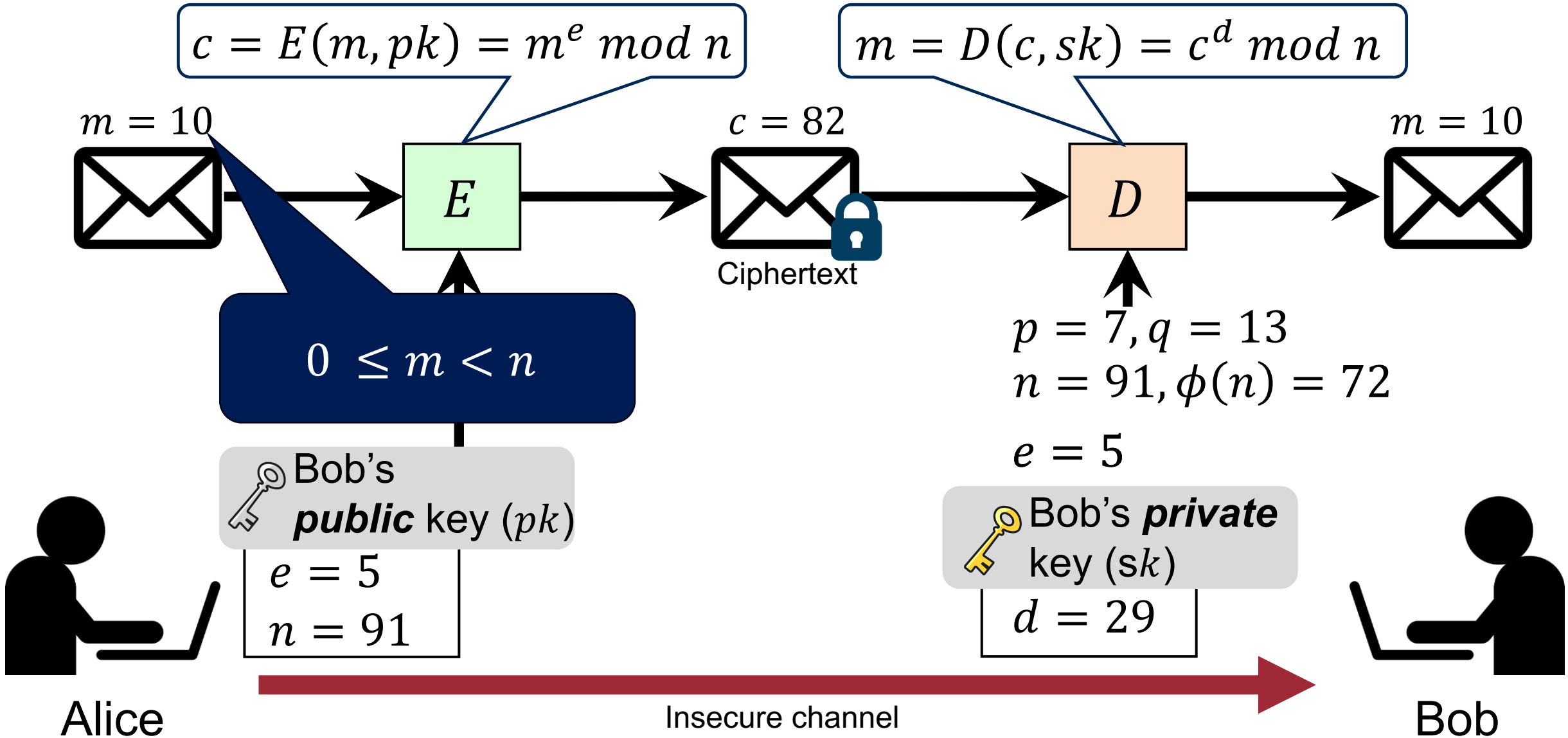


RSA Algorithm (1): Key Generation

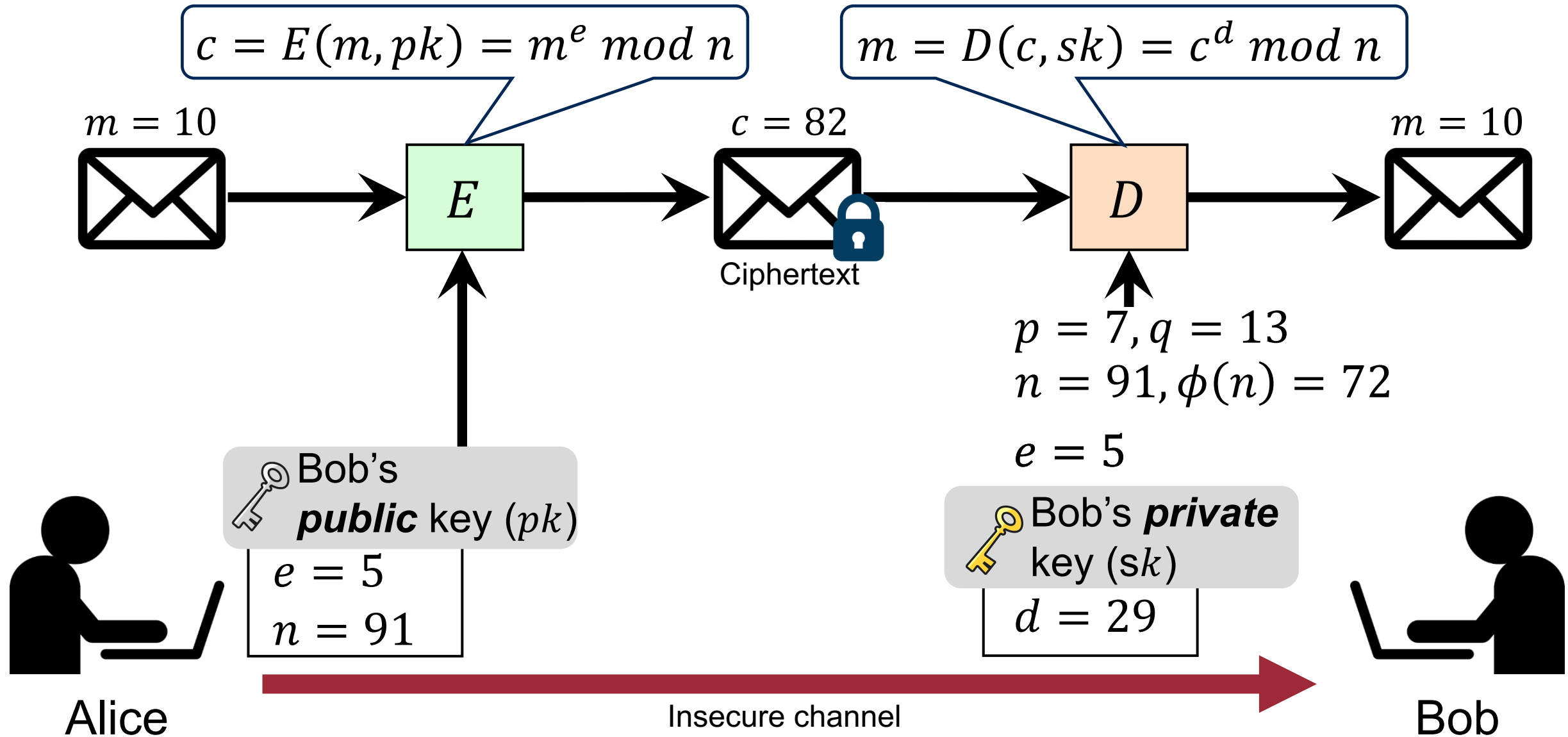
61



RSA Algorithm (2): Encryption and Decryption ⁶²



RSA Algorithm (2): Encryption and Decryption 63



Correctness of the RSA Algorithm

$$c = E(m, pk) = m^e \bmod n$$

$$m = D(c, sk) = c^d \bmod n$$

Correctness: $m = (m^e \bmod n)^d \bmod n$
 $= m^{ed} \bmod n$

Theorem:

$$((X \bmod p)^k \bmod p) = (X^k \bmod p)$$

Correctness of the RSA Algorithm

$$c = E(m, pk) = m^e \bmod n$$

$$m = D(c, sk) = c^d \bmod n$$

Correctness: $m = (m^e \bmod n)^d \bmod n$
 $= m^{ed} \bmod n$
 $= m^{1+k \cdot \phi(n)} \bmod n$

We choose d s.t.
 $(ed \bmod \phi(n)) = 1$

Theorem:

$$((X \bmod p)^k \bmod p) = (X^k \bmod p)$$

Correctness of the RSA Algorithm

$$c = E(m, pk) = m^e \bmod n$$

$$m = D(c, sk) = c^d \bmod n$$

Correctness: $m = (m^e \bmod n)^d \bmod n$

$$= m^{ed} \bmod n$$

$$= m^{1+k \cdot \phi(n)} \bmod n$$

$$= m \cdot (m^{\phi(n)})^k \bmod n$$

$$= m \bmod n$$

$$= m$$

We choose d s.t.
 $(ed \bmod \phi(n)) = 1$

Theorem:

$$((X \bmod p)^k \bmod p) = (X^k \bmod p)$$

Euler's Theorem:

$$(X^{\phi(n)} \bmod n) = 1 \text{ where } \gcd(X, n) = 1$$

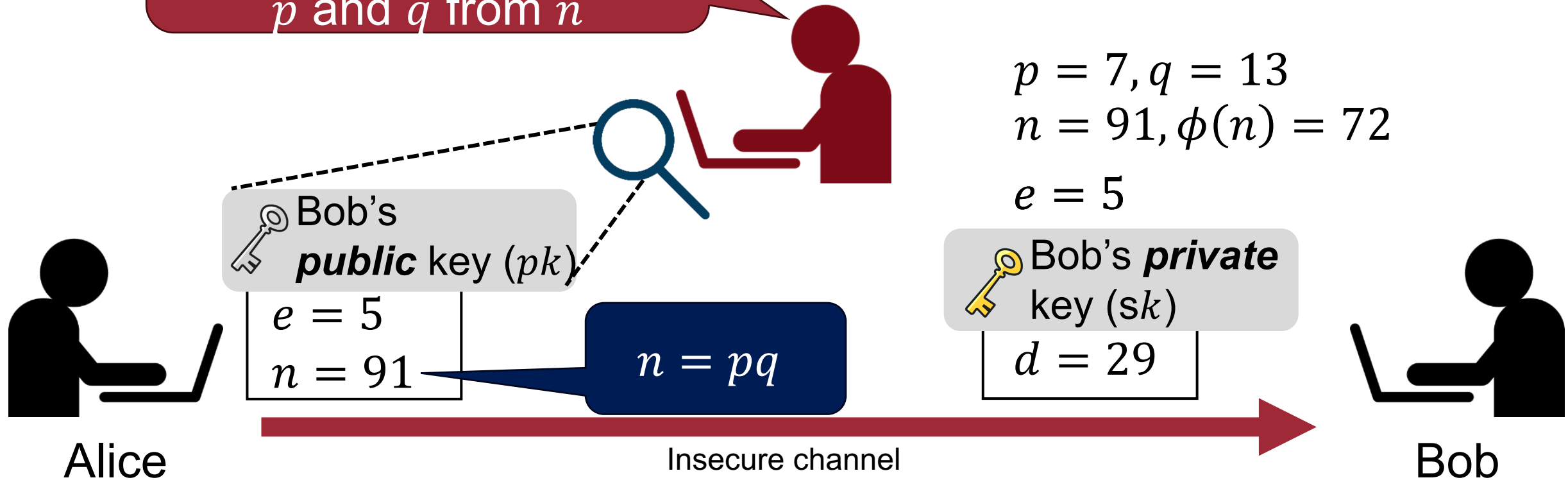
Also, refer to *Fermat's little theorem* ☺

Security of the RSA Algorithm

$$c = E(m, pk) = m^e \bmod n$$

$$m = D(c, sk) = c^d \bmod n$$

The attacker cannot efficiently compute p and q from n



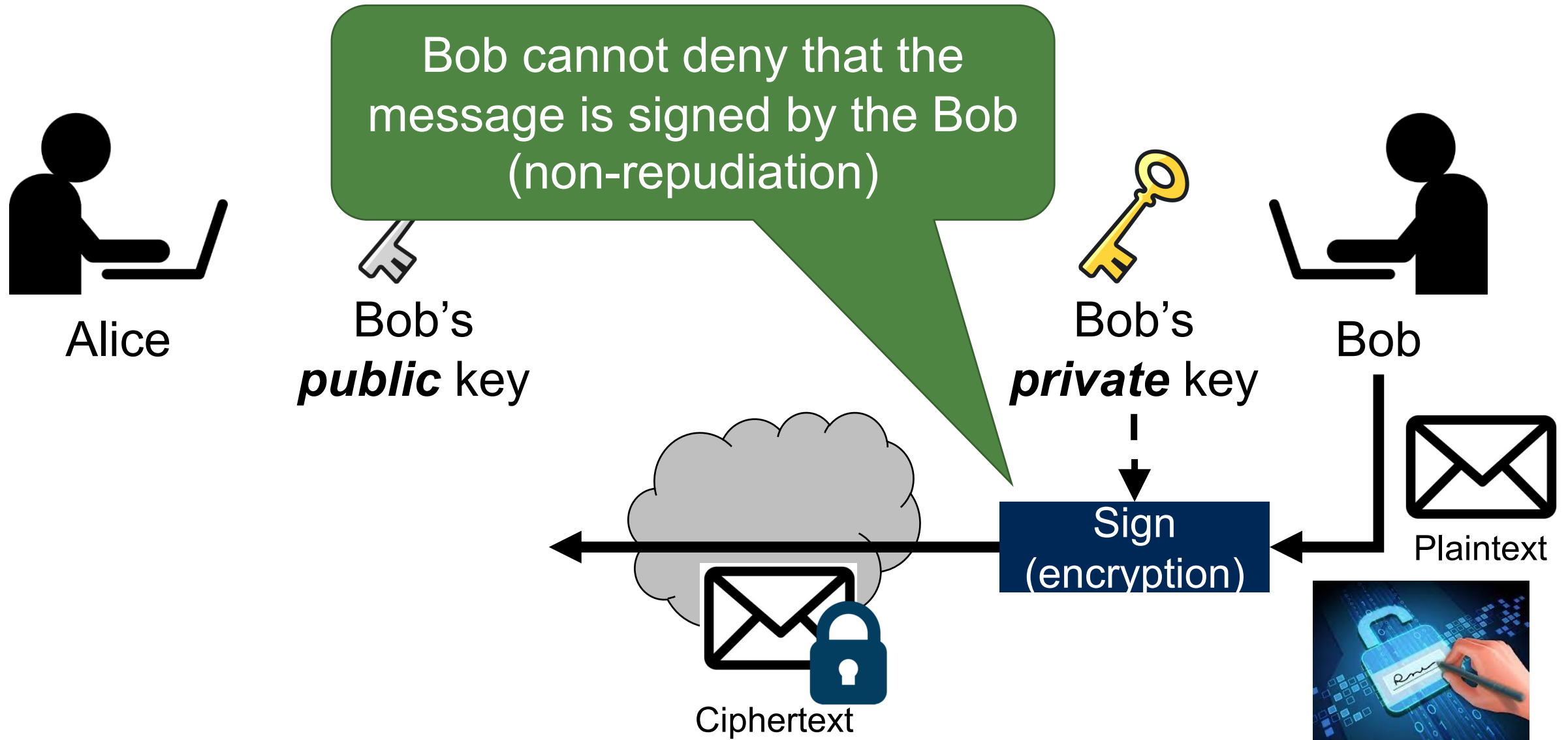
Comparison with Symmetric-Key Cryptography

68



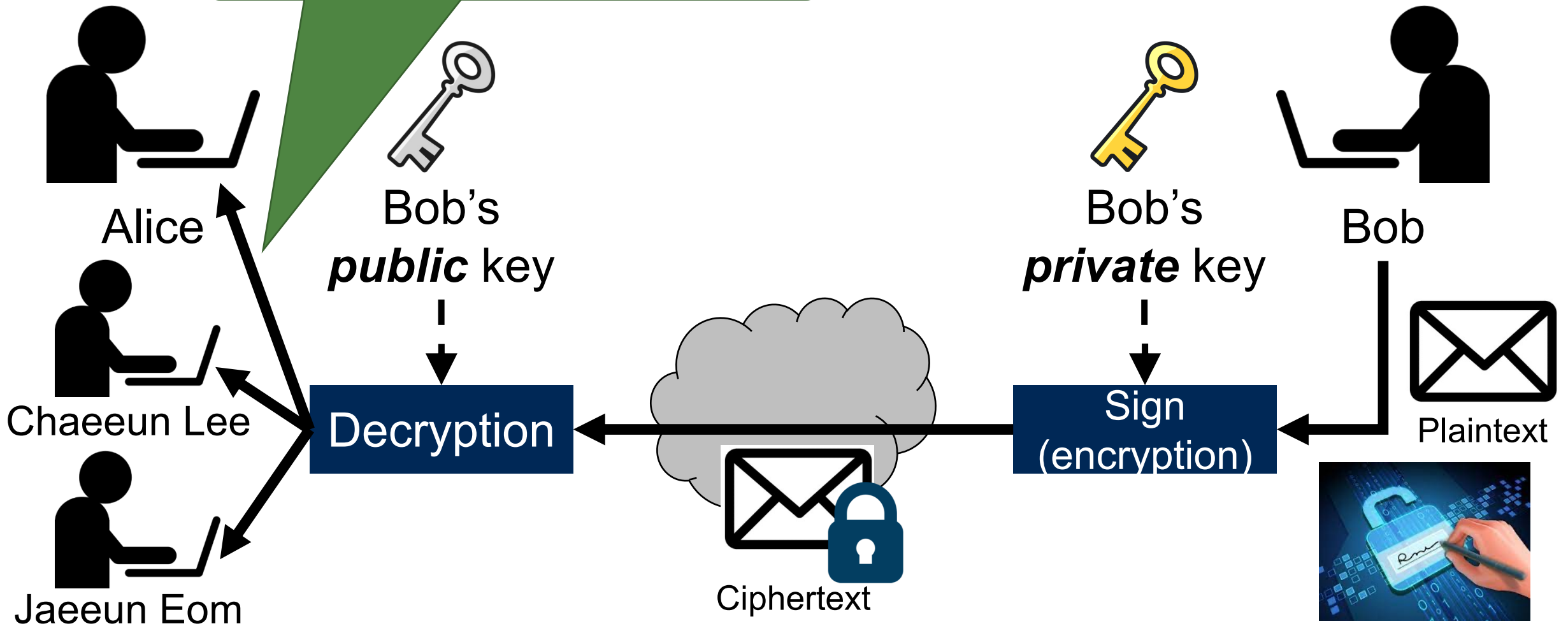
- Pros
 - No need to share a secret
 - More applications: Digital sign

Digital Signature



Digital Signature

This message is from Bob
(authentication)



Digital Signature in Detail (1)

71

Publicize the
verification message

$m = 10$

$p = 7, q = 13$
 $n = 91, \phi(n) = 72$
 $e = 5$

Bob's
public key (pk)

$e = 5$
 $n = 91$

Bob's **private**
key (sk)

$d = 29$



Alice

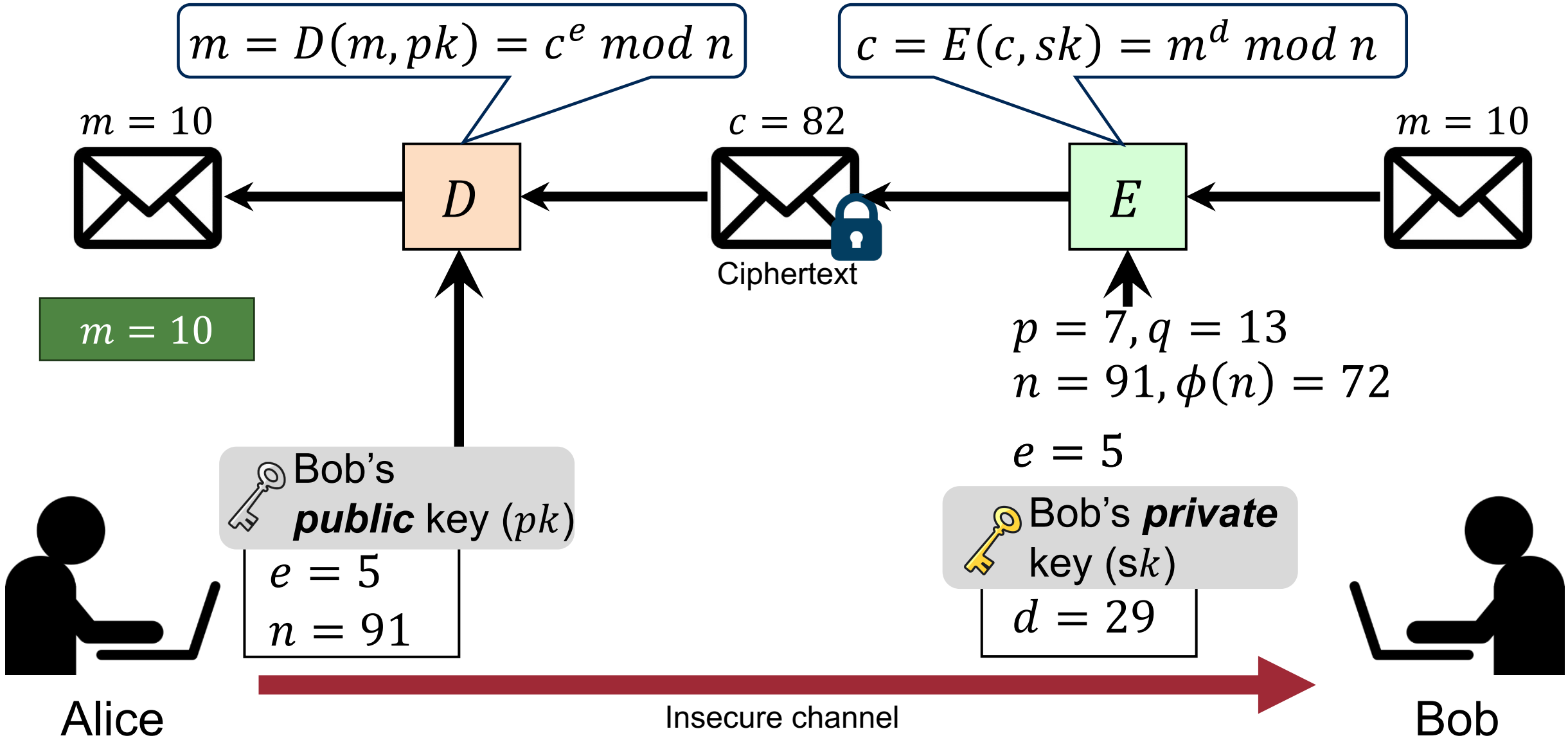
Insecure channel



Bob

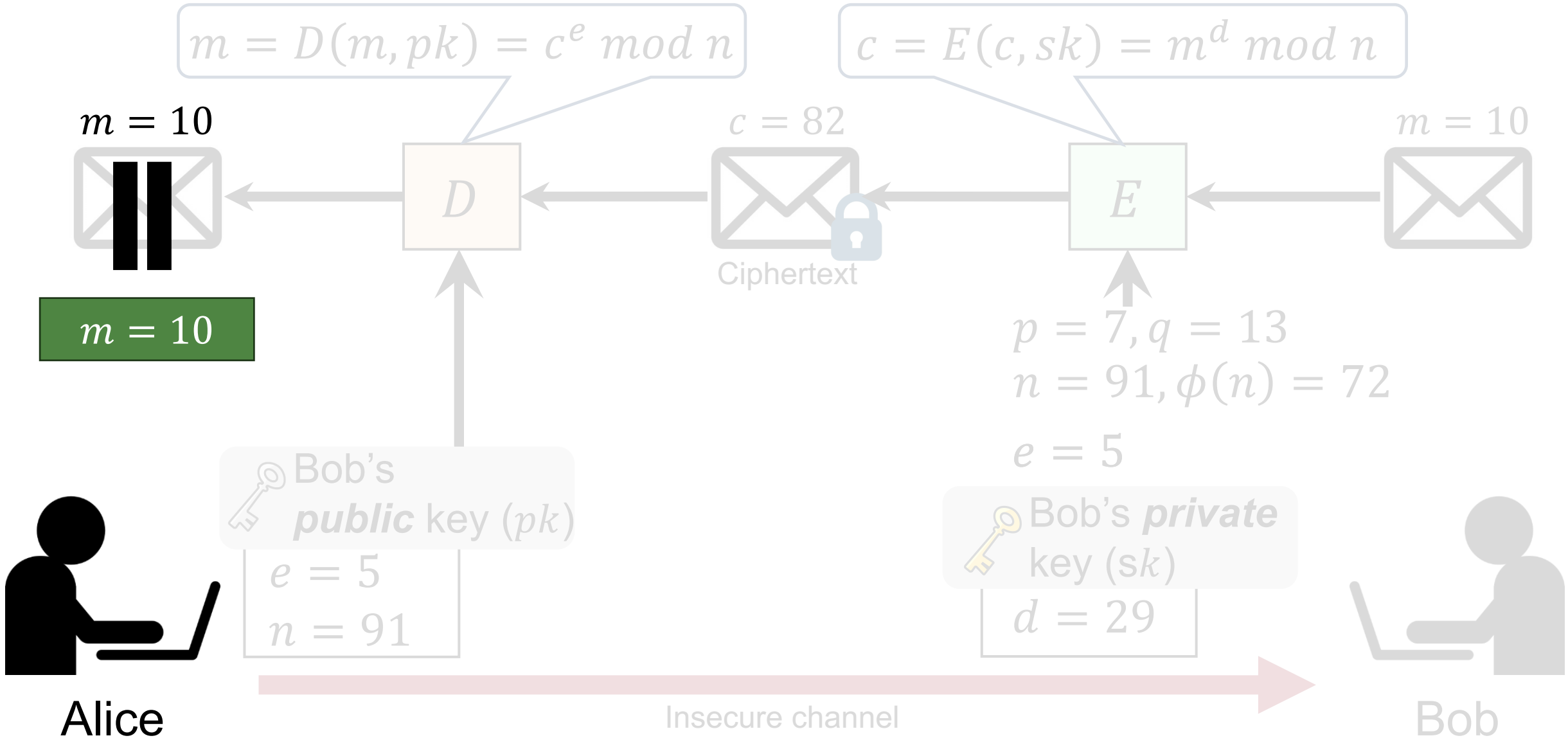
Digital Signature in Detail (2)

72



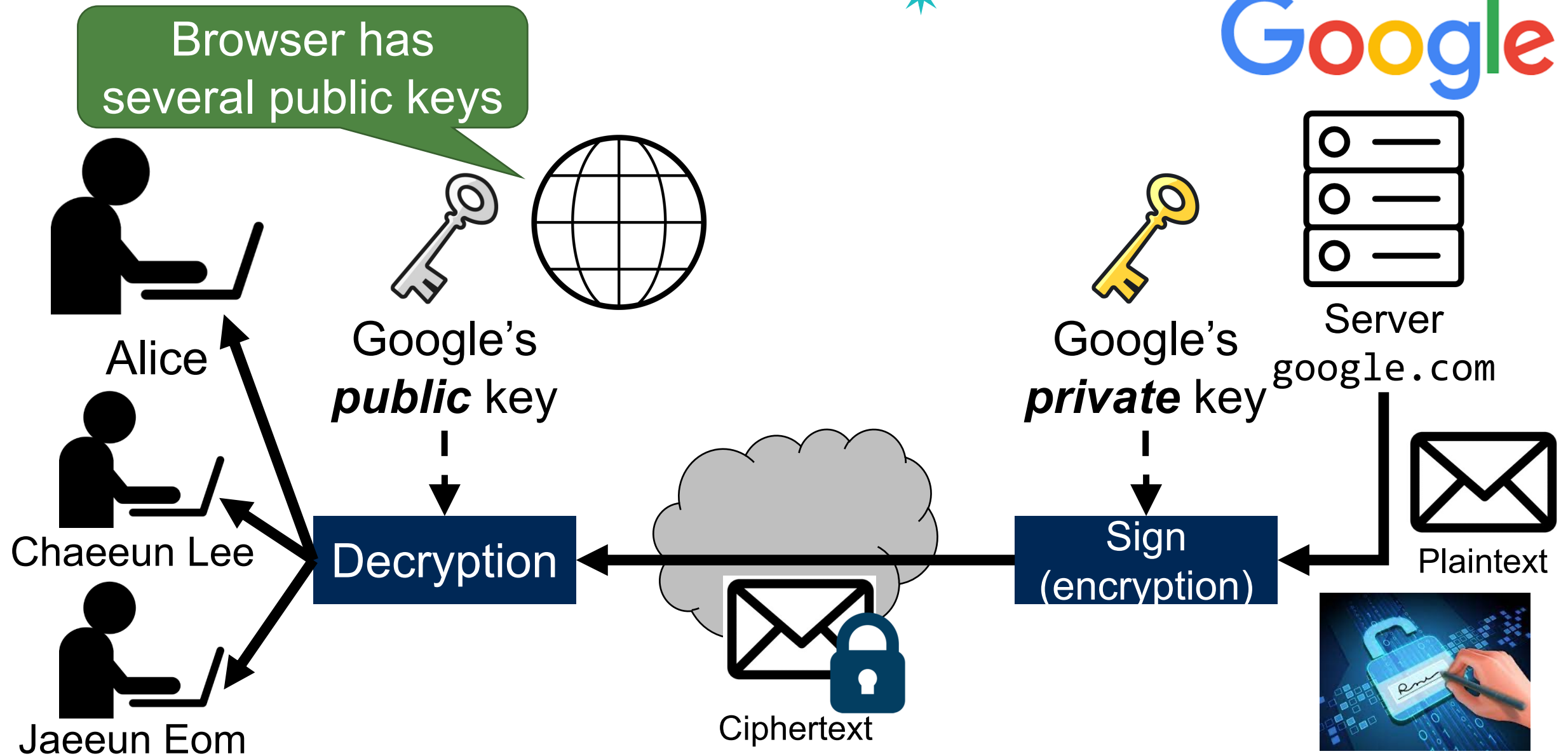
Digital Signature in Detail (3)

73



Application of Digital Signature in HTTPs ⁷⁴

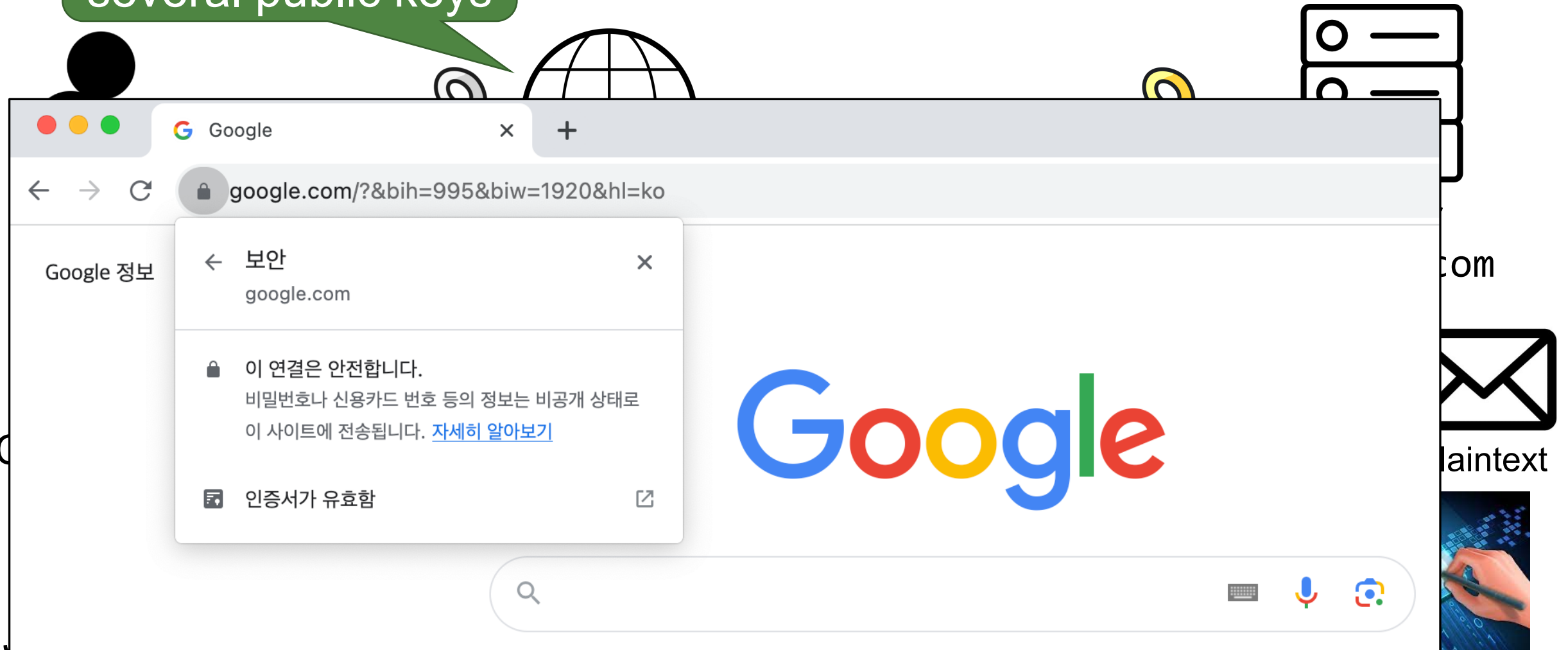
Google



Application of Digital Signature in HTTPs ⁷⁵

Browser has
several public keys

Google



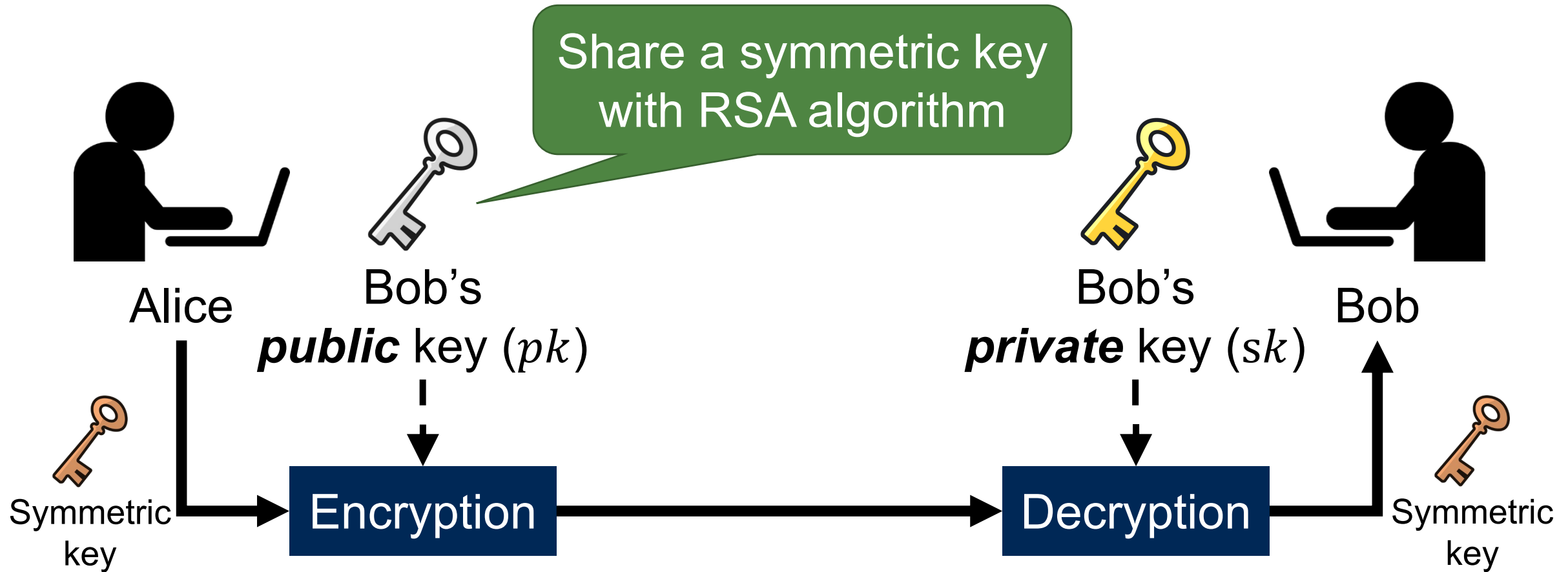
Comparison with Symmetric-Key Cryptography

76

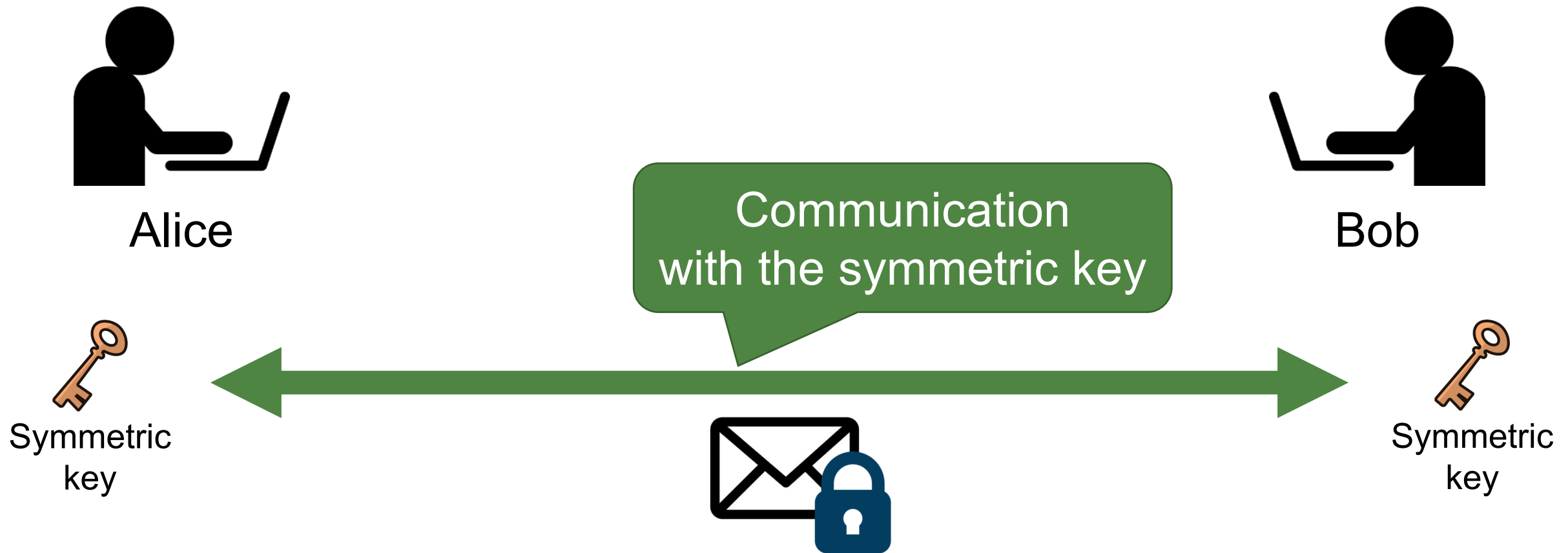


- Pros
 - No need to share a secret
 - Enable multiple senders to communicate privately with a single receiver
 - More applications: Digital sign
- Cons
 - Slower in general: due to the larger key
 - Roughly 2-3 orders of magnitude slower

In Practice: Combination of Two Schemes ⁷⁷



In Practice: Combination of Two Schemes⁷⁸



Summary



- Public-key revolution: solve key distribution and maintenance problem
 - Diffie-Hellman key exchange
 - Public-key encryption
 - Digital signature

- (Next lecture) Public key infrastructure, hash, MAC, and homomorphic encryption

Question?