Cyber Security

Lecture 3

Public–Key Encryption & Key exchange, RSA & Diffie-Hellman

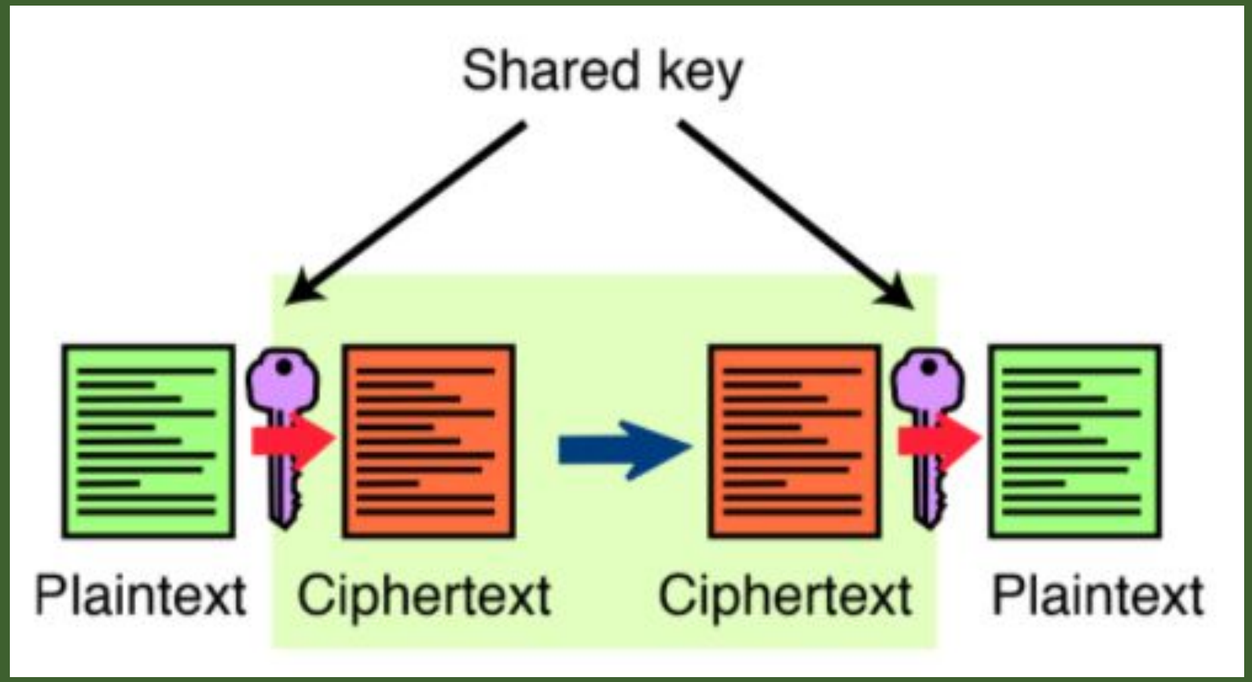
2020

NAZGUL ABDINUROVA

SULEYMAN DEMIREL UNIVERSITY

Encryption and the Key

Encryption and decryption share the same key.



Key Agreements

- In modern encryption the algorithms are public, the strength of the secure communication mechanism is based on the secrecy of the key,
- hence key agreement is a security mechanism that is of fundamental importance as it deals with agreement on shared key secure channel to exchange conventional encryption key

To exchange the keys used for encryption we need:

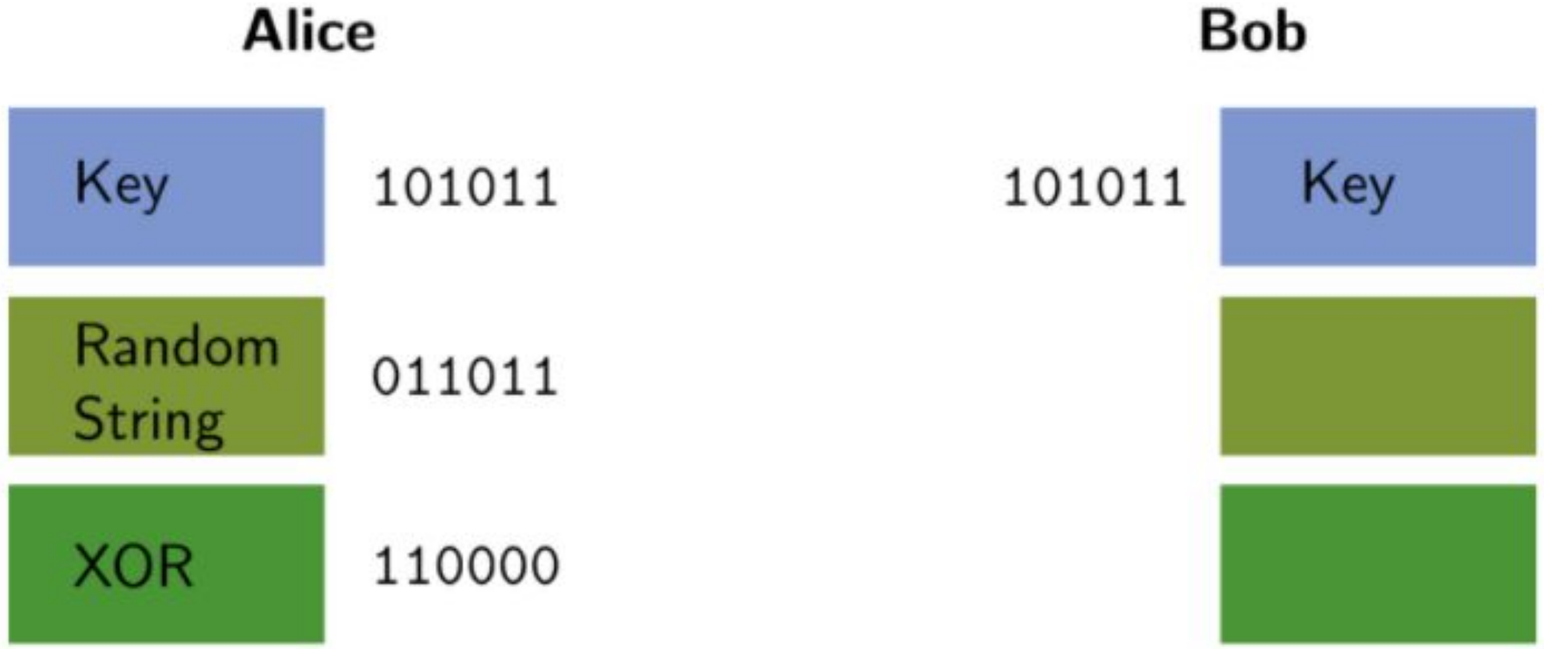
- Agreement of shared key
- Secure channel to exchange conventional key

Secure Key Exchange?

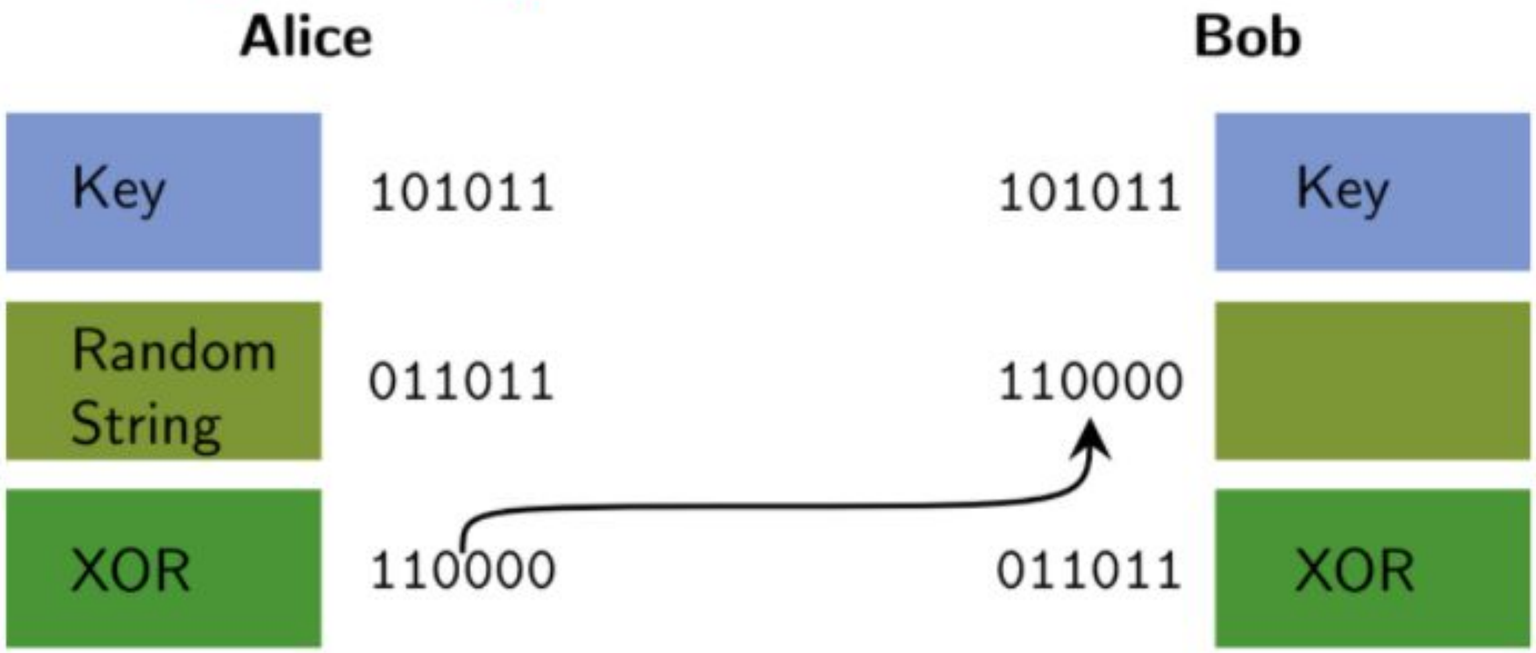
Is there a flaw in the following scheme to confirm that Alice and Bob are both in possession of the same secret key?
(example from the course textbook)

- Alice creates a random bit string the length of the key, XORs it with the key, and
- sends the result over the channel to Bob.
- Bob XORs the incoming block with the key (which should be the same as Alice's key) and
- sends it back.
- Alice checks and if what she receives is her original random string, she has verified that Bob has the same secret key, yet neither of them has ever transmitted the key.

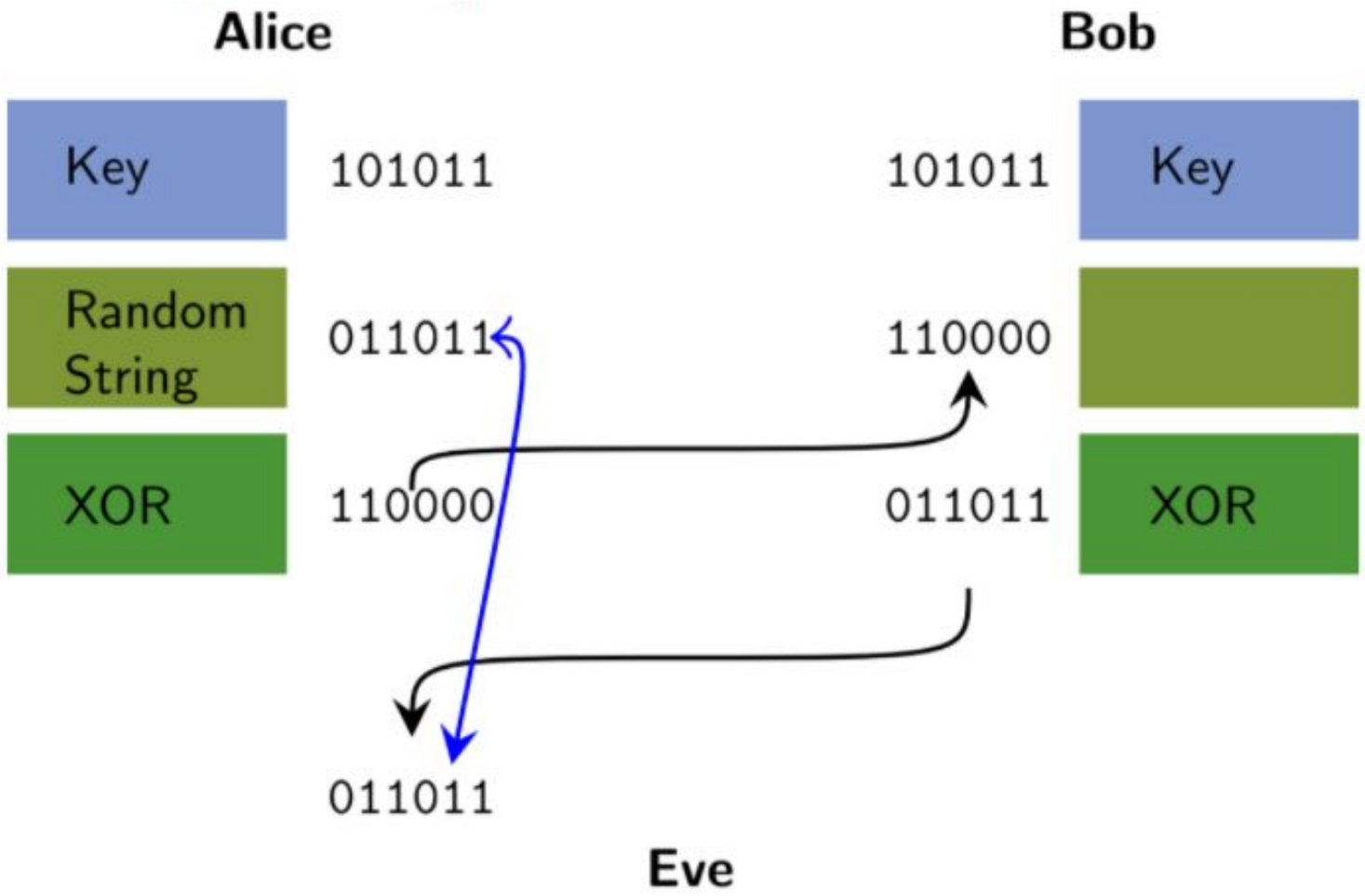
Secure Key Exchange?



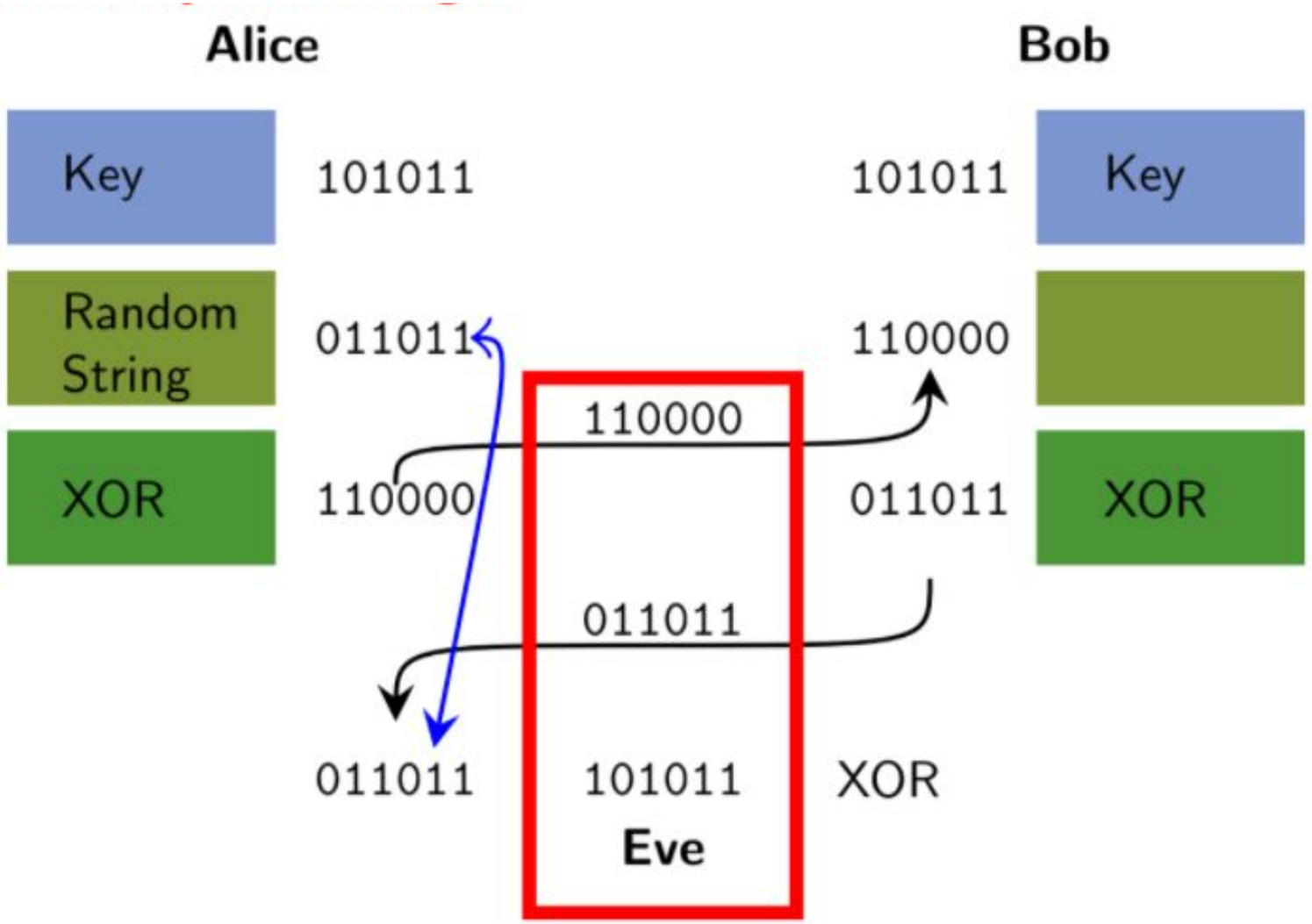
Secure Key Exchange?



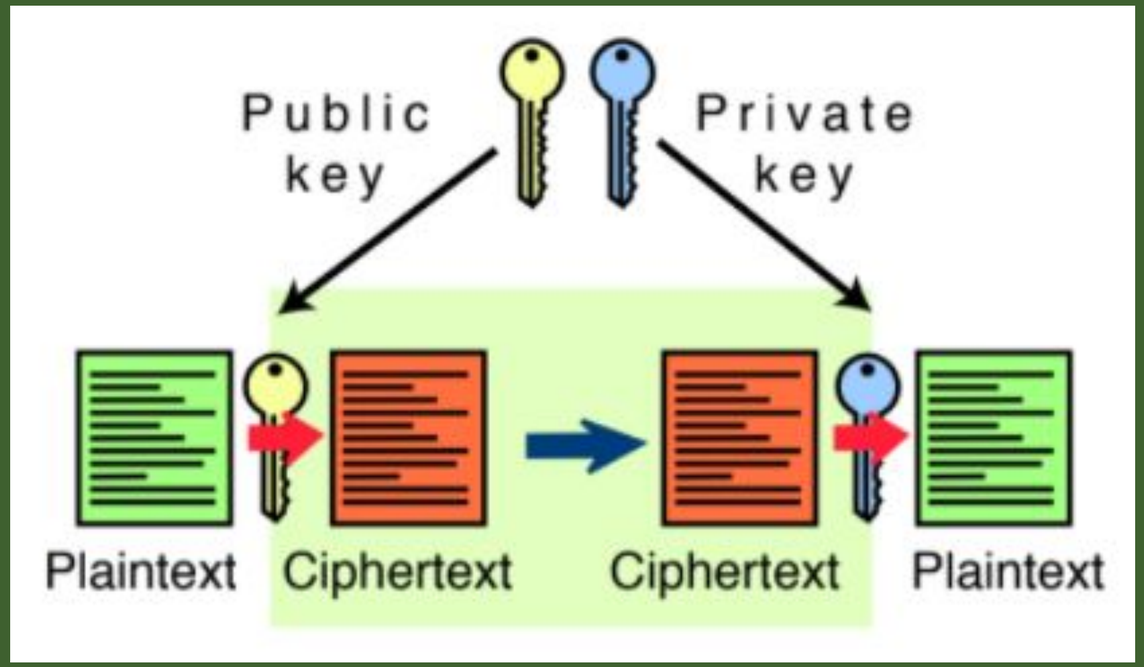
Secure Key Exchange?



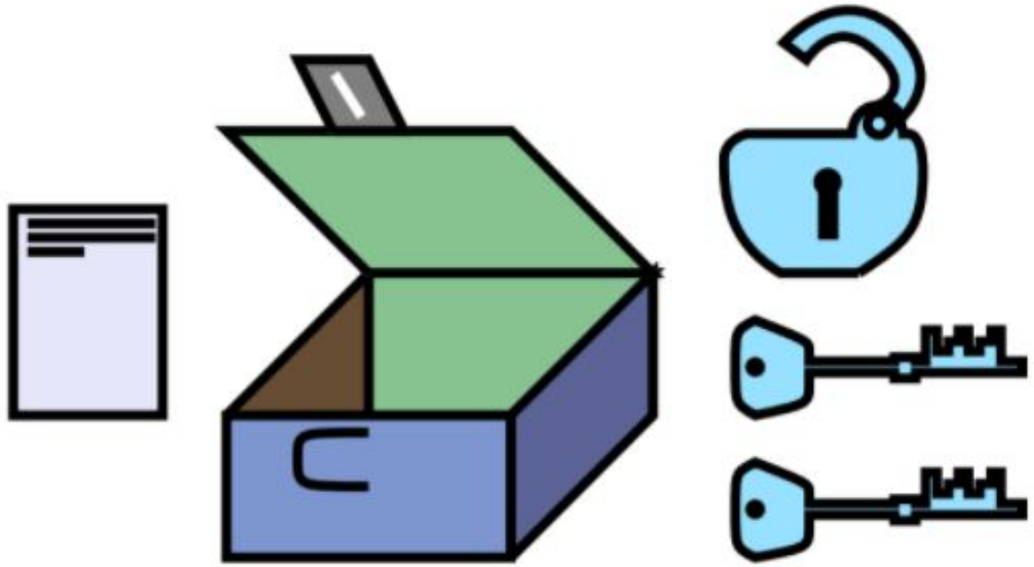
Secure Key Exchange?



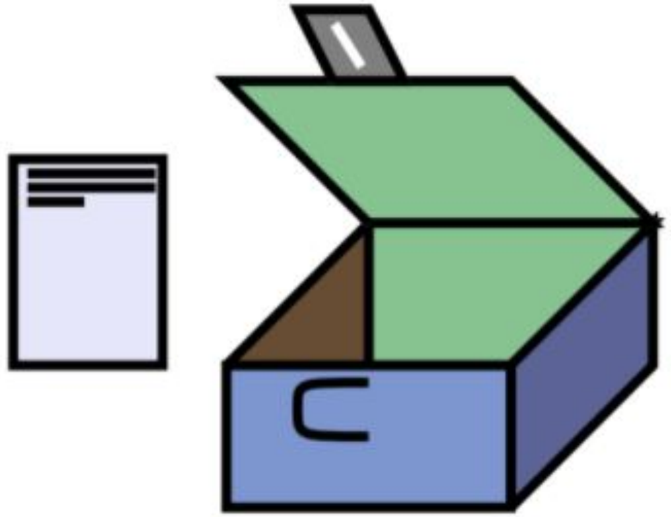
Public–Key Encryption



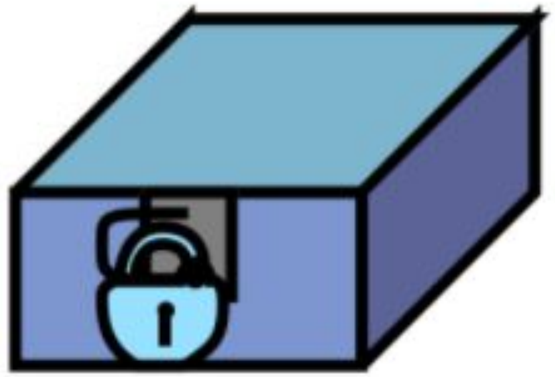
Conventional Encryption



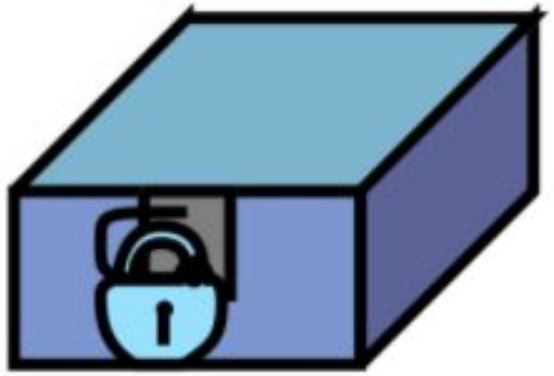
Conventional Encryption



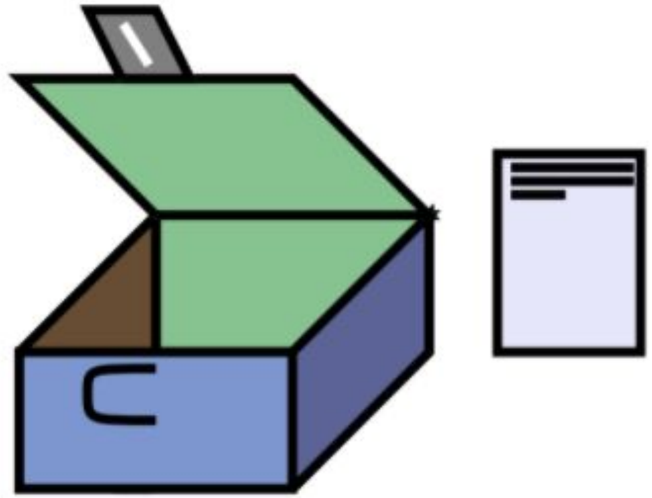
Conventional Encryption



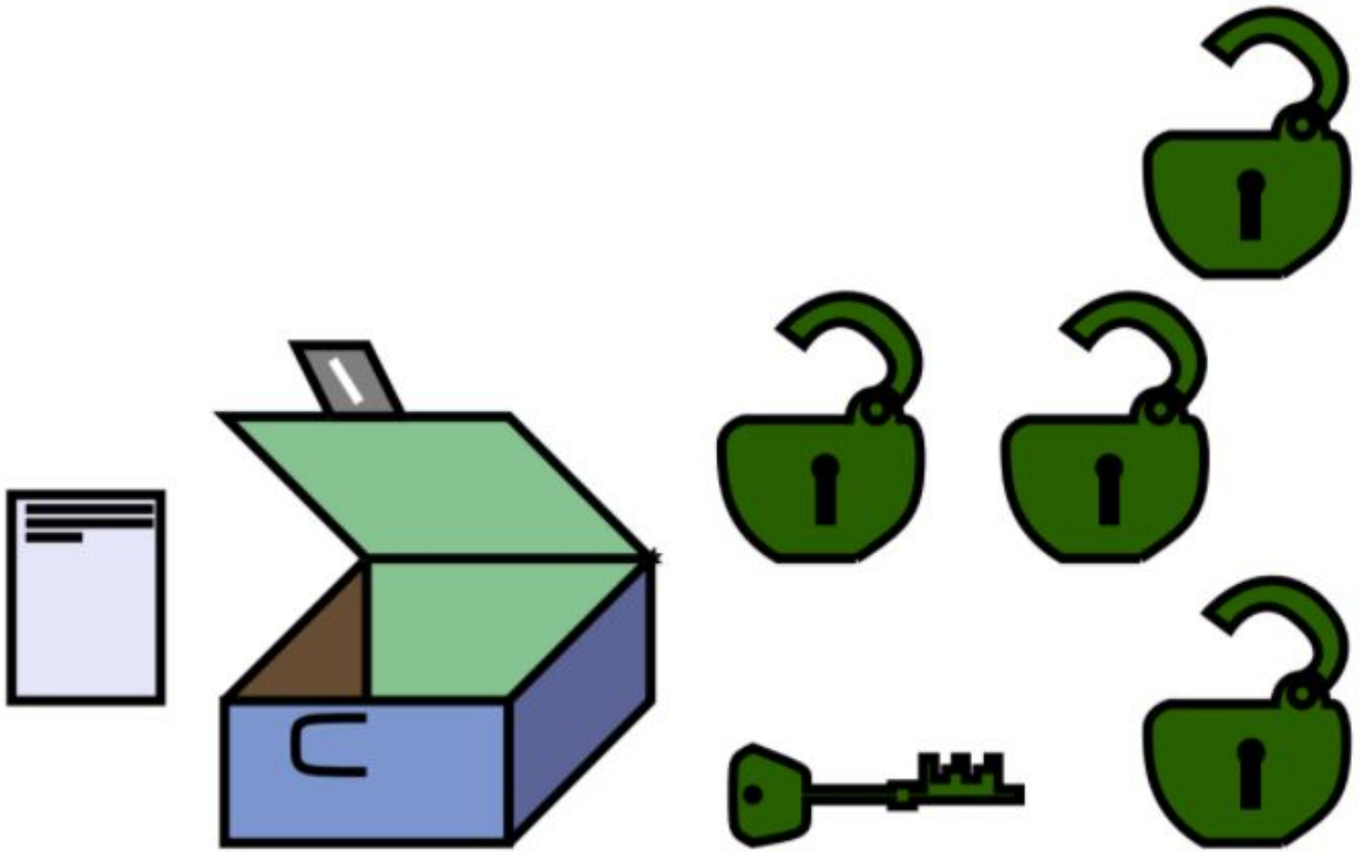
Conventional Encryption



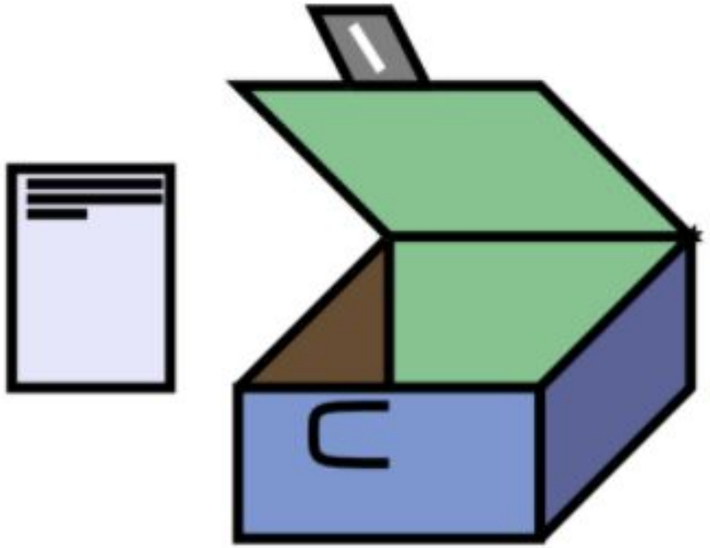
Conventional Encryption



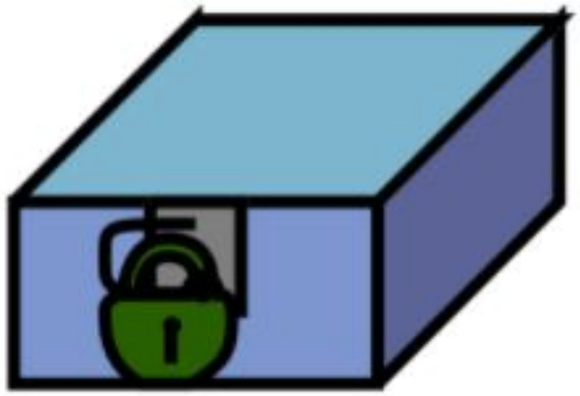
Conventional Encryption



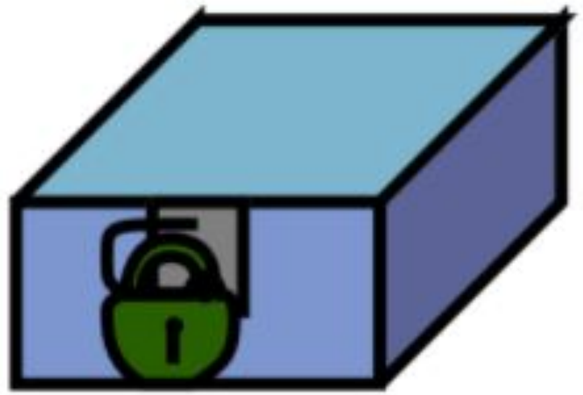
Conventional Encryption



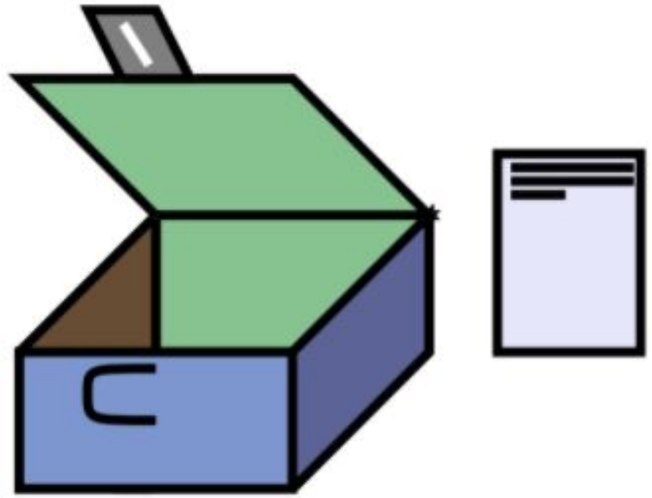
Conventional Encryption



Conventional Encryption



Conventional Encryption

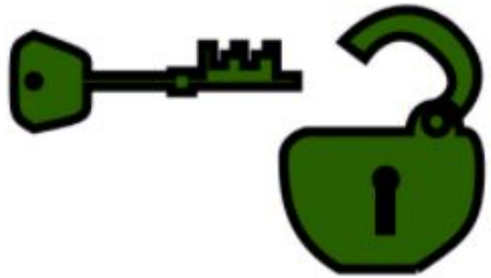


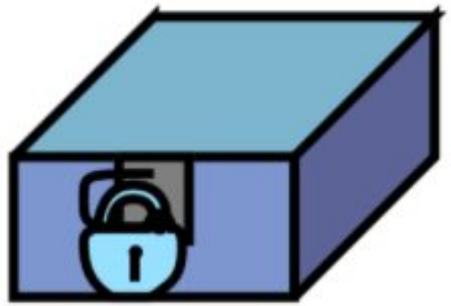
Conventional Encryption

Other Possibility

Conventional Encryption

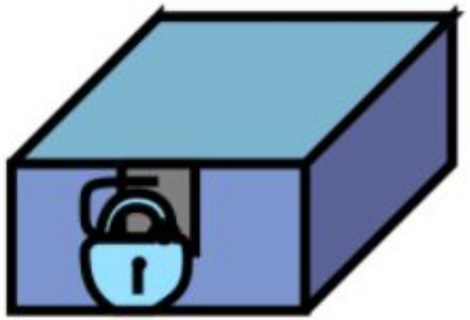
Other Possibility





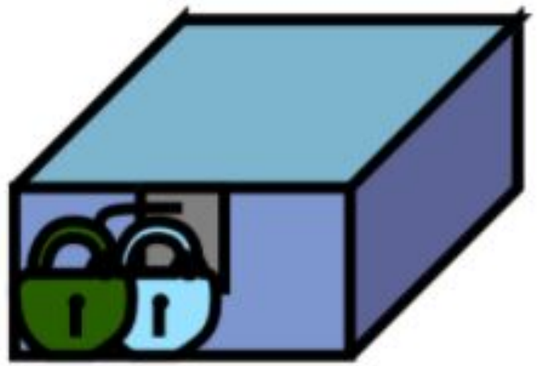
Conventional Encryption

Other Possibility



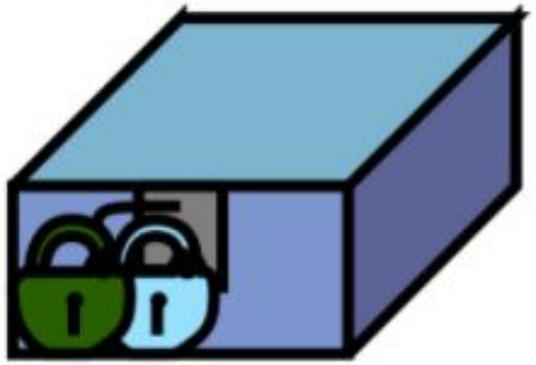
Conventional Encryption

Other Possibility



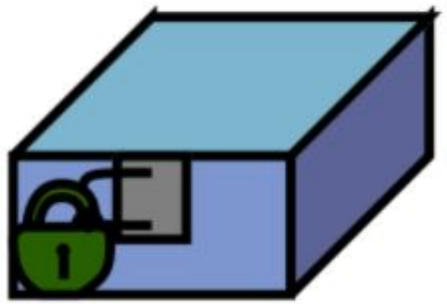
Conventional Encryption

Other Possibility



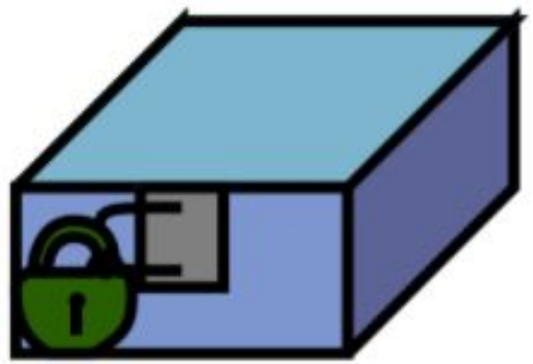
Conventional Encryption

Other Possibility



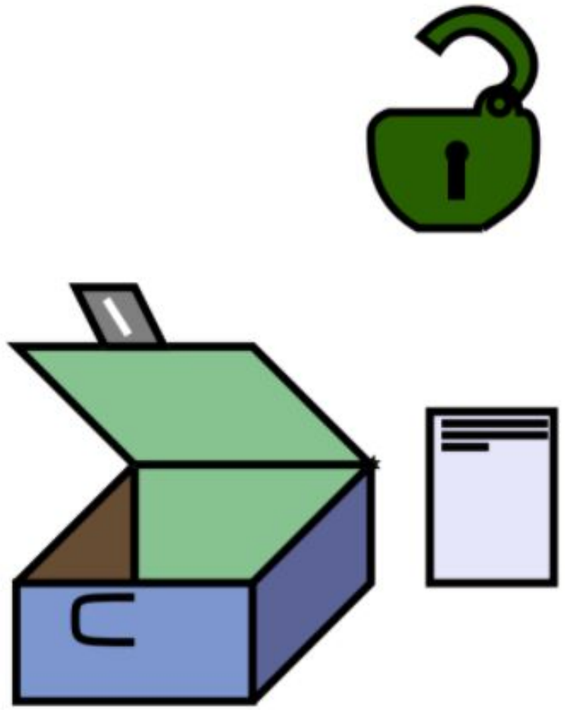
Conventional Encryption

Other Possibility



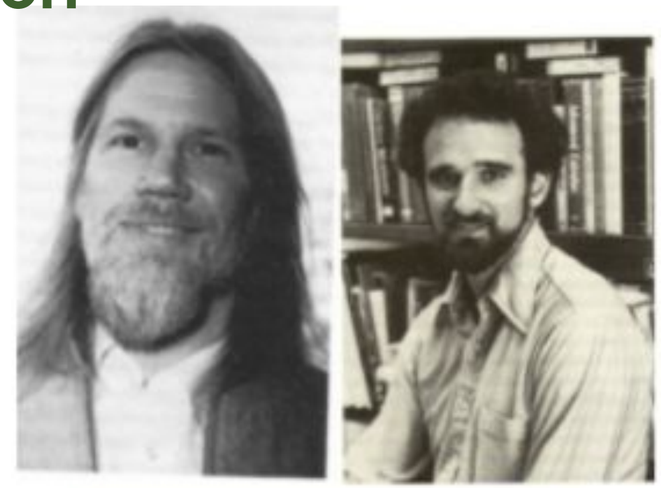
Conventional Encryption

Other Possibility



Public-Key Encryption

- Proposed in 1976 by Diffie and Hellman
- Based in mathematical functions
- Used in confidentiality, key distribution and Authentication



Diffie and Hellman

Public-Key Encryption

Ingredients:

- plaintext
- encryption algorithm
- public and private key
- ciphertext
- decryption algorithm

Public-Key Encryption

How does it work?

- Each user has two keys, a public key and a private key.
- The users put their public key in a public register. These public keys are accessible to anyone.

Public-Key Encryption

Requirements

- Easy to generate a pair of keys
- If A knows the public key of B it is easy to generate the ciphertext c from the original plaintext message m.
- It is easy for B to decrypt the message using the private key
- It is computationally infeasible for an opponent, knowing the ciphertext and the public key to recover the original message m

Public–Key algorithms

- RSA public–key encryption algorithm
- Diffie–Hellman key exchange
- Digital Signature Standard (DSS)
- Elliptic–Curve Cryptography

Rivest, Shamir and Adleman

Public–Key algorithms

Based on “one-way” mathematical functions.

A one-way mathematical function is very easy to do, but very difficult to undo.

Example: Easy to do

$$7\,919 \times 7\,927 = 62\,773\,913$$

difficult, what are the factors of

$$1\,689\,259\,081\,189$$

Prime numbers

An integer is prime if and only if its only divisors are ±1 and itself.

Some Prime numbers

2	3	5	7
13	17	19	23

Great Common divisor

A positive integer number can always be factored as

$$r = p_1^a + p_2^b + \dots$$

The great common divisor of two numbers a and b is the largest number c that divide both numbers exactly,that is the remainder is zero.

Example

$$11011 = 7 \times 11^2 \times 13$$

The great common divisor of 300 and 18 is: First notice that: $300 = 2^2 \times 3 \times 5^2$ and $18 = 2 \times 3^2$, then

$$gcd(18, 300) = 2 \times 3 = 6$$

Euler’s Totient Function

This function gives the number of positive integer less than n and relatively prime to n.
If n = pq where p and q are prime then

$$\varphi(n) = \varphi(pq) = (p - 1) \times (q - 1)$$

Example:

$$\varphi(21) = \varphi(3) \times \varphi(7) = 12$$

the integers are 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20

RSA algorithm

RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1.

- Encryption

$$c = m^e \bmod n$$

- Decryption

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

Uses two theorems. Fermat’s Little theorem and Euler’s Theorem

RSA algorithm

Both sender and receiver must known n and e. Only the receiver knows d

- Public–key k_u = {e, n}
- Private–key k_r = {d, n}

RSA algorithm

The algorithm satisfies

1. It is possible to find e, d and n such that m^{ed} = m mod n for all M < n.
2. It is easy to calculate m^e and c for all m < n
3. For large values of e and n it is not feasible to determine d given e and n.

RSA algorithm

Key generation
$(e*d)\%\varphi(n) = 1$

Select p, q $n = p \times q$ $\varphi(n) = (p - 1)(q - 1)$	p and q both prime
select integer e	$\gcd(\varphi(n), e) = 1;$ $1 < e < \varphi(n)$
d	$d \equiv e \bmod \varphi(n)$
Public Key	$= \{e, n\}$
Private Key	$= \{d, n\}$

Notice: $\gcd(\varphi(n), e) = 1$ means that $\varphi(n)$ and e are relative primes. To get d, evaluate $de \equiv 1 \bmod \varphi(n)$

RSA algorithm

Encryption

Plaintext	$m < n$
Ciphertext	$c = m^e \bmod n$

Decryption

Ciphertext	c
Plaintext	$m = c^d \bmod n$

RSA Example

Key generation
https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html

Select p, q	p = 47 and q = 59
$n = p \times q$	n = 2773
$\varphi(n)=(p - 1)(q - 1)$	$\varphi(n)$ = 2668
select integer e	e = 17
d	d_u= e-1 mod $\varphi(n)$, d = 157
Public Key	k = {17, 2773}
Private Key	k^r = {157, 2773}

RSA Example

Key generation

Encode the literal characters (space), a, b, ..., z with the biagrams 00, 01, . . . , 26.
The message is encoded in block of length two

e	r	r	a	r	e
05	18	18	01	18	05

0518 1801 1805

Encryption, e.g $c1 = 518^{17} \bmod 2773 = 1787$

1787 2003 2423

Decryption, e.g $c2 = 2003^{157} \bmod 2773 = 1801$

0518 1801 1805

RSA algorithm

Shortcomings

- need relatively long keys, 1024 or more bits
- is slower than DES by a factor of a thousand

Notes about RSA Problem: find e and d

- Encryption: $c = m^e \bmod n$
- Decryption: $m = c^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n$

- Great Common divisor
  $c = \gcd(a, b)$ is the great common divisor of a and b if
  - c is a divisor of a and b
  - any divisor of a and b is a divisor of c
- ex: $\gcd(300, 180)$
  $300 = 2^2 \times 3^1 \times 5^2$
  $18 = 2^1 \times 3^2$
  The $\gcd(300, 18) = 6$

- divisors: b $= 0 divides a if a = m b; m ∈ I
  ex: the divisors of 36 are
  1, 2, 3, 4, 6, 9, 12, 18
- residue: a = m b + r, r is the remainder
  ex: 7 = 2 × 3 + 1, remainder is 1

- prime numbers: p > 1 is prime if its only divisors are ±1 and ±p ex: 1,2,3,5,7

- prime factors: anv number can be factored as $a = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots$

  ex: $440 = 2^3 \times 5^1 \times 11^1$

Notes about RSA

- Encryption: $c = m^e \bmod n$
- Decryption: $m = c^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n$

- Great Common divisor
  $c = \gcd(a, b)$ is the great common divisor of a and b if
  - c is a divisor of a and b
  - any divisor of a and b is a divisor of c
- ex: $\gcd(300, 180)$
  $300 = 2^2 \times 3^1 \times 5^2$
  $18 = 2^1 \times 3^2$
  The $\gcd(300, 18) = 6$

- **relative primes:** def: a and b are relative primes if they have no prime factors in common (except from 1) or equivalent $\gcd(a, b)=1$
  ex: 8 and 15 are relative primes because $8 = 2^3$ and $15 = 3 \times 5$
- modular arithmetic: $a = n \times q + r$ where r is the remainder or $r = a \bmod q$ and $n \in I$
  ex: $11 \bmod 7=4 \rightarrow 11 = 7 \times 1+4$ - $11 \bmod 7=3 \rightarrow -11 = 7 \times (-2) + 2$
- congruent module n: If a and b satisfy $a \bmod n = b \bmod n$ we write this as $a \equiv b \bmod n$
  ex: $73 \bmod 23 = 4$ and $4 \bmod 23 = 4$ then $73 \equiv 4 \bmod 23$

Notes about RSA

- Encryption: $c = m^e \bmod n$
- Decryption: $m = c^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n$

- Euler's Totient: $\varphi(n)$ is the number of positive integers less than n and relative prime to n
  ex: n=10, then from the list 9, 8, 7, 6, 5, 4, 3, 2, 1 the numbers 9, 7, 3, 1 are relative primes of 10 so $\varphi(10) = 4$

- Observation: If p is prime then $\varphi(p) = p - 1$.

- **relative primes:** def: a and b are relative primes if they have no prime factors in common (except from 1) or equivalent $\gcd(a, b)=1$
  ex: 8 and 15 are relative primes because $8 = 2^3$ and $15 = 3 \times 5$
- modular arithmetic: $a = n \times q + r$ where r is the remainder or $r = a \bmod q$ and $n \in I$
  ex: $11 \bmod 7=4 \rightarrow 11 = 7 \times 1+4$ - $11 \bmod 7=3 \rightarrow -11 = 7 \times (-2) + 2$

- congruent module n: If a and b satisfy $a \bmod n = b \bmod n$ we write this as $a \equiv b \bmod n$
  ex: $73 \bmod 23 = 4$ and $4 \bmod 23 = 4$ then $73 \equiv 4 \bmod 23$

Notes about RSA

- Encryption: $c = m^e \bmod n$
- Decryption: $m = c^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n$

- Euler's Totient: $\varphi(n)$ is the number of positive integers less than n and relative prime to n
  ex: n=10, then from the list 9, 8, 7, 6, 5, 4, 3, 2, 1 the numbers 9, 7, 3, 1 are relative primes of 10 so $\varphi(10) = 4$

- Observation: If p is prime then $\varphi(p) = p - 1$.

- relative primes: $\gcd(a, b)=1$

- If $n = p \times q$ and p, q are primes then
  $\varphi(n) = \varphi(p) \times \varphi(q) = (p - 1) \times (q - 1)$

- Euler's Theorem: If a and n are relative primes then
  $a^{\varphi(n)} \equiv 1 \bmod n$
  or $a^{\varphi(n)+1} \equiv a \bmod n$

- Now take $n = p \times q$ where p and q are prime numbers and m with $0 < m < n$ if
  $m^{\varphi(n)+1} = m^{(p-1)(q-1)+1}$ then
  $m^{\varphi(n)+1} \equiv m \bmod n$
  if $\gcd(m, n)=1$

Notes about RSA

- Encryption: $c = m^e \bmod n$
- Decryption: $m = c^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n$

- Back to RSA: If $e\,d = k\varphi(n)+1$ with $k \in I$ then we can use Euler's Theorem that guarantees that RSA works.

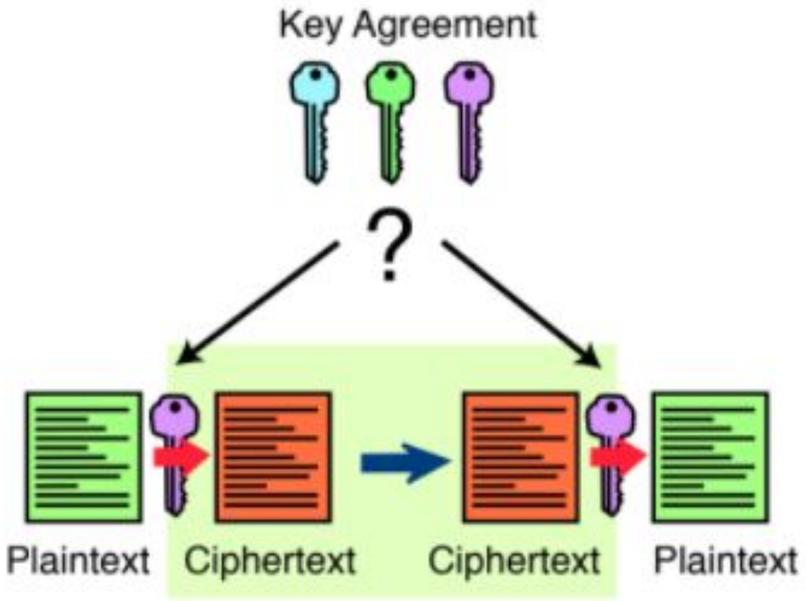
$$ed = k \times \varphi(n)+1 \quad or$$

$$ed \equiv 1 \bmod \varphi(n)$$

- relative primes: $\gcd(a, b)=1$

- If $n = p \times q$ and p, q are primes then $\varphi(n) = \varphi(p) \times \varphi(q) = (p - 1) \times (q - 1)$
- Euler's Theorem: If a and n are relative primes then
  $a^{\varphi(n)} \equiv 1 \bmod n$
  or $a^{\varphi(n)+1} \equiv a \bmod n$
- Now take $n = p \times q$ where p and q are prime numbers and m with $0 < m < n$ if
  $m^{\varphi(n)+1} = m^{(p-1)(q-1)+1}$ then
  $m^{\varphi(n)+1} \equiv m \bmod n$
  if $\gcd(m, n)=1$

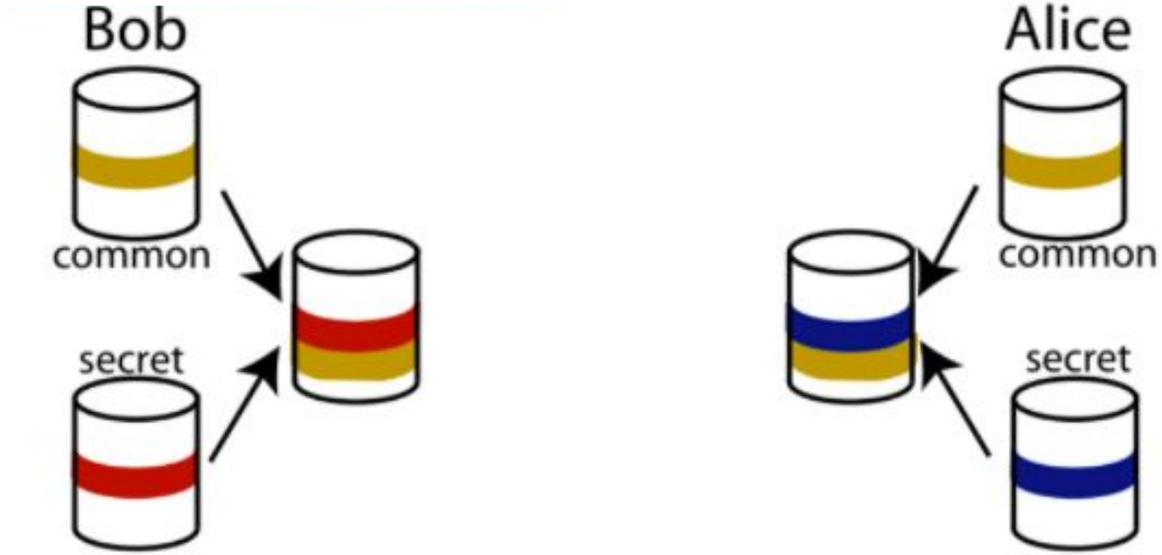
Diffie–Hellman Key Exchange



- The algorithm was developed to enable two users to exchange a secret key securely. The algorithm itself is limited to the exchange of keys.
- Based on the difficulty to compute discrete logarithms.

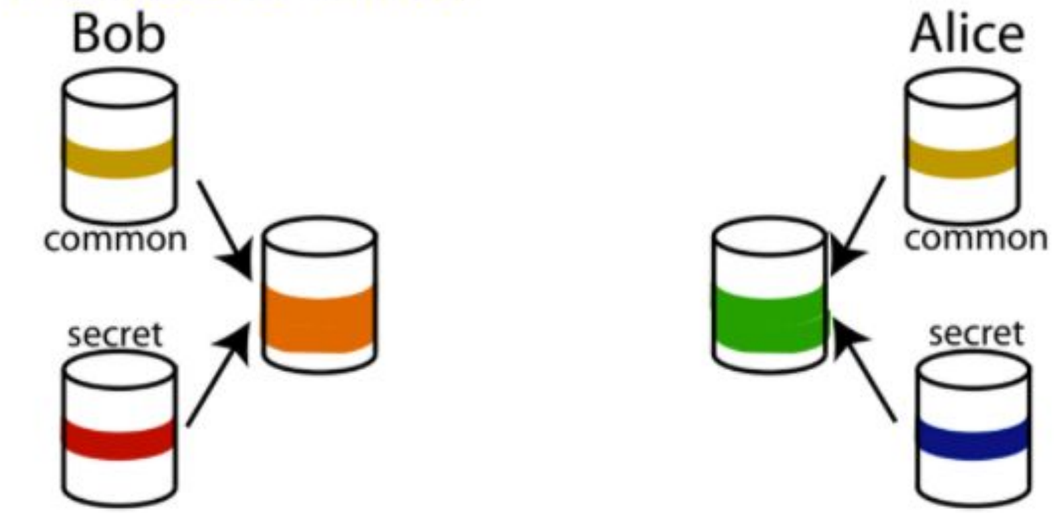
Diffie–Hellman Key Exchange

Analogy: The secret colour



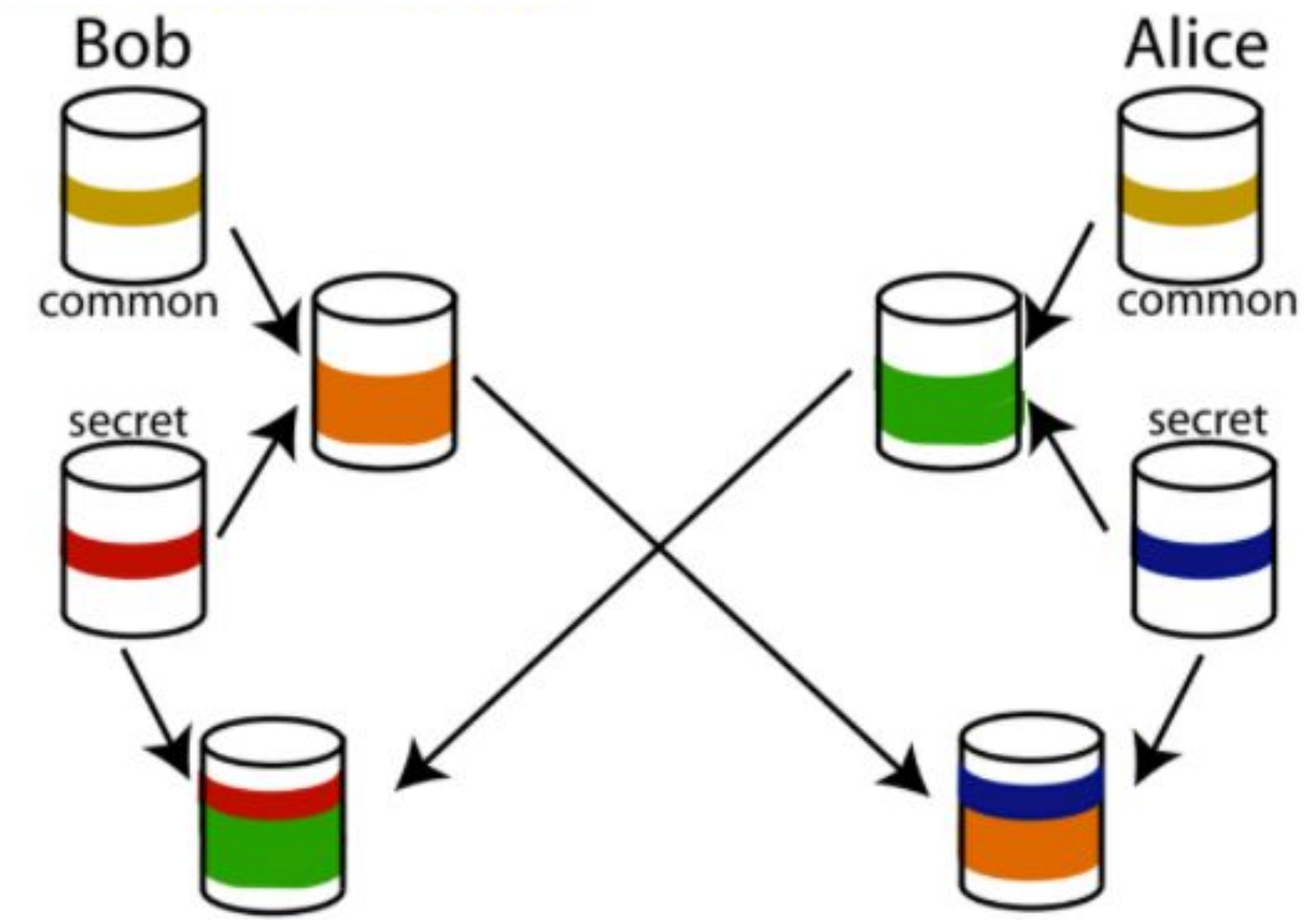
Diffie–Hellman Key Exchange

Analogy: The secret colour



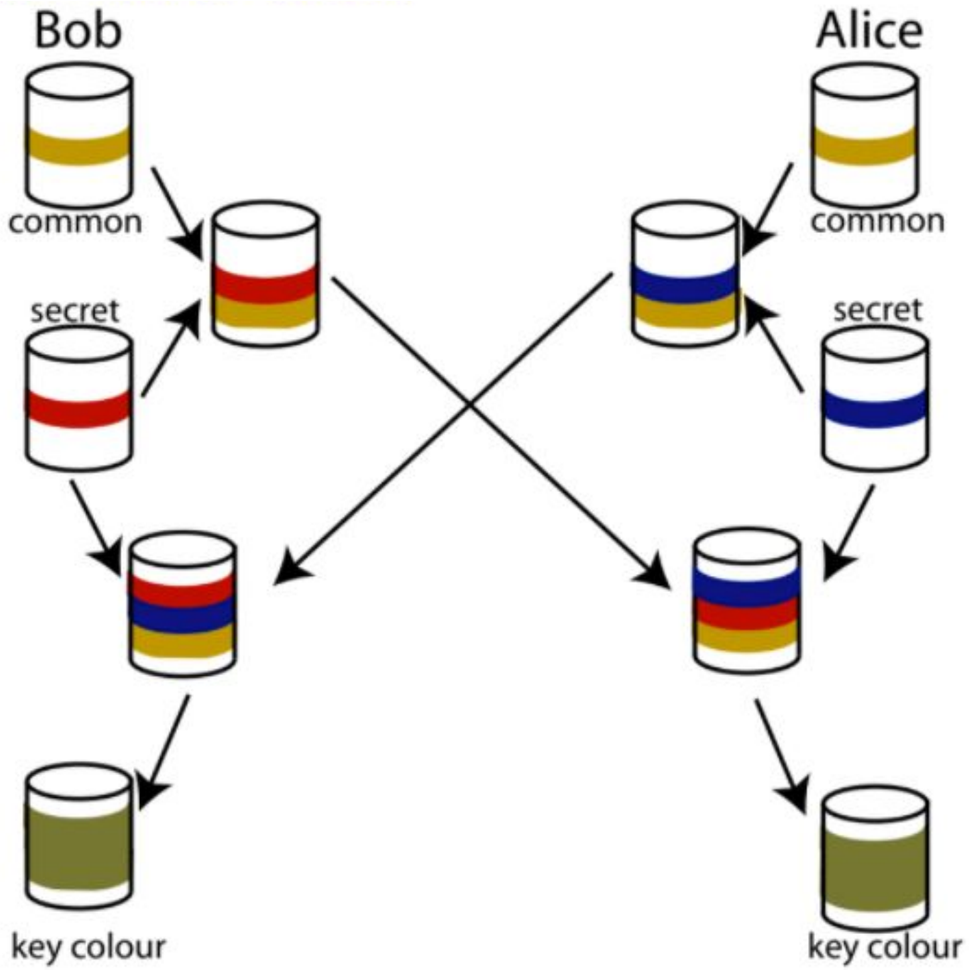
Diffie–Hellman Key Exchange

Analogy: The secret colour



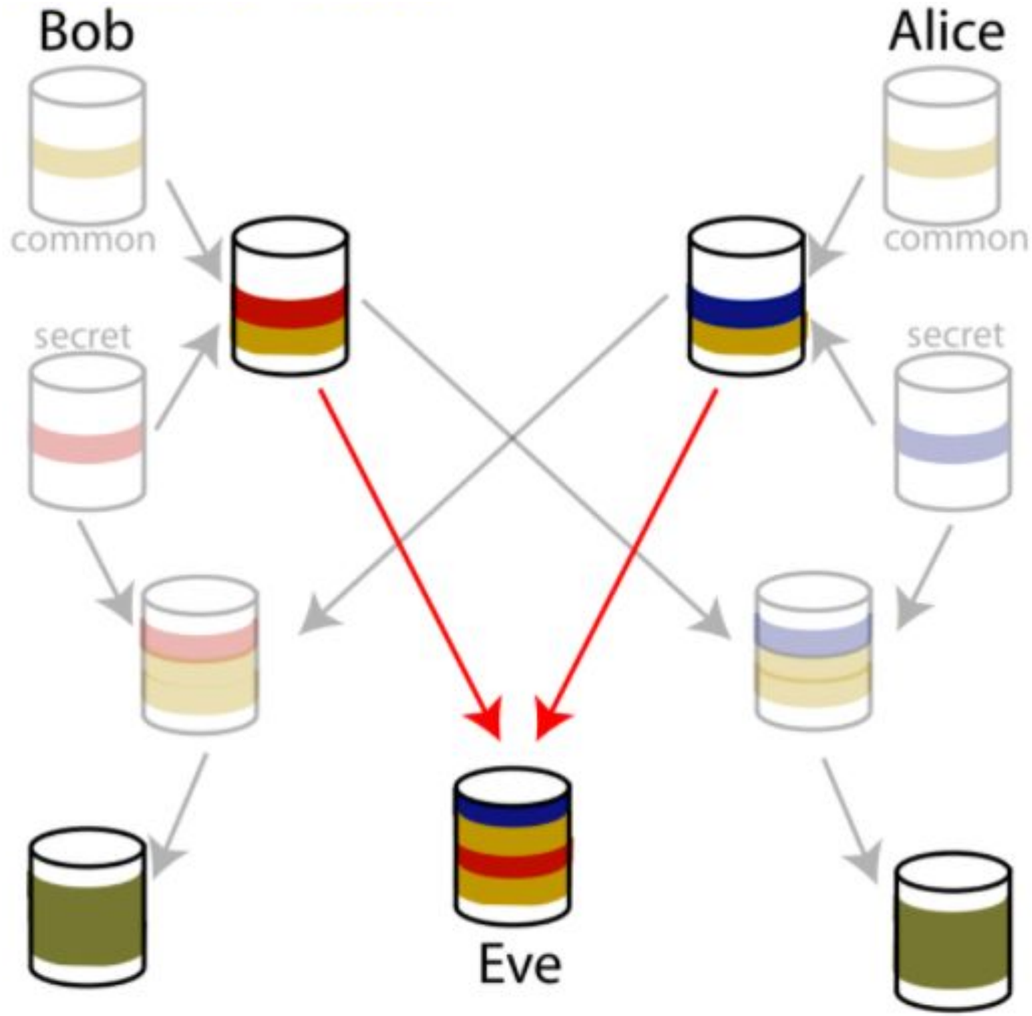
Diffie–Hellman Key Exchange

Analogy: The secret colour



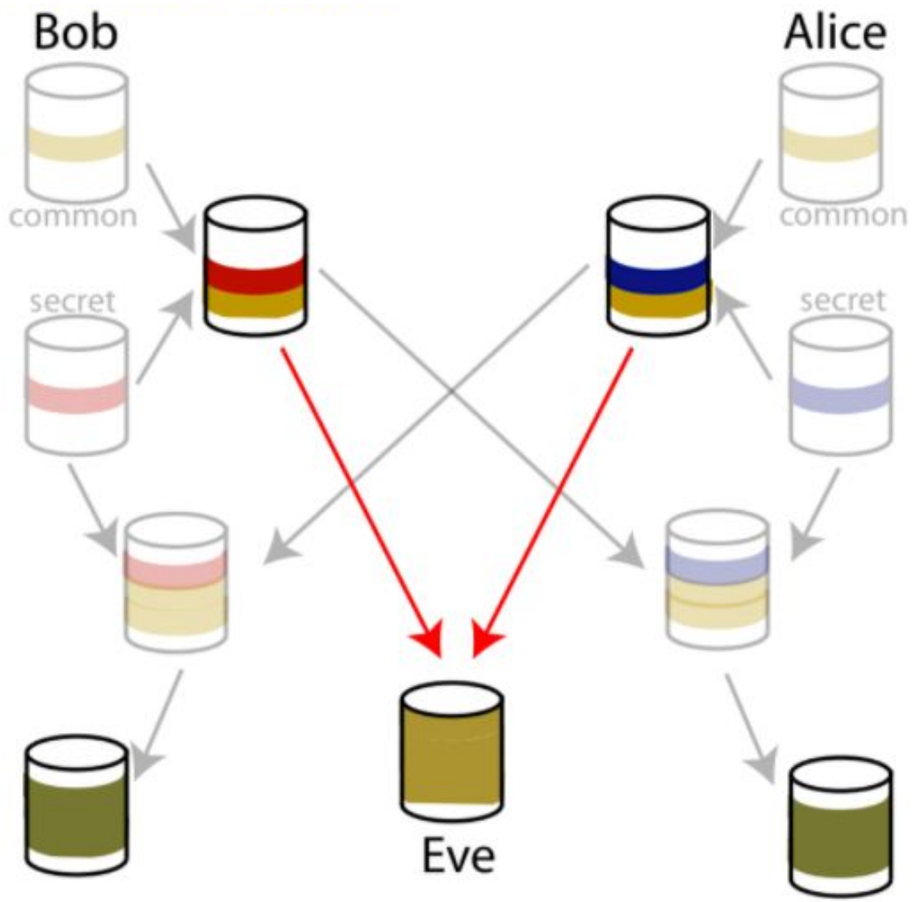
Diffie–Hellman Key Exchange

Analogy: The secret colour



Diffie–Hellman Key Exchange

Analogy: The secret colour



Diffie–Hellman Key Exchange

Discrete Algorithms

Definition: If a is a primitive root of the prime number p then

$$a \bmod p,\ a^2 \bmod p, \ldots\ a^{p-1} \bmod p,$$

are distinct and consist of the integers 1 through p - 1 in some permutation.
Example: If p = 71 and a = 7
The discrete logarithm, is the exponent i such that

$$b = a^i \bmod p \text{ where } 0 \leq i \leq p-1$$

where a is a primitive root of p.

Diffie–Hellman algorithm

Global Public Elements	
q	prime number
α	α < q, α a primitive root of q

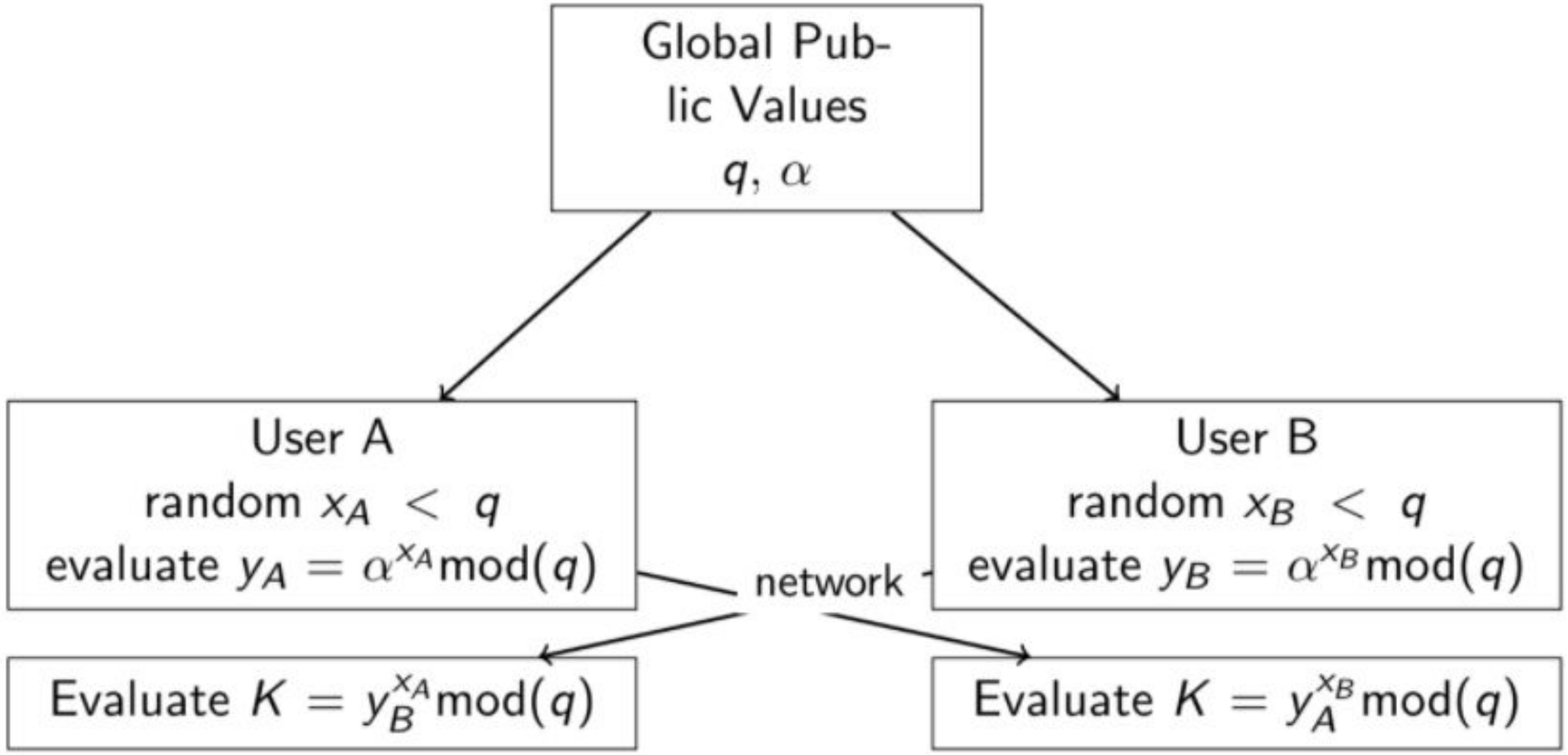
Diffie–Hellman algorithm

User Key generation

user A	
Select private x_A	$x_A < q$
Calculate public y_A	$y_A = \alpha^{x_A} \bmod q$

user B	
Select private x_B	$x_B < q$
Calculate public y_B	$y_B = \alpha^{x_B} \bmod q$

Diffie–Hellman algorithm



Diffie–Hellman algorithm

- User A generates a private key xA, evaluates yA and send that to B.
- User B responds by generating a private key xB evaluates yB and send that to A.
- Both users generate the key k

Diffie–Hellman algorithm

Generation of Secret Key

User A	User B
$k = y_B^{x_A} \bmod q$	$k = y_A^{x_B} \bmod q$

It works

because $k = y_A^{x_A}$ and $k = y_B^{x_B}$ produce identical results.

Diffie–Hellman algorithm

Example:

- q = 353 and α = 3.
- Alice’s secret key XA = 97,
- Bob’s secret key XB = 233

Key:

Diffie–Hellman algorithm

Example:

- q = 353 and α = 3.
- Alice’s secret key XA = 97,
- Bob’s secret key XB = 233

Key:

Diffie–Hellman algorithm

Example:

- q = 353 and α = 3.
- Alice's secret key XA = 97,
- Bob's secret key XB = 233
- Alice: YA = $3^{97} \bmod 353$ = 40
- Bob: YB = $3^{233} \bmod 353$ = 248

Key:

Diffie–Hellman algorithm

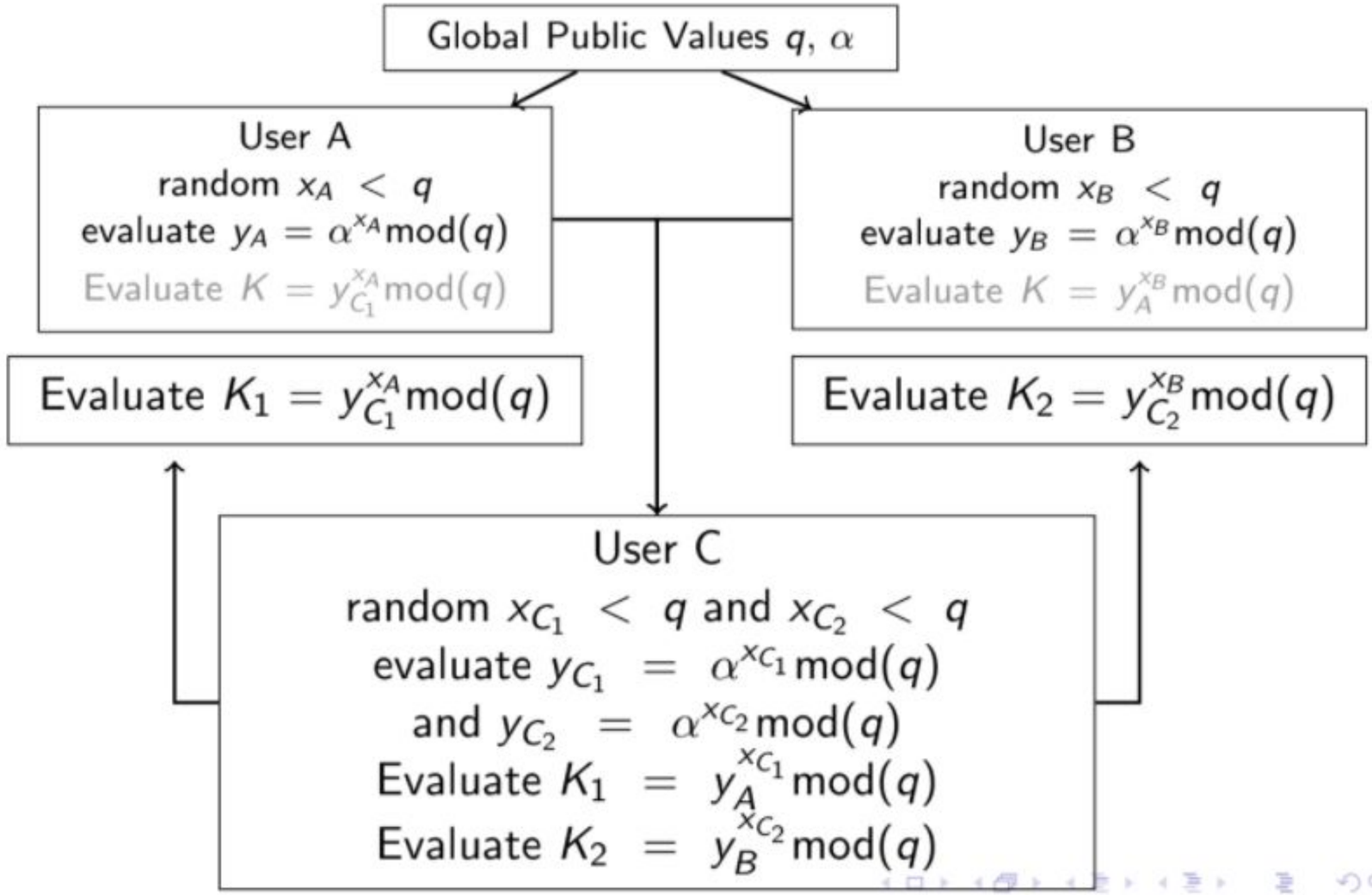
Example:

- q = 353 and α = 3.
- Alice's secret key XA = 97,
- Bob's secret key XB = 233
- Alice: YA = $3^{97} \bmod 353$ = 40
- Bob: YB = $3^{233} \bmod 353$ = 248

Key:

- Alice: $248^{97} \bmod 353$ = 160
- Bob: $40^{233} \bmod 353$ = 160

Man-in-the-middle attack



Summary

- RSA
- Diffie-Hellman
- Key exchange

LABWORK

- write own RSA
- input: p,q,m
- calculated by your code: n, totient function, e,d, ciphertext
- Diffie-Hellman