Theory of Computational Complexity

Lecture 14: Cryptography and Complexity
Overview of Cryptography

François Le Gall

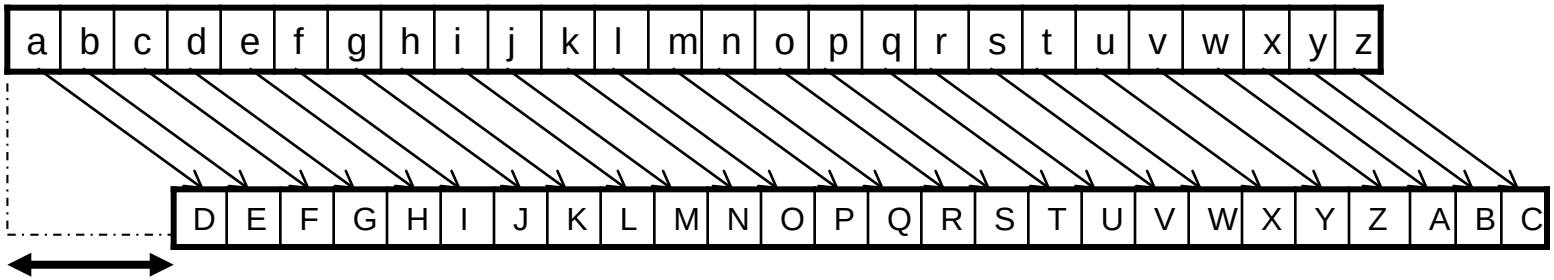
Nagoya University

1. History: Caesar Scheme

CAESAR SCHEME

- Invented around BC 100 by the roman emperor Caesar

- Extremely simple



Translate by *n* characters(here : n=3)

key n

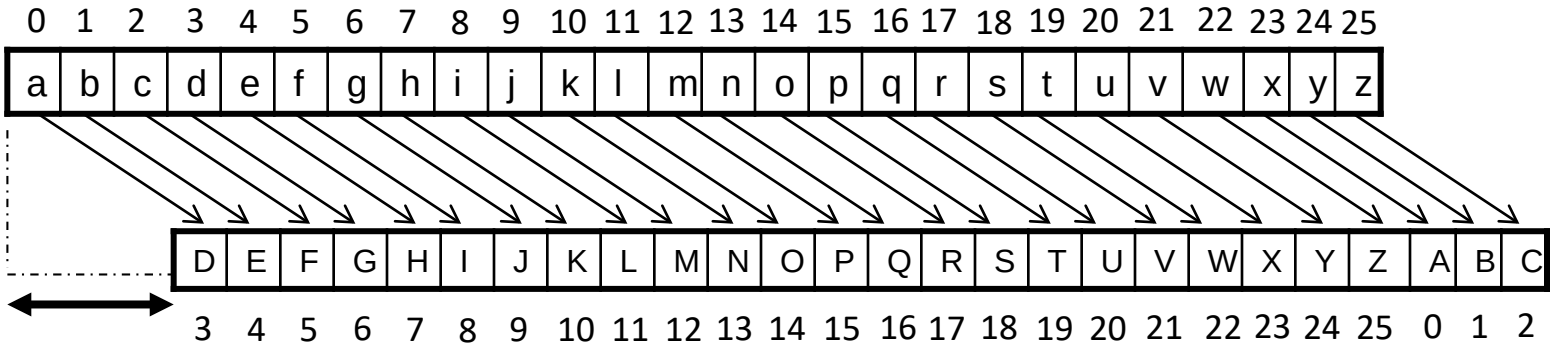
- encryption

konnichiha → NRQQLFKLKD

- decryption

NRQQLFKLKD → konnichiha

1. History: Caesar Scheme



Translate by *n* characters(here : n=3)

key n 

★ encryption Works by adding n to each symbol modulus 26

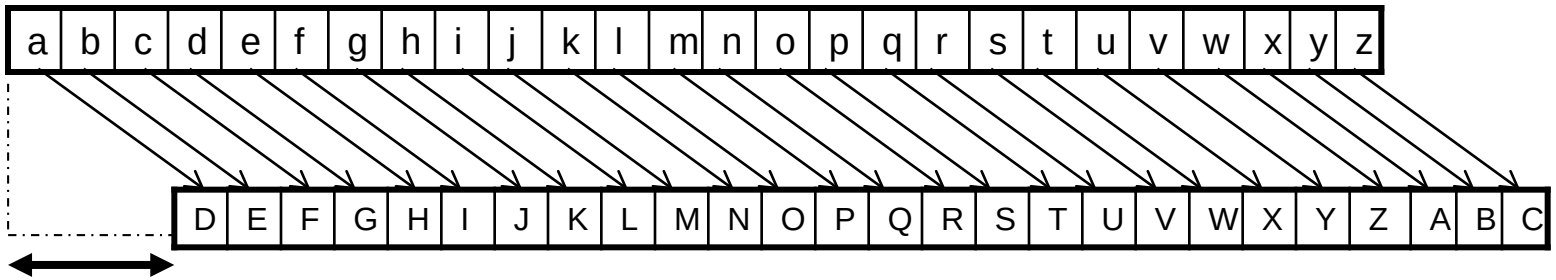
konnichiha  NRQQLFKLKD

★ decryption Works by substracting n to each symbol modulus 26

NRQQLFKLKD  konnichiha

1. History: Caesar Scheme

CAESAR SCHEME



Translate by *n* characters(here : n=3)

- Pros : simple, small key
- Cons : very weak security

The # of possible keys is too small!

Reason : only 26 possibilities for the key

NRQQLFKLKD

Encrypted message

n=0?→ NRQQLFKLKD

n=1?→ MQPPKEJKJC

n=2?→ LPOOJDIJIB

N=3?→ KONNICHIHA

HOW TO INCREASE THE SIZE OF THE KEY?

1. History: Variants of Caesar Scheme

Idea: instead of doing the encryption letter by letter, let do it on blocks of letters

Example: blocks of 6 letters (26^6=308,915,776 possibilities per block)

Each block is represented by an integer between 0 and 308,915,775

SCHEME

The key n is also an integer between 0 and 308,915,775
Encryption: add n modulus 308,915,776
Decryption: subtract n modulus 308,915,776

Use block encryption to encode the whole message

IWOULDLIKETOMEETYOUTOMORROW .....

Simplest method: use the same key for each block ("Electronic Code Book block encryption")

1. History: Variants of Caesar Scheme

We have solved one of the main problems of the Caesar scheme

6-letter blocks ⟹ 308,915,776 possibilities for the key
12-letter blocks ⟹ about 10^{17} possibilities for the key

The key is still small

Is it secure now?

DEARBOBIAMWRITINGTOTELLYOUTHAT…

Encrypted as “DEARBO” + n (mod 308,915,776)

If the adversary knows that the message starts with DEARBO then he can get the whole key (“known plaintext attack”)!

n = encrypted block – “DEARBO”

Solution: increase the size of the block significantly

Security increases but the scheme becomes less practical

1. History: “Vernam Cipher”

US patent by Gilbert Vernam in 1919

Idea: a Caesar scheme that uses only one block (size of the key = size of the message!)

Modern interpretation:

message encoding in binary

message of m letters encoded by 5m bits

- ✓ the secret key is a (random) string of 5m bits
- ✓ encryption is done by adding the key bit by bit modulo 2
- ✓ Decryption is done by subtracting the key bit by bit modulo 2

Example: sending YES (binary encoding: 11000 00100 10010)

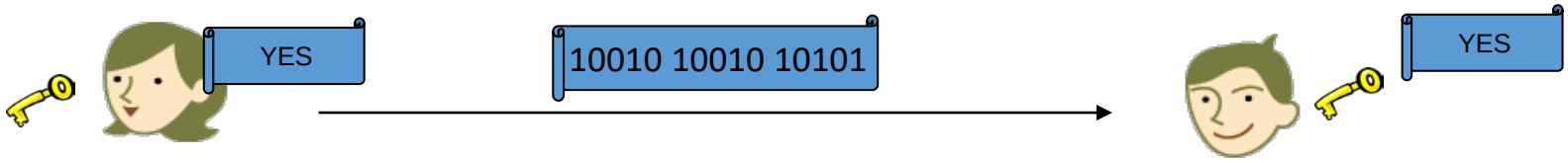
secret key: 01010 10110 00111

Encrypted message: 10010 10010 10101

decrypted message: 11000 00100 10010

example

A: 00000	Q: 10000
B: 00001	R: 10001
C: 00010	S: 10010
D: 00011	T: 10011
E: 00100	U: 10100
F: 00101	V: 10101
G: 00110	W: 10110
H: 00111	X: 10111
I : 01000	Y: 11000
J: 01001	Z: 11001
K: 01010	
L: 01011	
M: 01100	
N: 01101	
O: 01110	
P: 01111	



1. History: “Vernam Cipher”

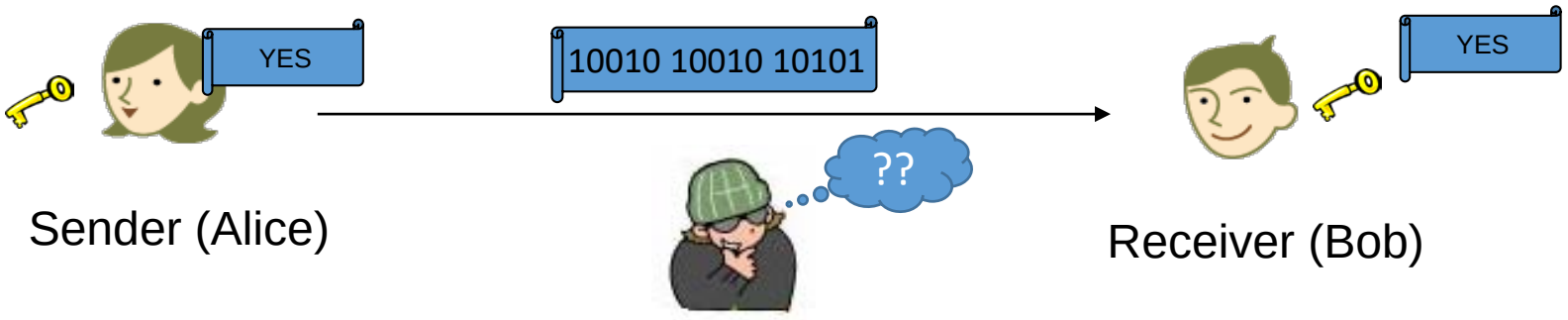
- ✓ the secret key is a (random) string of 5m bits
- ✓ encryption is done by adding the key bit by bit modulo 2
- ✓ Decryption is done by subtracting the key bit by bit modulo 2

Example: sending YES (binary encoding: 11000 00100 10010)

secret key: 01010 10110 00111

Encrypted message: 10010 10010 10101

decrypted message: 11000 00100 10010



For a key chosen uniformly at random, the probability distribution of the encrypted message does not depend on the original message

information-theoretic security (perfect security)

1. History: “Vernam Cipher”

We have perfect security but:

- ✓ the size of the key is the same as the size of the message to be sent!
- ✓ Perfect security is guaranteed only if the key is used only once:
  a new key is needed to send a new message (Vernam cipher also called “one-time pad”)
- ✓ the contents of the key must be a secret between the sender and the receiver

HOW TO DISTRIBUTE THE KEY ?

Some trusted third party has to distribute the key individually to Alice and Bob

Example: Soviet Union secret communications between Moscow and its embassy in Germany

Before WW2 many secret keys where exchanged via diplomatic bags
But the war consumed huge amounts a secret keys
At the end, they run short of keys and had to reuse the same key
Some of these messages were successfully decrypted by the United States and Great Britain

2. Public-key cryptography

Integer Factoring:

- prime number: natural number greater than one that has no positive divisor other than 1 and itself

  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, …

- integer factorization: given an integer, find its decomposition as a product of prime numbers

  $33=3 \times 11$

- notion taught in (junior) high school, but hard computational problem

  Is $2^{67}-1=147573952589676412927$ a prime?

  （question asked in 1644）

  Solved in 1903 by Frank Cole after 3 years of calculations

  $2^{67}-1=193707721 \times 761838257287$

Frank Cole
1861-1926

2. Integer Factorization

★ hard even for (current and future) supercomputers

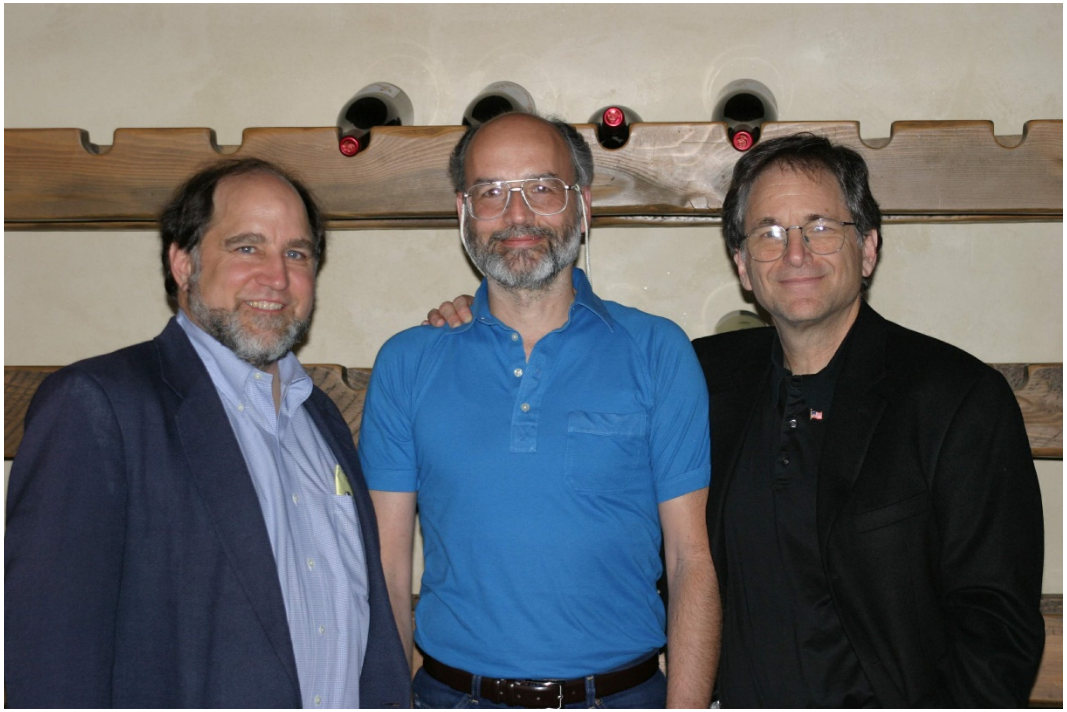
	1024 digits	2048 digits	4096 digits
Current super computers	10^5 years	10^{15} years	10^{29} years
Super computers in 2042	3 days	10^8 years	10^{22} years

complexity of integer factoring as a function of the number of digits

Current public-key cryptosystems assume the hardness of factoring numbers of 1024-2048 digits.

2. RSA cryptosystem

Public-key cryptosystem designed by Rivest, Shamir and Adleman in 1977



Ronald Rivest Adi Shamir Leonard Adleman

Turing Award 2002

2. Modular arithmetic modulo pq

Let p and q be two primes

Set N=pq

Consider the powers (modulo N) of integers 0, 1, …, N-1

$example: 22 = 11 \times 2$

$$7^2 = 49 \equiv 5 \bmod 22$$

$$7^3 = 343 \equiv 13 \bmod 22$$

…

Consider the power for which the number returns to itself

Theorem: for any integer a and any primes p and q,

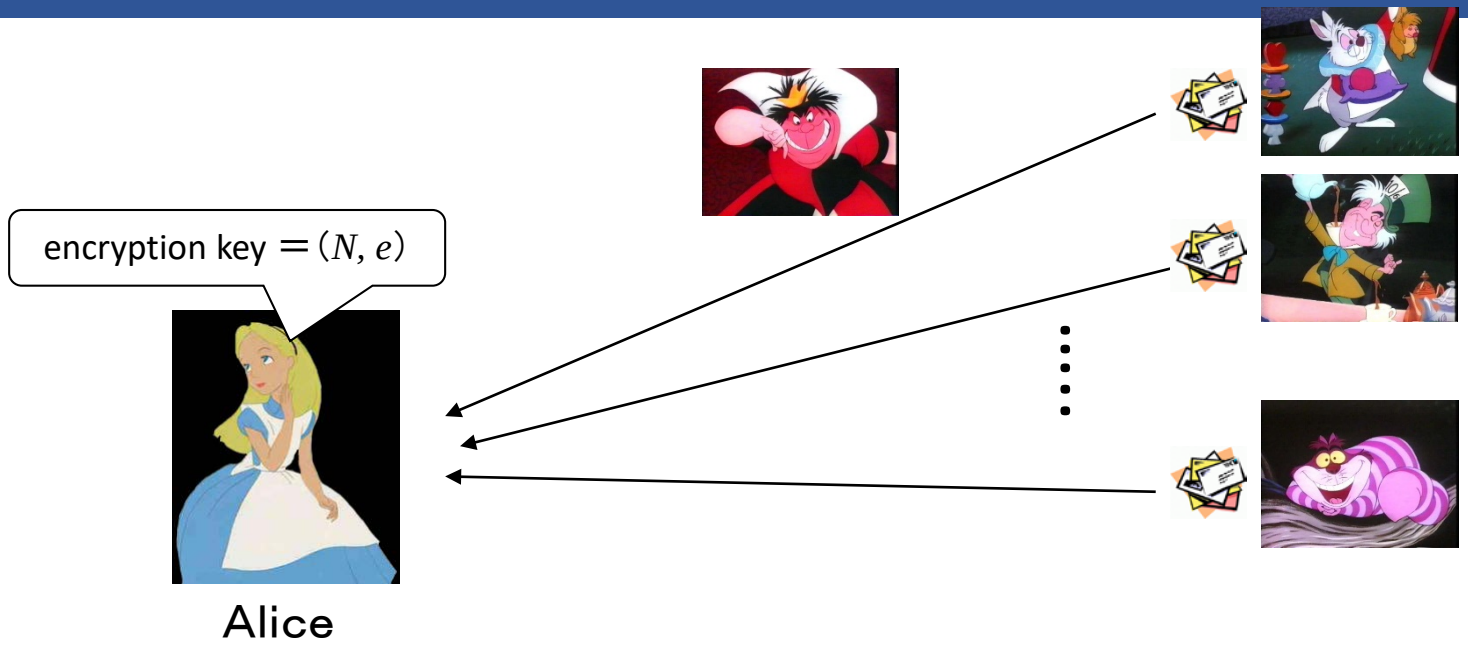
$$a^{(p-1)(q-1)+1} \equiv a \bmod pq$$

power

number	1	2	3	4	5	6	7	8	9	10	11	12	·····
1	1	1	1	1	1	1	1	1	1	1	1	1	·····
2	2	4	8	16	10	20	18	14	6	12	2	4	·····
3	3	9	5	15	1	3	9	5	15	1	3	9	·····
4	4	16	20	14	12	4	10	20	14	12	4	16	·····
5	5	3	15	9	1	5	3	15	9	1	5	3	·····
6	6	14	18	20	10	16	8	4	2	12	6	14	·····
7	7	5	13	3	21	15	17	9	19	1	7	5	·····
8	8	20	6	4	10	14	2	16	18	12	8	20	·····
9	9	15	3	5	1	9	15	3	5	1	9	15	·····
10	10	12	10	12	10	12	10	12	10	12	10	12	·····
11	11	11	11	11	11	11	11	11	11	11	11	11	·····
12	12	12	12	12	12	12	12	12	12	12	12	12	·····
13	13	15	19	5	21	9	7	3	17	1	13	15	·····
14	14	20	16	4	12	14	20	16	4	12	14	20	·····
15	15	5	9	3	1	15	5	9	3	1	15	5	·····
16	16	14	4	20	12	16	14	4	20	12	16	14	·····
17	17	3	7	9	21	5	19	15	13	1	17	3	·····
18	18	16	2	14	10	4	6	20	8	12	18	16	·····
19	19	9	17	15	21	3	13	5	7	1	19	9	·····
20	20	4	14	16	12	20	4	14	16	12	20	4	·····
21	21	1	21	1	21	1	21	1	21	1	21	1	·····

$$11 = (11-1)(2-1)+1$$

2. RSA Cryptosystem



- Alice chooses two large primes p, q and a large integer e coprime with (p-1)(q-1)

  Alice announces publicly $N = p \times q$ and e

- Assume that somebody wants to send Alice the message m

  some integer smaller than N

- The encrypted message is the *e*-th power of m modulo *N*

2. Example of Encryption

$(N=22, e=3)$

$N = 22 = 11 \times 2$

e=3

13

original message

7

encryption

$7^3 \bmod 22 = 13$

encryption : e-th power

	1	2	3	4	5	6	7	8	9	10	11	12		20	21	22	
1	1	1	1	1	1	1	1	1	1	1	1	1	.....	1	1	1	.....
2	2	4	8	16	10	20	18	14	6	12	2	4	.....	12	2	4	.....
3	3	9	5	15	1	3	9	5	15	1	3	9	.....	1	3	9	.....
4	4	16	20	14	12	4	10	20	14	12	4	16	.....	12	4	16	.....
5	5	3	15	9	1	5	3	15	9	1	5	3	.....	1	5	3	.....
6	6	14	18	20	10	16	8	4	2	12	6	14	.....	12	6	14	.....
7	7	5	13	3	21	15	17	9	19	1	7	5	.....	1	7	5	.....
8	8	20	6	4	10	14	2	16	18	12	8	20	.....	12	8	20	.....
9	9	15	3	5	1	9	15	3	5	1	9	15	.....	1	9	15	.....
10	10	12	10	12	10	12	10	12	10	12	10	12	.....	12	10	12	.....
11	11	11	11	11	11	11	11	11	11	11	11	11	.....	11	11	11	.....
12	12	12	12	12	12	12	12	12	12	12	12	12	.....	12	12	12	.....
13	13	15	19	5	21	9	7	3	17	1	13	15	.....	1	13	15	.....
14	14	20	16	4	12	14	20	16	4	12	14	20	.....	12	14	20	.....
15	15	5	9	3	1	15	5	9	3	1	15	5	.....	1	15	5	.....
16	16	14	4	20	12	16	14	4	20	12	16	14	.....	12	16	14	.....
17	17	3	7	9	21	5	19	15	13	1	17	3	.....	1	17	3	.....
18	18	16	2	14	10	4	6	20	8	12	18	16	.....	12	18	16	.....
19	19	9	17	15	21	3	13	5	7	1	19	9	.....	1	19	9	.....
20	20	4	14	16	12	20	4	14	16	12	20	4	.....	12	20	4	.....
21	21	1	21	1	21	1	21	1	21	1	21	1	.....	1	21	1	.....

2. Decryption

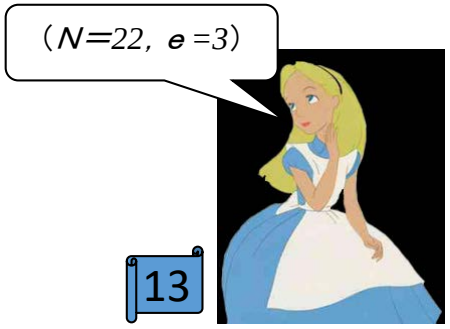
encryption : e-th power

decryption: d-th power

	1	2	3	4	5	6	7	8	9	10	11	12	.....	20	21	22	.....
1	1	1	1	1	1	1	1	1	1	1	1	1	.....	1	1	1	.....
2	2	4	8	16	10	20	18	14	6	12	2	4	.....	12	2	4	.....
3	3	9	5	15	1	3	9	5	15	1	3	9	.....	1	3	9	.....
4	4	16	20	14	12	4	10	20	14	12	4	16	.....	12	4	16	.....
5	5	3	15	9	1	5	3	15	9	1	5	3	.....	1	5	3	.....
6	6	14	18	20	10	16	8	4	2	12	6	14	.....	12	6	14	.....
7	7	5	13	3	21	15	17	9	19	1	7	5	.....	1	7	5	.....
8	8	20	6	4	10	14	2	16	18	12	8	20	.....	12	8	20	.....
9	9	15	3	5	1	9	15	3	5	1	9	15	.....	1	9	15	.....
10	10	12	10	12	10	12	10	12	10	12	10	12	.....	12	10	12	.....
11	11	11	11	11	11	11	11	11	11	11	11	11	.....	11	11	11	.....
12	12	12	12	12	12	12	12	12	12	12	12	12	.....	12	12	12	.....
13	13	15	19	5	21	9	7	3	17	1	13	15	.....	1	13	15	.....
14	14	20	16	4	12	14	20	16	4	12	14	20	.....	12	14	20	.....
15	15	5	9	3	1	15	5	9	3	1	15	5	.....	1	15	5	.....
16	16	14	4	20	12	16	14	4	20	12	16	14	.....	12	16	14	.....
17	17	3	7	9	21	5	19	15	13	1	17	3	.....	1	17	3	.....
18	18	16	2	14	10	4	6	20	8	12	18	16	.....	12	18	16	.....
19	19	9	17	15	21	3	13	5	7	1	19	9	.....	1	19	9	.....
20	20	4	14	16	12	20	4	14	16	12	20	4	.....	12	20	4	.....
21	21	1	21	1	21	1	21	1	21	1	21	1	.....	1	21	1	.....

$N = 22 = 11 \times 2$

e=3



encrypted message m^e

task: compute m from m^e

Note: in modular arithmetic taking the e-th root is hard

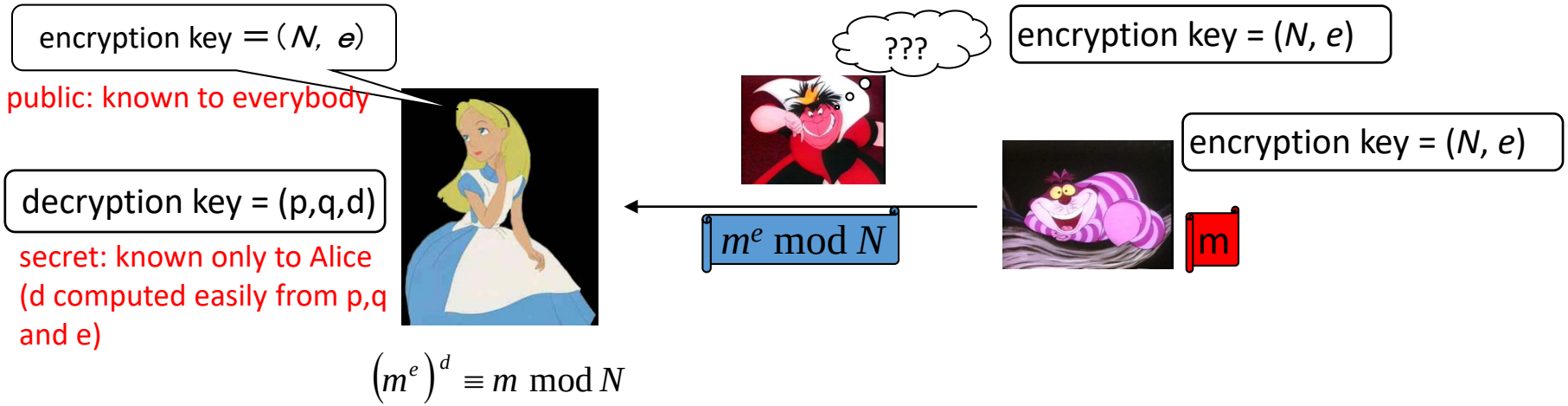
If there exist b and d such that $\left(m^e\right)^d = m^{b(p-1)(q-1)+1} \equiv m \mod N$

then taking the d-th power of the encrypted message gives m

such d exists if and only if e is coprime with (p-1)(q-1)

it can be computed easily if we know (p-1)(q-1)

2. RSA Cryptosystem: Summary



★ Alice chooses two large primes p, q and a large integer e coprime with (p-1)(q-1)

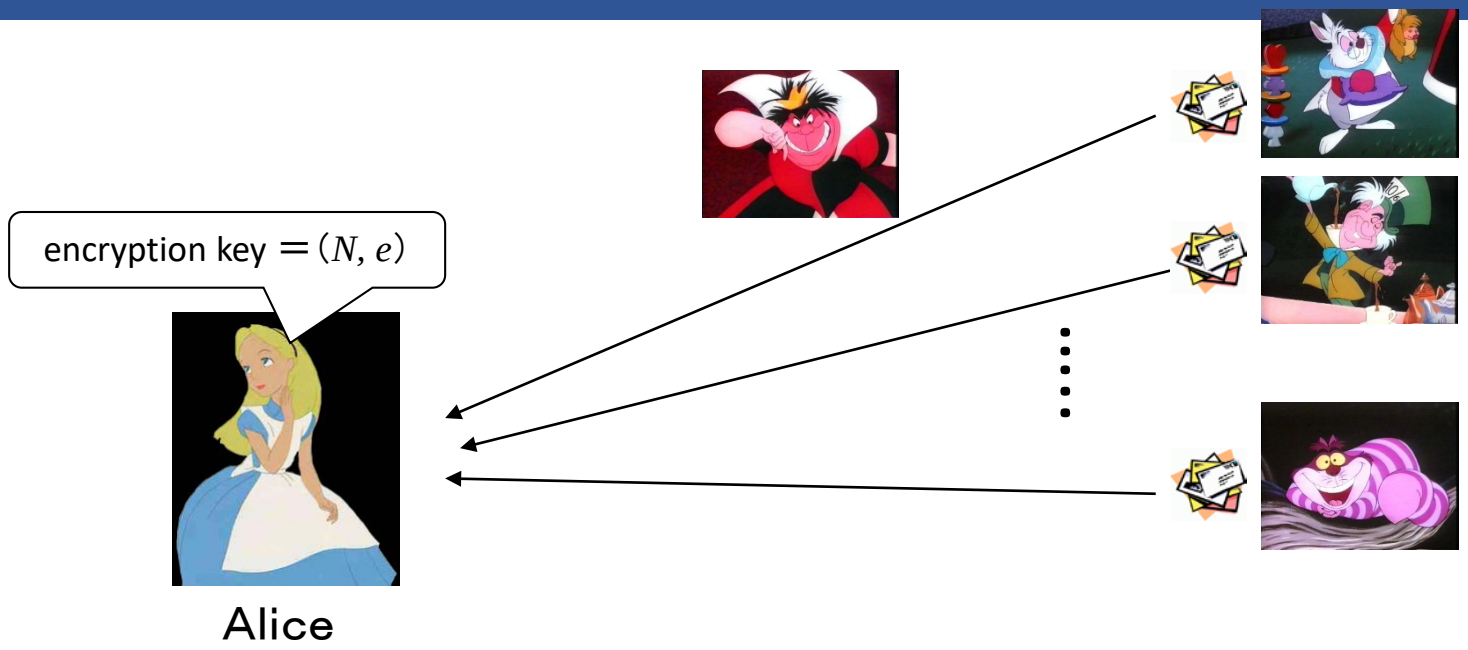
Alice announces publicly $N = p \times q$ and e

★ Alice computes d from p, q and e

★ To break this cryptosystem one need to compute d from e and N
To do this one need to find p and q (i.e., one need to factorize N)

security assuming the hardness of integer factoring

2. RSA Cryptosystem: Summary



Advantages:
- ✓ this completely solves the key distribution problem
- ✓ anybody can send a message to Alice

Disadvantages:
- ✓ secure only under an hardness assumption (hardness of integer factoring) and assuming that the adversary has not unlimited computational power
- ✓ slower than most private-key cryptosystems

RSA is widely used in practice

3. Cryptography in Practice

Recap: “Vernam Cipher” (1/2)

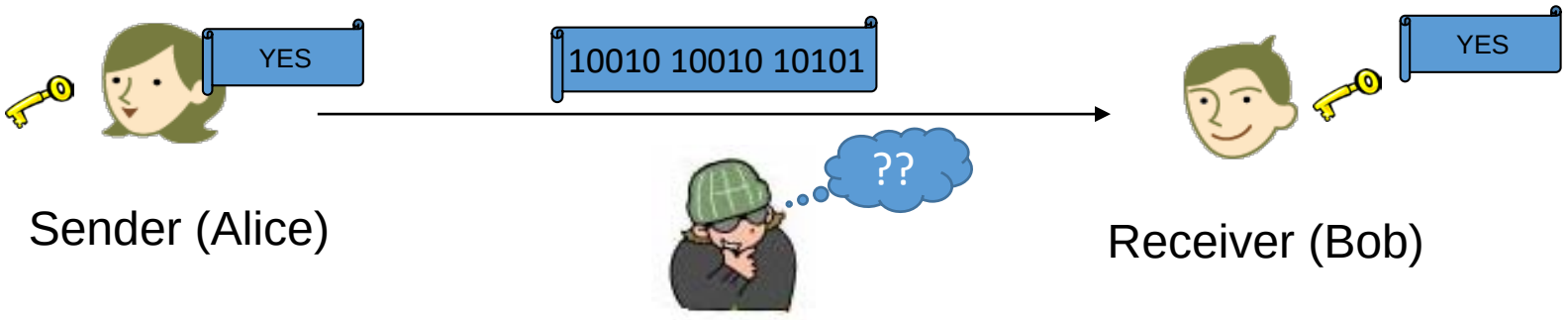
- ✓ the secret key is a (random) string of the same size as the original message
  encryption is done by adding the key bit by bit modulo 2
- ✓ Decryption is done by subtracting the key bit by bit modulo 2

Example: sending YES (binary encoding: 11000 00100 10010)

secret key: 01010 10110 00111

Encrypted message: 10010 10010 10101

decrypted message: 11000 00100 10010



For a key chosen uniformly at random, the probability distribution of the encrypted message does not depend on the original message

Recap: “Vernam Cipher” (2/2)

We have perfect security but:

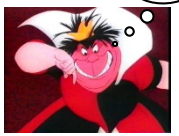
- ✓ the size of the key is the same as the size of the message to be sent!
- ✓ Perfect security is guaranteed only if the key is used only once:
  a new key is needed to send a new message (Vernam cipher also called “one-time pad”)
- ✓ the contents of the key must be a secret between the sender and the receiver

HOW TO DISTRIBUTE THE KEY ?
(same problem for any symmetric cryptosystem)

Some trusted third party has to distribute the key individually to Alice and Bob

Using public-key cryptography (RSA)!

encryption key = (N, e)



???

$k^e \bmod N$

k, generated at random

$$\left(k^e\right)^d \equiv k \bmod N$$

Recap: “Vernam Cipher” (2/2)

We have ~~perfect security~~ conditional security but:

still a problem

- ✓ the size of the key is the same as the size of the message to be sent!
- ✓ Perfect security is guaranteed only if the key is used only once:
  a new key is needed to send a new message (Vernam cipher also called “one-time pad”)

OK ✓ the contents of the key must be a secret between the sender and the receiver

HOW TO DISTRIBUTE THE KEY ?
(same problem for any symmetric cryptosystem)

Some trusted third party has to distribute the key individually to Alice and Bob

Using public-key cryptography (RSA)!

- ✓ Since RSA is slow, in practice we are limited to keys of a few thousands of bits
- ✓ We can use Vernam Cipher for small messages, but in practice we want to use symmetric cryptosystems for which the key is as small as possible and can be reused

Solution for the size of the key: Block ciphers

Divide the original message into blocks (typical size: 128 bits)

Perform encryption of each of the block

One “small” key is enough

m = 0010101 0010100 1001010 1010100 10101010

m_1 m_2 m_3 m_4 m_5

here block size = 7

Cryptography in Practice

public-key cryptography

RSA to share a key of size 128 bits

secret-key cryptography

And then can use freely secret-key cryptography on block size 128

Vernam's cipher cannot be used (since the key is reused)

Instead use cryptosystems like the Advanced Encryption Standard (AES), which uses a key of length 128 and is widely believed to be secure even if the key is reused