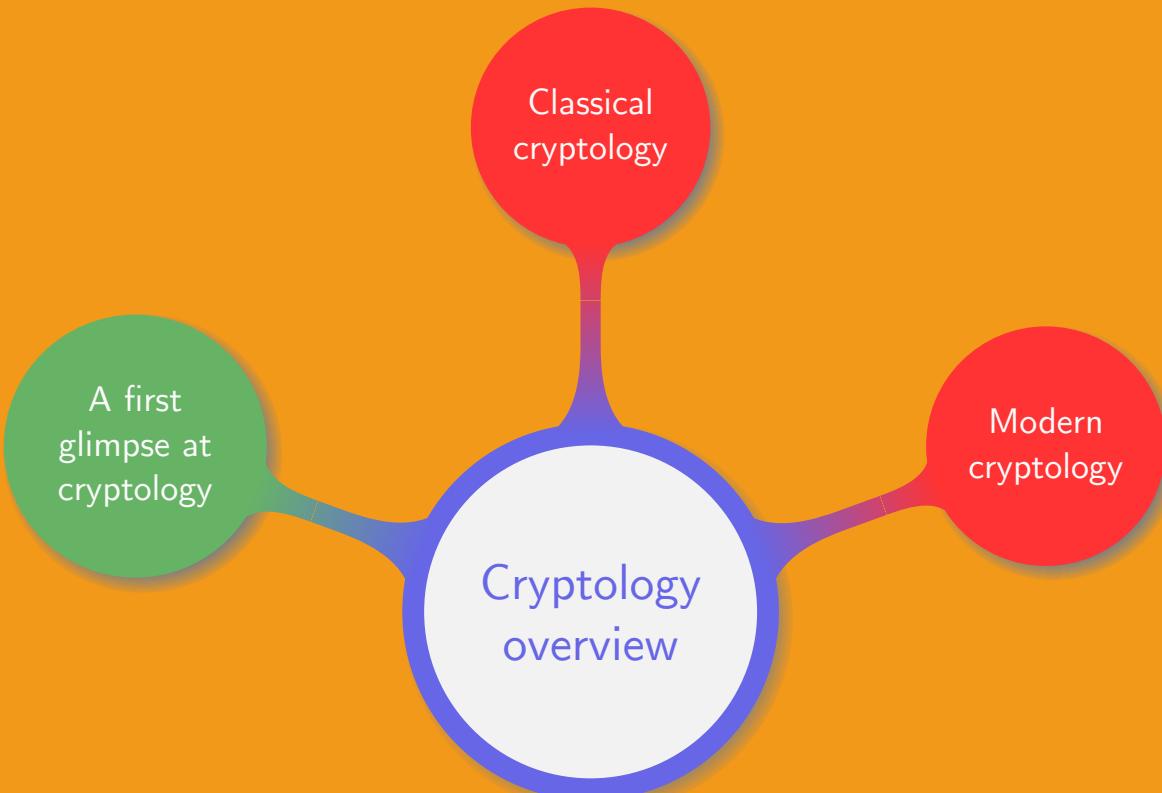


# Introduction to Cryptography

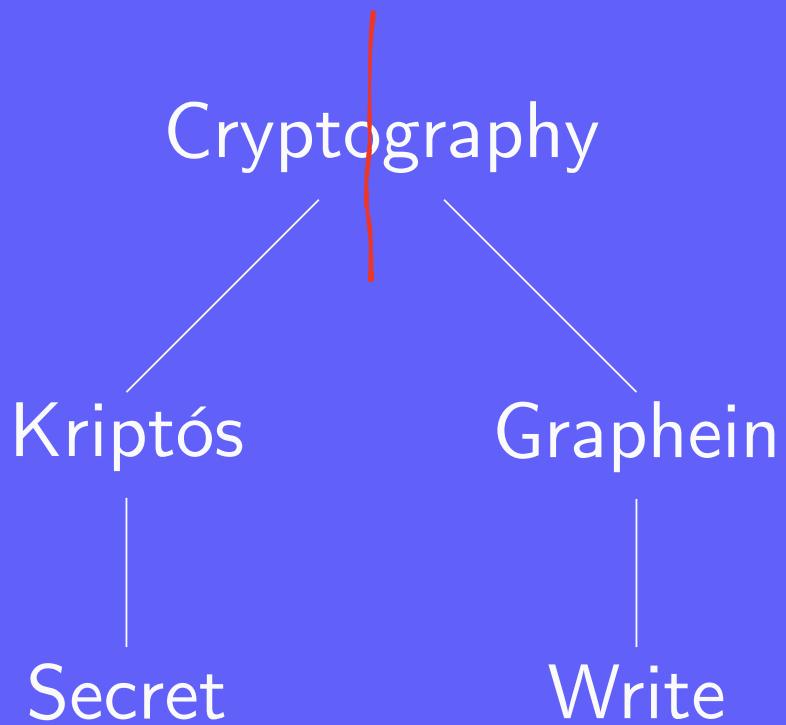
1. Cryptology overview

Manuel – Summer 2020

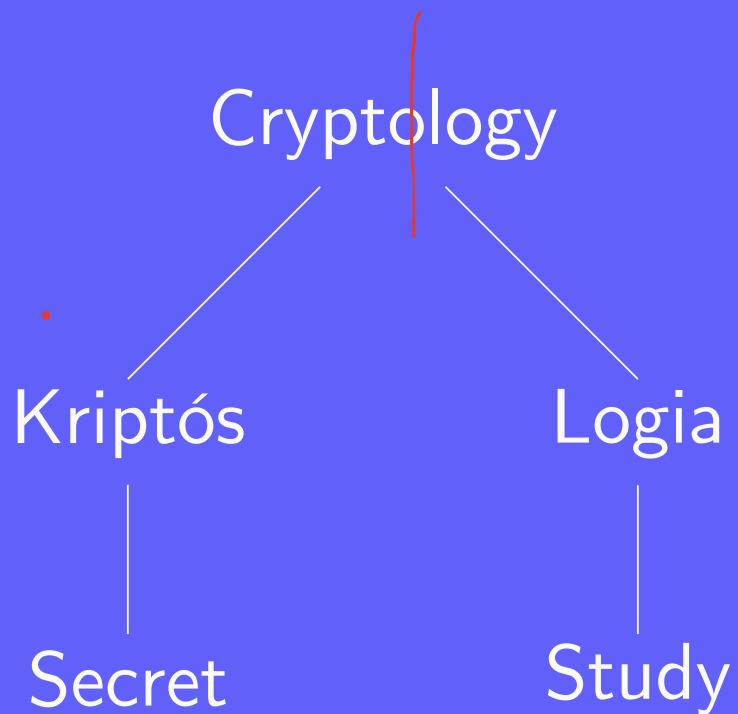
# Chapter organisation



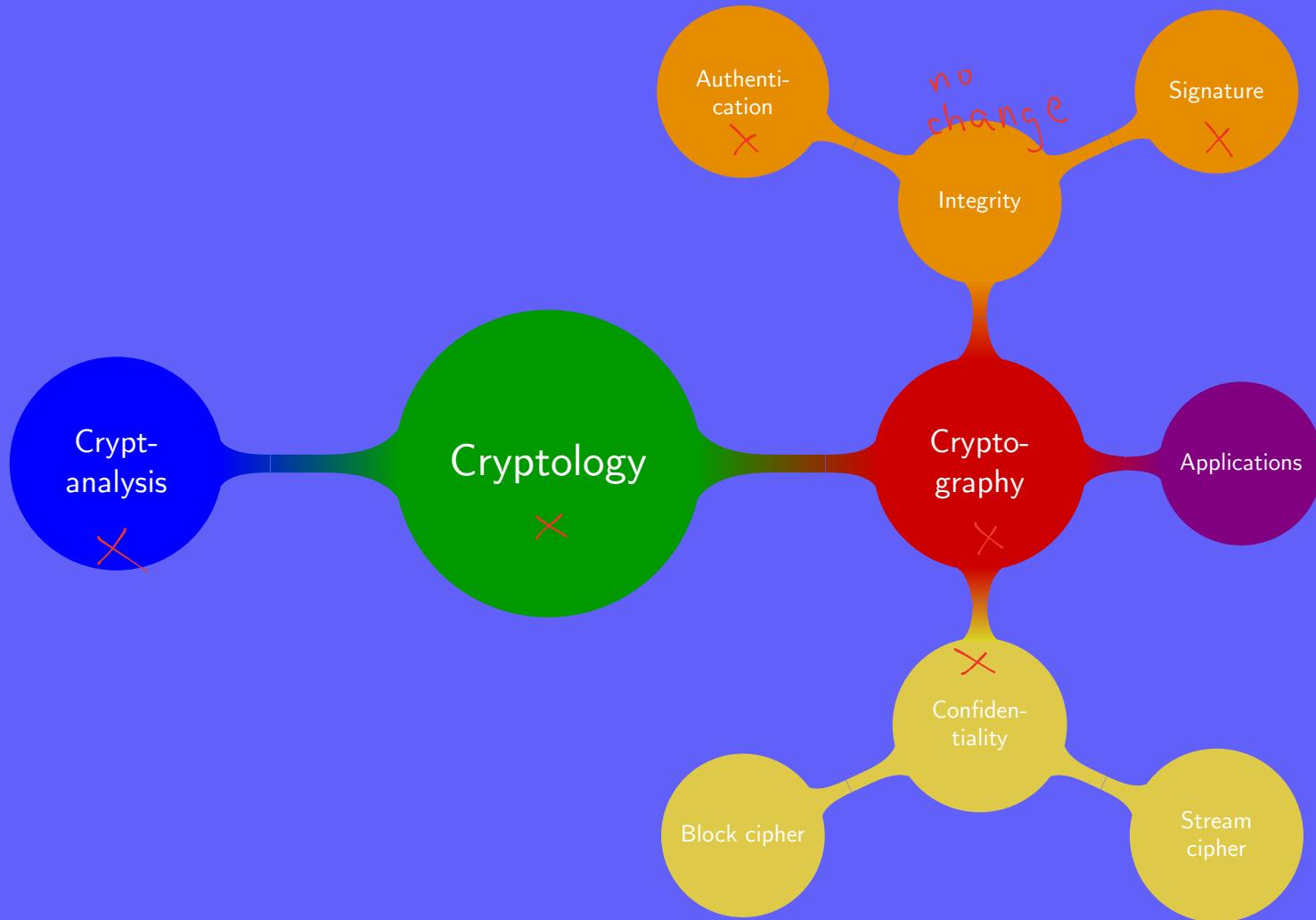
Are you following the right course?



## Etymology

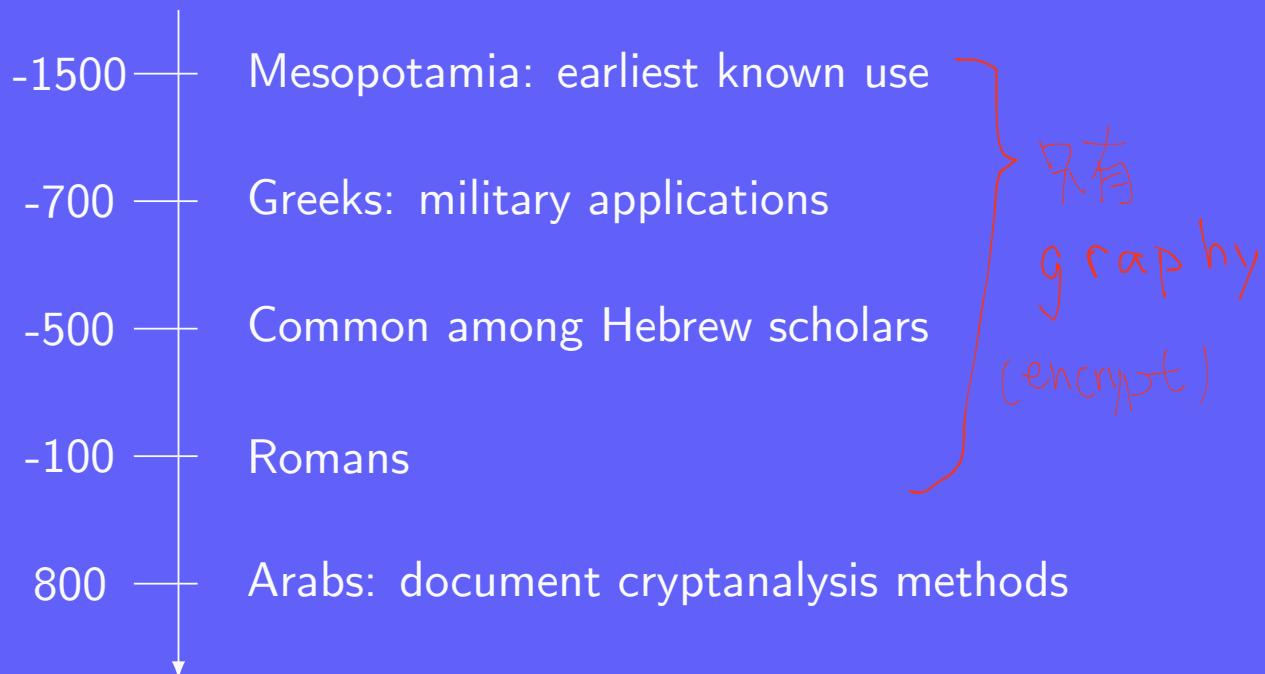


# Cryptology



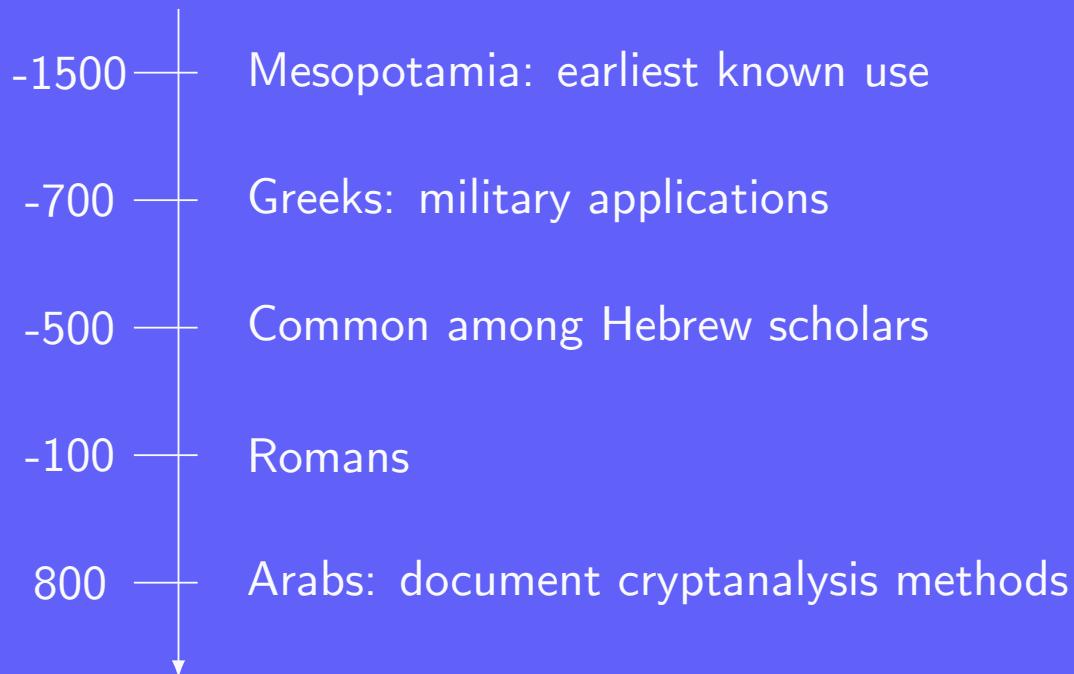
# A brief history of cryptology – Early times

Cryptology as an old science:



# A brief history of cryptology – Early times

Cryptology as an old science:



*Advantage was on the side of cryptanalysts*

# A brief history of cryptology – Until World War II

dict 不能丢失

No major advances until World War I:

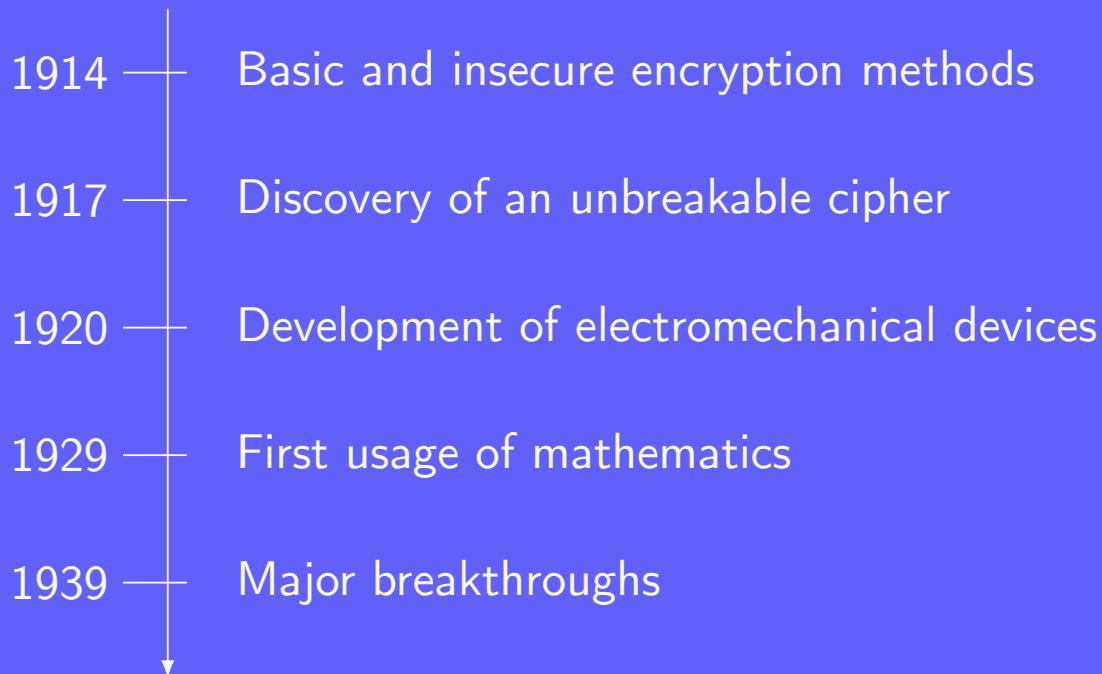
1914	Basic and insecure encryption methods
1917	Discovery of an <u>unbreakable cipher</u> → OTP
1920	Development of electromechanical devices
1929	First usage of mathematics
1939	Major breakthroughs

$$\begin{array}{ccc} A & \xrightarrow{k} & B \\ & \downarrow & \\ C & \xrightarrow{k'} & D \end{array}$$

k要不同才行

# A brief history of cryptology – Until World War II

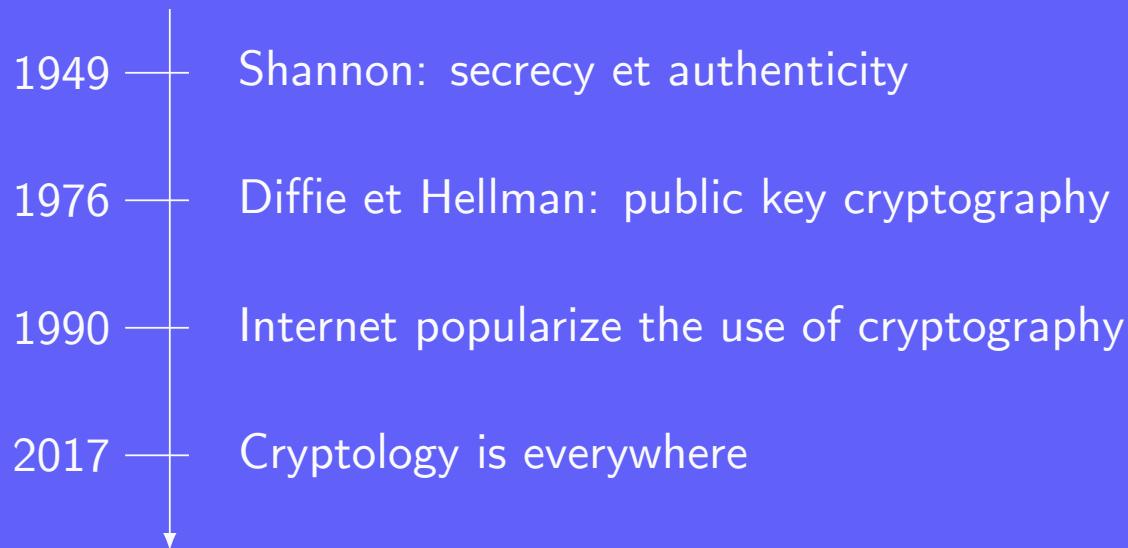
No major advances until World War I:



*Advantage is still on the side of cryptanalysts*

# A brief history of cryptology – Modern times

Mathematics becomes the heart of cryptography:



NsA hire most mathematicians .

# A brief history of cryptology – Modern times

Mathematics becomes the heart of cryptography:



*Politics try to kill cryptography and give governments the monopoly*

backdoor

# Basic communication scenario

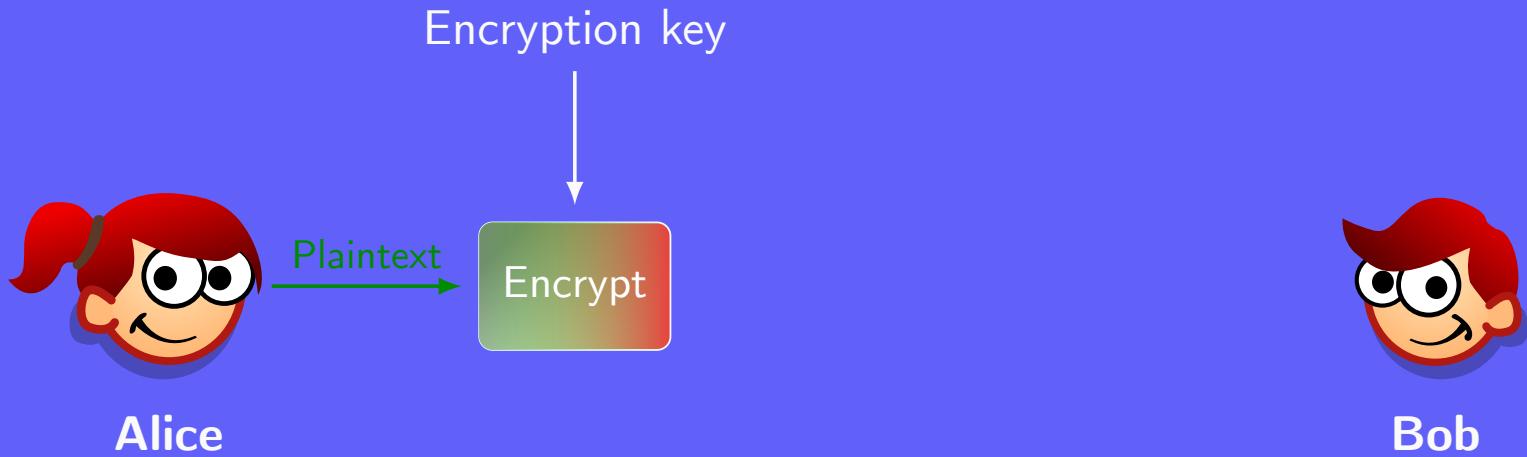


Alice

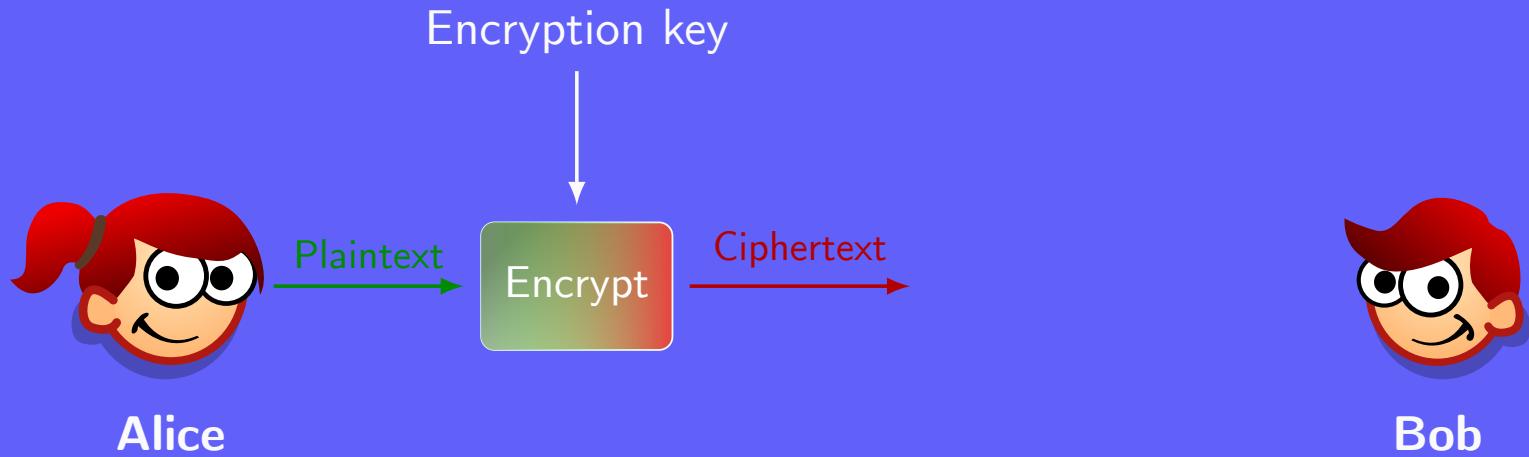


Bob

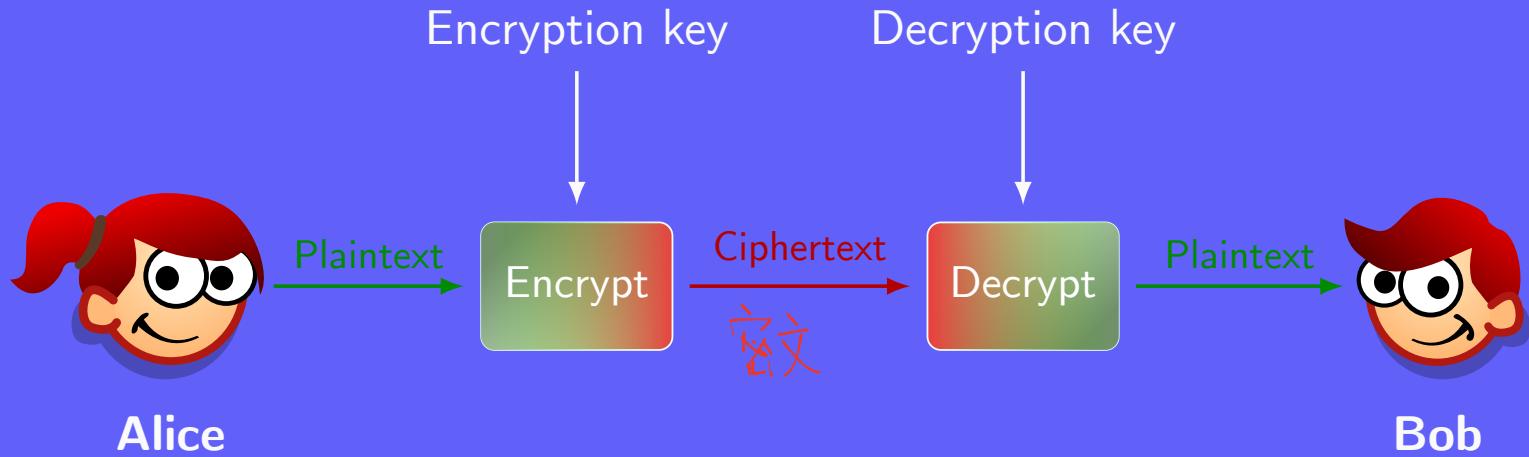
# Basic communication scenario



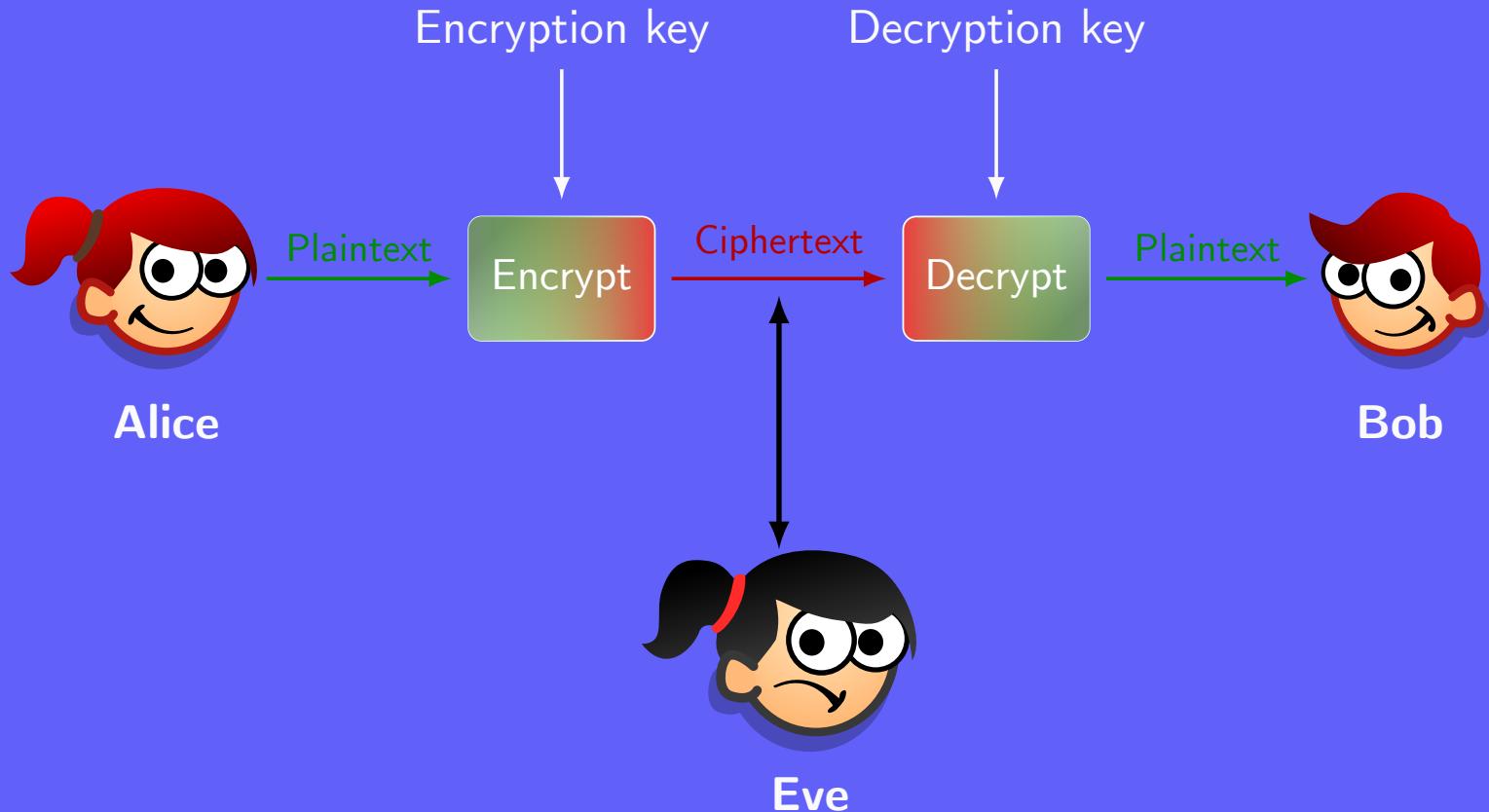
# Basic communication scenario



# Basic communication scenario



# Basic communication scenario



# Eve's goals

Eve has one of the following goals:

- Read a message
- Find the key
- Corrupt Alice's message
- Masquerade as Alice

Phylos

Most dangerous

weak

Eve's strategy

其 CPA = CCA,

strong

There are the five main types of attacks:

- Eve only has a copy of the ciphertext: *ciphertext only*  
密文
- Eve has a copy of the ciphertext but also of the corresponding plaintext: *Known Plaintext Attack (KPA)*  
明文
- Eve chooses the plaintext to be encrypted: *Chosen Plaintext Attack (CPA)*  
选明文  
CPA-2 (adaptive/反向尝试)
- Eve chooses the ciphertext to be decrypted: *Chosen Ciphertext Attack (CCA)*  
选密文  
CCA-2
- Eve chooses any plaintext to be encrypted or ciphertext to be decrypted: *Chosen Plaintext and Ciphertext Attack (CPCA)*

★ CCA slightly stronger than CPA 有时 ciphertext 会 invalid

## Eve's strategy

### A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.  
LET'S BUILD A MILLION-DOLLAR  
CLUSTER TO CRACK IT.

NO GOOD! IT'S  
4096-BIT RSA!

BLAST! OUR  
EVIL PLAN  
IS FOILED!



### WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.  
DRUG HIM AND HIT HIM WITH  
THIS \$5 WRENCH UNTIL  
HE TELLS US THE PASSWORD.

GOT IT.



# Eve's strategies

Methods to collect data:

- On fiber cables and infrastructures as the flow passes
- From the servers of service providers

收集

Methods to retrieve encrypted data:

- Break the encryption
- Influence industrial standards
- Pressure manufacturers to make insecure devices
- Infiltrate hardware and software

# Who is Eve and why is she evil?

Eve is anyone that might want to read or temper the data:

- Low threat: friends, family members, etc.
- High threat: governmental agencies and companies

# Who is Eve and why is she evil?

Eve is anyone that might want to read or temper the data:

- Low threat: friends, family members, etc.
- High threat: governmental agencies and companies

Reasons for mass surveillance: 監視

- Combat terrorism
- Assess foreign policies and economical stability
- Gather commercial secrets

# Why fear Eve?

What does your phone know about you?

# Why fear Eve?

What does your phone know about you?

*"They (the NSA) can use the system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with, and attack you on that basis to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer."*

「汝加之罪」

Edward Snowden

# Kerckhoffs' principle

## Principle (Kerckhoffs' principle)

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

# Kerckhoffs' principle

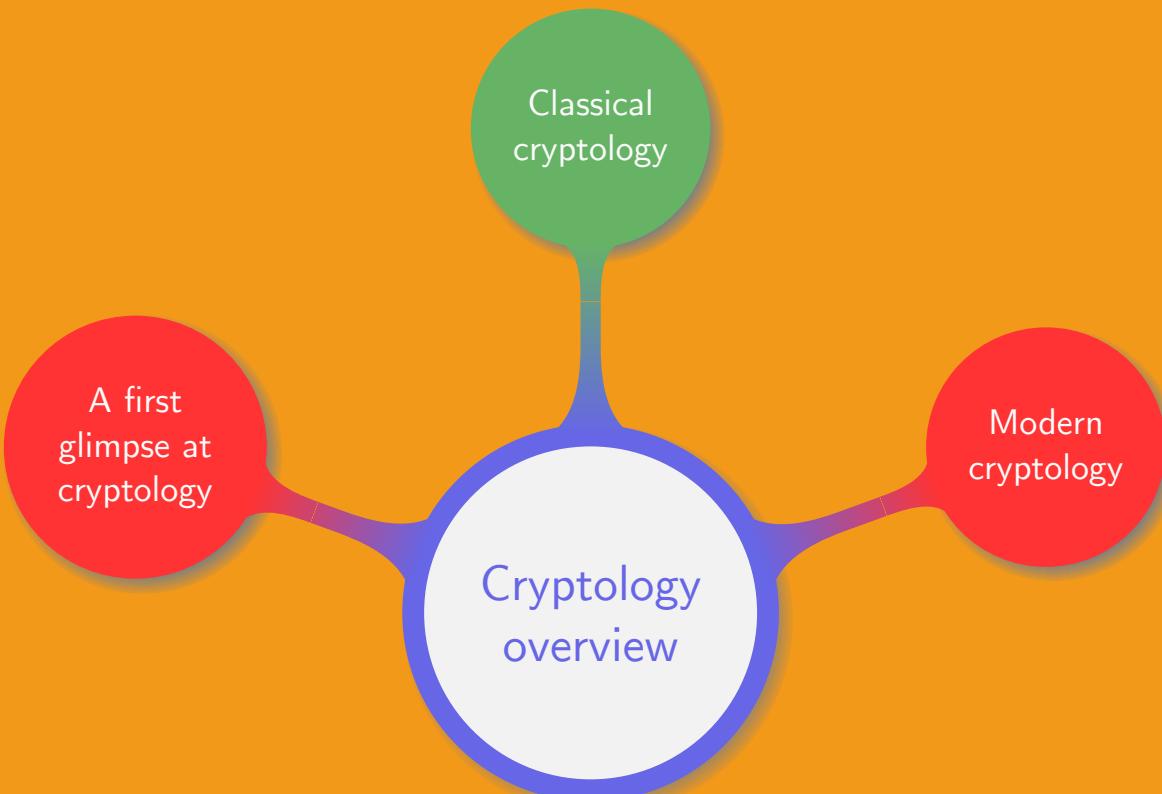
## Principle (Kerckhoffs' principle)

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

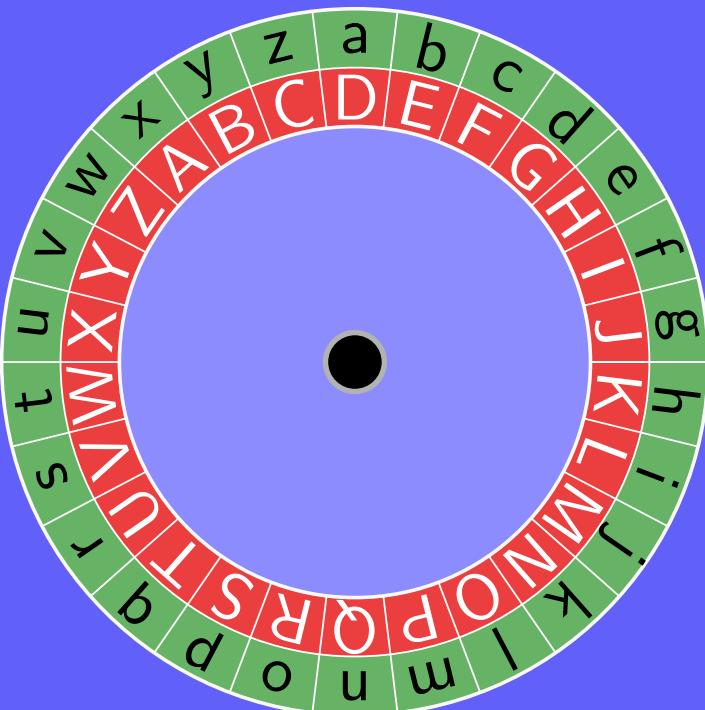
In other words:

- Security through obscurity is not security
- Data should be encrypted using standard, publicly known algorithms
- The implementation must be accessible to all

# Chapter organisation



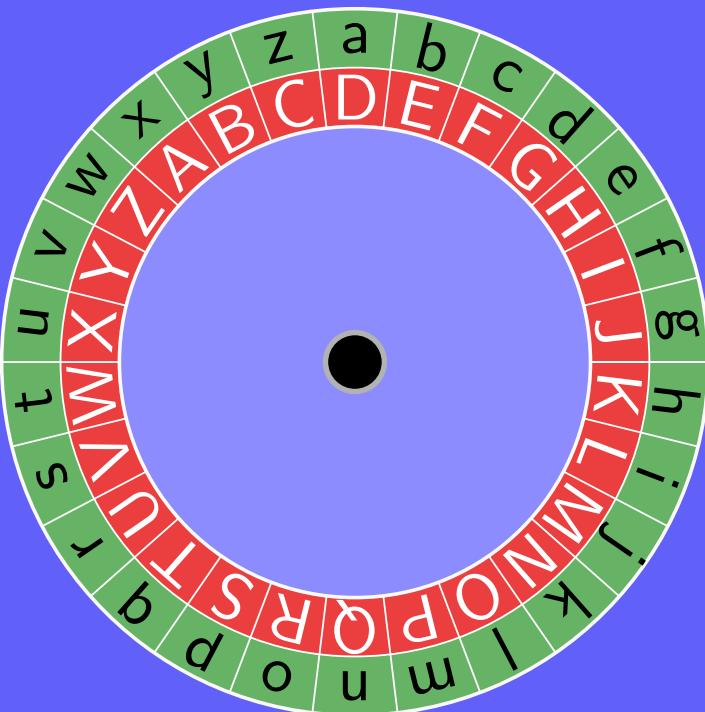
# Caesar cipher



Simple description:

- One of the earliest cipher
- Attributed to Julius Caesar
- Letters are shifted by a given number of places
- The shift is called the *key* of the cipher

# Caesar cipher



Simple description:

- One of the earliest cipher
- Attributed to Julius Caesar
- Letters are shifted by a given number of places
- The shift is called the *key* of the cipher

good morning

Exercise.

Recover the plaintext given the ciphertext JRRGPRUQLQJ

## Definitions

- ① Let  $a$  and  $b$  be two integers, with  $a \neq 0$ . We say that  $a$  divides  $b$  if there exists an integer  $k$  such that  $b = ak$ , and we denote it  $a|b$ .
- ② Let  $a$ ,  $b$  and  $n$  be three integers with  $n \neq 0$ . We say that  $a$  is congruent to  $b$  modulo  $n$ , if  $n$  divides  $a - b$ . It is denoted  $a \equiv b \pmod{n}$

## Definitions

- ① Let  $a$  and  $b$  be two integers, with  $a \neq 0$ . We say that  $a$  divides  $b$  if there exists an integer  $k$  such that  $b = ak$ , and we denote it  $a|b$ .
- ② Let  $a$ ,  $b$  and  $n$  be three integers with  $n \neq 0$ . We say that  $a$  is congruent to  $b$  modulo  $n$ , if  $n$  divides  $a - b$ . It is denoted  $a \equiv b \pmod{n}$

In modern cryptography:

- The plaintext is first converted into a numerical value
- If the alphabet is composed of  $n$  symbols then each one is assigned a value between 0 and  $n - 1$

# Revisiting Caesar cipher

Caesar cipher in mathematical terms:

- ① Label letters as integers from 0 to 25
- ② Choose a key  $\kappa$  in the range 0 – 25
- ③ Encrypt using the function  $x \mapsto x + \kappa \bmod 26$
- ④ Decrypt using the function  $x \mapsto x - \kappa \bmod 26$
- ⑤ Label integers from 0 to 25 as letters

# Revisiting Caesar cipher

Caesar cipher in mathematical terms:

- ① Label letters as integers from 0 to 25
- ② Choose a key  $\kappa$  in the range 0 – 25
- ③ Encrypt using the function  $x \mapsto x + \kappa \bmod 26$
- ④ Decrypt using the function  $x \mapsto x - \kappa \bmod 26$
- ⑤ Label integers from 0 to 25 as letters

Exercise.

Encrypt and decrypt “students are working hard” using Caesar cipher with the key  $\kappa = -5$

# Breaking Caesar cipher

Using the different types of attacks:

- Ciphertext only:

# Breaking Caesar cipher

Using the different types of attacks:

- Ciphertext only: only 26 possible keys  $\Rightarrow$  exhaustive search
- KPA:

# Breaking Caesar cipher

Using the different types of attacks:

- Ciphertext only: only 26 possible keys  $\Rightarrow$  exhaustive search
- KPA: deduce the key from the plaintext/ciphertext pair
- CPA:

# Breaking Caesar cipher

Using the different types of attacks:

- Ciphertext only: only 26 possible keys  $\Rightarrow$  exhaustive search
- KPA: deduce the key from the plaintext/ciphertext pair
- CPA: for the plaintext “a”, the ciphertext gives  $\kappa$
- CCA:

# Breaking Caesar cipher

Using the different types of attacks:

- Ciphertext only: only 26 possible keys  $\Rightarrow$  exhaustive search
- KPA: deduce the key from the plaintext/ciphertext pair
- CPA: for the plaintext “a”, the ciphertext gives  $\kappa$
- CCA: for the ciphertext “A”, the plaintext gives  $-\kappa \bmod 26$

# Substitution ciphers

In 1776 Thomas Jefferson sent a message to Benjamin Franklin:

LWNSOZBNWVWBAYBNVBSQWVUOHWDIZWRBBNPBPOOUWRPAWX  
AWPBWZWMYPOBNPBBNWJPAWWRZSLWZQJBNSIAWPBSALIBNX  
WABPIRYRPOIWRPQOWAIENBVBNPBPUSREBNWVWPWOIHWOiQWA  
BJPRZBNWFYAVYIBSHNPFFIRWVVBNPBBSVWXYAWBNWVWAIENBV  
ESDWARUWRBVPAPWIRVBIBYWZPUSREUWRZWAIDIREBHVIATYVBF  
SLWAVHASUBNWXSRVWRBSHBOTESDWARWZBNPBLNWWDWAPRJH  
SAUSHESDWARUWRBQWXSUWVZWVBAYXBIDWSHBNWVWRZVIBI  
VBNVAIENBSHBNWFWSFOWBSPOBWASABSPqSOIVNIBPRZBSIRVBIB  
YBWRWLESDWARUWRBOPJIREIBVHSYRZPBISRSRVYXNFAIRXIFOOT  
PRZSAEPRIKIREIBVFSLWAVIRVYXNHSAUPVBSVWMJSVBOICWOJBSW  
HHWXBBNWIAVPHWBJPRZNPFFIRWW

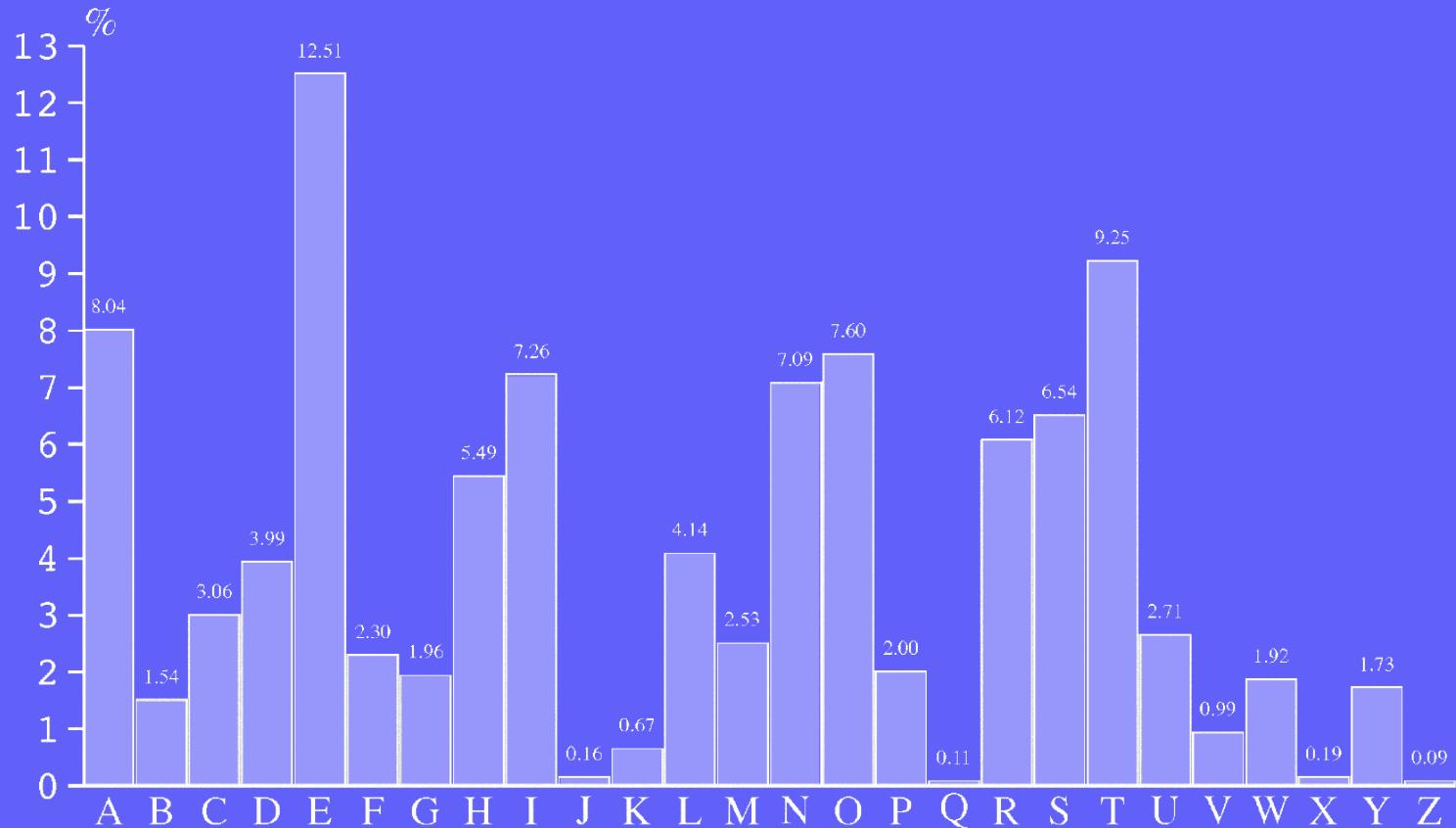
# Substitution ciphers

In 1776 Thomas Jefferson sent a message to Benjamin Franklin:

LWNSOZBNWVWBAYBNVBSQWVUOHWDIZWRBBNPBPOOUWRPAWX  
AWPBWZWMYPOBNPBBNWJPAWWRZSLWZQJBNSIAWPBSALIBNX  
WABPIRYRPOIWRPQOWAIENBVBNPBPUSREBNWVWPWOIHWOiQWA  
BJPRZBNWFYAVYIBSHNPFFIRWVVBNPBBSVWXYAWBNWVWAIENBV  
ESDWARUWRBVPWAIRVBIBYWZPUSREUWRZWAIDIREBHVIATYVBF  
SLWAVHASUBNWXSRVWRBSHBOTESDWARWZBNPBLNWWDWAPRJH  
SAUSHESDWARUWRBQWXSUWVZWVBAYXBIDWSHBNWVWRZVIBI  
VBNVAIENBSHBNWFWSFOWBSPOBWASABSPqSOIVNIBPRZBSIRVBIB  
YBWRWLESDWARUWRBOPJIREIBVHSYRZPBISRSRVYXNFAIRXIFOOT  
PRZSAEPRIKIREIBVFSLWAVIRVYXNHSAUPVBSVWMJSVBOICWOJBSW  
HHWXBBNWIAVPHWBJPRZNPFFIRWW

*Your job is to decipher it*

# Letters distribution in English



# Decrypting the message – Monograms

For the 10 most common letters their count gives:

W	B	R	S	I	V	A	P	N	O
76	64	39	36	36	35	34	32	30	16

# Decrypting the message – Monograms

For the 10 most common letters their count gives:

W	B	R	S	I	V	A	P	N	O
76	64	39	36	36	35	34	32	30	16

We can guess:

- W is probably e
- B, R, S, I, V, A, P, and N are probably t, a, o, i, n, s, h, and r
- In what order?

# Decrypting the message – Digrams

Digrams count

	W	B	R	S	I	V	A	P	N
W	3	4	12	2	4	10	14	3	1
B	4	4	0	11	5	5	2	4	20
R	5	5	0	1	1	5	0	3	0
S	1	0	5	0	1	3	5	2	0
I	1	8	10	1	0	2	3	0	0
V	8	10	0	0	2	2	0	3	1
A	7	3	4	2	5	4	0	1	0
P	0	8	6	0	1	1	4	0	0
N	14	3	0	1	1	1	0	7	0

Rules in English

- e contacts most of other letters
- a, i, o tend to avoid each other
- 80% of the letters preceding n are vowels 元音
- the most common digram is th
- h often appears before e, rarely after
- r pairs more with vowels and s with consonants 辅音
- rn more common than nr and to than ot

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
e	h	o			t	h	e	s	e	t	r		
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	h	s	t	o		e	s	e			e		i
Z	W	R	B	B	N	P	B	P	...				
e	n	t	t	h	a	t	a						

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
e	h	o			t	<b>h</b>	e	s	e	t	r		
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	h	s	t	o		e	s	e			e		i
Z	W	R	B	B	N	P	B	P	...				
e	n	t	t	h	a	t	a						

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
e	h	o			t	h	e	s	e	t	r		
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	<b>h</b>	<b>s</b>	t	o		e	s	e			e		i
Z	W	R	B	B	N	P	B	P	...				
e	n	t	t	h	a	t	a						

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
e	h	o			t	h	e	s	e	t	r	u	
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	<b>h</b>	<b>s</b>	t	o		e	s	e			e		i
Z	W	R	B	B	N	P	B	P	...				
e	n	t	t	h	a	t	a						

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
e	h	o			t	h	e	s	e	t	r	u	
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	h	s	<b>t</b>	<b>o</b>		<b>e</b>	s	e			e		i
Z	W	R	B	B	N	P	B	P	...				
e	n	t	t	h	a	t	a						

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
e	h	o			t	h	e	s	e	t	r	u	
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	h	s	<b>t</b>	<b>o</b>	<b>b</b>	<b>e</b>	s	e			e		i
Z	W	R	B	B	N	P	B	P	...				
e	n	t	t	h	a	t	a						

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
e	h	o			t	h	e	s	e	t	r	u	
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	h	s	t	o	b	e	s	e			e		i
Z	W	R	B	B	N	P	B	P	...				
e	n	t	t	h	a	t	a						

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
e	h	o			t	h	e	s	e	t	r	u	
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	h	s	t	o	b	e	s	e			e		i
Z	W	R	B	B	N	P	B	P	...				
e	n	t	t	h	a	t	a						

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
e	h	o				t	h	e	s	e	t	r	u
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	h	s	t	o	b	e	s	e			e		i
Z	W	R	B	B	N	P	B	P	...				
e	n	t	t	h	a	t	a						

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
e	h	o	I	d	t	h	e	s	e	t	r	u	
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	h	s	t	o	b	e	s	e	I	f	e	v	i
Z	W	R	B	B	N	P	B	P	...				
d	e	n	t	t	h	a	t	a					

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
e	h	o	I	d	t	h	e	s	e	t	r	u	
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	h	s	t	o	b	e	s	e	I	f	e	v	i
Z	W	R	B	B	N	P	B	P	...				
d	e	n	t	t	h	a	t	a					

# Completing the decryption

Summarizing all the guesses and carrying on:

L	W	N	S	O	Z	B	N	W	V	W	B	A	Y
w	e	<b>h</b>	<b>o</b>	<b>I</b>	<b>d</b>	t	h	e	s	e	t	r	u
B	N	V	B	S	Q	W	V	W	O	H	W	D	I
t	h	s	t	o	<b>b</b>	e	s	e	I	f	e	v	i
Z	W	R	B	B	N	P	B	P	...				
d	e	n	t	t	h	a	t	a					

## Deciphered text

The deciphered text is from the Declaration of independence:

we hold these truths to be self evident that all men are created equal  
that they are endowed by their creator with certain unalienable rights  
that among these are life liberty and the pursuit of happiness that to  
secure these rights governments are instituted among men deriving their  
just powers from the consent of the governed that whenever any form  
of government becomes destructive of these ends it is the right of the  
people to alter or to abolish it and to institute new government laying  
its foundation on such principles and organizing its powers in such form  
as to seem most likely to effect their safety and happiness

# Mary, the queen of Scots

a b c d e f g h i k l m n o p q r s t u x y z  
 ɔ † ʌ ɒ ɒθ ɒɒ ɪ ɔ̄ ʌn // ʃ ʊ ɔ ʌm ʃ ʌm ɛ ɔ 7 8 9

Nulles ff — — d <sup>ꝑ</sup>

Dowbleth σ <sup>F-4?</sup> → ??

and for with that if but where as of the from by  
 2 3 4 4 4 3 7 ʌ ʌ 8 8 8 8

so not when there this in wiche is what say me my wyrt  
 8 x + ƿ 6 x t ȝ m n m m d

send l̄e receave bearer I pray you Mte your name myne  
 1 8 t T L H - 3 7 ss

Using the One Time Pad:

- ① Represent the message as a sequence of 0s and 1s of length  $l$
- ② Generate a key of length  $l$  and composed of 0s and 1s
- ③ XOR the message and the key

好样的例子太好了！

# One Time Pad

Using the One Time Pad:

- ① Represent the message as a sequence of 0s and 1s of length  $l$
- ② Generate a key of length  $l$  and composed of 0s and 1s
- ③ XOR the message and the key



Breaking the One Time Pad:

- Ciphertext only: all the messages of same length have equal probability
- KPA, CPA, CCA: only reveal part of the key used during the attack

A *block cipher* encrypts several letters at once:

- Changing one letter in the plaintext impacts several letters in the ciphertext
  - Frequency analysis of letters and digrams cannot be applied
- 



A *block cipher* encrypts several letters at once:

- Changing one letter in the plaintext impacts several letters in the ciphertext
- Frequency analysis of letters and digrams cannot be applied

Hill cipher:

- Invented in 1929
- One of the first cipher to use algebraic methods
- Never been used much in practice

# Algebraic digression – Greatest common divisor

## Definition

The *greatest common divisor* of two integers  $a$  and  $b$ , with  $|a|+|b| \neq 0$ , is the largest positive integer dividing both  $a$  and  $b$ . It is noted  $\gcd(a, b)$ , and  $a$  and  $b$  are said to be *coprime* if  $\gcd(a, b) = 1$ .

In fact  $\gcd(a, b)$  can be expressed as a linear combination of  $a$  and  $b$  with integer coefficients.

## Lemma (Bézout's identity)

Let  $a$  and  $b$  be two integers where at least one of them is not zero, and  $d = \gcd(a, b)$ . Then there exists two integers  $s$  and  $t$ , called *Bézout coefficients*, such that  $as + bt = d$ .

# Algebraic digression – Computing the gcd

Algorithm. (*Extended Euclidean Algorithm*) 

**Input** :  $a, b$ , two positive integers

**Output:**  $r_1 = \gcd(a, b)$  and  $\langle s_1, t_1 \rangle$ , Bézout coefficients

```

1  $r_0 \leftarrow b; r_1 \leftarrow a;$ 
2  $s_0 \leftarrow 0; s_1 \leftarrow 1;$ 
3  $t_0 \leftarrow 1; t_1 \leftarrow 0;$ 
4 while  $r \neq 0$  do
5    $q \leftarrow r_1 \text{ div } r_0;$ 
6    $\langle r_1, r_0 \rangle \leftarrow \langle r_0, r_1 - qr_0 \rangle;$ 
7    $\langle s_1, s_0 \rangle \leftarrow \langle s_0, s_1 - qs_0 \rangle;$ 
8    $\langle t_1, t_0 \rangle \leftarrow \langle t_0, t_1 - qt_0 \rangle;$ 
9 end while
10 return  $r_1, \langle s_1, t_1 \rangle$ 
```

背一下

# Algebraic digression – Multiplicative inverse

## Proposition

Let  $a$  and  $n$  be two coprime integers and  $s$  and  $t$  be such that  $as + nt = 1$ . Then  $as \equiv 1 \pmod{n}$ , and  $s$  is called the *multiplicative inverse* of  $a$  modulo  $n$ . Besides  $s$  is unique.

Example.

What is the multiplicative inverse of 11111 modulo 12345?

# Algebraic digression – Multiplicative inverse

## Proposition

Let  $a$  and  $n$  be two coprime integers and  $s$  and  $t$  be such that  $as + nt = 1$ . Then  $as \equiv 1 \pmod{n}$ , and  $s$  is called the *multiplicative inverse* of  $a$  modulo  $n$ . Besides  $s$  is unique.

Example.

What is the multiplicative inverse of 11111 modulo 12345?

Running the extended Euclidean algorithm confirms that 11111 and 12345 are coprime and therefore 11111 is invertible modulo 12345. Moreover since

$$11111 \cdot 2471 + 12345 \cdot (-2224) = 1,$$

we conclude that  $11111 \cdot 2471 \equiv 1 \pmod{12345}$ .

# Algebraic digression – Matrix inversion

## Theorem (Cramer's rule)

Let  $A$  be an  $m \times m$  matrix, then

$$\text{Adj}(A) \cdot A = \det(A) I_m, \quad (1.1)$$

where  $\text{Adj}(A)$  denotes the adjugate of  $A$ ,  $\det(A)$  the determinant of  $A$ , and  $I_m$  the  $m \times m$  identity matrix.

From equation (1.1) we see that for  $A$  to be invertible,  $\det(A)$  must be invertible. In particular if  $A$  is defined modulo  $n$ ,  $\det(A)$  must be invertible modulo  $n$ , that is there exists  $t$  such that

$$\det(A) \cdot t \equiv 1 \pmod{n}.$$



## Algebraic digression – Modular matrix inversion

Example.

Compute the inverse of the matrix

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{pmatrix} \text{ mod } 11.$$

# Algebraic digression – Modular matrix inversion

Example.

Compute the inverse of the matrix

怎樣求逆

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{pmatrix} \text{ mod } 11.$$

Since  $\det(A) = 2$  and  $\gcd(2, 11) = 1$ ,  $A$  is invertible modulo 11 and

$\text{adj}$

$$A^{-1} = \frac{1}{2} \left( \begin{array}{c} + \begin{vmatrix} 2 & 3 \\ 4 & 9 \end{vmatrix} - \begin{vmatrix} 1 & 1 \\ 4 & 9 \end{vmatrix} + \begin{vmatrix} 1 & 1 \\ 2 & 3 \end{vmatrix} \\ - \begin{vmatrix} 1 & 3 \\ 1 & 9 \end{vmatrix} + \begin{vmatrix} 1 & 1 \\ 1 & 9 \end{vmatrix} - \begin{vmatrix} 1 & 1 \\ 1 & 3 \end{vmatrix} \\ + \begin{vmatrix} 1 & 2 \\ 1 & 4 \end{vmatrix} - \begin{vmatrix} 1 & 1 \\ 1 & 4 \end{vmatrix} + \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} \end{array} \right) \text{ mod } 11.$$

# Algebraic digression

Then calculating all the cofactors yields

$$A^{-1} = \frac{1}{2} \begin{pmatrix} 6 & -5 & 1 \\ -6 & 8 & -2 \\ 2 & -3 & 1 \end{pmatrix} \text{ mod } 11.$$

In this case it is easy to see that 6 is the inverse of 2 modulo 11, such that we get

$$A^{-1} = \begin{pmatrix} 36 & -30 & 6 \\ -36 & 48 & -12 \\ 12 & -18 & 6 \end{pmatrix} \equiv \begin{pmatrix} 3 & 3 & 6 \\ 8 & 4 & 10 \\ 1 & 4 & 6 \end{pmatrix} \text{ mod } 11.$$

Constructing Hill cipher:

- Key: generate a random  $n \times n$  matrix  $K$  modulo 26, with  $\gcd(\det(K), n) = 1$
- Encrypt:
  - Split the plaintext into blocks of size  $n$ , padding with extra letters if necessary
  - Multiply each block considered as a vector by the matrix  $K$
- Decrypt:
  - Split the ciphertext into blocks of size  $n$
  - Multiply each block considered as a vector by the matrix  $K^{-1}$

Example.

Encrypt “good morning” with the key  $K = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 9 & 7 & 8 \end{pmatrix}$ .

Example.

Encrypt “good morning” with the key  $K = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 9 & 7 & 8 \end{pmatrix}$ .

- 1 Split and pad the plaintext

g	o	o	d	m	o	r	n	i	n	g	x	
6	14	14	3	12	14	17	13	8	13	6	23	
$\underbrace{\quad}_{A}$			$\underbrace{\quad}_{B}$			$\underbrace{\quad}_{C}$			$\underbrace{\quad}_{D}$			$\_\_$

- 2 Multiply each vector by  $K$

$\overbrace{\quad\quad\quad}^{A'}$			$\overbrace{\quad\quad\quad}^{B'}$					$\overbrace{\quad\quad\quad}^{C'}$			$\overbrace{\quad\quad\quad}^{D'}$		
6	24	6	21	8	11	11	25	11	10	9	25		
G	Y	G	V	I	L	L	Z	L	K	J	Z		

## KPA on Hill cipher

Knowing “goodmorningx” and “GYGVILLZLKJZ” recover the key.

Knowing “goodmorningx” and “GYGVILLZLKJZ” recover the key.

- ① Find  $n$ : since  $n|12$ , try some values until the right one is found

## KPA on Hill cipher

Knowing “goodmorningx” and “GYGVILLZLKJZ” recover the key.

- ① Find  $n$ : since  $n|12$ , try some values until the right one is found
- ② Use the three first blocks to construct the equation

$$\underbrace{\begin{pmatrix} 6 & 14 & 14 \\ 3 & 12 & 14 \\ 17 & 13 & 8 \end{pmatrix}}_A \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \equiv \begin{pmatrix} 6 & 24 & 6 \\ 21 & 8 & 11 \\ 11 & 25 & 11 \end{pmatrix} \pmod{26}$$

# KPA on Hill cipher

Knowing “goodmorningx” and “GYGVILLZLKJZ” recover the key.

- ① Find  $n$ : since  $n|12$ , try some values until the right one is found
- ② Use the three first blocks to construct the equation

$$\underbrace{\begin{pmatrix} 6 & 14 & 14 \\ 3 & 12 & 14 \\ 17 & 13 & 8 \end{pmatrix}}_A \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \equiv \begin{pmatrix} 6 & 24 & 6 \\ 21 & 8 & 11 \\ 11 & 25 & 11 \end{pmatrix} \pmod{26}$$

- ③ Since  $A$  is not invertible modulo 26, try with the three last blocks

$$\underbrace{\begin{pmatrix} 3 & 12 & 14 \\ 17 & 13 & 8 \\ 13 & 6 & 23 \end{pmatrix}}_A \cdot \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \equiv \begin{pmatrix} 21 & 8 & 11 \\ 11 & 25 & 11 \\ 10 & 9 & 25 \end{pmatrix} \pmod{26}$$

## KPA on Hill cipher

- ④ Since  $A$  is now invertible we calculate

$$K = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \equiv \begin{pmatrix} 3 & 12 & 14 \\ 17 & 13 & 8 \\ 13 & 6 & 23 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 21 & 8 & 11 \\ 11 & 25 & 11 \\ 10 & 9 & 25 \end{pmatrix} \pmod{26}$$

$$K = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \equiv \begin{pmatrix} 11 & 18 & 4 \\ 7 & 11 & 10 \\ 1 & 22 & 11 \end{pmatrix} \cdot \begin{pmatrix} 21 & 8 & 11 \\ 11 & 25 & 11 \\ 10 & 9 & 25 \end{pmatrix} \pmod{26}$$

# KPA on Hill cipher

- ④ Since  $A$  is now invertible we calculate

$$K = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \equiv \begin{pmatrix} 3 & 12 & 14 \\ 17 & 13 & 8 \\ 13 & 6 & 23 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 21 & 8 & 11 \\ 11 & 25 & 11 \\ 10 & 9 & 25 \end{pmatrix} \pmod{26}$$

$$K = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \equiv \begin{pmatrix} 11 & 18 & 4 \\ 7 & 11 & 10 \\ 1 & 22 & 11 \end{pmatrix} \cdot \begin{pmatrix} 21 & 8 & 11 \\ 11 & 25 & 11 \\ 10 & 9 & 25 \end{pmatrix} \pmod{26}$$

And the key is

$$K = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 9 & 7 & 8 \end{pmatrix}.$$

Remarks on Hill cipher:

- In a substitution cipher, changing one letter from the plaintext alters one letter from the ciphertext
- In Hill cipher changing one letter from the plaintext alters the whole corresponding block from the ciphertext
- Hill cipher is not vulnerable to frequency analysis attacks
- As a drawback a small error in the transmission can induce a major error in the encrypted message and the deciphered text becomes unreadable

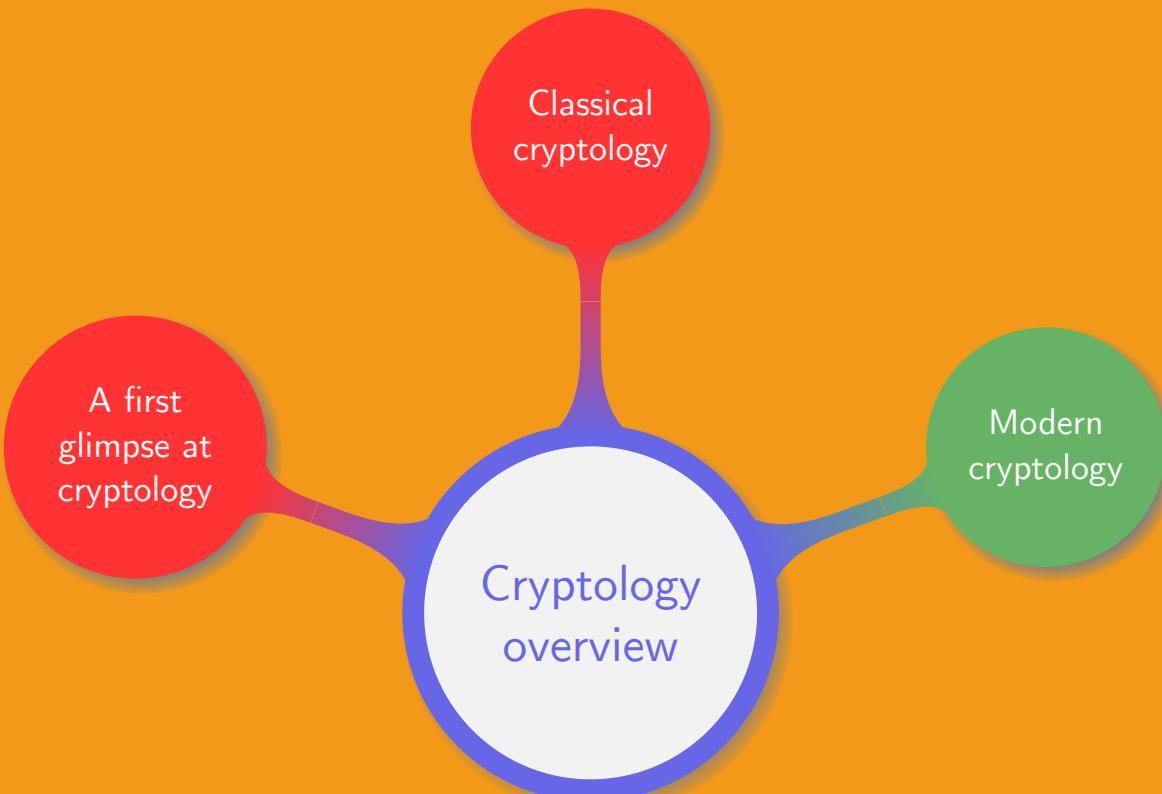
# The Enigma machine

Device information:

- Developed in Germany during the 1920s
- 1054560 ways to initialise the machine
- 100391791500 ways to interchange six pairs of letters
- Secretly broken in Poland in the 1930s
- Techniques extended by the British during World War II



# Chapter organisation



# Symmetric vs. Asymmetric

All the previous schemes are symmetric:

- The same key is used to both encrypt and decrypt
- The decryption key is easily derived from the encryption key

# Symmetric vs. Asymmetric

All the previous schemes are symmetric:

- The same key is used to both encrypt and decrypt
- The decryption key is easily derived from the encryption key

Limitations:

- Alice and Bob need to meet in order to exchange, generate, or share the secret keys
- Key management problem:
  - 2 users  $\rightarrow$  1 key
  - 5 users  $\rightarrow$  4 keys each, total 10 keys
  - $n$  users  $\rightarrow$   $n - 1$  keys each, total  $O(n^2)$  keys

# Public key cryptography



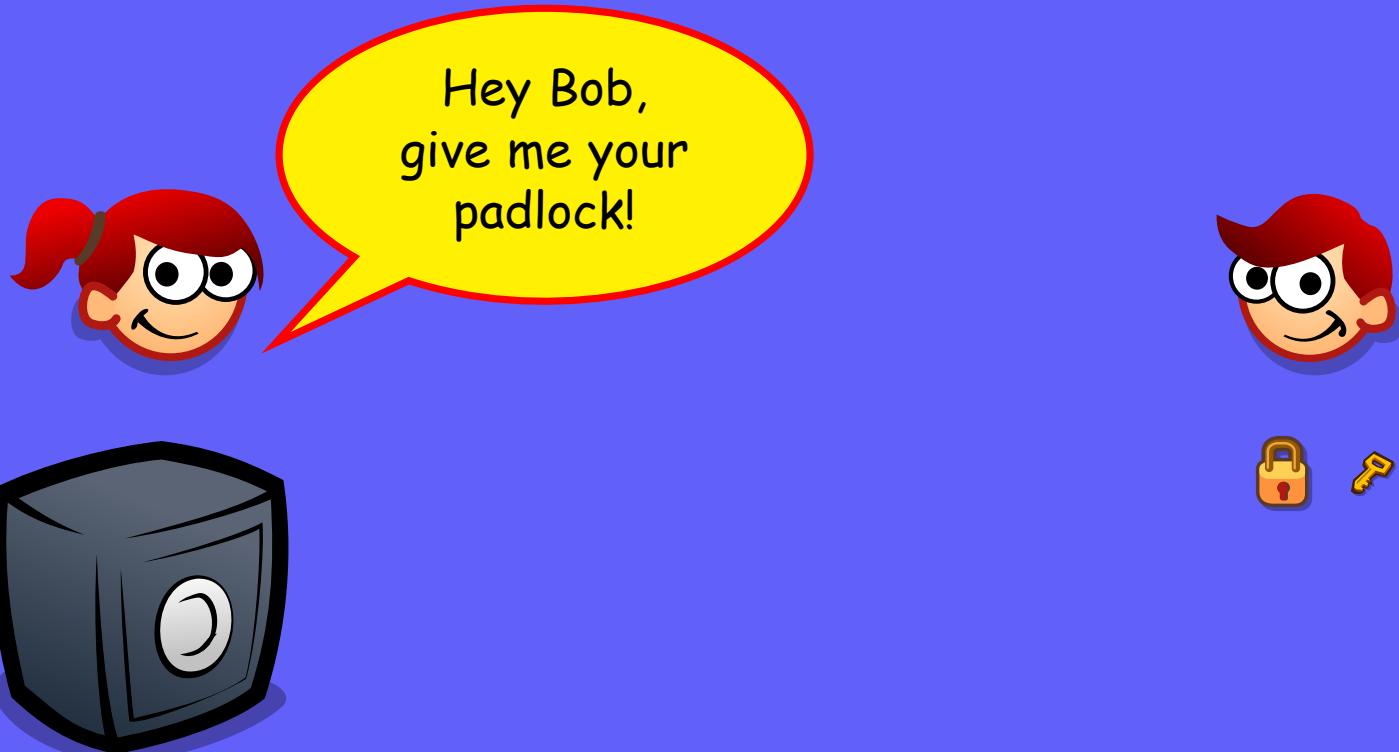
# Public key cryptography



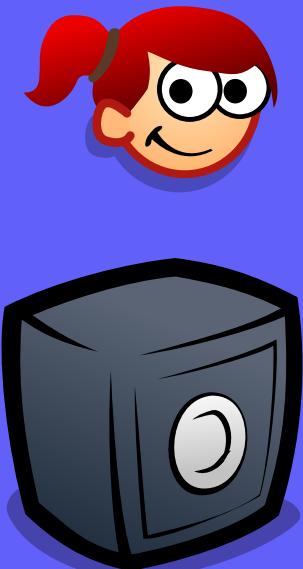
# Public Key Cryptography



# Public Key Cryptography



# Public Key Cryptography



Here it is!



# Public Key Cryptography



# Public Key Cryptography



Sorry, I  
open it and  
send it back.



# Public Key Cryptography



# Public Key Cryptography



# Public Key Cryptography



# Public Key Cryptography



Package re-  
ceived...and  
opened. Thanks.



# Implementing public key cryptography

*Anybody can lock the padlock but only Bob can unlock it*

# Implementing public key cryptography

*Anybody can lock the padlock but only Bob can unlock it*

Mathematical problems used in Public Key Cryptography (PKC):

- Easy to generate by anybody
- Hard to solve for everybody
- Easy to solve when knowing a small secret

公钥密码

# Implementing public key cryptography

*Anybody can lock the padlock but only Bob can unlock it*

Mathematical problems used in Public Key Cryptography (PKC):

- Easy to generate by anybody
- Hard to solve for everybody
- Easy to solve when knowing a small secret

Common examples:

- Multiplication and factorisation
- Exponentiation and discrete logarithm problem

$$\text{Handwritten note: } a^x \equiv b \pmod{n}$$

# Historical progression

Over time security has depended on:

- Early years: keeping the encryption method secret
- After WW I: keeping the secret key unknown
- Modern cryptography:
  - The method, the encryption key, and how to find the secret key are known
  - Security depends on the computational infeasibility of finding it

# Historical progression

Over time security has depended on:

- Early years: keeping the encryption method secret
- After WW I: keeping the secret key unknown
- Modern cryptography:
  - The method, the encryption key, and how to find the secret key are known
  - Security depends on the computational infeasibility of finding it

*PKC adds much flexibility at a high computational cost*

---

# Measuring security – Key space

Basic security feeling:

- Obvious strategy: brute force all possible keys
- Intuition: the larger the key space the harder finding the key

# Measuring security – Key space

Basic security feeling:

- Obvious strategy: brute force all possible keys
- Intuition: the larger the key space the harder finding the key

Example.

Substitution cipher:

- Key space:  $26! \approx 4 \cdot 10^{26} \approx 2^{89}$
- Very simple to break using frequency analysis



# Measuring security – Key space

Basic security feeling:

- Obvious strategy: brute force all possible keys
- Intuition: the larger the key space the harder finding the key

Example.

Substitution cipher:

- Key space:  $26! \approx 4 \cdot 10^{26} \approx 2^{89}$
- Very simple to break using frequency analysis

*Brute force is to be used only if no other attack is possible*

never brute force .

# Measuring security – Computational complexity

Best CPUs available in 2015:

- Regular user: 298,190 MIPS (Intel Core i7 5960x)
- Supercomputer: 10,000,000,000 MIPS (Fujitsu K – 705,024 cores)

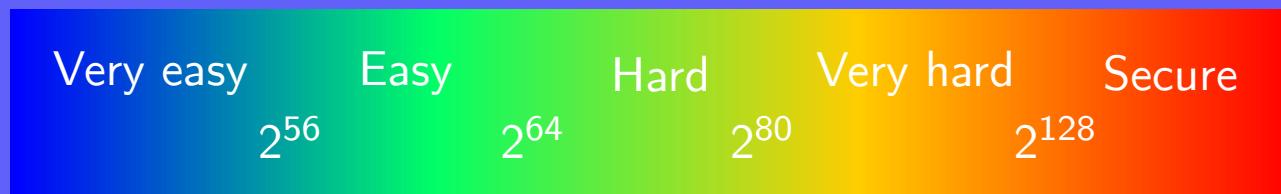
How many such computers need to run for a year to complete a program composed of  $2^{80}$  instructions?

# Measuring security – Computational complexity

Best CPUs available in 2015:

- Regular user: 298,190 MIPS (Intel Core i7 5960x)
- Supercomputer: 10,000,000,000 MIPS (Fujitsu K – 705,024 cores)

How many such computers need to run for a year to complete a program composed of  $2^{80}$  instructions?



# Complexity and security

*The goal is to be secure in the worst case*

In the worst case the attacker:

- Has the best computational facilities
- Uses the most efficient attack available

memory the computational power 難度提升.

*The goal is to be secure in the worst case*

In the worst case the attacker:

- Has the best computational facilities
- Uses the most efficient attack available

To be secure against such an attacker:

- Check to complexity of the best algorithm available
- Adjust the parameters of the cipher such that more than  $2^{128}$  operations are required to break the encryption

# Complexity and security

时间复杂度与常数项级大

Example.

Assuming that the best attack on a mathematical problem requires  $\sqrt{n}$  operations, where  $n$  is the size of the key, what key size should be chosen to be secure?

Since secure means that the attacker has to compute at least  $2^{128}$  operations to break the encryption it suffices to calculate

$$(2^{128})^2 = 2^{256}.$$

Hence the key space should contain  $2^{256}$  elements, that is the key should be at least 256 bits long.

# Improving security?

*Is double encryption with two different keys enhancing security?*

# Improving security?

*Is double encryption with two different keys enhancing security?*

Improving security:

- Naive answer: for a key of length  $k$ ,  $2^{2k}$  operations are needed

# Improving security?

*Is double encryption with two different keys enhancing security?*

Improving security:

- Naive answer: for a key of length  $k$ ,  $2^{2k}$  operations are needed
- Better answer:
  - It does not change anything, e.g. Hill cipher
  - It is possible to do better than  $2^{2k}$ : meet in the middle attack

Symmetric encryption using a function  $f$  and a key  $k$ :

- Simple encryption:  $c = f_k(m)$
- Double encryption:  $c = f_{k_2}(f_{k_1}(m))$
- Decryption:  $m = f_{k_1}^{-1}(f_{k_2}^{-1}(c))$

# Meet in the middle attack

Assuming a KPA setup:

- ① For all the keys, compute and store the ciphertexts  $c_i = f_{k_i}(m)$
- ② Compute all plaintexts  $m_i = f_{k_i}^{-1}(c)$  and find any matching  $c_i$
- ③ Recover the corresponding keys  $k_1$  and  $k_2$
- ④ Test  $k_1$  and  $k_2$  on more plaintext/ciphertext pairs

# Meet in the middle attack

Assuming a KPA setup:

- ① For all the keys, compute and store the ciphertexts  $c_i = f_{k_i}(m)$
- ② Compute all plaintexts  $m_i = f_{k_i}^{-1}(c)$  and find any matching  $c_i$
- ③ Recover the corresponding keys  $k_1$  and  $k_2$
- ④ Test  $k_1$  and  $k_2$  on more plaintext/ciphertext pairs

Exercise.

Assuming no attack applies on an encryption scheme and a key size of 64 bits, what is its security if applying double encryption?

# Complexity theory

Main complexity classes related to cryptology:



- $\mathcal{P}$ : decision problems for which there exists a deterministic polynomial time algorithm
- $\mathcal{NP}$ : decision problems for which the answer “yes” can be verified using a deterministic polynomial time algorithm
- $\mathcal{NP}$ -complete: hardest problems in  $\mathcal{NP}$
- co- $\mathcal{NP}$ : decision problems for which the answer “no” can be verified using a deterministic polynomial time algorithm
- co- $\mathcal{NP}$ -complete: hardest problems in co- $\mathcal{NP}$

Hint

# Complexity theory

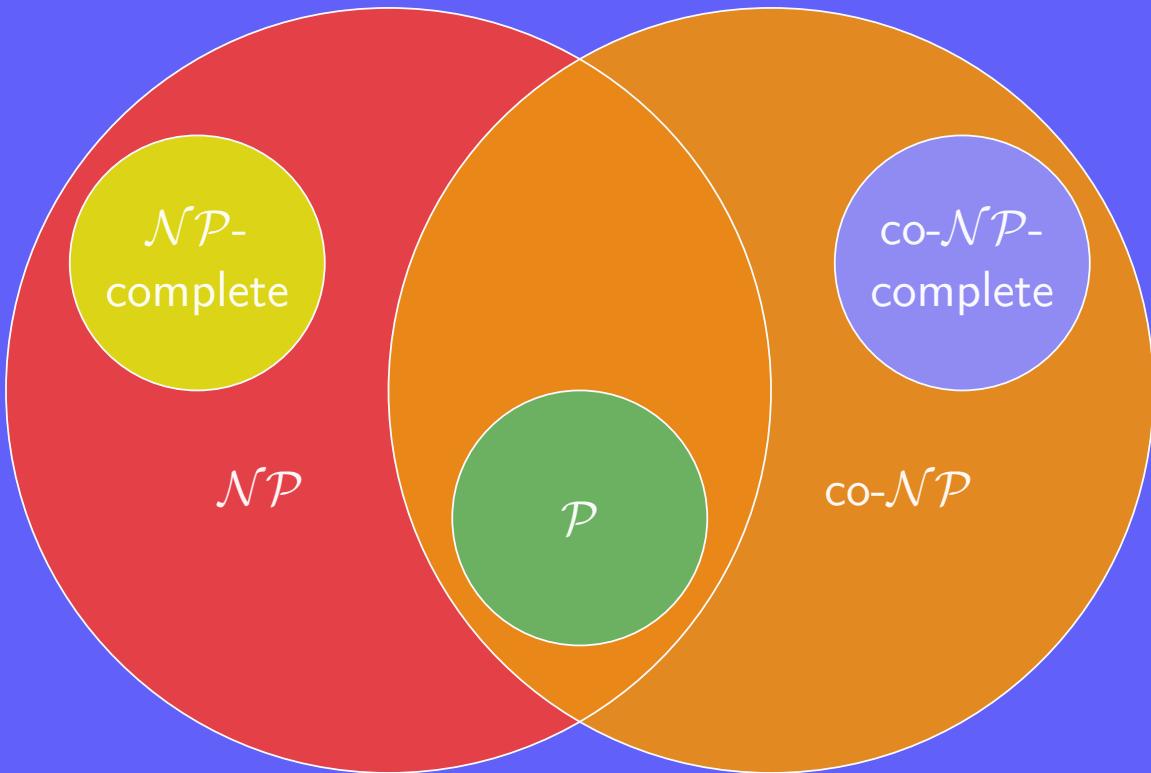
## Example.

Integer factorization is in both  $\mathcal{NP}$  and co- $\mathcal{NP}$

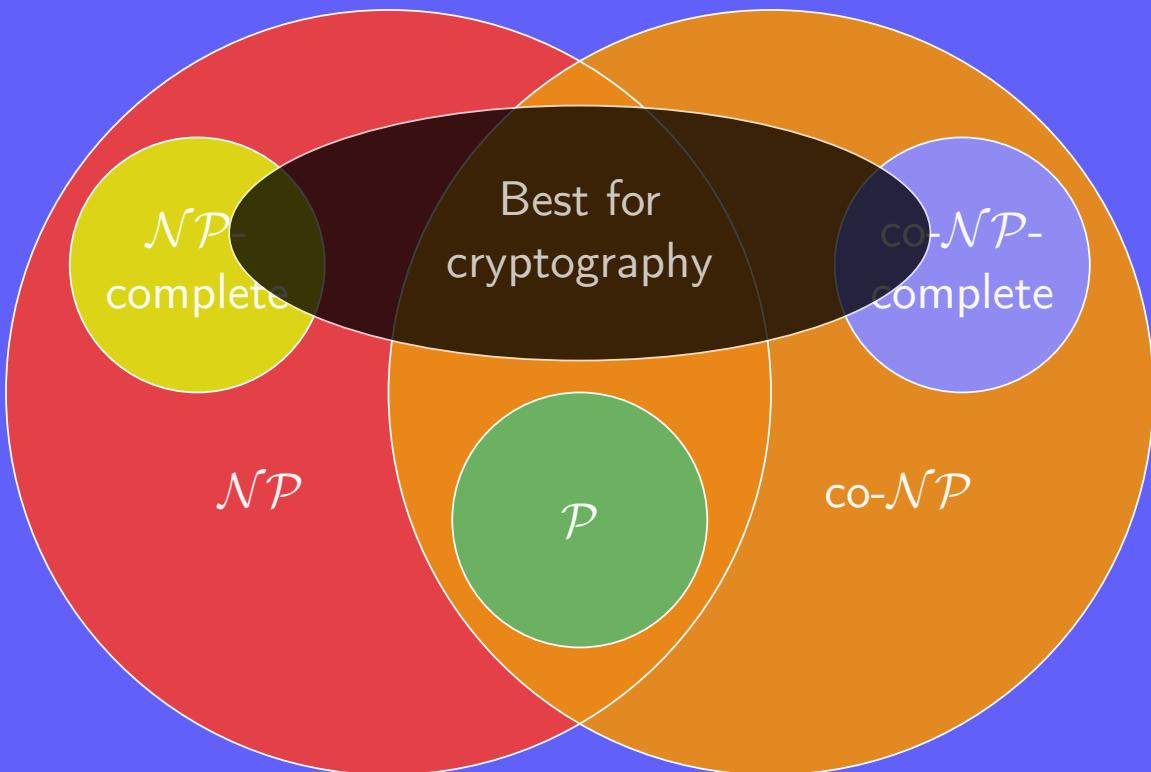
Let  $n$  be a large integer and  $1 < m < n$ . Does  $n$  have a factor  $p$ , with  $1 < p < m$ ?

- $\mathcal{NP}$ : with certificate “ $p$  a factor of  $n$ ” verify in polynomial time that  $1 < p < m$  and  $p|n$
- co- $\mathcal{NP}$ : with certificate “the list of all the prime factors of  $n$ ” verify in polynomial time that:
  - They are all prime
  - Their product is  $n$
  - None of them is between 1 and  $m$

# Complexity theory



# Complexity theory

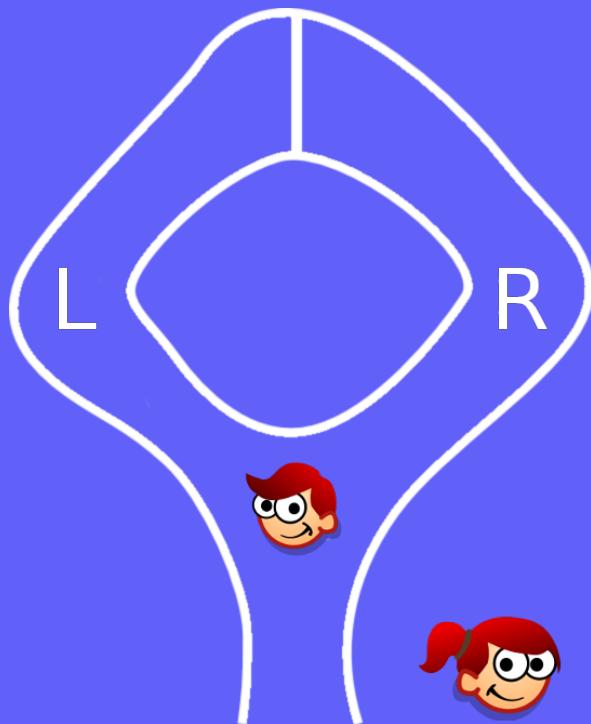


# Zero knowledge proofs

*Bob knows a secret path, and wants to prove it without revealing it*

# Zero knowledge proofs

*Bob knows a secret path, and wants to prove it without revealing it*

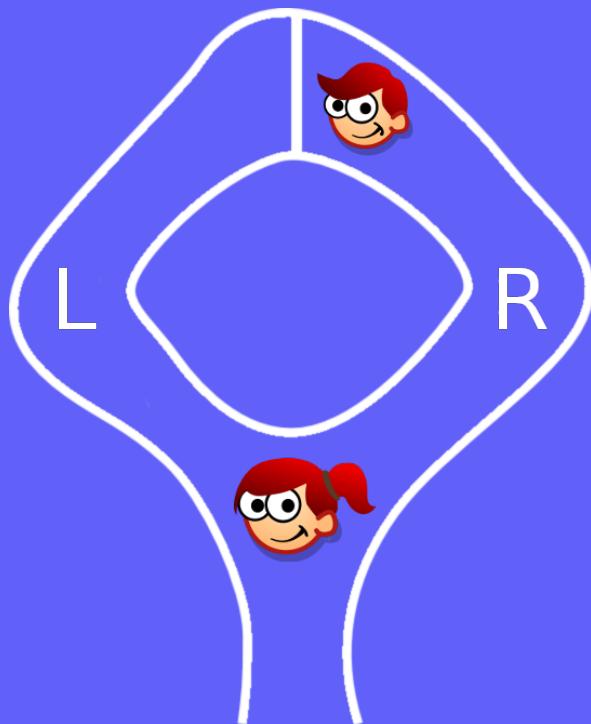


Strategy:

- ① Alice hides while Bob chooses to go Left (L) or Right (R)

# Zero knowledge proofs

*Bob knows a secret path, and wants to prove it without revealing it*

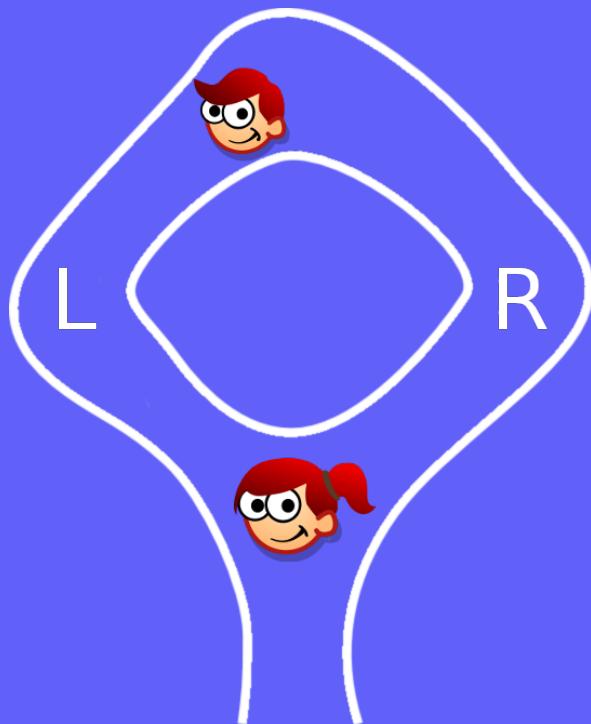


Strategy:

- ① Alice hides while Bob chooses to go Left (L) or Right (R)
- ② Alice randomly asks Bob to exit on L or R

# Zero knowledge proofs

*Bob knows a secret path, and wants to prove it without revealing it*

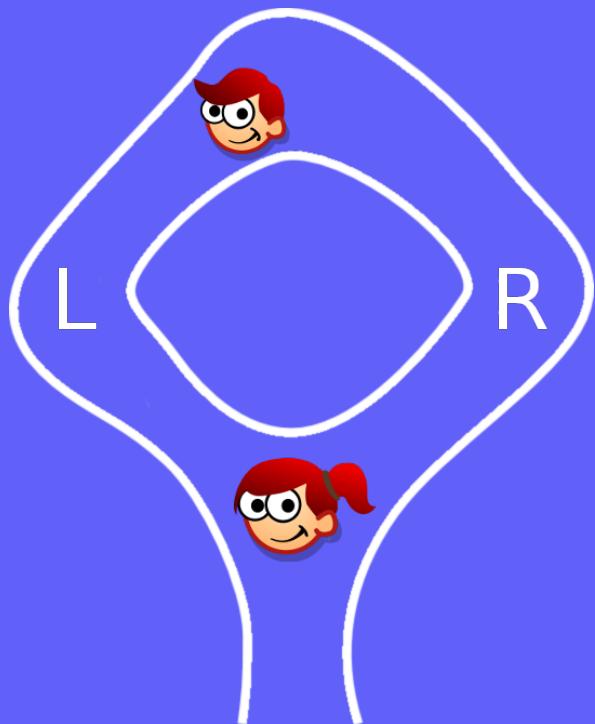


Strategy:

- ① Alice hides while Bob chooses to go Left (L) or Right (R)
- ② Alice randomly asks Bob to exit on L or R
- ③ If Bob is on the wrong side he uses the secret path or otherwise returns

# Zero knowledge proofs

*Bob knows a secret path, and wants to prove it without revealing it*



Strategy:

- ① Alice hides while Bob chooses to go Left (L) or Right (R)
- ② Alice randomly asks Bob to exit on L or R
- ③ If Bob is on the wrong side he uses the secret path or otherwise returns
- ④ Repeat steps 1 to 3 many times

# Mathematical digression – Graphs

## Definitions

- ① Let  $G_1 = (V_1, E_1)$  and  $G_2 = (V_2, E_2)$  be two simple graphs. Then we say that  $G_1$  and  $G_2$  are *isomorphic* if there exists a bijective function  $\varphi: V_1 \rightarrow V_2$  such that the induced map

$$\varphi_*: E_1 \rightarrow E_2, \quad (a, b) \mapsto (\varphi(a), \varphi(b))$$

is bijective. Such a function  $\varphi$  is called a *graph isomorphism*.

- ② A *Hamilton circuit* in a graph  $G$  is a simple circuit that passes through every vertex of  $G$  exactly once.

# Complexity digression – Graphs

Hard problems related to graph theory:

- Graph isomorphism:
  - No known polynomial time algorithm
  - Not proven to be  $\mathcal{NP}$ -complete
  - Best known algorithm has exponential complexity
- Finding a Hamiltonian circuit:
  - Proven to be  $\mathcal{NP}$ -complete
  - Best known algorithm has exponential complexity

# Zero knowledge proofs – Authentication

Initial setup:



- A graph  $G$
- A Hamiltonian circuit in  $G$
- Bob's graph  $G$



# Zero knowledge proofs – Authentication

Initial setup:



- A graph  $G$
- Bob's graph  $G$
- A Hamiltonian circuit in  $G$



Process:

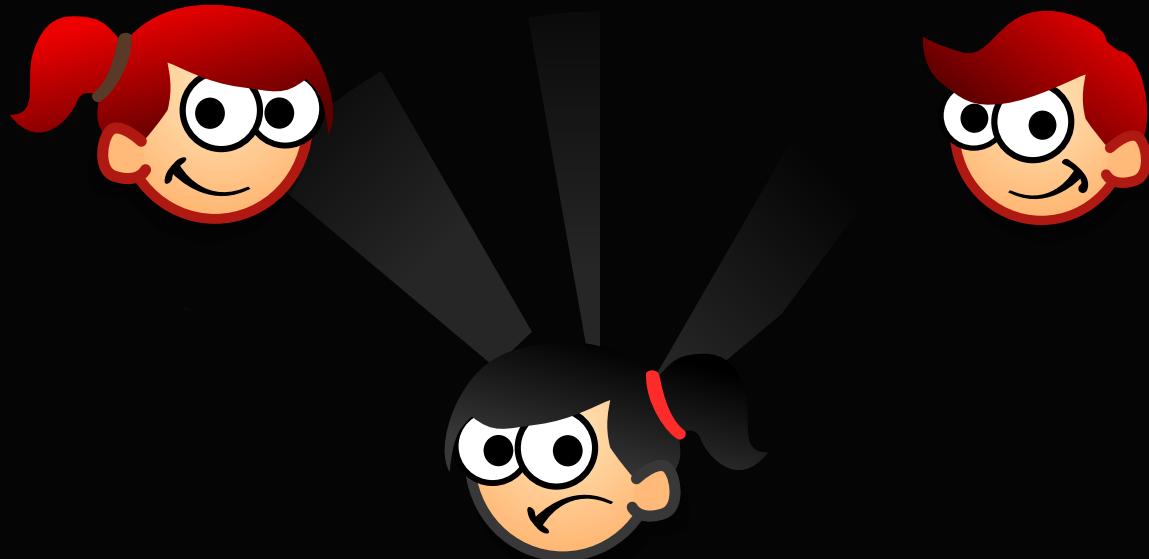
- ① Bob generates  $H$ , a graph isomorphic to  $G$
- ② Bob commits  $H$
- ③ Alice randomly asks for either the isomorphism or a Hamiltonian circuit in  $H$
- ④ Bob either shows the isomorphism or translates the Hamiltonian circuit in  $G$  onto  $H$  and shows it

# Zero knowledge proofs

Regarding the process and setup:

- Is Bob revealing any sensitive information?
- Why does Bob commit  $H$ ? 不能再換  $H$  了。
- Why is Alice randomly asking for  $H$  or a Hamiltonian circuit?
- Can Bob or Alice cheat?
- How many times should the process be repeated for Bob to prove that he really knows a Hamiltonian circuit in  $G$ ?





Thank you!

## References I

- 1.12 <https://www.xkcd.com/538/>
- 1.28 Simon Singh, *The Code Book – How to make it, break it, hack it, crack it?*
- 1.42 <https://cdn.globalauctionplatform.com/7187abcf-14de-4d26-9a48-a48e012a3bd3/1f194fa9-87f4-45cd-b6db-a48e012de5c7/original.jpg>