La fabuleuse histoire des codes secrets

Prof. Claude CRÉPEAU

McGill

INTRIQ

UTA Chambly, 1981, boul. de Périgny, Chambly, Qc J3L 4C3 • • • 27 septembre 2018

Cryptographie

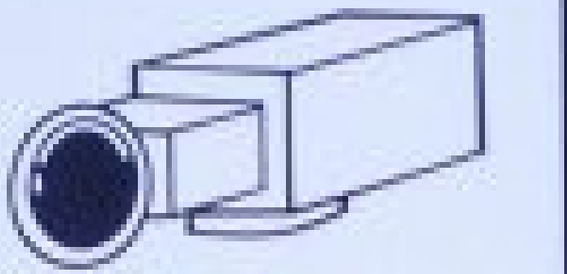
Combat millénaire entre

FAISEURS DE CODES (cryptographes) **BIEN**

BRISEURS DE CODES (cryptanalystes) **MAL**

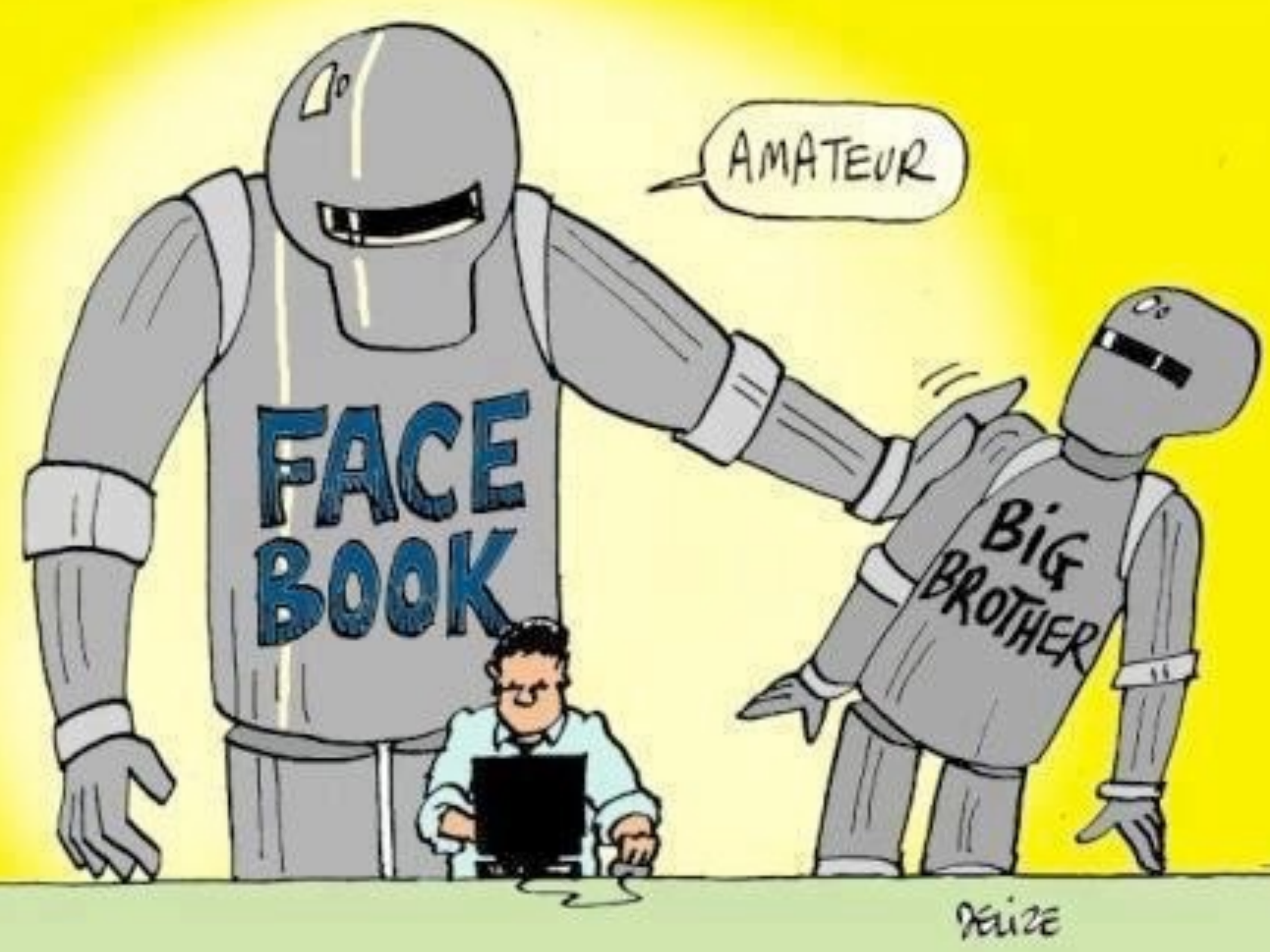
Ajuntament de Barcelona

Zona vigilada
en un radi de 500 m



Pl. George Orwell

PLAÇA
DE
GEORGE ORWELL


AMATEUR
FACE BOOK
BIG BROTHER
DELIZE

Mark Zuckerberg says Facebook made mistakes on Cambridge Analytica

'We have a responsibility to protect your data,' CEO says in statement

The Associated Press ·
Posted: Mar 21, 2018 4:01 PM ET | Last Updated: an hour ago

Facebook founder and CEO Mark Zuckerberg, seen here in an April 2017 photo, made his first public comments Wednesday amid a scandal over a political analytics firm getting the data of millions of Facebook users. (Stephen Lam/Reuters)

Breaking more than four days of silence, Facebook CEO Mark Zuckerberg admitted mistakes and outlined steps to protect user data in light of a privacy scandal involving a Trump-connected data-mining firm.

[Suggestion pour vous] L'Oiseau de feu avec l'Orchestre Métropolitain

"Place des Arts" <infoflash@placedesarts.com>

21 mars 2018 19:01

À: [redacted]

Profitez d'offres spéciales pour ce concert : achetez un billet et obtenez le second à moitié prix ou obtenez 2 billets pour 40$ au balcon (34 ans et moins)!
Pas d'images? Version Web

PLACE DES ARTS

Bonjour [redacted]

L'Orchestre Métropolitain vous invite à une soirée envoûtante lors de laquelle deux oeuvres mythiques de **Stravinski** côtoieront celles de **Respighi** et de **Pierre Jalbert,** interprétées par la mezzo-soprano **Sasha Cooke**. Selon ce que nous avons pu observer dans votre compte Place des Arts, nous croyons que vous apprécierez ce concert.

Bonjour [redacted]

L'Orchestre Métropolitain vous invite à une soirée envoûtante lors de laquelle deux oeuvres mythiques de **Stravinski** côtoieront celles de **Respighi** et de **Pierre Jalbert,** interprétées par la mezzo-soprano **Sasha Cooke**. Selon ce que nous avons pu observer dans votre compte Place des Arts, nous croyons que vous apprécierez ce concert.

Bonjour [redacted]

L'Orchestre Métropolitain vous invite à une soirée envoûtante lors de laquelle deux oeuvres mythiques de **Stravinski** côtoieront celles de **Respighi** et de **Pierre Jalbert,** interprétées par la mezzo-soprano **Sasha Cooke**. Selon ce que nous avons pu observer dans votre compte Place des Arts, nous croyons que vous apprécierez ce concert.

Cryptographie

Combat millénaire entre

FAISEURS DE CODES

BRISEURS DE CODES

BIEN

MAL

Cryptographie

Combat millénaire entre

FAISEURS DE CODES **BRISEURS DE CODES**

MAL **BIEN**

"BENEDICT CUMBERBATCH IS OUTSTANDING"
RADIO TIMES

"THE BEST BRITISH FILM OF THE YEAR"
★★★★★
THE INDEPENDENT

"AN INSTANT CLASSIC"
★★★★★
GLAMOUR

"A SUPERB THRILLER"
★★★★
EMPIRE

★★★★ TIME OUT
★★★★ THE TIMES

THE IMITATION GAME

BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY

12A MODERATE SEX REFERENCES

BASED ON THE INCREDIBLE TRUE STORY

BLACK BEAR PICTURES PRESENTS IN ASSOCIATION WITH FILMNATION ENTERTAINMENT A BLACK BEAR PICTURES PRODUCTION A BRISTOL AUTOMOTIVE PRODUCTION "THE IMITATION GAME" BENEDICT CUMBERBATCH KEIRA KNIGHTLEY MATTHEW GOODE RORY KINNEAR WITH CHARLES DANCE AND MARK STRONG CASTING NINA GOLD HMDG IVANA PRIMORAC DESIGNER SAMMY SHEDDON DIFFER PRODUCTION DESIGNER MARIA DJURKOVIC MUSIC ALEXANDRE DESPLAT EDITOR WILLIAM GOLDENBERG, A.C.E. DIRECTOR OF PHOTOGRAPHY OSCAR FAURA PRODUCER PETER HESLOP EXECUTIVE PRODUCER GRAHAM MOORE PRODUCED BY NORA GROSSMAN p.g.a. IDO OSTROWSKY p.g.a. TEDDY SCHWARZMAN p.g.a. WRITTEN BY GRAHAM MOORE DIRECTED BY MORTEN TYLDUM

FILMNATION STUDIOCANAL

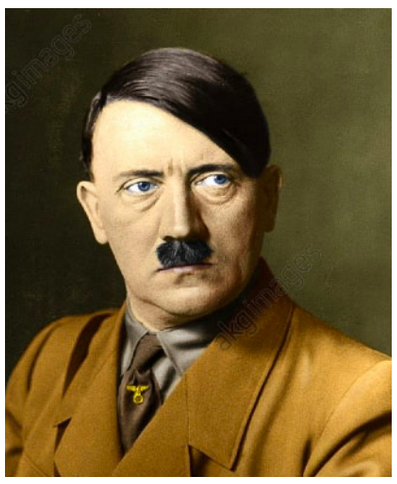
/ImitationGameUK

ENIGMA

Cryptographie

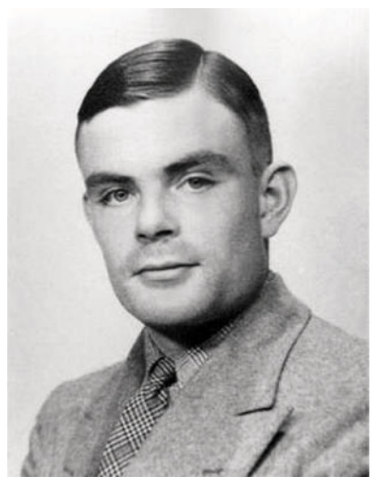
Combat millénaire entre

FAISEURS DE CODES



?

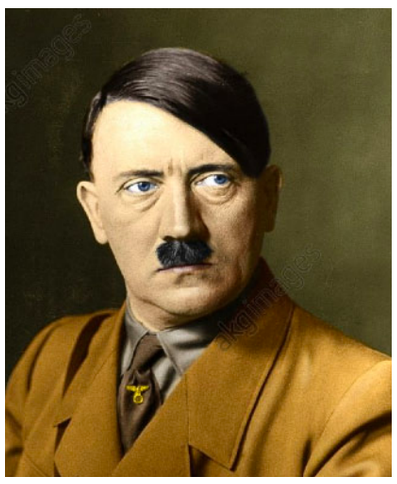
BRISEURS DE CODES



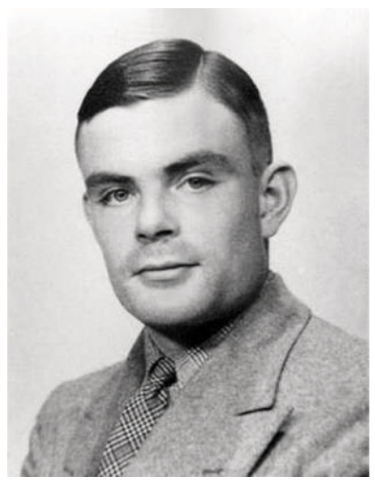
Cryptographie

Combat millénaire entre

FAISEURS DE CODES



BRISEURS DE CODES



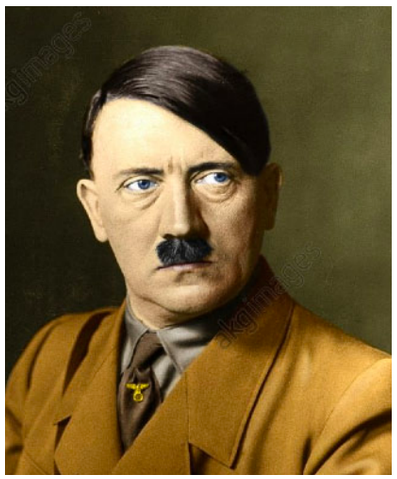
Cryptographie

Combat millénaire entre

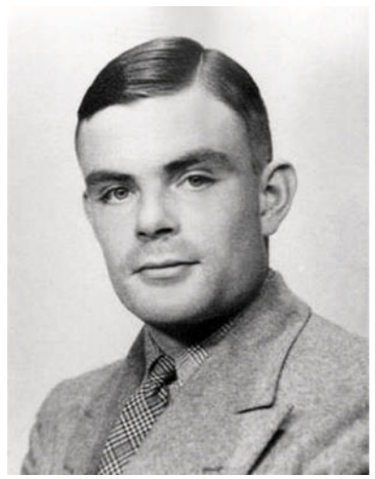
UTILISATEURS

FAISEURS DE CODES

BRISEURS DE CODES



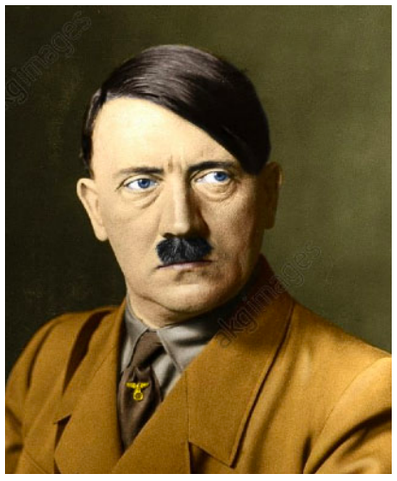
?



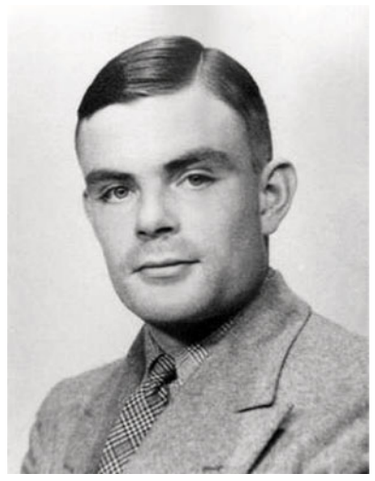
Cryptographie

Combat millénaire entre

UTILISATEURS DE CODES



BRISEURS DE CODES



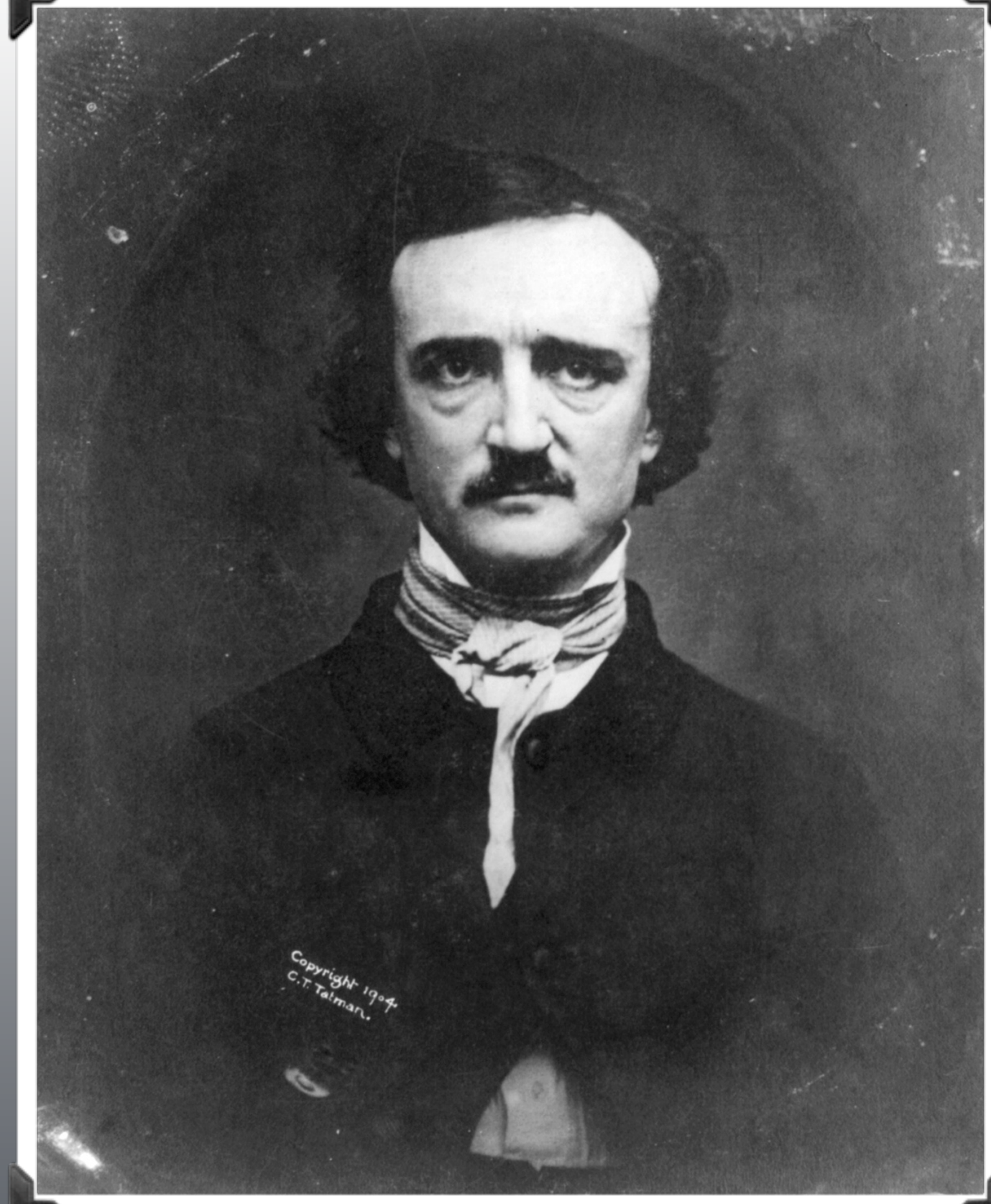
Qui gagnera ?

FAISEURS DE CODES

ou

BRISEURS DE CODES

?



Edgar Allan Poe (1809–1849)

Qui gagnera ?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

Edgar Allan Poe

(Graham's Lady's and Gentleman's Magazine, juillet 1841)

Qui gagnera ?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

« On peut affirmer rondement que l'ingéniosité humaine ne peut concocter de chiffre que l'ingéniosité humaine ne puisse résoudre »

Edgar Allan Poe

(Graham's Lady's and Gentleman's Magazine, juillet 1841)

Qui gagnera ?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

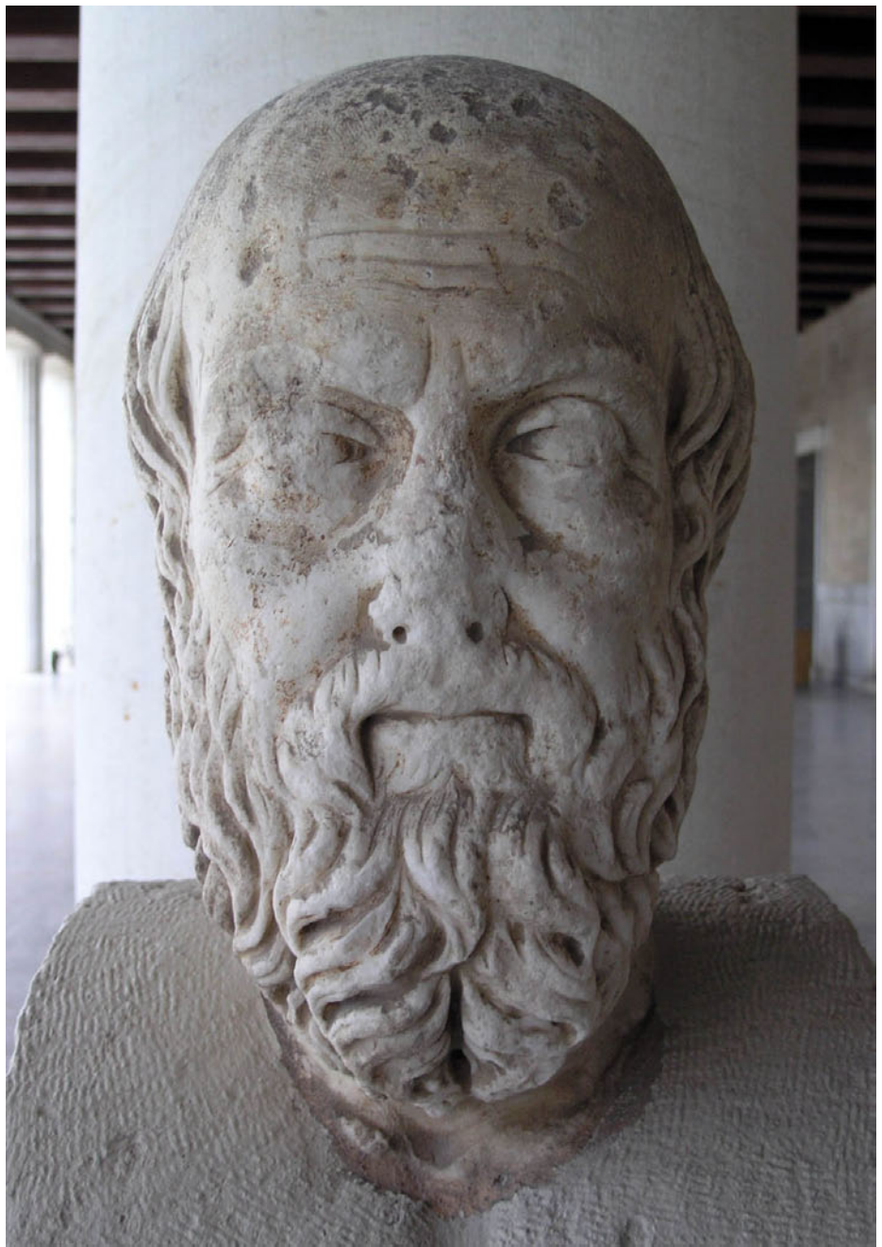
« On peut affirmer rondement que l'ingéniosité humaine ne peut concocter de chiffre que l'ingéniosité humaine ne puisse résoudre »

Avait-il raison ?

Antiquité

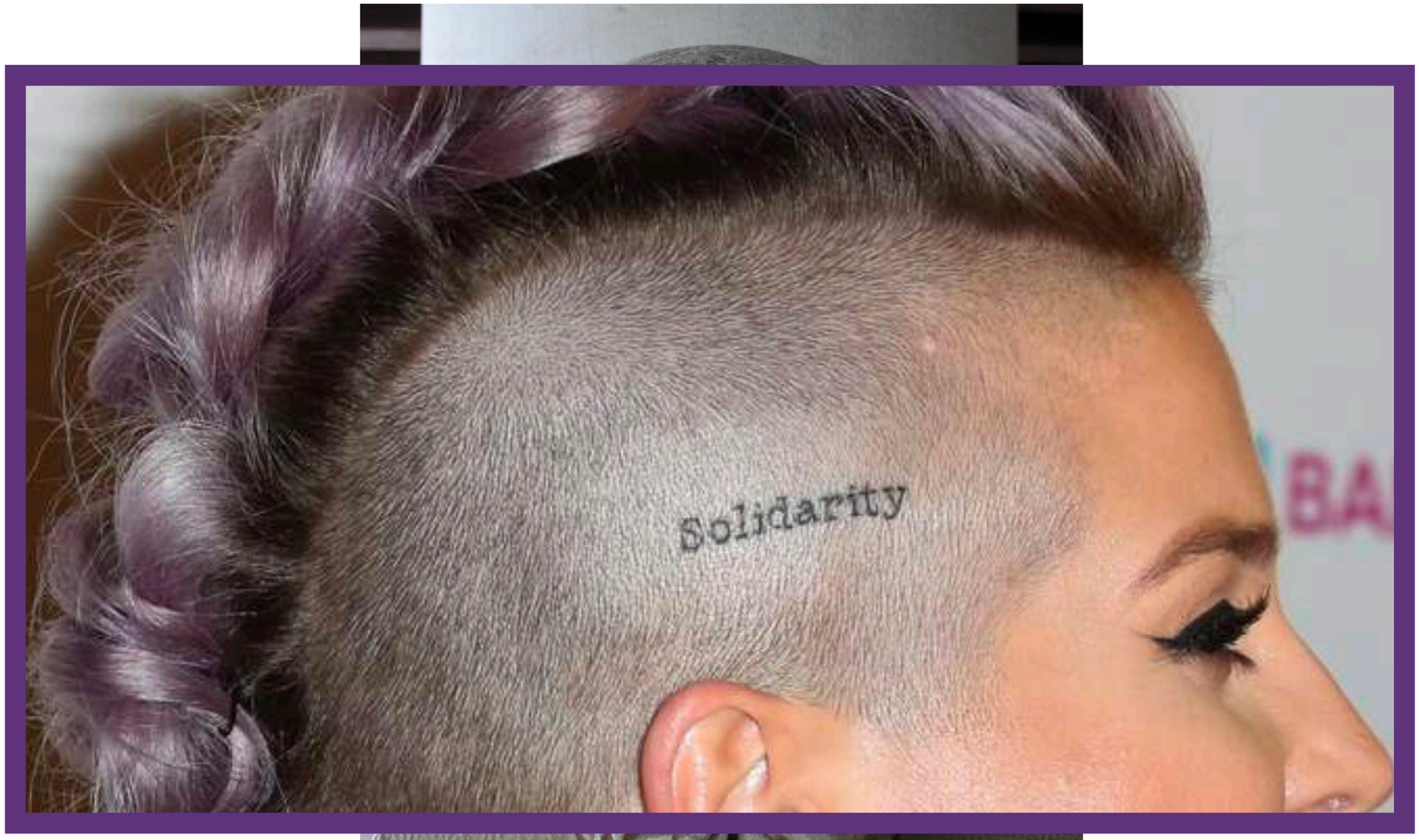
Antiquité

Hérodote et l'esclave rasé
(5e siècle avant J.-C. ou avant?)



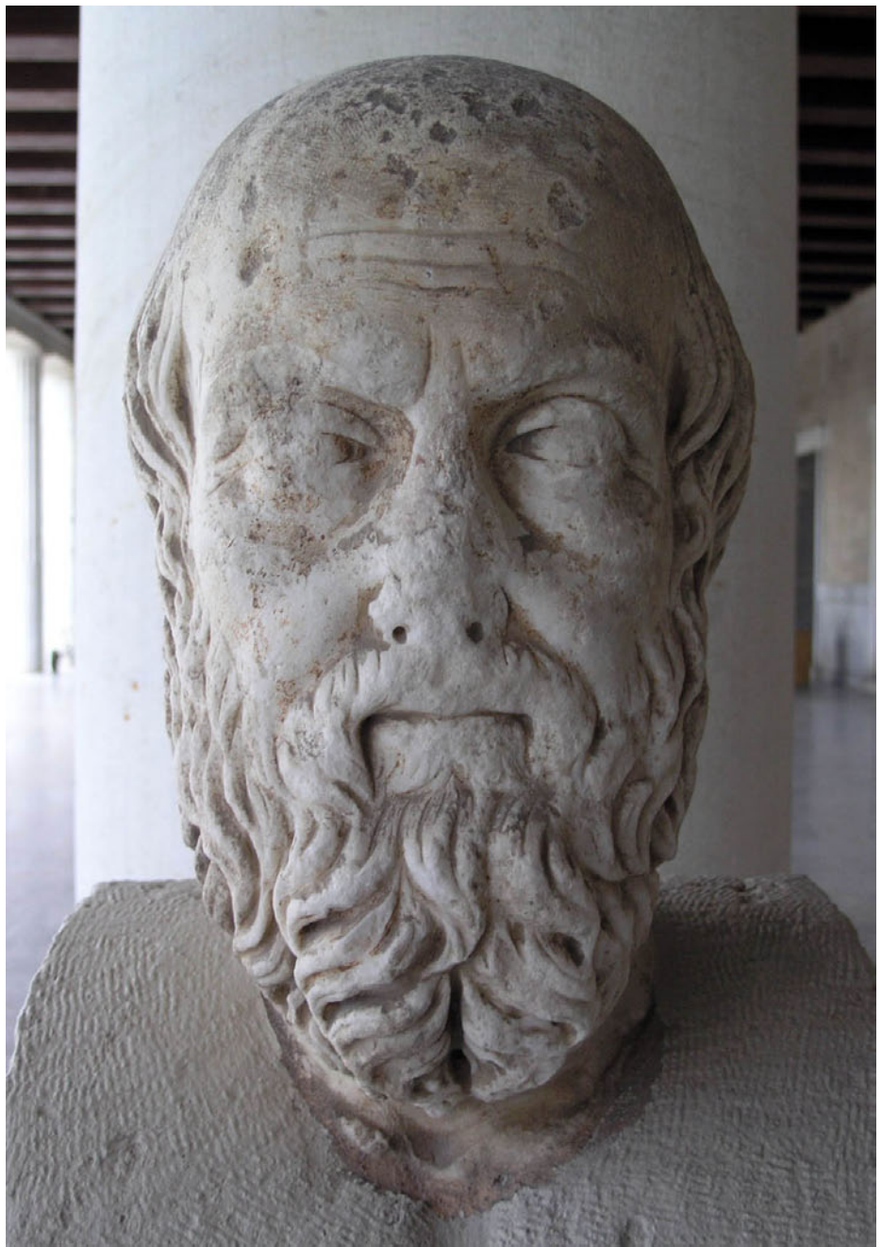
Antiquité

Hérodote et l'esclave rasé
(5e siècle avant J.-C. ou avant?)



Antiquité

Hérodote et l'esclave rasé
(5e siècle avant J.-C. ou avant?)



Antiquité

Hérodote et l'esclave rasé
(5e siècle avant J.-C. ou avant?)

C'était de la stéganographie…

Antiquité

Hérodote et l'esclave rasé
(5e siècle avant J.-C. ou avant?)

C'était de la stéganographie…
et la « vraie » cryptographie alors ?

Antiquité

Hérodote et l'esclave rasé
(5e siècle avant J.-C. ou avant?)

La scytale de Lysandre de Sparte
(404 avant J.-C. ou avant?)

Antiquité

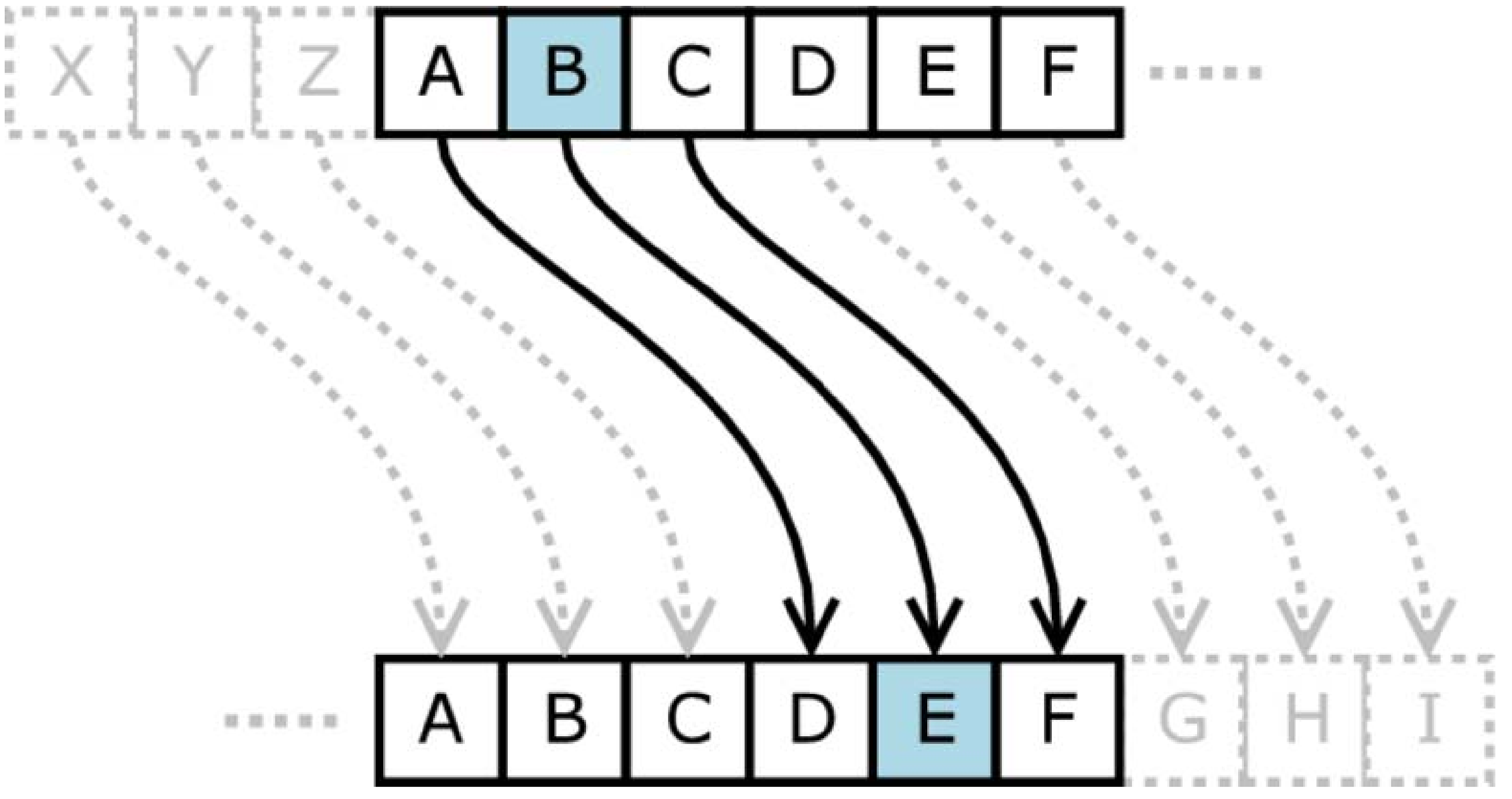
Hérodote et l'esclave rasé
(5e siècle avant J.-C. ou avant?)

La scytale de Lysandre de Sparte
(404 avant J.-C. ou avant?)

Le chiffre de Jules César
(1er siècle avant J.-C.)

Antiquité

Hérodote et l'esclave rasé
(5e siècle avant J.-C. ou avant?)



Antiquité

Hérodote et l'esclave rasé
(5e siècle avant J.-C. ou avant?)

La scytale de Lysandre de Sparte
(404 avant J.-C. ou avant?)

Le chiffre de Jules César
(1er siècle avant J.-C.)

Seulement des militaires ?

Antiquité

Hérodote et l'esclave rasé
(5e siècle avant J.-C. ou avant?)

La scytale de Lysandre de Sparte
(404 avant J.-C. ou avant?)

Le chiffre de Jules César
(1er siècle avant J.-C.)

Le Kāmasūtra de Vātsyāyana
45e yoga (sur 64) : mlecchita-vikalpā

Vocabulaire

Vocabulaire

Un code travaille au niveau du mot

Vocabulaire

Un code travaille au niveau du mot

attaquez → LAPIN

Vocabulaire

Un code travaille au niveau du mot

attaquez → LAPIN

aube → MOUTARDE

Vocabulaire

Un code travaille au niveau du mot

attaquez → LAPIN

aube → MOUTARDE

attaquez à l'aube →

Vocabulaire

Un code travaille au niveau du mot

attaquez → LAPIN

aube → MOUTARDE

attaquez à l'aube →
LAPIN À LA MOUTARDE

Vocabulaire

Un code travaille au niveau du mot

Un chiffre travaille au niveau de la lettre (ou du bit)

La fabuleuse histoire des codes secrets

Un chiffre travaille au niveau de la lettre (ou du bit)

La fabuleuse histoire des chiffres secrets

Un chiffre travaille au niveau de la lettre (ou du bit)

texte clair + *clef secrète*

$\Rightarrow$ TEXTE CHIFFRÉ

La fabuleuse histoire des chiffres secrets

Un chiffre travaille au niveau de la lettre (ou du bit)

Principe de Kerckhoffs (1883)

La fabuleuse histoire des chiffres secrets

Un chiffre travaille au niveau de la lettre (ou du bit)

Principe de Kerckhoffs (1883)

Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs von Nieuwenhoff

La fabuleuse histoire des chi secrets

Un chiffre t u niveau de la lettre (ou du

Principe de Kerckhoffs (1883)

Jean-Guillaume-Hubert-Victor-François-Alexandre-Auguste Kerckhoffs von Nieuwenhoff

La fabuleuse histoire des chiffres secrets

Un chiffre t[illegible] niveau de la lettre (ou du

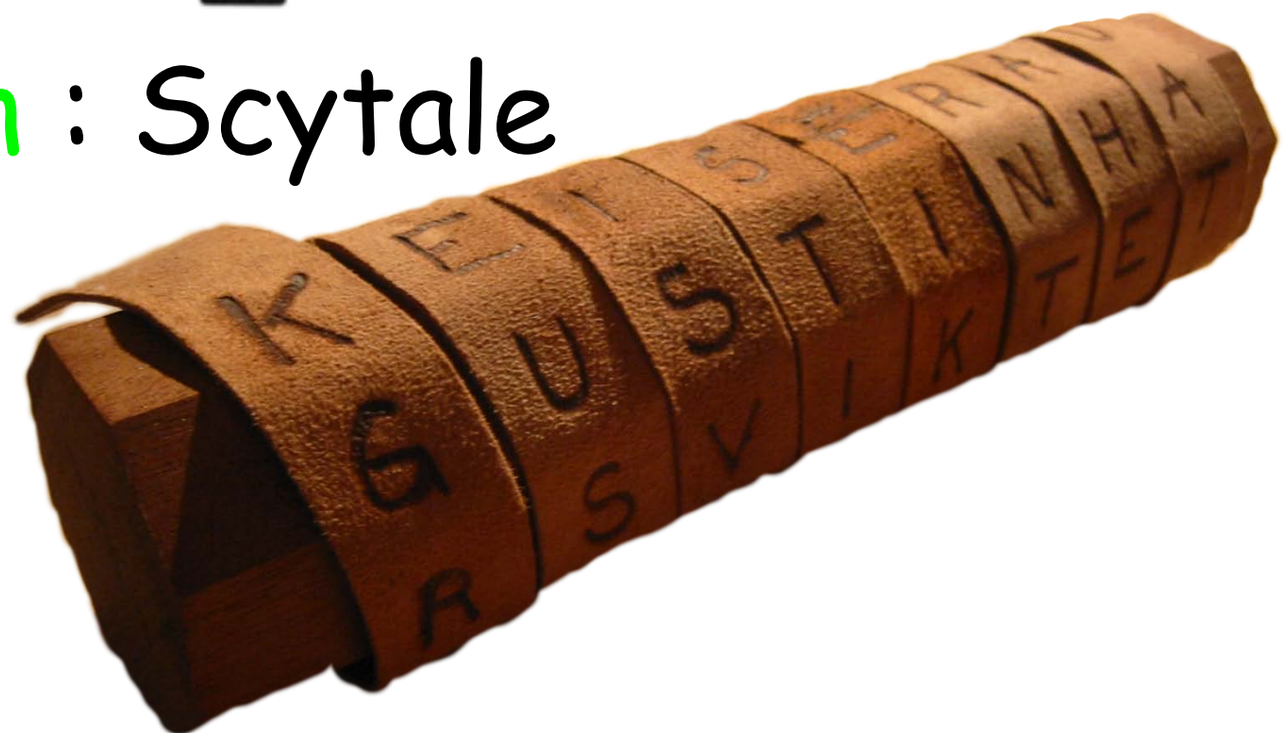
Principe de Kerckhoffs (1883)

« La sécurité du chiffrement ne doit reposer que sur le secret de la clef »

La fabuleuse histoire des chi secrets

Un chiffre t u niveau de la lettre (ou du

Transposition : Scytale



La fabuleuse histoire des chi secrets

Un chiffre t u niveau de la lettre (ou du

Transposition : Scytale

Substitution : César

Substitution
(chiffre de César)

Substitution
(chiffre de César)

abcdefghijklmnopqrstuvwxyz

Substitution
(chiffre de César)

abcdefghijklmnopqrstuvwxyz

DEFGHIJKLMNOPQRSTUVWXYZABC

Substitution
(chiffre de César)

abcdefghijklmnopqrstuvwxyz

DEFGHIJKLMNOPQRSTUVWXYZABC

bonjour

Substitution
(chiffre de César)

abcdefghijklmnopqrstuvwxyz

DEFGHIJKLMNOPQRSTUVWXYZABC

bonjour

E

Substitution
(chiffre de César)

abcdefghijklmnopqrstuvwxyz

DEFGHIJKLMNOPQRSTUVWXYZABC

bonjour

ER

Substitution
(chiffre de César)

abcdefghijklmnopqrstuvwxyz

DEFGHIJKLMNOPQRSTUVWXYZABC

bonjour

ERQ

Substitution
(chiffre de César)

abcdefghijklmnopqrstuvwxyz

DEFGHIJKLMNOPQRSTUVWXYZABC

bonjour

ERQMRXU

Substitution
(chiffre de César)

abcdefghijklmnopqrstuvwxyz

DEFGHIJKLMNOPQRSTUVWXYZABC

bonjour

ERQMRXU

Seulement 26 clefs possibles

Substitution mono-alphabétique

abcdefghijklmnopqrstuvwxyz

QWERTYUIOPASDFGHJKLZXCVBNM

Substitution mono-alphabétique

abcdefghijklmnopqrstuvwxyz

QWERTYUIOPASDFGHJKLZXCVBNM

bonjour

Substitution mono-alphabétique

abcdefghijklmnopqrstuvwxyz

QWERTYUIOPASDFGHJKLZXCVBNM

bonjour

W

Substitution mono-alphabétique

abcdefghijklmnopqrstuvwxyz

QWERTYUIOPASDFGHJKLZXCVBNM

bonjour

WG

Substitution mono-alphabétique

abcdefghijklmnopqrstuvwxyz

QWERTYUIOPASDFGHJKLZXCVBNM

bonjour

WGF

Substitution mono-alphabétique

abcdefghijklmnopqrstuvwxyz

QWERTYUIOPASDFGHJKLZXCVBNM

bonjour

WGFPGXK

Substitution mono-alphabétique

abcdefghijklmnopqrstuvwxyz

QWERTYUIOPASDFGHJKLZXCVBNM

bonjour

WGFPGXK

403291461126605635584000000 clefs !

Substitution mono-alphabétique

abcdefghijklmnopqrstuvwxyz

QWERTYUIOPASDFGHJKLZXCVBNM

bonjour

WGFPGXK

403291461126605635584000000 clefs !

Substitution mono-alphabétique

abcdefghijklmnopqrstuvwxyz

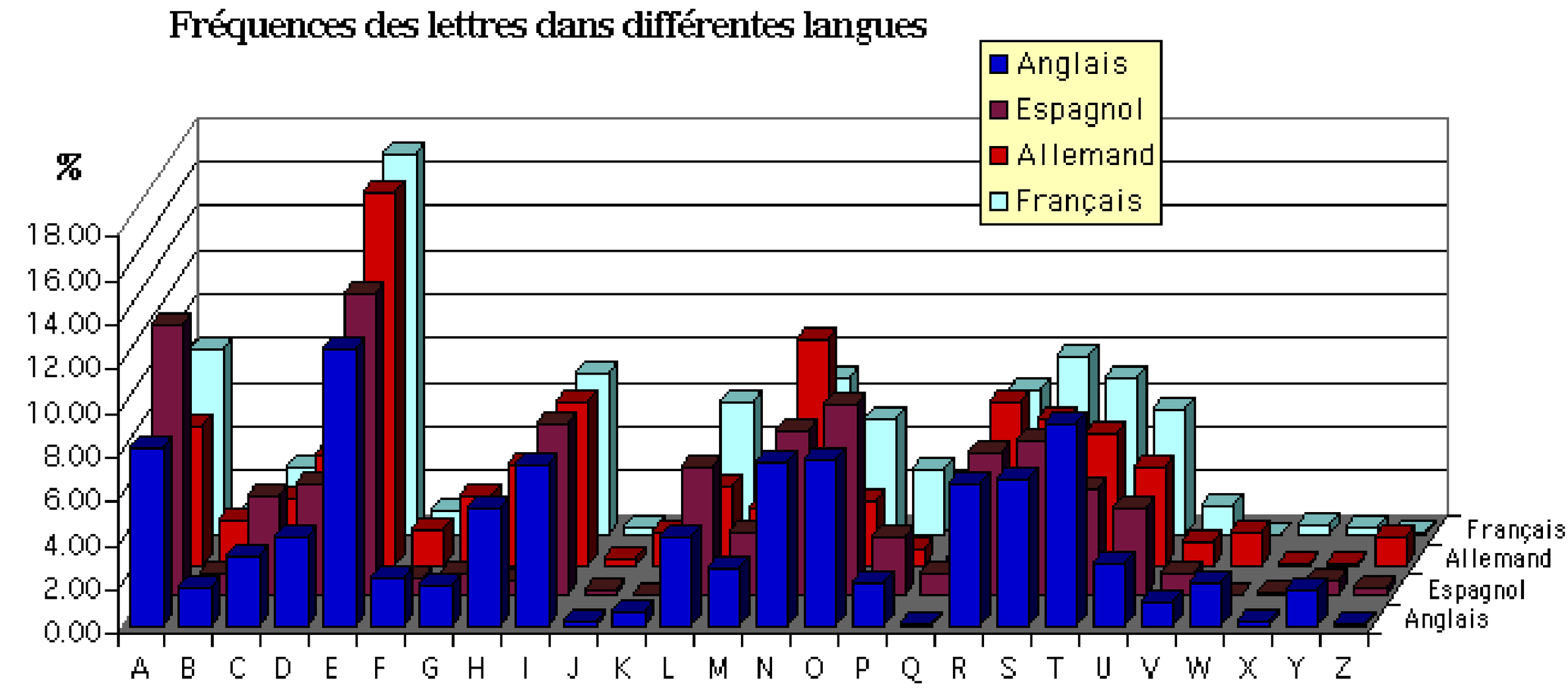
QWERTYUIOPASDFGHJKLZXCVBNM

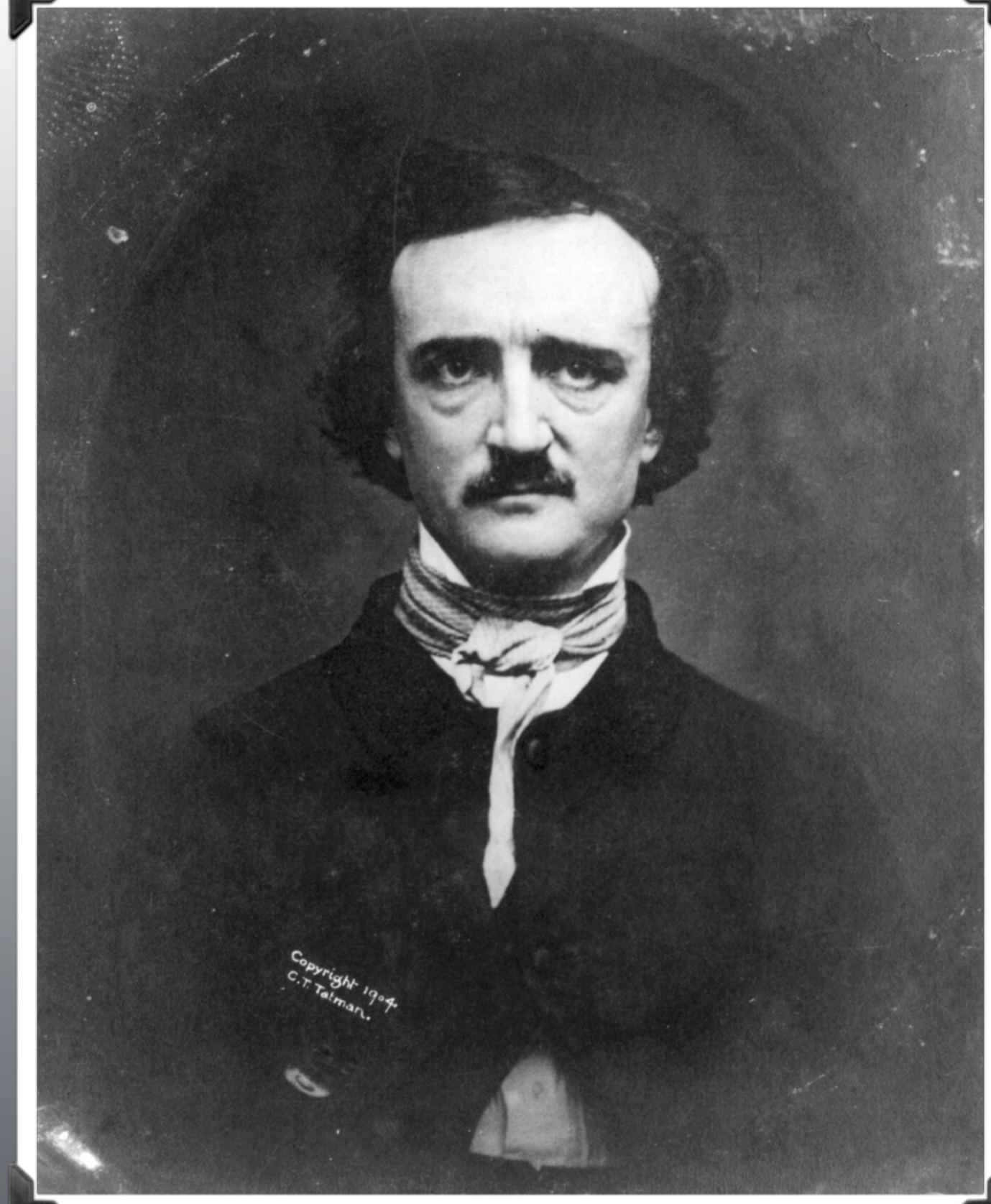
bonjour

WGFPGXK

403291461126605635584000000 clefs !

Analyse des fréquences





Edgar Allan Poe (1809–1849)

EDGAR ALLAN POE

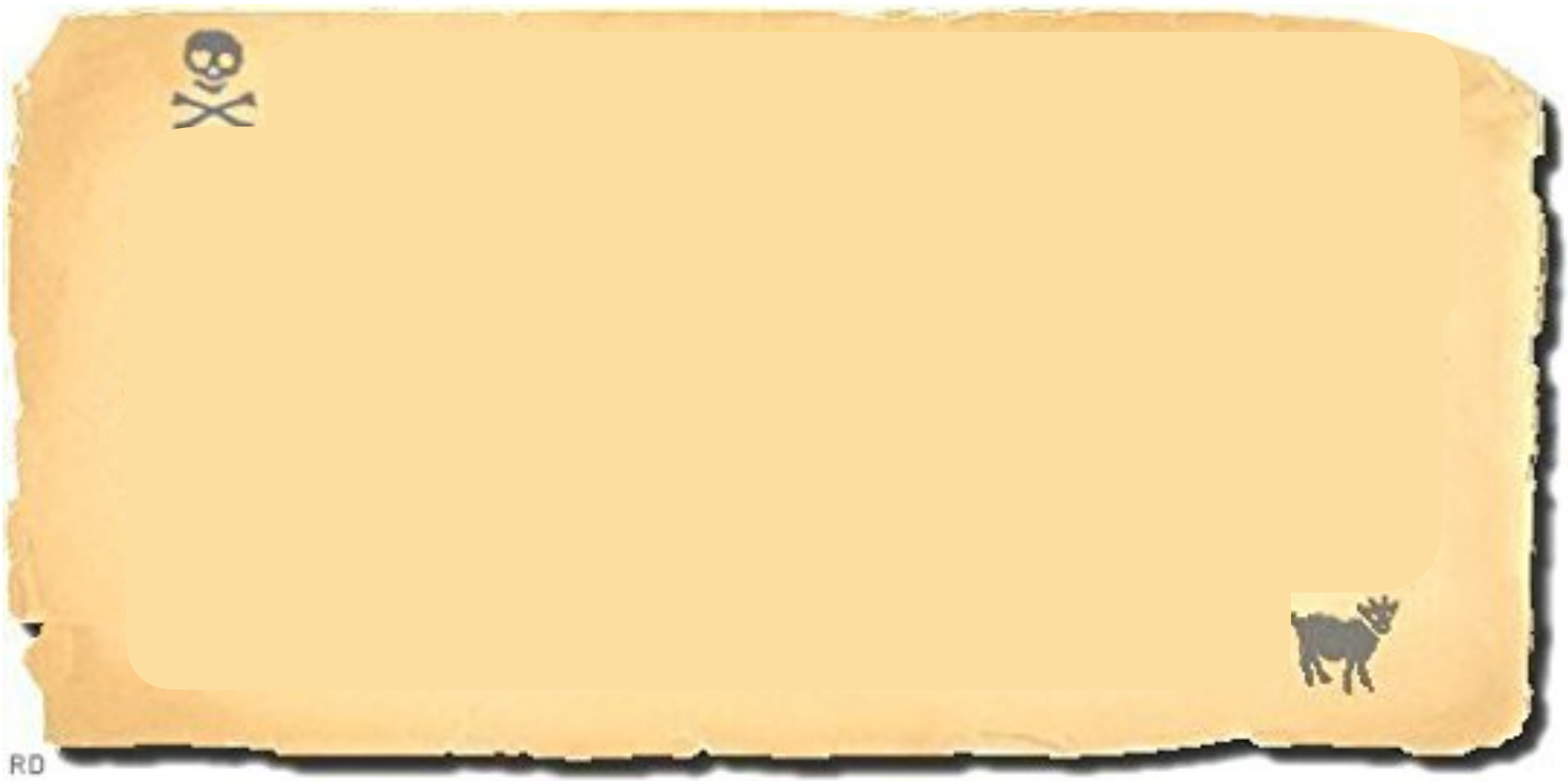
Le scarabée d'or

et autres histoires

Le Livre de Poche Jeunesse

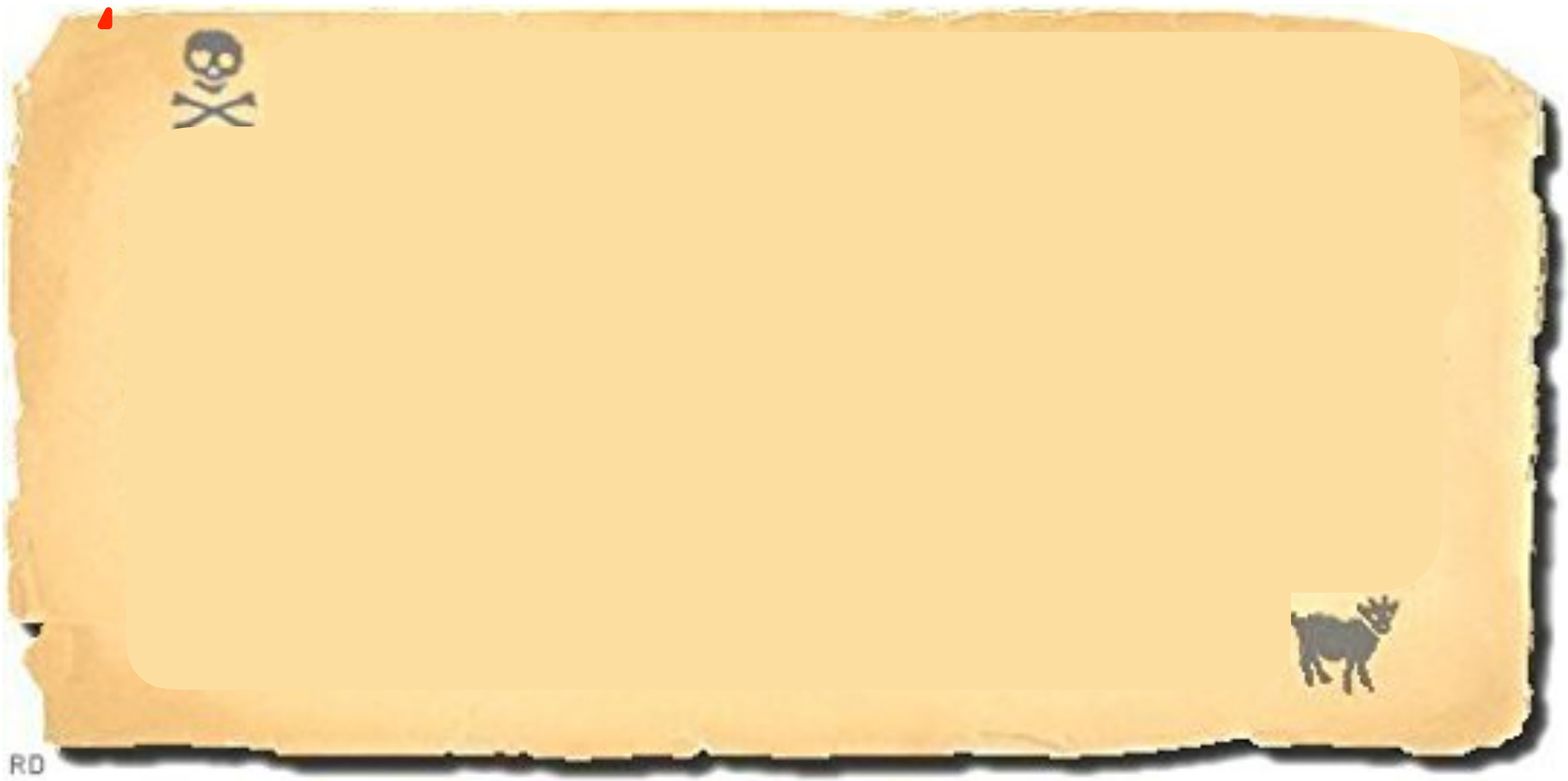
Le scarabée d'or

Edgar Allan Poe, juin 1843



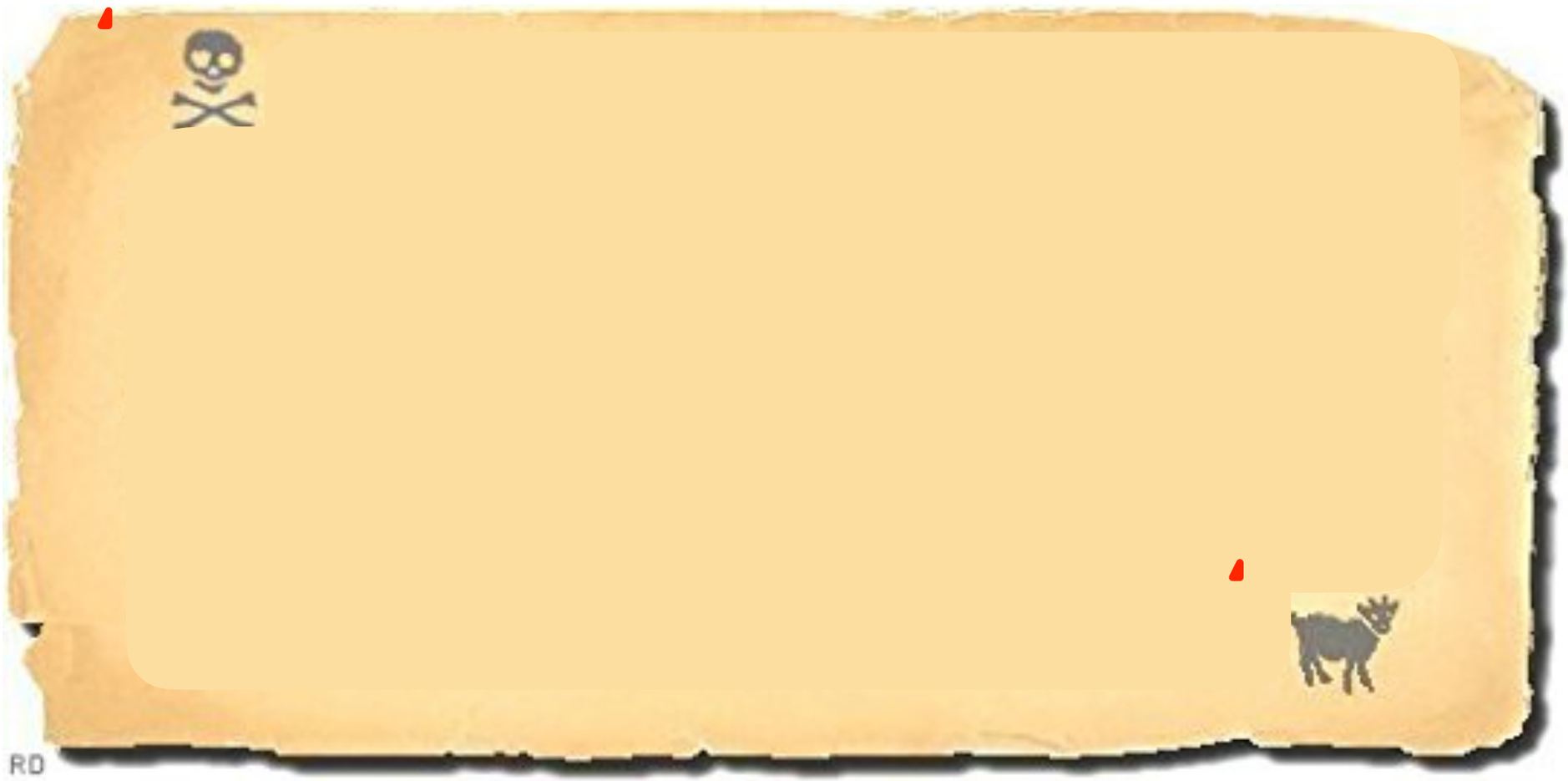
Le scarabée d'or

Edgar Allan Poe, juin 1843



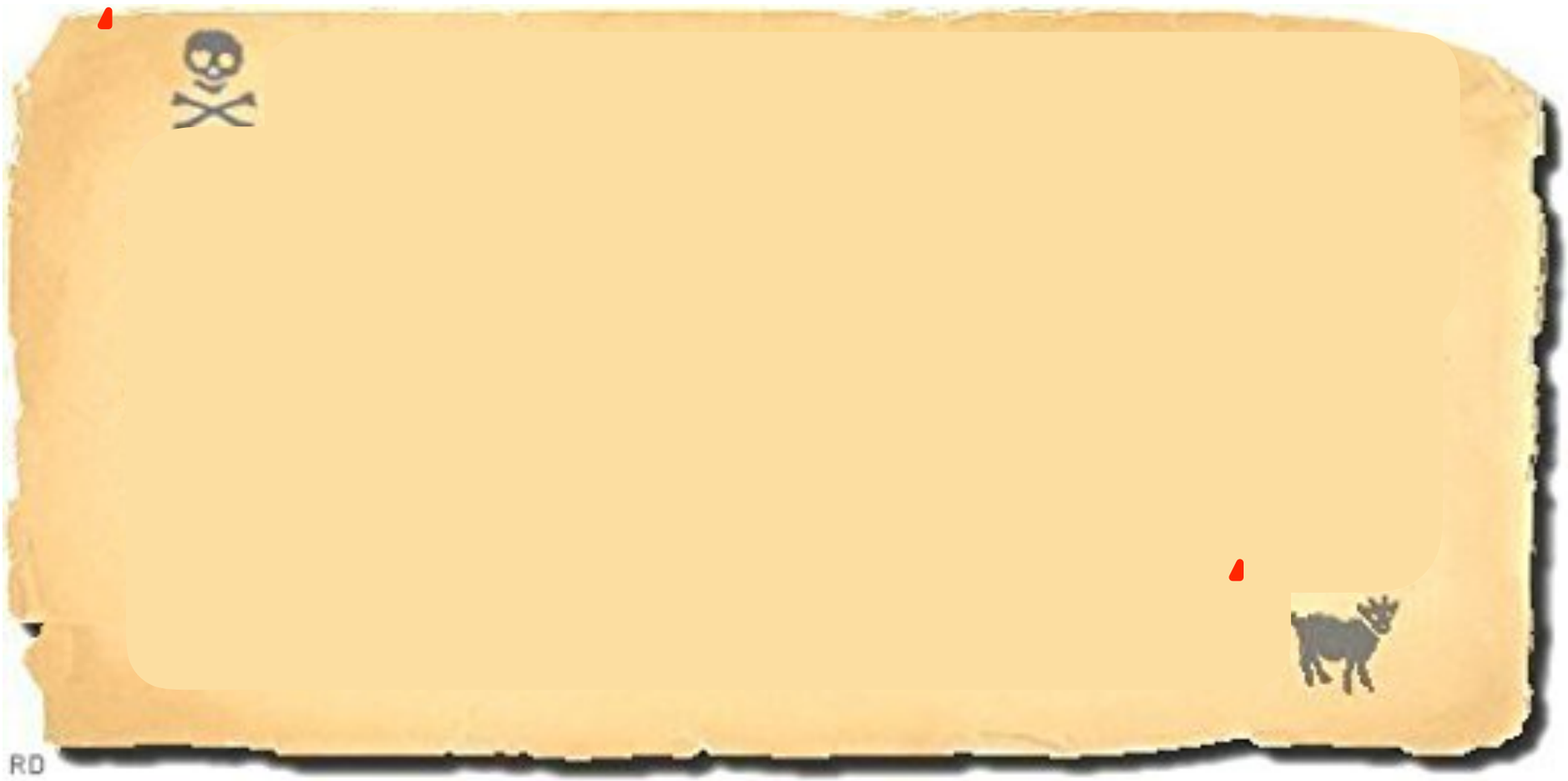
Le scarabée d'or

Edgar Allan Poe, juin 1843



Le scarabée d'or

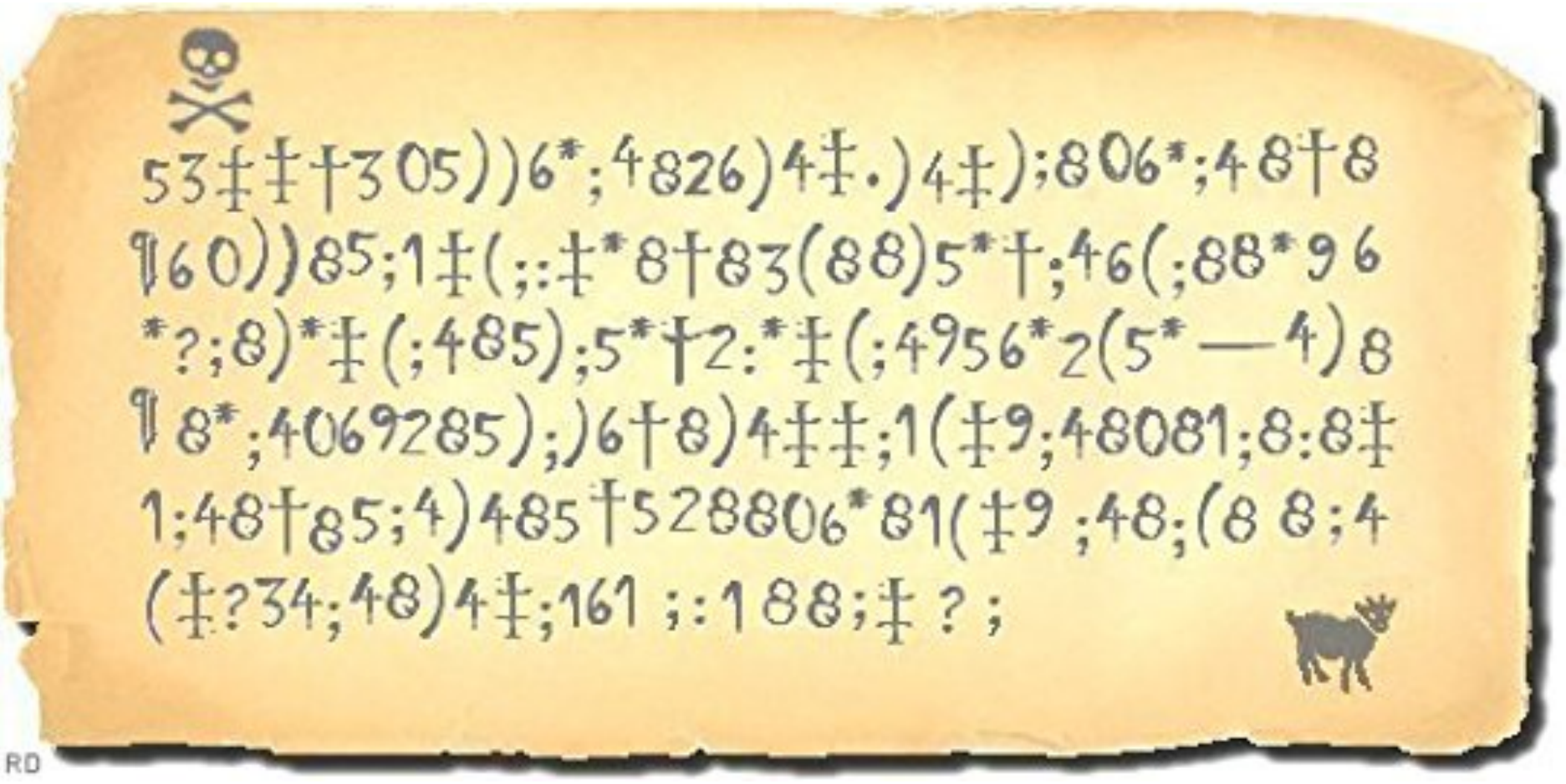
Edgar Allan Poe, juin 1843



Captain Kidd

Le scarabée d'or

Edgar Allan Poe, juin 1843



Captain Kidd

Le scarabée d'or

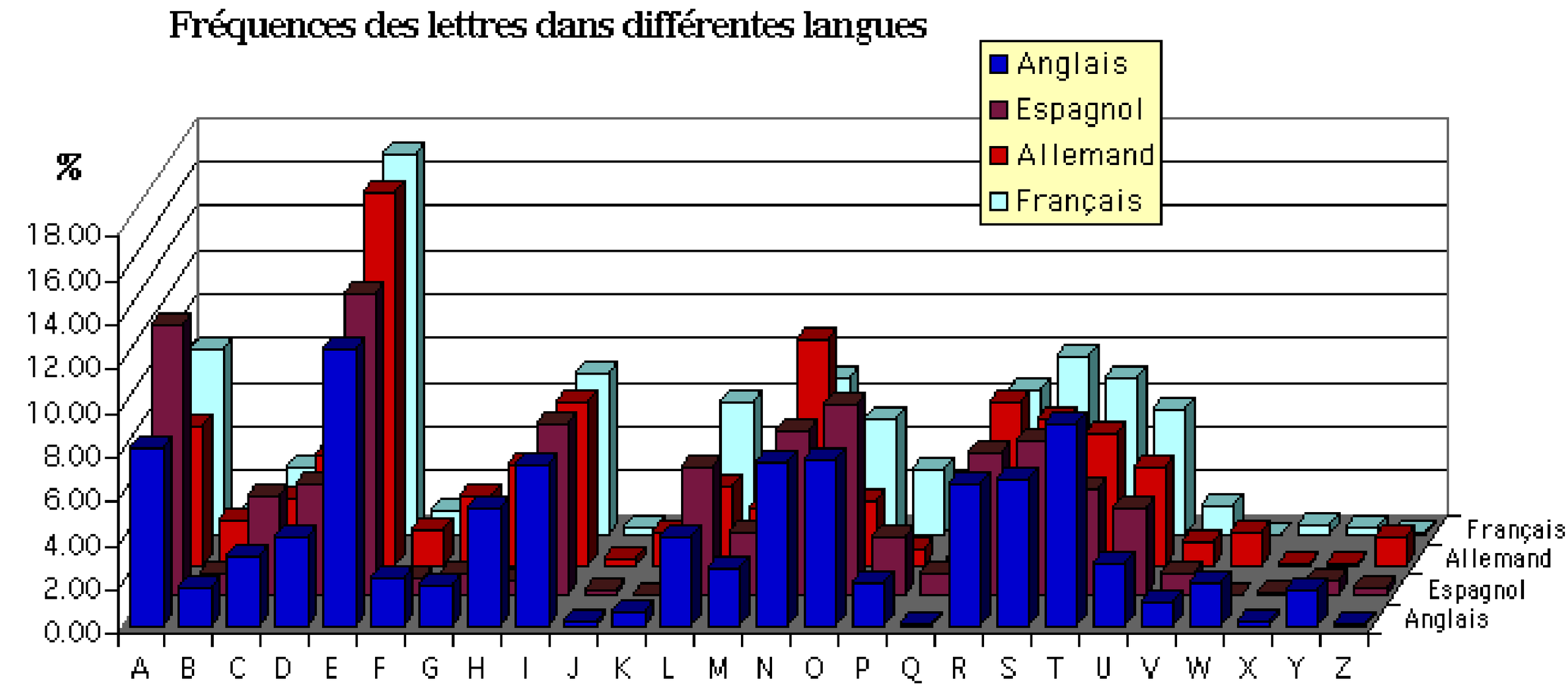
Edgar Allan Poe, juin 1843

```
53‡‡†305))6*;4826)4‡.)4‡);806*;48‡8
¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96
*?;8)*‡(;485);5*†2:*‡(;4956*2(5*—4)8
¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4
(‡?34;48)4‡;161;:188;‡?;
```

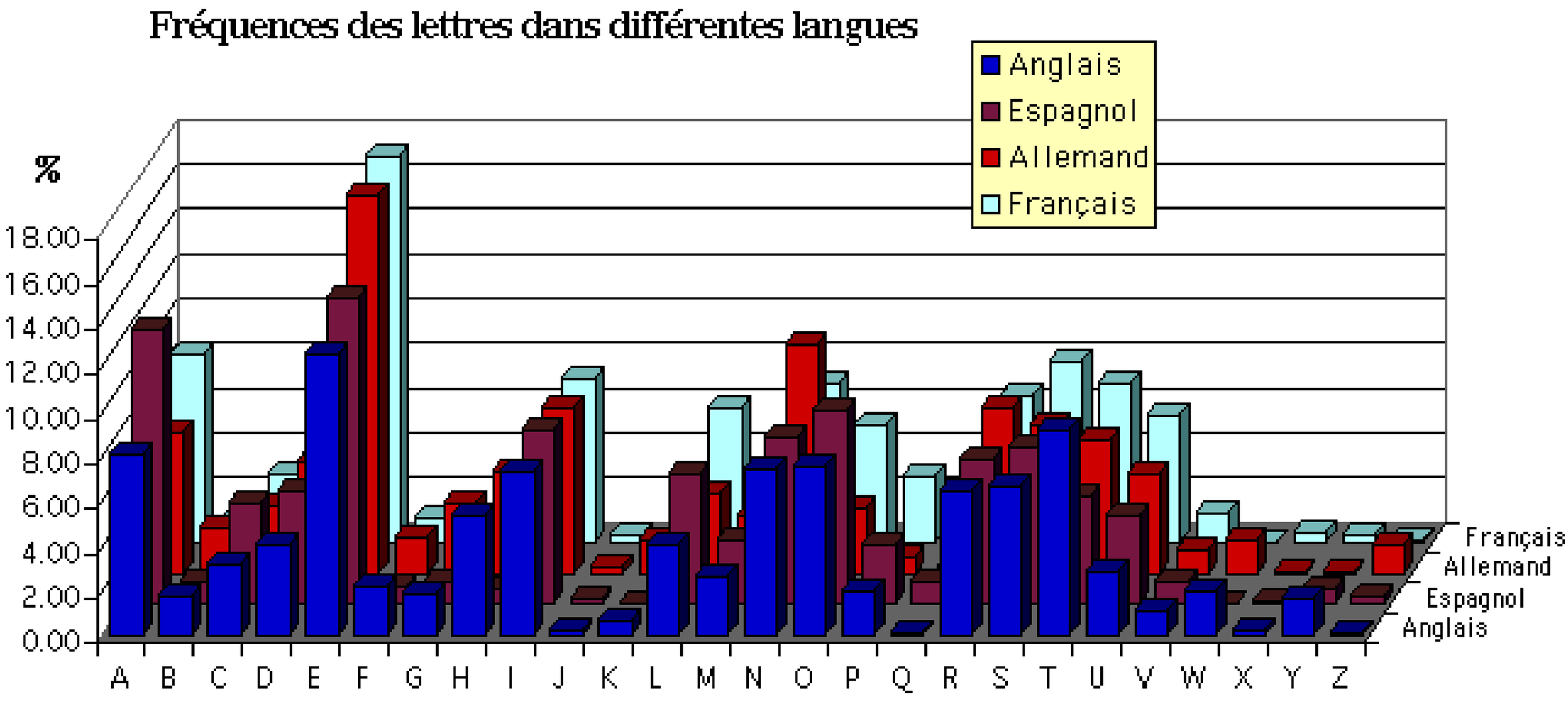
Of the character 8 there are 33

;	"	26
4	"	19
+)	"	16
*	"	13
5	"	12
6	"	11
! 1	"	8
0	"	6
9 2	"	5
: 3	"	4
?	"	3
'	"	2
- .	"	1

Analyse des fréquences

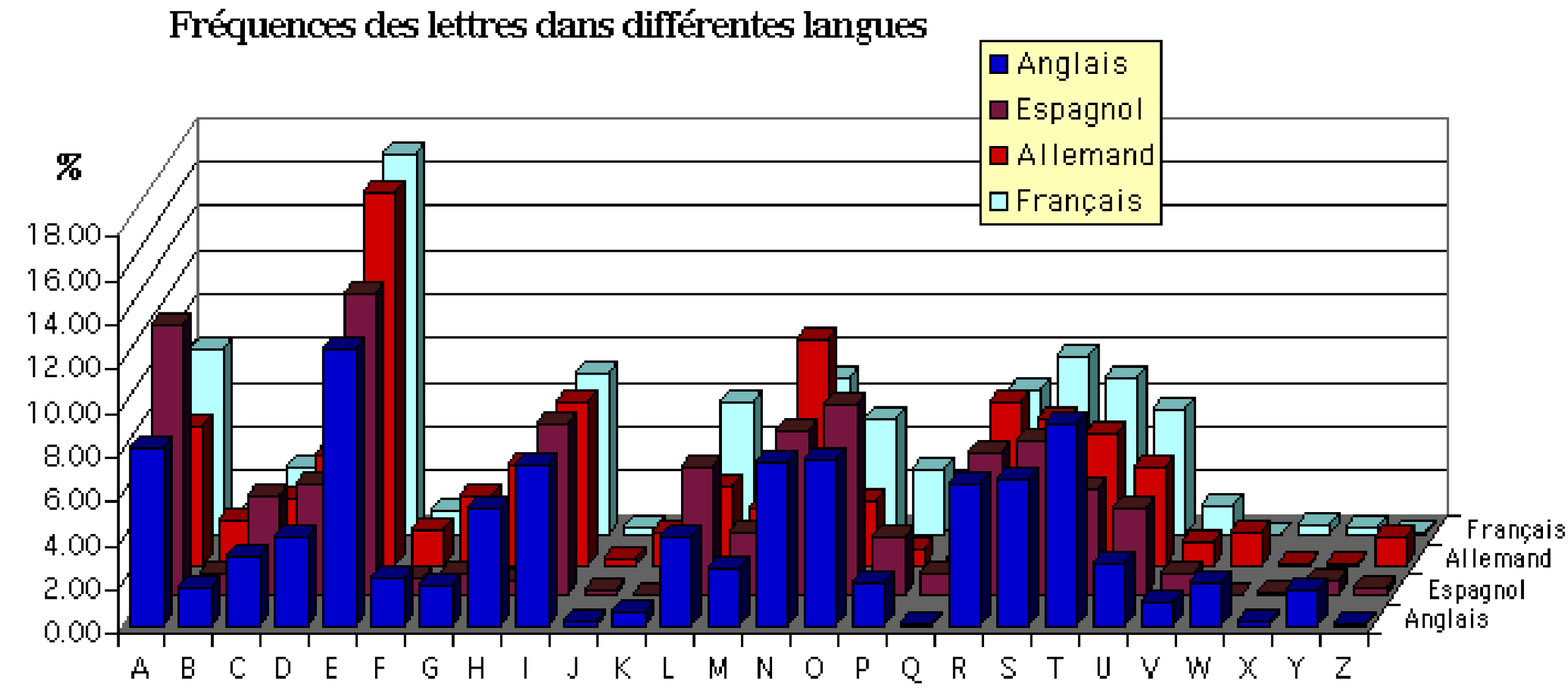


Analyse des fréquences



= Captain Kidd

Analyse des fréquences



= Captain Kidd ⇒ en anglais

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*;4826)4‡.)4‡);806*;48‡8
¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96
*?;8)*‡(;485);5*†2:*‡(;4956*2(5*—4)8
¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4
(‡?34;48)4‡;161;:188;‡?;
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*;4826)4‡.)4‡);806*;48‡8
¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96
*?;8)*‡(;485);5*†2:*‡(;4956*2(5*—4)8
¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†52880 6*81(‡9;48;(88;4
(‡?34;48)4‡;161;:188;‡?;
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*;4e26)4‡.)4‡);e06*;4e‡e
¶60))e5;1‡(;:‡*e†e3(ee)5*†;46(;ee*96
*?;e)*‡(;4e5);5*†2:*‡(;4956*2(5*—4)e
¶e*;40692e5);)6†e)4‡‡;1(‡9;4e0e1;e:e‡
1;4e†e5;4)4e5†52ee06*e1(‡9;4e;(ee;4
(‡?34;4e)4‡;161;:1ee;‡?;
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*;4e26)4‡.)4‡);e06*;4e‡e
¶60))e5;1‡(;:‡*e†e3(ee)5*†;46(;ee*96
*?;e)*‡(;4e5);5*†2:*‡(;4956*2(5*—4)e
¶e*;40692e5);)6†e)4‡‡;1(‡9;4e0e1;e:e‡
1;4e†e5;4)4e5†52ee06*e1(‡9;4e;(ee;4
(‡?34;4e)4‡;161;:1ee;‡?;
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*the26)4‡.)4‡);e06*the‡e
¶60))e5;1‡(;:‡*e†e3(ee)5*†;46(;ee*96
*?;e)*‡(the5);5*†2:*‡(;4956*2(5*—4)e
¶e*;40692e5);)6†e)4‡‡;1(‡9the0e1;e:e‡
1the†e5;4)4e5†52ee06*e1(‡9the;(ee;4
(‡?34the)4‡;161;:1ee;‡?;
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*the26)4‡.)4‡);e06*the‡e
¶60))e5;1‡(;:‡*e†e3(ee)5*†;46(;ee*96
*?;e)*‡(the5);5*†2:*‡(;4956*2(5*—4)e
¶e*;40692e5);)6†e)4‡‡;1(‡9the0e1;e:e‡
1the†e5;4)4e5†52ee06*e1(‡9the;(ee;4
(‡?34the)4‡;161;:1ee;‡?;
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*the26)h‡.)h‡)te06*the‡e
¶60))e5t1‡(t:‡*e†e3(ee)5*†th6(tee*96
*?te)*‡(the5)t5*†2:*‡(th956*2(5*—h)e
¶e*th0692e5)t)6†e)h‡‡t1(‡9the0e1te:e‡
1the†e5th)he5†52ee06*e1(‡9thet(eeth
(‡?3hthe)h‡t161t:1eet‡?t
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*the26)h‡.)h‡)te06*the‡e
¶60))e5t1‡(t:‡*e†e3(ee)5*†th6(tee*96
*?te)*‡(the5)t5*†2:*‡(th956*2(5*—h)e
¶e*th0692e5)t)6†e)h‡‡t1(‡9the0e1te:e‡
1the†e5th)he5†52ee06*e1(‡9thet(eeth
(‡?3hthe)h‡t161t:1eet‡?t
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*the26)h‡.)h‡)te06*the‡e
¶60))e5t1‡(t:‡*e†e3(ee)5*†th6(tee*96
*?te)*‡(the5)t5*†2:*‡(th956*2(5*—h)e
¶e*th0692e5)t)6†e)h‡‡t1(‡9the0e1te:e‡
1the†e5th)he5†52ee06*e1(‡9thet(eeth
(‡?3hthe)h‡t161t:1eet‡?t
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

53‡‡†305))6*the26)h‡.)h‡)te06*the‡e
¶60))e5t1‡(t:‡*e†e3(ee)5*†th6(tee*96
?te)‡(the5)t5*†2:*‡(th956*2(5*—h)e
¶e*th0692e5)t)6†e)h‡‡t1(‡9the0e1te:e‡
1the†e5th)he5†52ee06*e1(‡9thetreeth
(‡?3hthe)h‡t161t:1eet‡?t

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*the26)h‡.)h‡)te06*the‡e
¶60))e5t1‡(t:‡*e†e3(ee)5*†th6(tee*96
*?te)*‡(the5)t5*†2:*‡(th956*2(5*—h)e
¶e*th0692e5)t)6†e)h‡‡t1(‡9the0e1te:e‡
1the†e5th)he5†52ee06*e1(‡9thetreeth
(‡?3hthe)h‡t161t:1eet‡?t
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*the26)h‡.)h‡)te06*the‡e
¶60))e5t1‡rt:‡*e†e3ree)5*†th6rtee*96
*?te)*‡rthe5)t5*†2:*‡rth956*2r5*—h)e
¶e*th0692e5)t)6†e)h‡‡t1r‡9the0e1te:e‡
1the†e5th)he5†52ee06*e1r‡9thetreeth
r‡?3hthe)h‡t161t:1eet‡?t
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*the26)h‡.)h‡)te06*the‡e
¶60))e5t1‡rt:‡*e†e3ree)5*†th6rtee*96
*?te)*‡rthe5)t5*†2:*‡rth956*2r5*—h)e
¶e*th0692e5)t)6†e)h‡‡t1r‡9the0e1te:e‡
1the†e5th)he5†52ee06*e1r‡9thetreeth
r‡?3hthe)h‡t161t:1eet‡?t
```

8	e
;	t
4	h
(	r

e	8
t	;
h	4
r	(

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*the26)h‡.)h‡)te06*the‡e
¶60))e5t1‡rt:‡*e†e3ree)5*†th6rtee*96
*?te)*‡rthe5)t5*†2:*‡rth956*2r5*—h)e
¶e*th0692e5)t)6†e)h‡‡t1r‡9the0e1te:e‡
1the†e5th)he5†52ee06*e1r‡9thetreeth
r‡?3hthe)h‡t161t:1eet‡?t
```

8	e	5	a	*	n	2	b	?	u
;	t	†	d	‡	o	.	p	:	y
4	h	3	g	0	l	¶	v	1	f
(	r	6	i	)	s	9	m	—	c

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
53‡‡†305))6*the26)h‡.)h‡)te06*the‡e
¶60))e5t1‡rt:‡*e†e3ree)5*†th6rtee*96
*?te)*‡rthe5)t5*†2:*‡rth956*2r5*-h)e
¶e*th0692e5)t)6†e)h‡‡t1r‡9the0e1te:e‡
1the†e5th)he5†52ee06*e1r‡9thetreeth
r‡?3hthe)h‡t161t:1eet‡?t
```

8	e	5	a	*	n	2	b	?	u
;	t	†	d	‡	o	.	p	:	y
4	h	3	g	0	l	¶	v	1	f
(	r	6	i	)	s	9	m	—	c

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
agoodglassinthebishopshostelinthede
vilsseatfortyonedegreesandthirteenmi
nutesnortheastandbynorthmainbranchse
venthlimbeastsideshootfromthelefteyeo
fthedeathsheadabeelinefromthetreeth
roughtheshotfiftyfeetout
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

```
A good glass in the bishop's hostel in the
devil's seat forty-one degrees and thirteen
minutes northeast and by north main branch
seventh limb east side shoot from the left
eye of the death's-head a bee-line from
the tree through the shot fifty feet out.
```

Le scarabée d'or

Edgar Allan Poe, juin 1843

A good glass in the bishop's hostel in the devil's seat forty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee-line from the tree through the shot fifty feet out.

« Un bon verre dans l'hostel de l'évêque dans la chaise du diable / quarante et un degrés et treize minutes / nord-est quart de nord / principale tige septième branche côté est / lâchez de l'œil gauche de la tête de mort / une ligne d'abeille de l'arbre à travers la balle cinquante pieds au large. »

Première percée

Première percée

- 9e siècle

Première percée

- 9e siècle
- أبو يوسف يعقوب ابن إسحاق الكندي

Première percée

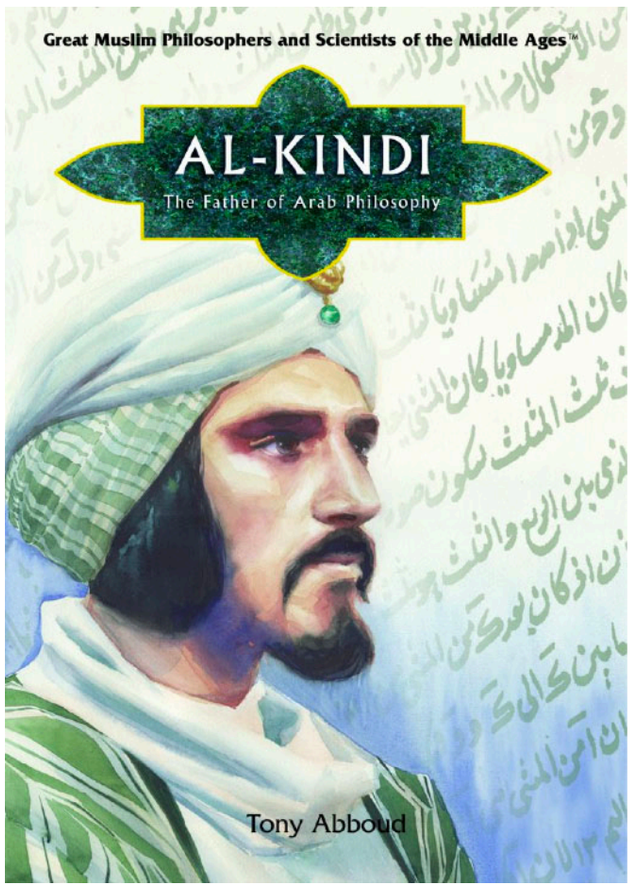
- 9e siècle
- Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn Oòmran ibn Ismaïl Al-Kindi

Première percée

- 9e siècle
- Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn Oòmran ibn Ismaïl Al-Kindi

Première percée

- 9e siècle
- Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn Oòmran ibn Ismaïl Al-Kindi



Première percée

- 9e siècle
- Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn Oòmran ibn Ismaïl Al-Kindi
- Auteur (801-873) de 290 livres

Première percée

- 9e siècle
- Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn Oòmran ibn Ismaïl Al-Kindi
- Auteur (801-873) de 290 livres dont
- *Manuscrit sur le déchiffrement des messages cryptographiques*

[illegible]

تم الكتاب — والحمد لله رب العالمين وصلى الله على سيدنا محمد وآله وسلم

بسم الله الرحمن الرحيم وحسبنا الله وحده

رسالة ابي يوسف يعقوب بن اسحق الكندي في استخراج المعمى [illegible]

[illegible]

Première percée

- 9e siècle
- Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah ibn Oòmran ibn Ismaïl Al-Kindi
- Auteur (801-873) de 290 livres dont
- *Manuscrit sur le déchiffrement des messages cryptographiques*
- Retrouvé en 1987

Et à l'ouest ?

Et à l'ouest ?

➢ Essentiellement rien avant le 15e siècle !

Et à l'ouest ?

- Essentiellement rien avant le 15e siècle !
- Leone Battista Alberti (1404-1472)

Et à l'ouest ?

- Essentiellement rien avant le 15e siècle !
- Leone Battista Alberti

Et à l'ouest ?

- Essentiellement rien avant le 15e siècle !
- Leone Battista Alberti (1404-1472)
  - Père de la cryptographie occidentale

Et à l'ouest ?

- Essentiellement rien avant le 15e siècle !
- Leone Battista Alberti (1404-1472)
  - Père de la cryptographie occidentale
  - Disque de chiffrement (1467)

Et à l'ouest ?

- Essentiellement rien avant le 15e siècle !
- Leone Battista Alberti (1404-1472)
  - Père de la cryptographie occidentale
  - Disque de chiffrement

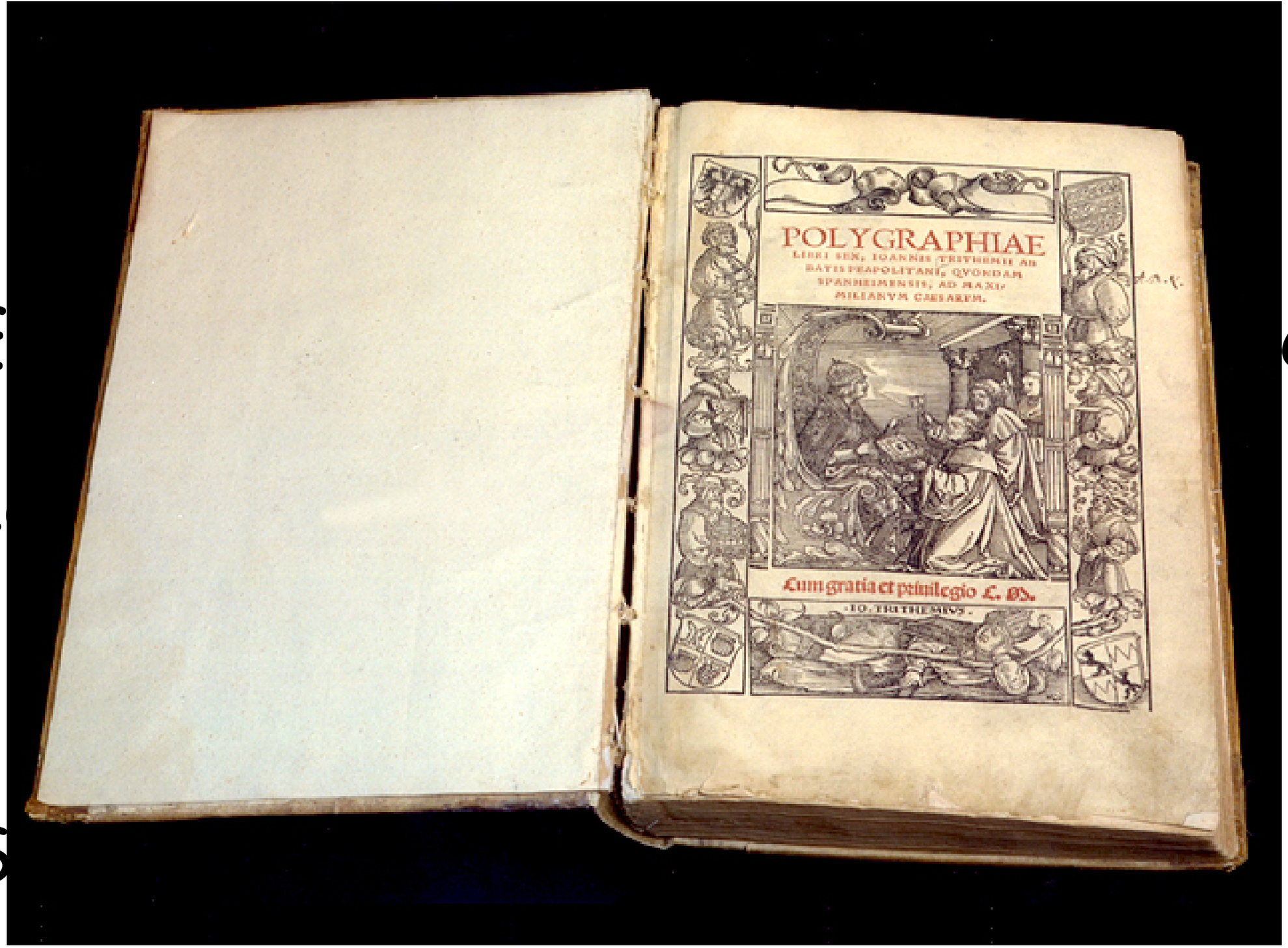
Et à l'ouest ?

- Essentiellement rien avant le 15e siècle !
- Leone Battista Alberti (1404-1472)
  - Père de la cryptographie occidentale
  - Disque de chiffrement (1467)
- Substitution poly-alphabétique

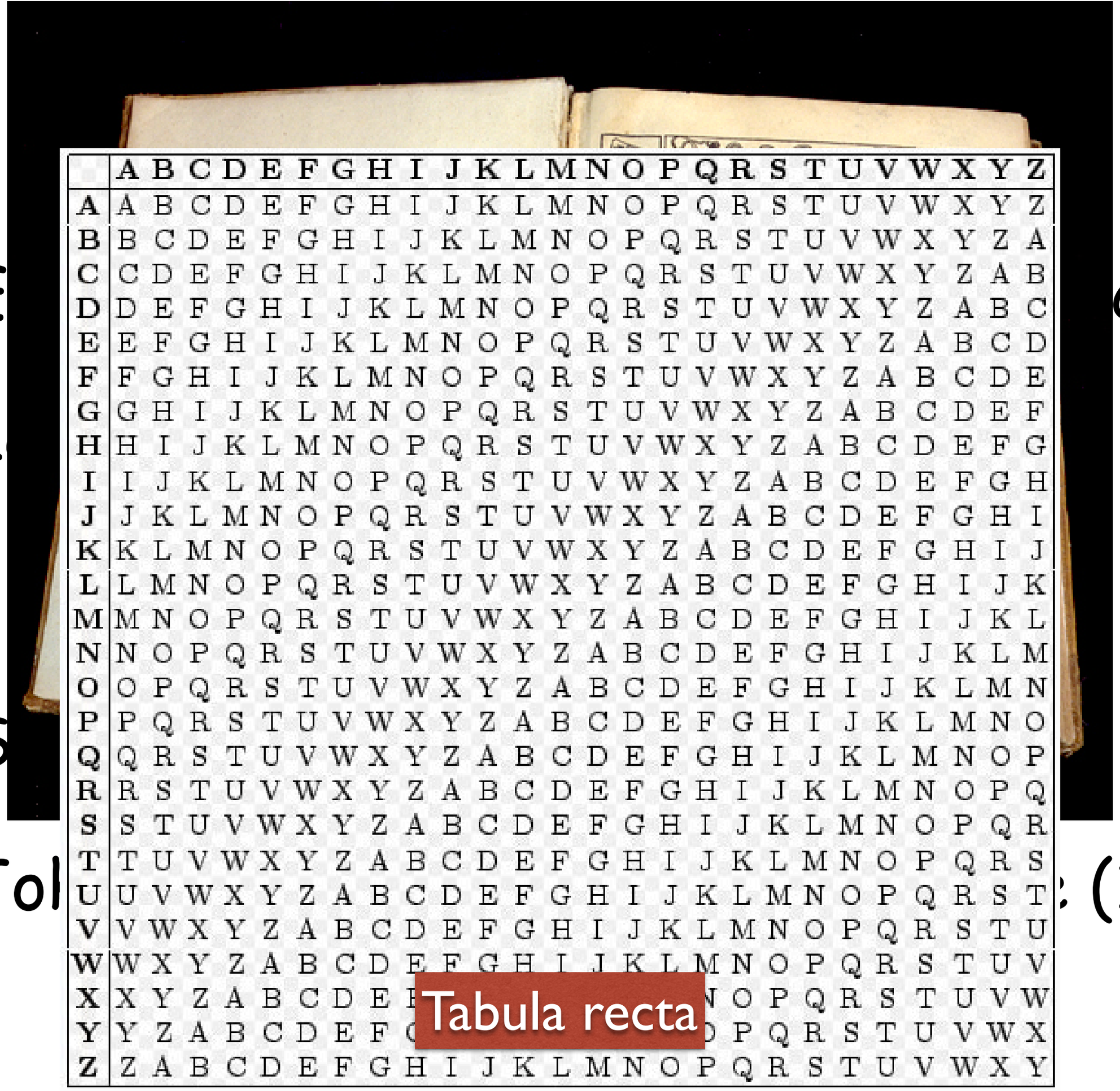
Et à l'ouest ?

- Essentiellement rien avant le 15e siècle !
- Leone Battista Alberti (1404-1472)
  - Père de la cryptographie occidentale
  - Disque de chiffrement (1467)
- Substitution poly-alphabétique
- Johannes Trithemius: Polygraphiae (1518)

- E cle !
- L
- S



- Johannes Trithemius: Polygraphiae (1518)



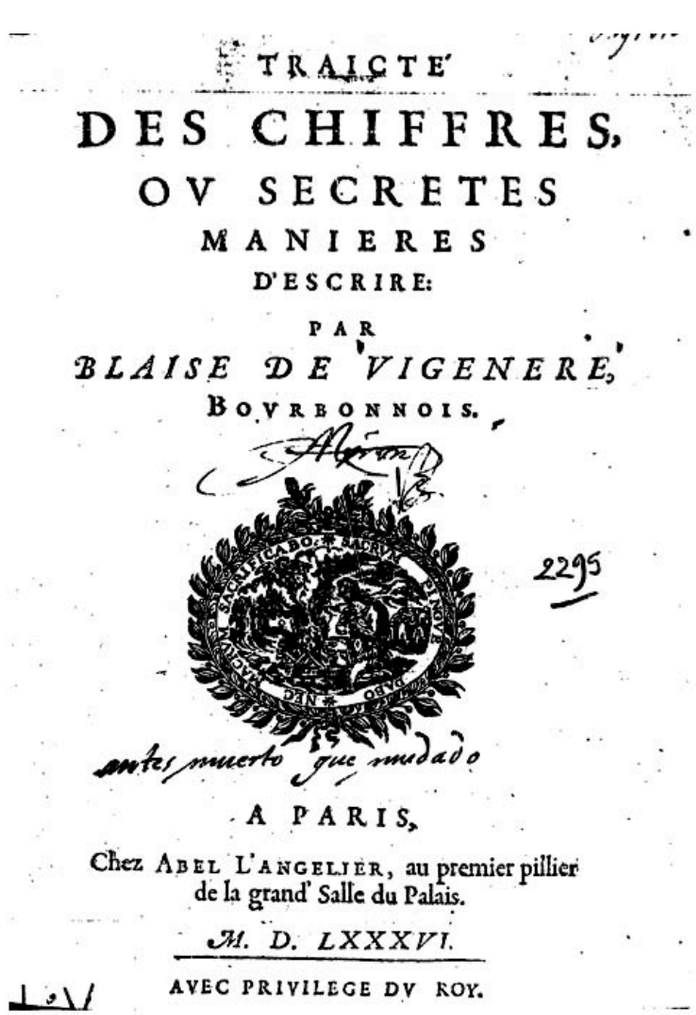
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tabula recta

- E cle !
- L
- S
- Jol : (1518)

Le chiffre indéchiffrable

- Inventé par Giovan Battista Bellaso (1553)
- Attribué à Blaise de Vigenère (1585)



TRAICTE'

DES CHIFFRES,

OV SECRETES

MANIERES

D'ESCRIRE:

PAR

BLAISE DE VIGENERE,

BOVRBONNOIS.

2295

antes muerto que mudado

A PARIS,

Chez ABEL L'ANGELIER, au premier pillier de la grand' Salle du Palais.

M. D. LXXXVI.

AVEC PRIVILEGE DV ROY.

Le chiffre indéchiffrable

Le chiffre indéchiffrable

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Le chiffre indéchiffrable

clef

clair

chiffré

Le chiffre indéchiffrable

clef

clair bonjour

chiffré

Le chiffre indéchiffrable

clef KOALA

clair bonjour

chiffré

Le chiffre indéchiffrable

clef KOALAKO

clair bonjour

chiffré

Le chiffre indéchiffrable

clef KOALAKO

clair bonjour

chiffré

Le chiffre indéchiffrable

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Le chiffre indéchiffrable

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Le chiffre indéchiffrable

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Le chiffre indéchiffrable

clef KOALAKO

clair bonjour

chiffré

Le chiffre indéchiffrable

clef	KOALAKO
clair	bonjour
chiffré	L

Le chiffre indéchiffrable

clef	KOALAKO
clair	bonjour
chiffré	L

Le chiffre indéchiffrable

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Le chiffre indéchiffrable

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Le chiffre indéchiffrable

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Le chiffre indéchiffrable

clef	KOALAKO
clair	bonjour
chiffré	L

Le chiffre indéchiffrable

clef	KOALAKO
clair	bonjour
chiffré	LC

Le chiffre indéchiffrable

clef	KOALAKO
clair	bonjour
chiffré	LCNUOEF

Le chiffre indéchiffrable

clef	KOALAKO
clair	bonjour
chiffré	LCNUOEF

Le chiffre indéchiffrable

clef	KOALAKO
clair	bonjour
chiffré	LCNUOEF

Le chiffre indéchiffrable

clef	KOALAKO
clair	bonjour
chiffré	LCNUOEF

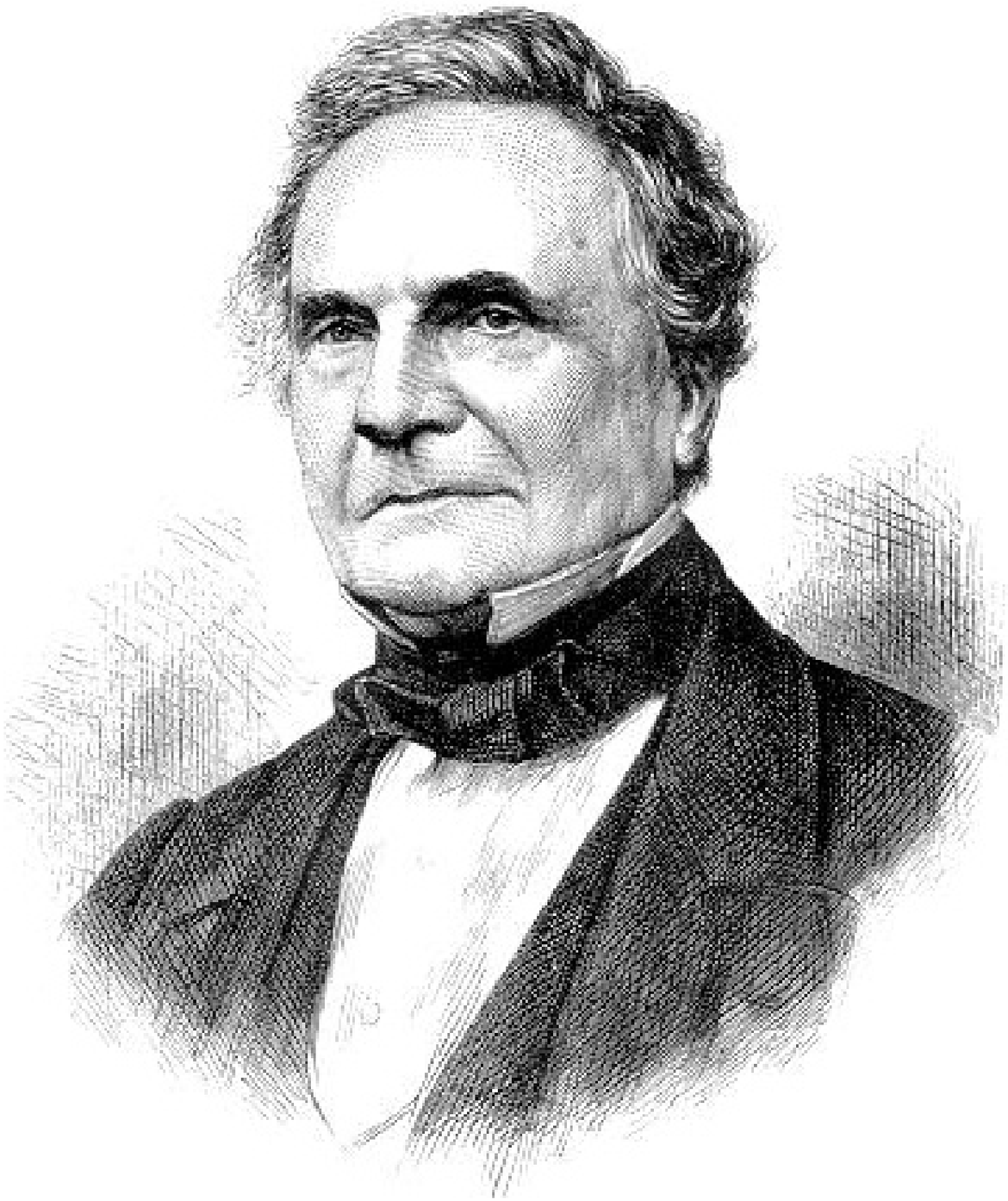
Le chiffre indéchiffrable

- Inventé par Giovan Battista Bellaso (1553)
- Attribué à Blaise de Vigenère (1585)

Le chiffre indéchiffrable

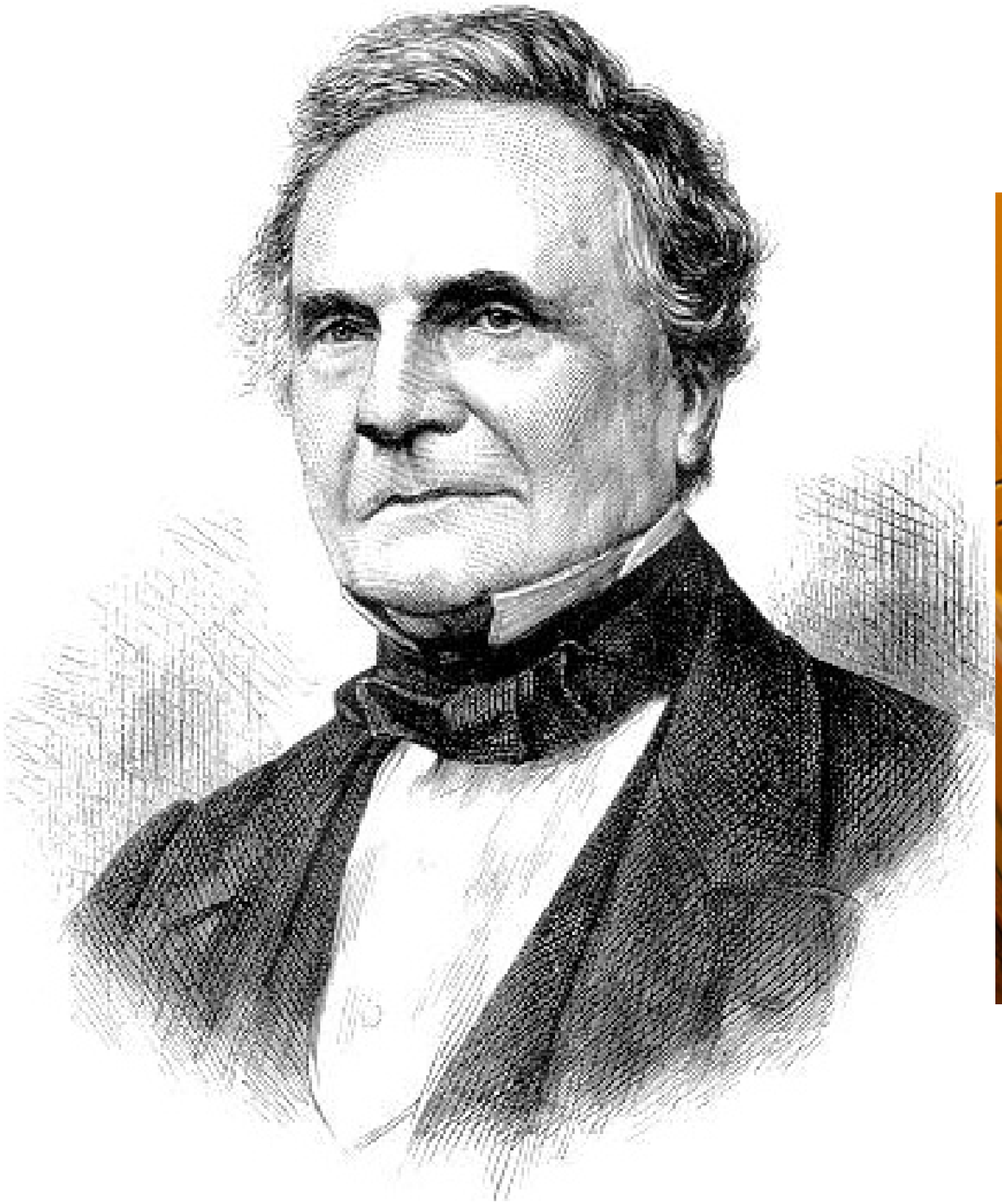
- Inventé par Giovan Battista Bellaso (1553)
- Attribué à Blaise de Vigenère (1585)
- Résolu par Charles Babbage (1854)

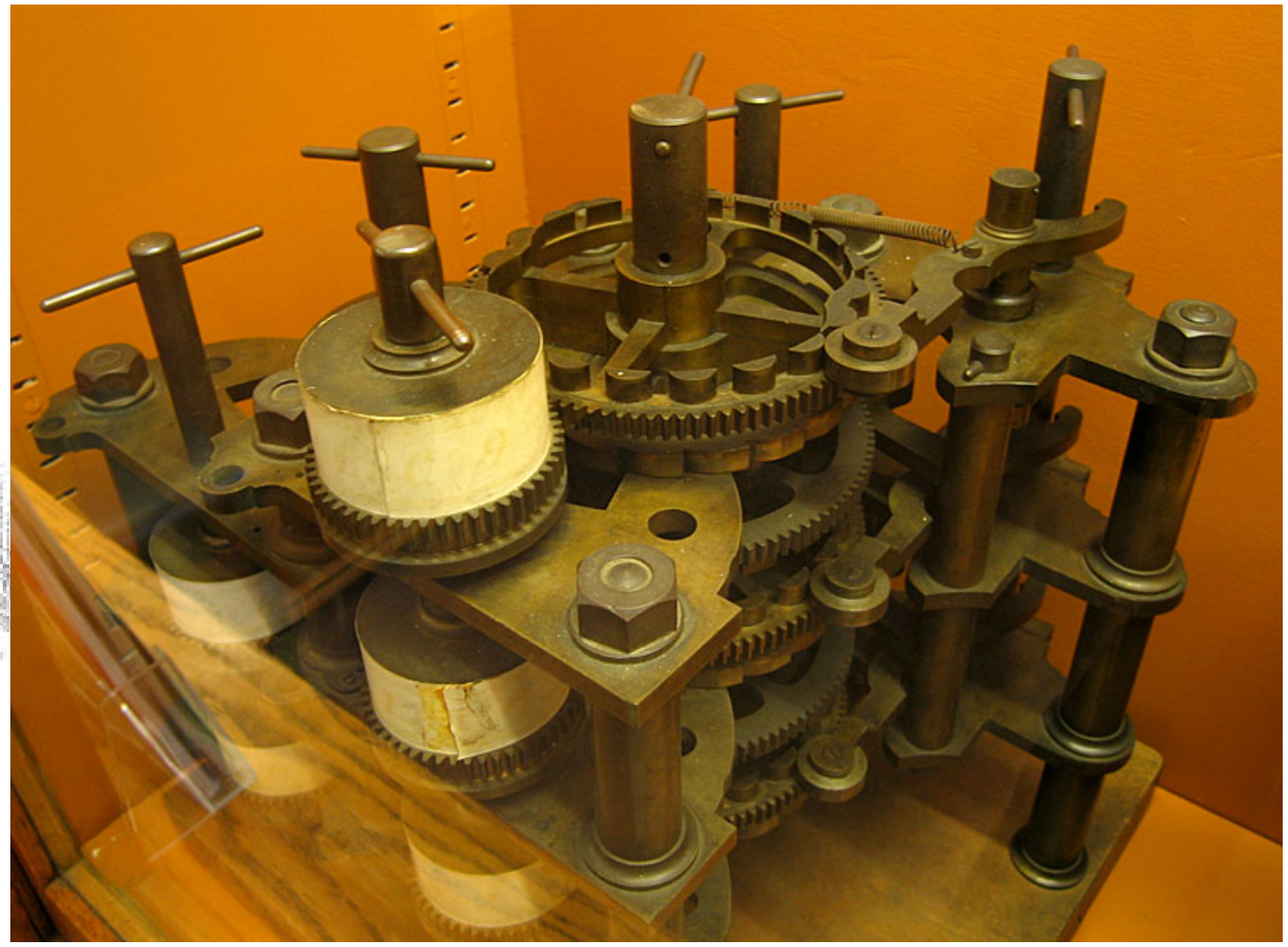
Le chiffre indéchiffrable



Babbage (1854)

Le chiffre indéchiffrable





Le chiffre indéchiffrable

- Inventé par Giovan Battista Bellaso (1553)
- Attribué à Blaise de Vigenère (1585)
- Résolu par Charles Babbage (1854)

  (indépendamment par Friedrich Wilhelm Kasiski, 1863)

Le chiffre indéchiffrable

- Inventé par Giovan Battista Bellaso (1553)
- Attribué à Blaise de Vigenère (1585)
- Résolu par Charles Babbage (1854)

  (indépendamment par Friedrich Wilhelm Kasiski, 1863)

Le chiffre indéchiffrable

- Inventé par Giovan Battista Bellaso (1553)
- Attribué à Blaise de Vigenère (1585)
- Résolu par Charles Babbage (1854)

(indépendamment par Friedrich Wilhelm Kasiski, 1863)

Il a fallu plus de 300 ans !

Qui gagnera ?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

« On peut affirmer rondement que l'ingéniosité humaine ne peut concocter de chiffre que l'ingéniosité humaine ne puisse résoudre »

Edgar Allan Poe

(Graham's Lady's and Gentleman's Magazine, juillet 1841)

Qui gagnera ?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

« On peut affirmer rondement que l'ingéniosité humaine ne peut concocter de chiffre que l'ingéniosité humaine ne puisse résoudre »

Edgar Allan Poe

(Graham's Lady's and Gentleman's Magazine, juillet 1841)

Chiffre indéchiffrable résolu par Charles Babbage (1854)

Qui gagnera ?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

« On peut affirmer rondement que l'ingéniosité humaine ne peut concocter de chiffre que l'ingéniosité humaine ne puisse résoudre »

Edgar Allan Poe

(Graham's Lady's and Gentleman's Magazine, juillet 1841)

Chiffre indéchiffrable résolu par Charles Babbage (1854)

Le chiffre indéchiffrable?

Vraiment indéchiffrable!

Vraiment indéchiffrable!

- Masque jetable (one-time pad)

Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)

Vraiment indéchiffrable !

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Attribué à Gilbert Vernam et Joseph Mauborgne (1919)

Vraiment ind

- Masque jetable (one
- Inventé par Frank M
- Attribué à Gilbert Vernam

UNITED STATES PATENT OFFICE.

GILBERT S. VERNAM, OF BROOKLYN, NEW YORK, ASSIGNOR TO AMERICAN TELEPHONE AND TELEGRAPH COMPANY, A CORPORATION OF NEW YORK.

SECRET SIGNALING SYSTEM.

1,310,719. Specification of Letters Patent. Patented July 22, 1919.

Application filed September 13, 1918. Serial No. 253,962.

To all whom it may concern:

Be it known that I, GILBERT S. VERNAM, residing at Brooklyn, in the county of Kings and State of New York, have invented certain Improvements in Secret Signaling Systems, of which the following is a specification.

This invention relates to signaling systems and especially to telegraph systems. Its object is to insure secrecy in the transmission of messages and, further, to provide a system in which messages may be transmitted and received in plain characters or a well-known code but in which the signaling impulses are so altered before transmission over the line that they are unintelligible to anyone intercepting them.

The invention is here illustrated as applied to a well-known form of printing telegraph systems but, as will be readily understood, it is applicable to other signaling systems. The invention will be more fully described in connection with the accompanying drawings, in which Figure 1 illustrates circuit arrangements at one end of the line in a system embodying the invention, and Figs. 2 and 3 show modifications in the circuits of the sending apparatus.

Like sending and receiving apparatus is located at each end of the line. Normally the message is recorded by both the local and the distant receiving apparatus and since their operation is identical it will be unnecessary to show and describe the opposite end of the line.

Referring to Fig. 1, A and B represent the transmitting and receiving faces respectively of a known form of distributer used in printing telegraph systems. Only such parts of the distributer and such parts of the circuit of the known apparatus are here illustrated as are necessary to an understanding of the present invention. Accordingly only two of the usual four rows of segments on the distributer are shown. The outer row on the transmitting side comprises five segments 1, 2, 3, 4 and 5 from which the code impulses are transmitted. It also includes the segment 6 on which the distributer arm normally rests, and the starting segment S. The inner contact ring 7 is continuous and is connected to one side of the transmitting circuit 9 which is normally closed through a suitable source of current not shown. The distributer arm 10 carries a brush 11 whose opposite ends contact with the ring 7 and the segmental contacts repectively. When the apparatus is at rest this arm is detained by the latch 12 which may be withdrawn by means of magnet 13 under the control of the operator. The receiving side of the distributer has five segments 1′, 2′, 3′, 4′ and 5′, corresponding to the five sending segments but shortened to receive only the central part of the current impulses transmitted. It also has a contact 6′, upon which the distributer arm normally rests, and a contact P for controlling the energization of a relay whose purpose will appear hereinafter. The receiving distributer arm 10′ carries a brush 11′ and is controlled by a latch 12′ and magnet 13′ as in the case of the transmitting distributer arm.

The "sending relays" commonly used in the form of printing telegraph system here shown are indicated at 14, 15, 16, 17 and 18. The circuits controlled by these relays ordinarily run directly to the distributer segments 1 to 5 for transmitting the signal impulses. In accordance with this invention, however, these sending relays control the circuits to the distributer segments through another set of relays 19, 20, 21, 22 and 23 which may be called "cipher sending relays." The circuits through the contacts of relays 14 to 18 accordingly run from the source of current 24 through the windings of the relays 19 to 23 and thence to an automatic ciphering device D.

The relays 14 to 18 are under the control of a sending device here indicated at C as a known form of keyboard transmitter, which is provided with a set of contacts 25, 26, 27, 28 and 29, these being under the control of the key levers of the keyboard, as is well understood. The circuit of each of the relays 14 to 18 runs from ground through one of these contacts and to a source of current 30. The relays are in actual practice provided with locking windings, not shown, which facilitate the transmitting of the message; and their circuits are furthermore usually arranged to be transferred at will to the contacts of a tape transmitter which may be used instead of the keyboard transmitter, all as is now well known in the art. The circuit of each of the relays 19 to 23 is provided with a branch to ground through a resistance 31, to enable the relays to be controlled by the ciphering device as will appear hereinafter.

Vraiment ind

- Masque jetable (one
- Inventé par Frank M
- Attribué à Gilbert Vernam

UNITED STATES PATENT OFFICE.

GILBERT S. VERNAM, OF BROOKLYN, NEW YORK, ASSIGNOR TO AMERICAN TELEPHONE AND TELEGRAPH COMPANY, A CORPORATION OF NEW YORK.

SECRET SIGNALING SYSTEM.

1,310,719. Specification of Letters Patent. Patented July 22, 1919.

Application filed September 13, 1918. Serial No. 253,962.

To all whom it may concern:

Be it known that I, GILBERT S. VERNAM, residing at Brooklyn, in the county of Kings and State of New York, have invented certain Improvements in Secret Signaling Systems, of which the following is a specification.

This invention relates to signaling systems and especially to telegraph systems. Its object is to insure secrecy in the transmission of messages and, further, to provide a system in which messages may be transmitted and received in plain characters or a well-known code but in which the signaling impulses are so altered before transmission over the line that they are unintelligible to anyone intercepting them.

The invention is here illustrated as applied to a well-known form of printing telegraph systems but, as will be readily understood, it is applicable to other signaling systems. The invention will be more fully described in connection with the accompanying drawings, in which Figure 1 illustrates circuit arrangements at one end of the line in a system embodying the invention, and

tact with the ring 7 and the segmental contacts repectively. When the apparatus is at rest this arm is detained by the latch 12 which may be withdrawn by means of magnet 13 under the control of the operator. The receiving side of the distributer has five segments 1′, 2′, 3′, 4′ and 5′, corresponding to the five sending segments but shortened to receive only the central part of the current impulses transmitted. It also has a contact 6′, upon which the distributer arm normally rests, and a contact P for controlling the energization of a relay whose purpose will appear hereinafter. The receiving distributer arm 10′ carries a brush 11′ and is controlled by a latch 12′ and magnet 13′ as in the case of the transmitting distributer arm.

The "sending relays" commonly used in the form of printing telegraph system here shown are indicated at 14, 15, 16, 17 and 18. The circuits controlled by these relays ordinarily run directly to the distributer segments 1 to 5 for transmitting the signal impulses. In accordance with this invention, however, these sending relays control the

UNITED STATES PATENT OFFICE.

GILBERT S. VERNAM, OF BROOKLYN, NEW YORK, ASSIGNOR TO AMERICAN TELEPHONE AND TELEGRAPH COMPANY, A CORPORATION OF NEW YORK.

SECRET SIGNALING SYSTEM.

1,310,719. Specification of Letters Patent. Patented July 22, 1919.

Application filed September 13, 1918. Serial No. 253,962.

Vraiment indéchiffrable !

- Mas
- Inve
- Attri ie (1919)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Attribué à Gilbert Vernam et Joseph Mauborgne (1919)

clef

clair

chiffré

Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Attribué à Gilbert Vernam et Joseph Mauborgne (1919)

clef

clair bonjour

chiffré

Vraiment indéchiffrable !

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Attribué à Gilbert Vernam et Joseph Mauborgne (1919)

clef	KOALA
clair	bonjour
chiffré	

Vraiment indéchiffrable !

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Attribué à Gilbert Vernam et Joseph Mauborgne (1919)

clef	KOALAKO
clair	bonjour
chiffré	

Vraiment indéchiffrable !

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Attribué à Gilbert Vernam et Joseph Mauborgne (1919)

clef	KOALAKO
clair	bonjour
chiffré	LCNUOEF

Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Attribué à Gilbert Vernam et Joseph Mauborgne (1919)

clef

clair bonjour

chiffré

Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Attribué à Gilbert Vernam et Joseph Mauborgne (1919)

clef LFKJKAC

clair bonjour

chiffré

Vraiment indéchiffrable !

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Attribué à Gilbert Vernam et Joseph Mauborgne (1919)

clef	LFKJKAC
clair	bonjour
chiffré	MTXSYUT

Vraiment indéchiffrable !

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Attribué à Gilbert Vernam et Joseph Mauborgne (1919)

clef ?	MAESIAP
clair	bonjour
chiffré	MTXSYUT

Vraiment indéchiffrable !

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Attribué à Gilbert Vernam et Joseph Mauborgne (1919)

clef ?	MAESIAP
clair !	attaque
chiffré	MTXSYUT

Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)

Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Chiffre de Vigenère (1553) avec clef

Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Chiffre de Vigenère (1553) avec clef
  - aussi longue que le message

Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Chiffre de Vigenère (1553) avec clef
  - aussi longue que le message
  - purement aléatoire

Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Chiffre de Vigenère (1553) avec clef
  - aussi longue que le message
  - purement aléatoire
  - utilisée une seule fois

Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Chiffre de Vigenère (1553) avec clef
  - aussi longue que le message
  - purement aléatoire
  - utilisée une seule fois
- Pas pratique militairement, mais…

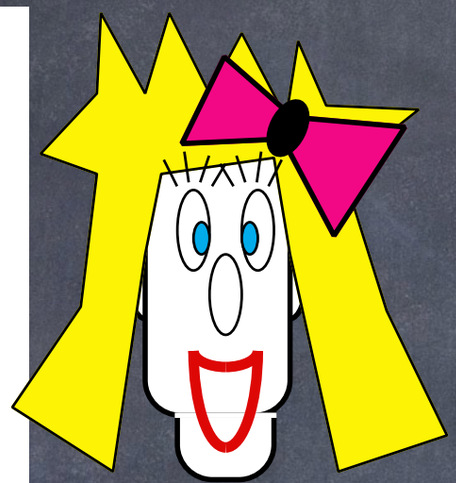
Vraiment indéchiffrable!

- Masque jetable (one-time pad)
- Inventé par Frank Miller (1882)
- Chiffre de Vigenère (1553) avec clef
  - aussi longue que le message
  - purement aléatoire
  - utilisée une seule fois
- Pas pratique militairement, mais…
- Utilisé sur le téléphone rouge!

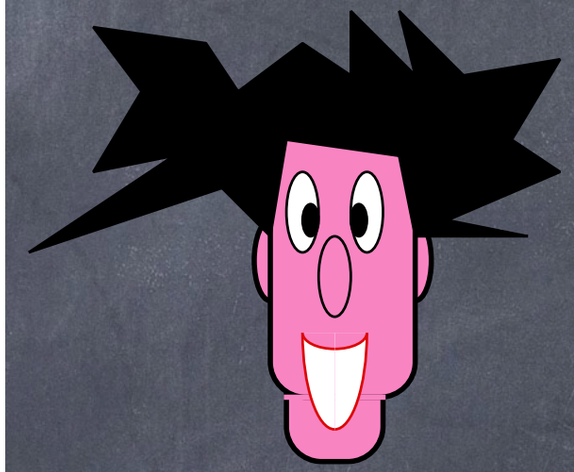
Chiffrement de Vernam

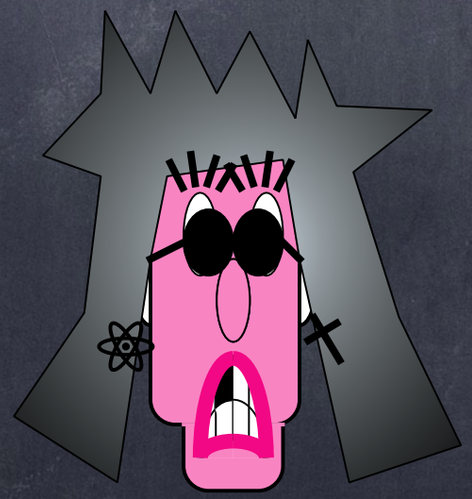
m

1
0
1
0
0
1
0
0
1
1
1
1
1
1
0
0
1



1917

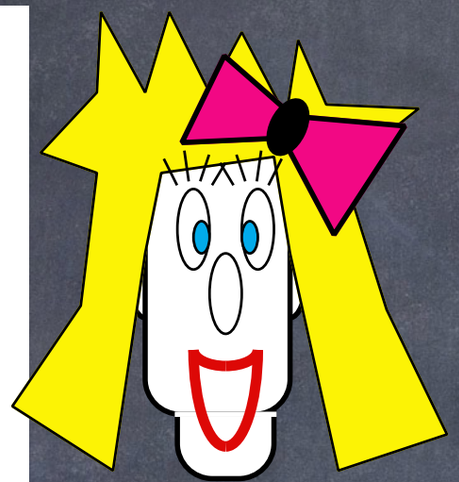


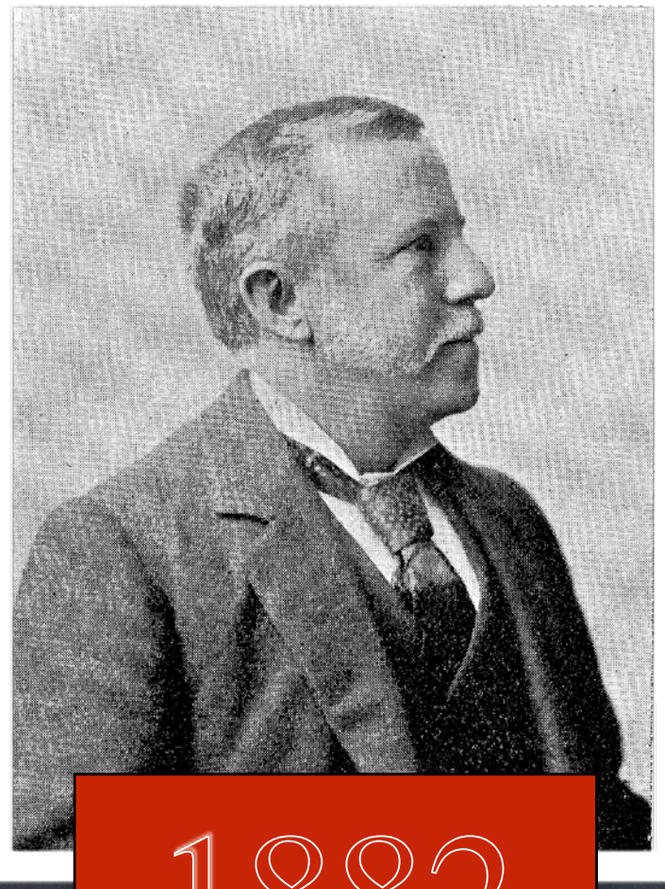


Chiffrement de Vernam-Miller

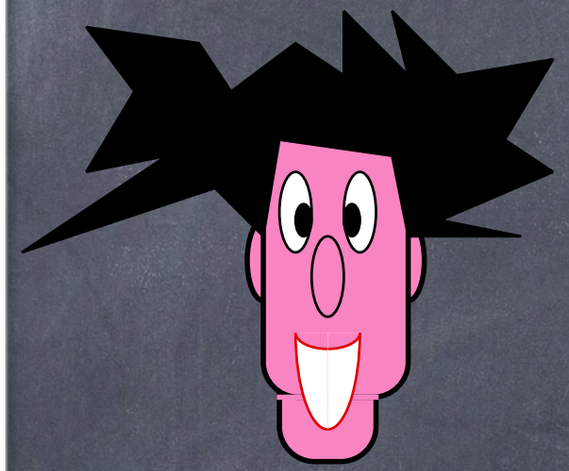
m

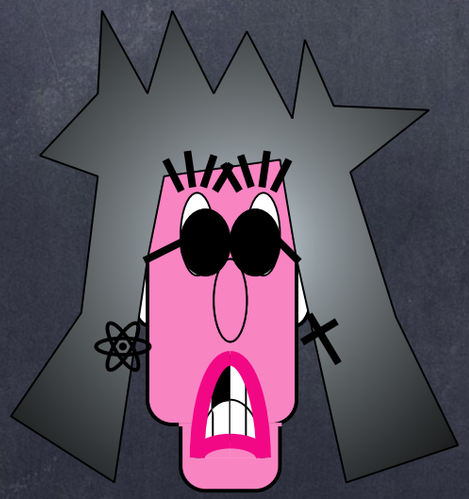
1
0
1
1
0
0
0
1
0
0
1
1
1
1
1
1
1
0
0
1





1882

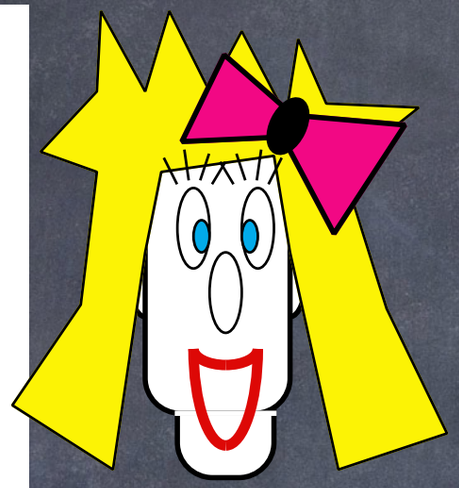


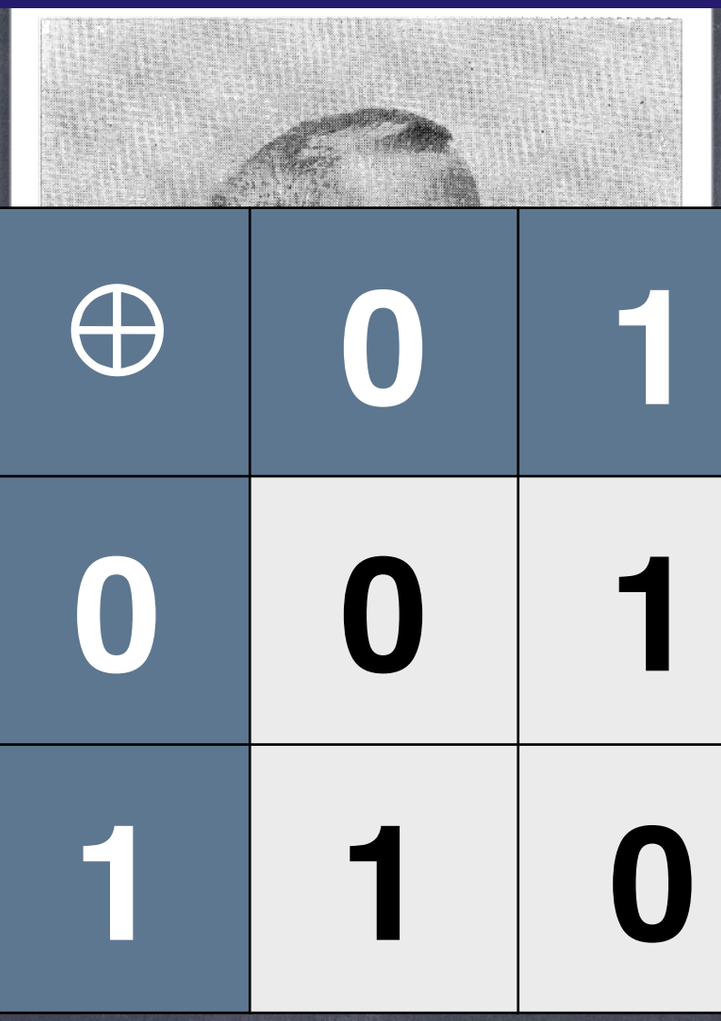


Chiffrement de Vernam-Miller

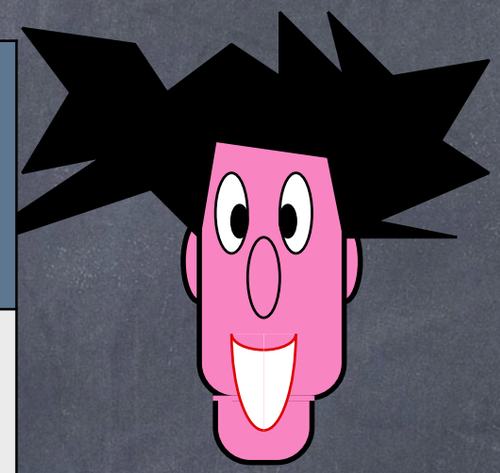
m

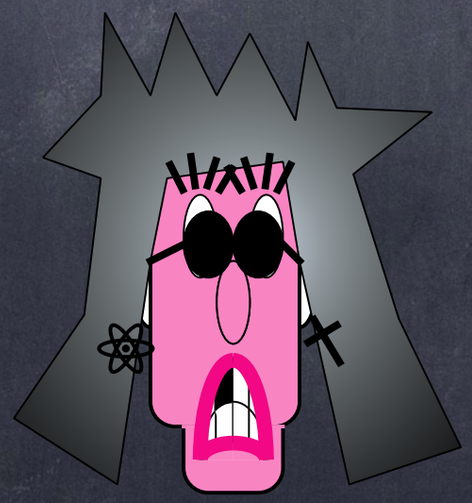
1
0
1
0
0
1
0
0
1
1
1
1
1
1
0
0
1





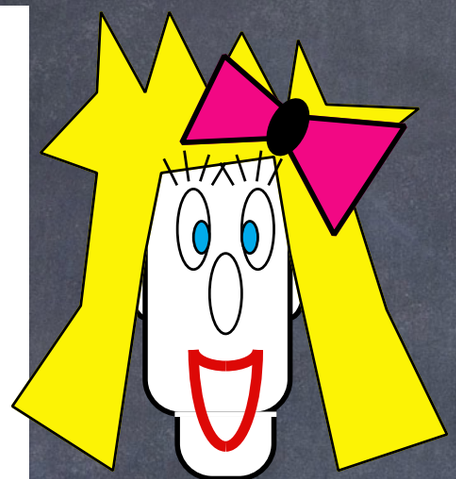
⊕	0	1
0	0	1
1	1	0

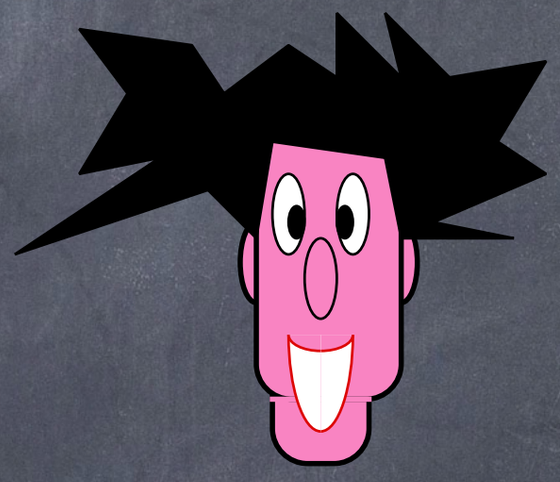


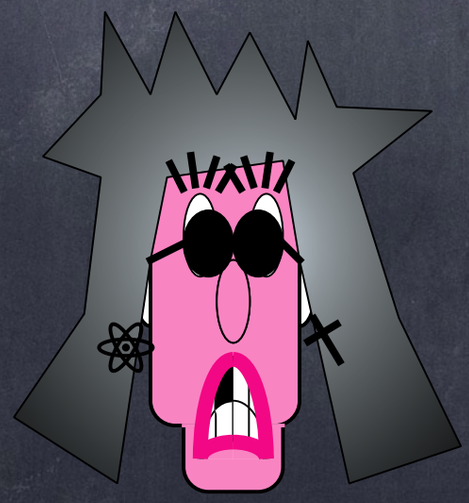


Chiffrement de Vernam-Miller

m	⊕	k
1		1
0		1
1		1
0		0
0		0
1		1
0		1
0	⊕	0
1		1
1		1
1		0
1		1
1		0
0		1
0		1
1		1

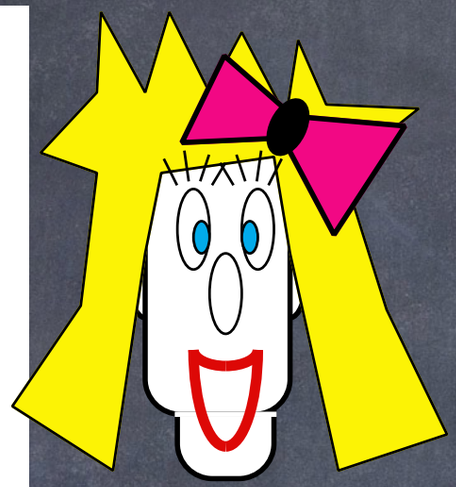


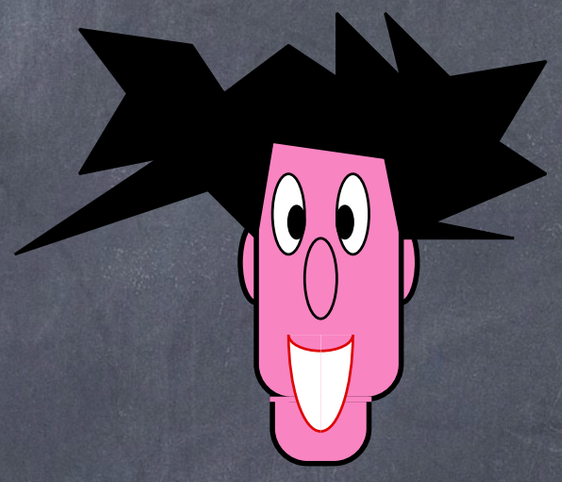


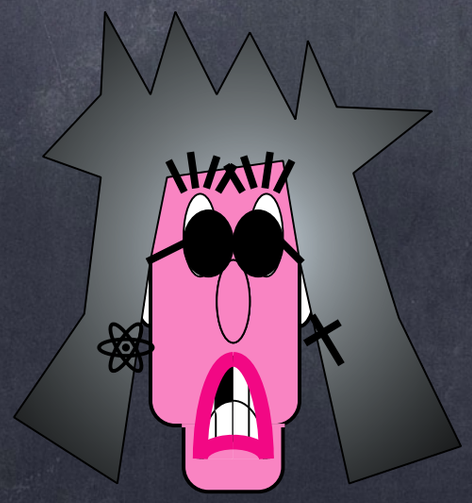


Chiffrement de Vernam-Miller

m	⊕	k	=	c
1		1		0
0		1		1
1		1		0
0		0		0
0		0		0
1		1		0
0		1		1
0		0		0
1		1		0
1		1		0
1		0		1
1		1		0
1		0		1
0		1		1
0		1		1
1		1		0

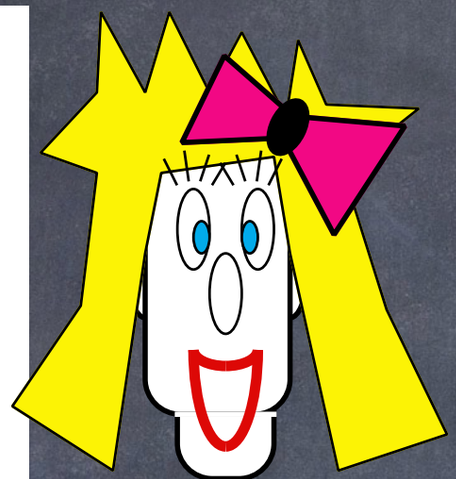


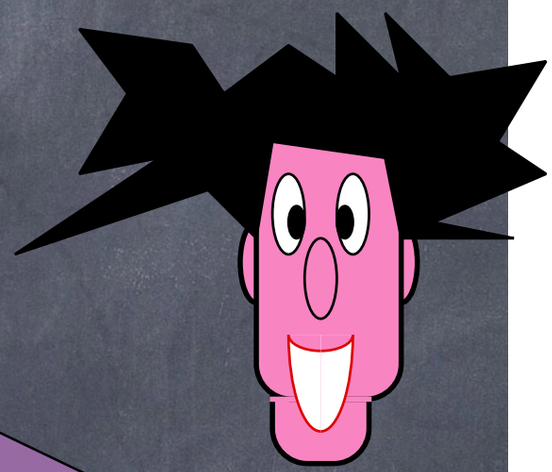




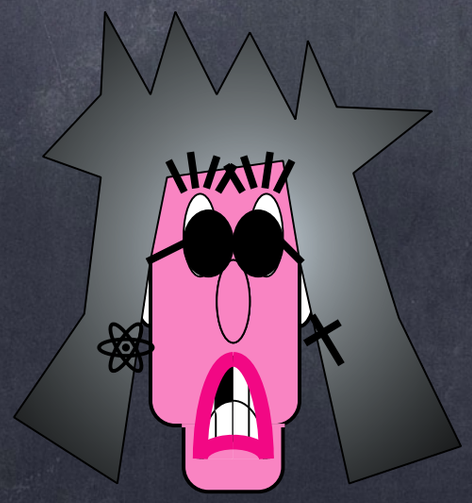
Chiffrement de Vernam-Miller

m	⊕	k	=	c
1		1	=	0
0		1	=	1
1		1	=	0
0		0	=	0
0		0	=	0
1		1	=	0
1		1	=	0
1		1	=	0
1		0	=	1
1		1	=	0
1		0	=	1
0		1	=	1
0		1	=	1
1		1	=	0





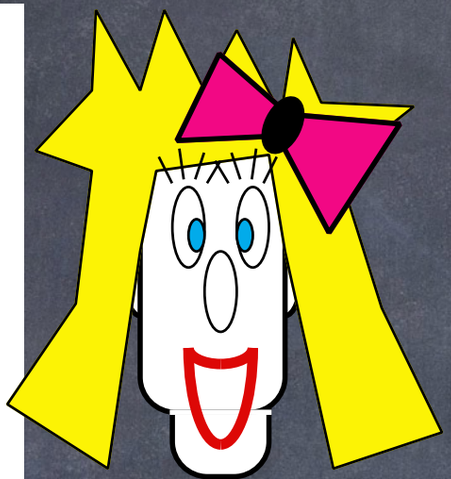
c

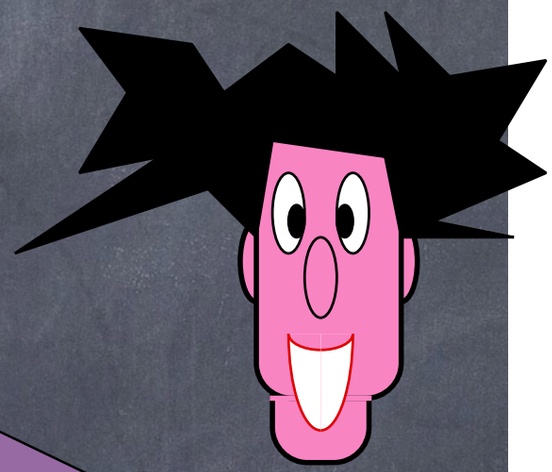


c
0
1
0
0
0
0
0
0
0
1
0
1
1
1
0

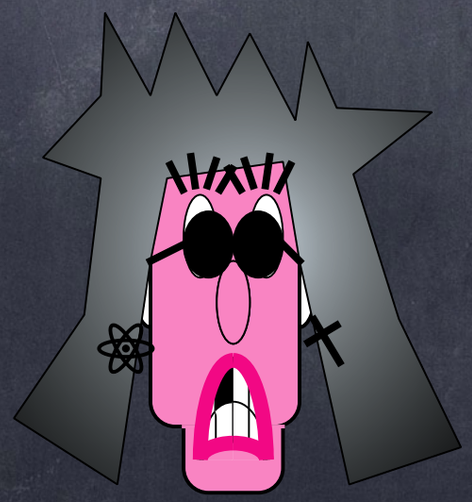
Chiffrement de Vernam-Miller

m	⊕	k	=	c
1		1		0
0		1		1
1		1		0
0		0		0
0		0		0
1		1		0
0		1		1
1		1		0
1		0		1
1		1		0
1		0		1
0		1		1
0		1		1
1		1		0





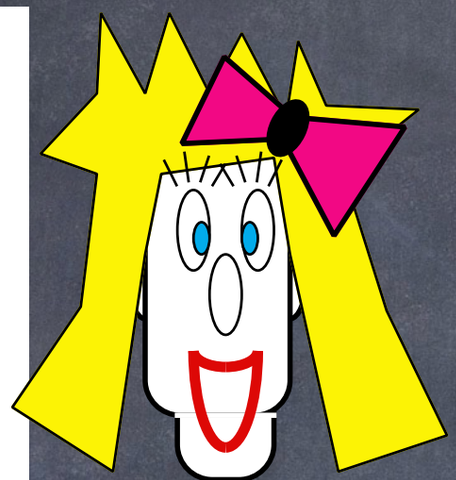
c

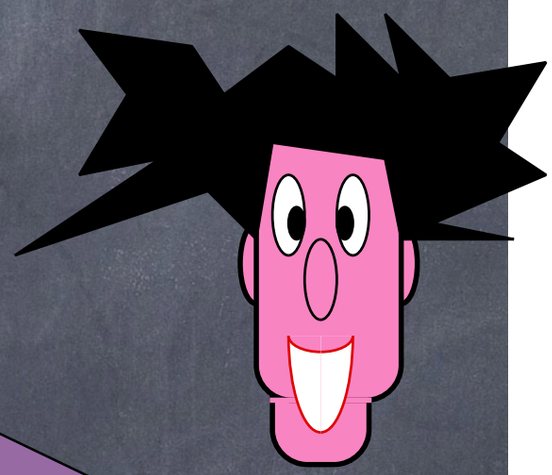


c	⊕	k
0		1
1		1
0		1
0		0
0		0
0		1
1		1
0		0
0		1
1		0
0		1
1		0
1		1
1		1
0		1

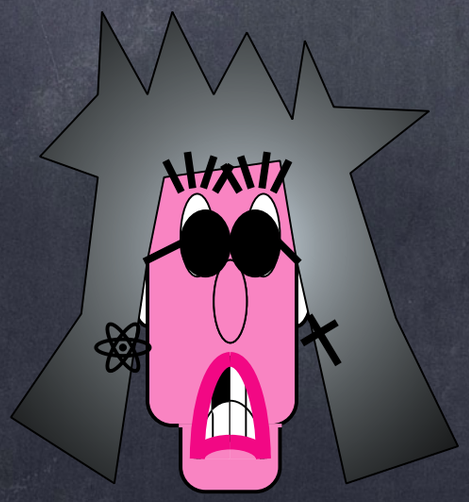
Chiffrement de Vernam-Miller

m	⊕	k	=	c
1		1		0
0		1		1
1		1		0
0		0		0
0		0		0
1		1		0
0		1		1
0	⊕	0	=	0
1		1		0
1		1		0
1		0		1
1		1		0
1		0		1
0		1		1
0		1		1
1		1		0





c



c	⊕	k	=	m
0		1		1
1		1		0
0		1		1
0		0		0
0		0		0
0		1		1
1		1		0
0	⊕	0	=	0
0		1		1
1		1		0
1		0		1
0		1		1
1		0		1
1		1		0
1		1		0
0		1		1

CLE

CHIFFRÉ

CLE

CHIFFRÉ

CLÉ

CHIFFRÉ

CLE

CHIFFRÉ

CLE

CHIFFRÉ

CHIFFRÉ

CLE

CHIFFRÉ

CHIFFRÉ

CLE

CHIFFRÉ

CHIFFRÉ

CLE

CHIFFRÉ

CHIFFRÉ

CLÉ

CHIFFRÉ

CHIFFRÉ

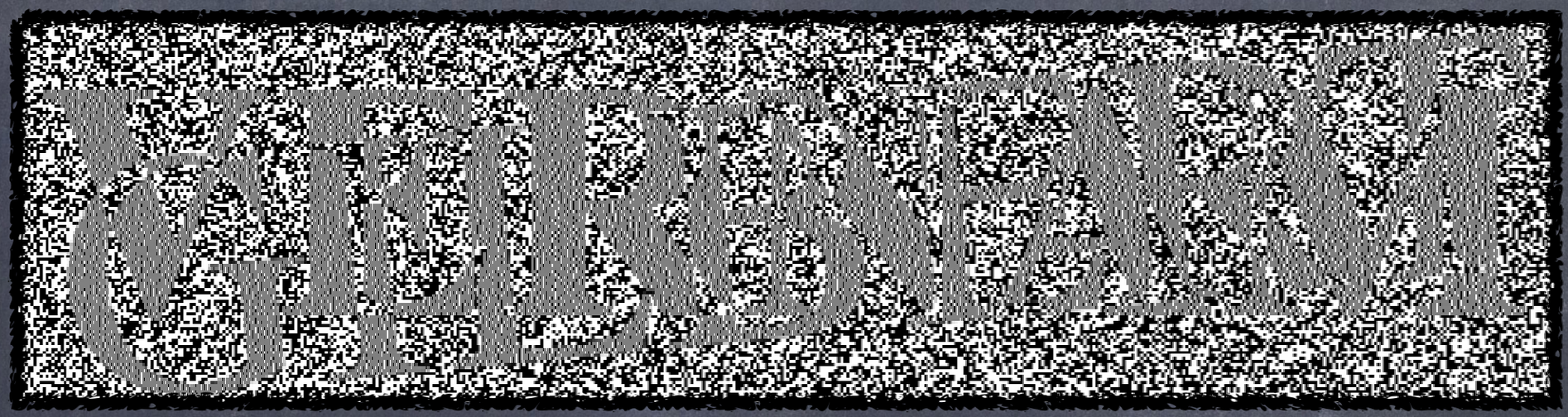
CLÉ

CHIFFRÉ

CHIFFRÉ

CHIFFRÉ

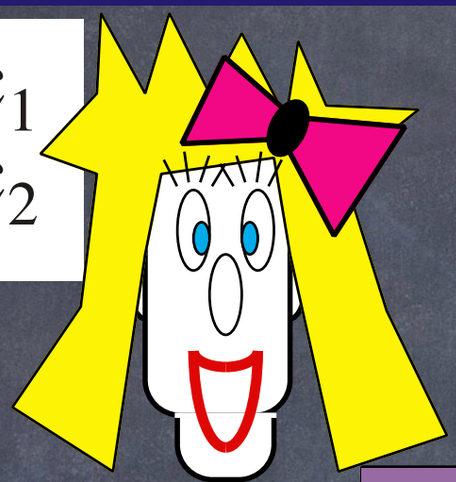
CHIFFRÉ

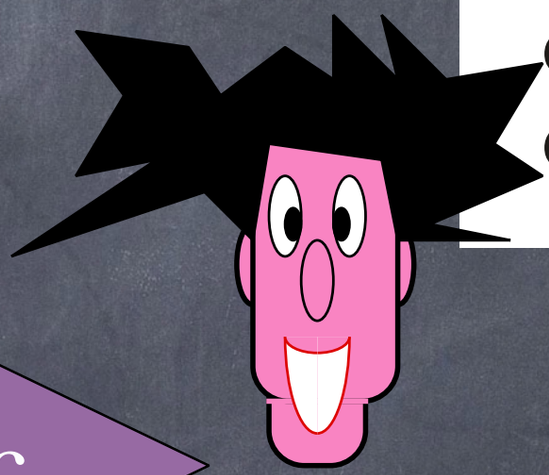


CHIFFRÉ

Chiffrement de Vernam-Miller
Chiffrement à masques jetables

$m_1 \oplus k = c_1$
$m_2 \oplus k = c_2$

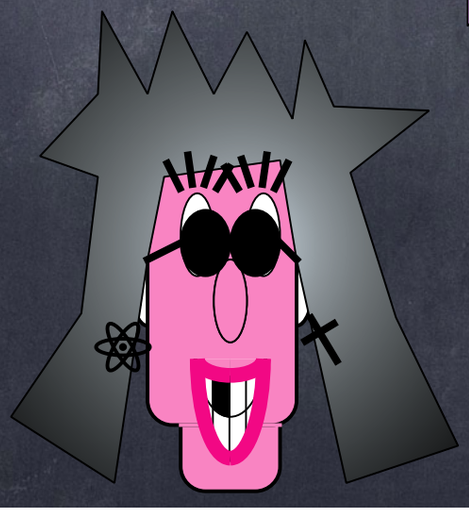




$c_1 \oplus k = m_1$
$c_2 \oplus k = m_2$

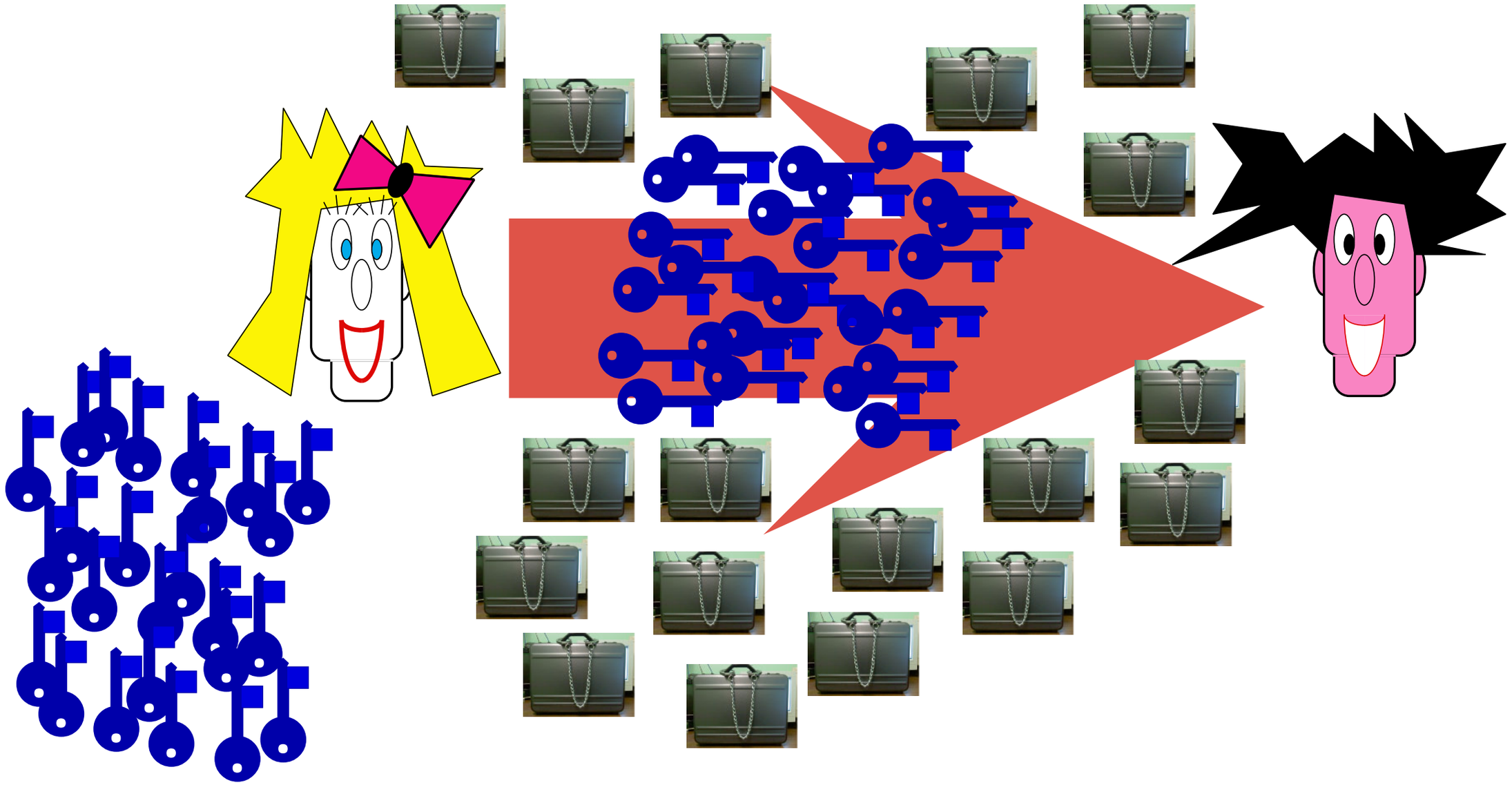
c_1

c_2



$c_1 \oplus c_2 = m_1 \oplus m_2$

Chiffrement à masques jetables



19e siècle

19e siècle

- Le chiffre de Beale (1822)

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975, 14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485, 604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370, 11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500, 538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283, 118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21, 24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131, 160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62, 116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568, 614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4, 30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461, 44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216, 728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5, 81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86, 36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985, 233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62, 194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895, 10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62, 31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31, 86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216, 548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56, 216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617, 84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18, 212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88, 612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132, 40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936, 447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216, 814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84, 221, 736, 820, 214, 11, 60, 760.

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56,
239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122,
106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140,
287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41,
78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196,
81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 191, 122, 43,
234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46,
10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28,
248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113,
140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107,
603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8,
14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53,
79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 515,
125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115,
48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121,
12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49,
47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2
270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31,
10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250,
557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106,
160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353,
320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11,
110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27,
8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25,
44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51,
50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140,
112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150,
112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811,
30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205,
185, 112, 125, 540, 65, 106, 807, 188, 96, 110, 16, 73, 33, 807, 150, 409, 400, 50,
154, 285, 96, 106, 316, 270, 205, 101, 811, 400, 8, 44, 37, 52, 40, 241, 34, 205,
38, 16, 46, 47, 85, 24, 44, 15, 64, 73, 138, 807, 85, 78, 110, 33, 420, 505, 53, 37,
38, 22, 31, 10, 110, 106, 101, 140, 15, 38, 3, 5, 44, 7, 98, 287, 135, 150, 96, 33, 84,
125, 807, 191, 96, 511, 118, 440, 370, 643, 466, 106, 41, 107, 603, 220, 275, 30,
150, 105, 49, 53, 287, 250, 208, 134, 7, 53, 12, 47, 85, 63, 138, 110, 21, 112, 140,
485, 486, 505, 14, 73, 84, 575, 1005, 150, 200, 16, 42, 5, 4, 25, 42, 8, 16, 811,
125, 160, 32, 205, 603, 807, 81, 96, 405, 41, 600, 136, 14, 20, 28, 26, 353, 302,
246, 8, 131, 160, 140, 84, 440, 42, 16, 811, 40, 67, 101, 102, 194, 138, 205, 51,
63, 241, 540, 122, 8, 10, 63, 140, 47, 48, 140, 288.

317, 8, 92, 73, 112, 89, 67, 318, 28, 96, 107, 41, 631, 78, 146, 397, 118, 98, 114, 246, 348, 116, 74, 88, 12, 65, 32, 14, 81, 19, 76, 121, 216, 85, 33, 66, 15, 108, 68, 77, 43, 24, 122, 96, 117, 36, 211, 301, 15, 44, 11, 46, 89, 18, 136, 68, 317, 28, 90, 82, 304, 71, 43, 221, 198, 176, 310, 319, 81, 99, 264, 380, 56, 37, 319, 2, 44, 53, 28, 44, 75, 98, 102, 37, 85, 107, 117, 64, 88, 136, 48, 154, 99, 175, 89, 315, 326, 78, 96, 214, 218, 311, 43, 89, 51, 90, 75, 128, 96, 33, 28, 103, 84, 65, 26, 41, 246, 84, 270, 98, 116, 32, 59, 74, 66, 69, 240, 15, 8, 121, 20, 77, 89, 31, 11, 106, 81, 191, 224, 328, 18, 75, 52, 82, 117, 201, 39, 23, 217, 27, 21, 84, 35, 54, 109, 128, 49, 77, 88, 1, 81, 217, 64, 55, 83, 116, 251, 269, 311, 96, 54, 32, 120, 18, 132, 102, 219, 211, 84, 150, 219, 275, 312, 64, 10, 106, 87, 75, 47, 21, 29, 37, 81, 44, 18, 126, 115, 132, 160, 181, 203, 76, 81, 299, 314, 337, 351, 96, 11, 28, 97, 318, 238, 106, 24, 93, 3, 19, 17, 26, 60, 73, 88, 14, 126, 138, 234, 286, 297, 321, 365, 264, 19, 22, 84, 56, 107, 98, 123, 111, 214, 136, 7, 33, 45, 40, 13, 28, 46, 42, 107, 196, 227, 344, 198, 203, 247, 116, 19, 8, 212, 230, 31, 6, 328, 65, 48, 52, 59, 41, 122, 33, 117, 11, 18, 25, 71, 36, 45, 83, 76, 89, 92, 31, 65, 70, 83, 96, 27, 33, 44, 50, 61, 24, 112, 136, 149, 176, 180, 194, 143, 171, 205, 296, 87, 12, 44, 51, 89, 98, 34, 41, 208, 173, 66, 9, 35, 16, 95, 8, 113, 175, 90, 56, 203, 19, 177, 183, 206, 157, 200, 218, 260, 291, 305, 618, 951, 320, 18, 124, 78, 65, 19, 32, 124, 48, 53, 57, 84, 96, 207, 244, 66, 82, 119, 71, 11, 86, 77, 213, 54, 82, 316, 245, 303, 86, 97, 106, 212, 18, 37, 15, 81, 89, 16, 7, 81, 39, 96, 14, 43, 216, 118, 29, 55, 109, 136, 172, 213, 64, 8, 227, 304, 611, 221, 364, 819, 375, 128, 296, 1, 18, 53, 76, 10, 15, 23, 19, 71, 84, 120, 134, 66, 73, 89, 96, 230, 48, 77, 26, 101, 127, 936, 218, 439, 178, 171, 61, 226, 313, 215, 102, 18, 167, 262, 114, 218, 66, 59, 48, 27, 19, 13, 82, 48, 162, 119, 34, 127, 139, 34, 128, 129, 74, 63, 120, 11, 54, 61, 73, 92, 180, 66, 75, 101, 124, 265, 89, 96, 126, 274, 896, 917, 434, 461, 235, 890, 312, 413, 328, 381, 96, 105, 217, 66, 118, 22, 77, 64, 42, 12, 7, 55, 24, 83, 67, 97, 109, 121, 135, 181, 203, 219, 228, 256, 21, 34, 77, 319, 374, 382, 675, 684, 717, 864, 203, 4, 18, 92, 16, 63, 82, 22, 46, 55, 69, 74, 112, 134, 186, 175, 119, 213, 416, 312, 343, 264, 119, 186, 218, 343, 417, 845, 951, 124, 209, 49, 617, 856, 924, 936, 72, 19, 28, 11, 35, 42, 40, 66, 85, 94, 112, 65, 82, 115, 119, 236, 244, 186, 172, 112, 85, 6, 56, 38, 44, 85, 72, 32, 47, 73, 96, 124, 217, 314, 319, 221, 644, 817, 821, 934, 922, 416, 975, 10, 22, 18, 46, 137, 181, 101, 39, 86, 103, 116, 138, 164, 212, 218, 296, 815, 380, 412, 460, 495, 675, 820, 952.

IN CONGRESS, JULY 4, 1776.

The unanimous Declaration of the thirteen united States of America,

When in the Course of human events, it becomes necessary for one people to dissolve the political bands which have connected them with another, and to assume among the powers of the earth, the separate and equal station to which the Laws of Nature and of Nature's God entitle them, a decent respect to the opinions of mankind requires that they should declare the causes which impel them to the separation. — 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 them shall seem most likely to effect their Safety and Happiness. Prudence, indeed, will dictate that Governments long established should not be changed for light and transient causes; and accordingly all experience hath shewn, that mankind are more disposed to suffer, while evils are sufferable, than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security. — Such has been the patient sufferance of these Colonies; and such is now the necessity which constrains them to alter their former Systems of Government. The history of the present King of Great Britain is a history of repeated injuries and usurpations, all having in direct object the establishment of an absolute Tyranny over these States. To prove this, let Facts be submitted to a candid world. — He has refused his Assent to Laws, the most wholesome and necessary for the public good. — He has forbidden his Governors to pass Laws of immediate and pressing importance, unless suspended in their operation till his Assent should be obtained; and when so suspended, he has utterly neglected to attend to them. — He has refused to pass other Laws for the accommodation of large districts of people, unless those people would relinquish the right of Representation in the Legislature, a right inestimable to them and formidable to tyrants only. — He has called together legislative bodies at places unusual, uncomfortable, and distant from the depository of their public Records, for the sole purpose of fatiguing them into compliance with his measures. — He has dissolved Representative Houses repeatedly, for opposing with manly firmness his invasions on the rights of the people. — He has refused for a long time, after such dissolutions, to cause others to be elected; whereby the Legislative powers, incapable of Annihilation, have returned to the People at large for their exercise; the State remaining in the mean time exposed to all the dangers of invasion from without, and convulsions within. — He has endeavoured to prevent the population of these States; for that purpose obstructing the Laws for Naturalization of Foreigners; refusing to pass others to encourage their migrations hither, and raising the conditions of new Appropriations of Lands. — He has obstructed the Administration of Justice, by refusing his Assent to Laws for establishing Judiciary powers. — He has made Judges dependent on his Will alone, for the tenure of their offices, and the amount and payment of their salaries. — He has erected a multitude of New Offices, and sent hither swarms of Officers to harass our people, and eat out their substance. — He has kept among us, in times of peace, Standing Armies without the consent of our legislatures. — He has affected to render the Military independent of and superior to the Civil power. — He has combined with others to subject us to a jurisdiction foreign to our constitution, and unacknowledged by our laws; giving his Assent to their Acts of pretended Legislation: — For Quartering large bodies of armed troops among us: — For protecting them, by a mock Trial, from punishment for any Murders which they should commit on the Inhabitants of these States: — For cutting off our Trade with all parts of the world: — For imposing Taxes on us without our Consent: — For depriving us in many cases, of the benefits of Trial by jury: — For transporting us beyond Seas to be tried for pretended offences: — For abolishing the free System of English Laws in a neighbouring Province, establishing therein an Arbitrary government, and enlarging its Boundaries so as to render it at once an example and fit instrument for introducing the same absolute rule into these Colonies: — For taking away our Charters, abolishing our most valuable Laws, and altering fundamentally the Forms of our Governments: — For suspending our own Legislatures, and declaring themselves invested with power to legislate for us in all cases whatsoever. — He has abdicated Government here, by declaring us out of his Protection and waging War against us. — He has plundered our seas, ravaged our Coasts, burnt our towns, and destroyed the lives of our people. — He is at this time transporting large Armies of foreign Mercenaries to compleat the works of death, desolation and tyranny, already begun with circumstances of Cruelty & perfidy scarcely paralleled in the most barbarous ages, and totally unworthy the Head of a civilized nation. — He has constrained our fellow Citizens taken Captive on the high Seas to bear Arms against their Country, to become the executioners of their friends and Brethren, or to fall themselves by their Hands. — He has excited domestic insurrections amongst us, and has endeavoured to bring on the inhabitants of our frontiers, the merciless Indian Savages, whose known rule of warfare, is an undistinguished destruction of all ages, sexes and conditions. In every stage of these Oppressions We have Petitioned for Redress in the most humble terms: Our repeated Petitions have been answered only by repeated injury. A Prince, whose character is thus marked by every act which may define a Tyrant, is unfit to be the ruler of a free people. Nor have We been wanting in attentions to our British brethren. We have warned them from time to time of attempts by their legislature to extend an unwarrantable jurisdiction over us. We have reminded them of the circumstances of our emigration and settlement here. We have appealed to their native justice and magnanimity, and we have conjured them by the ties of our common kindred to disavow these usurpations, which, would inevitably interrupt our connections and correspondence. They too have been deaf to the voice of justice and of consanguinity. We must, therefore, acquiesce in the necessity, which denounces our Separation, and hold them, as we hold the rest of mankind, Enemies in War, in Peace Friends. —

We, therefore, the Representatives of the united States of America, in General Congress, Assembled, appealing to the Supreme Judge of the world for the rectitude of our intentions, do, in the Name, and by Authority of the good People of these Colonies, solemnly publish and declare, That these United Colonies are, and of Right ought to be Free and Independent States; that they are Absolved from all Allegiance to the British Crown, and that all political connection between them and the State of Great Britain, is and ought to be totally dissolved; and that as Free and Independent States, they have full Power to levy War, conclude Peace, contract Alliances, establish Commerce, and to do all other Acts and Things which Independent States may of right do. — And for the support of this Declaration, with a firm reliance on the protection of divine Providence, we mutually pledge to each other our Lives, our Fortunes and our sacred Honor.

John Hancock

Button Gwinnett
Lyman Hall
Geo Walton.

Wm Hooper
Joseph Hewes,
John Penn

Edward Rutledge
Thos Heyward Junr.
Thomas Lynch Junr.
Arthur Middleton

Samuel Chase
Wm Paca
Thos Stone
Charles Carroll of Carrollton

George Wythe
Richard Henry Lee
Th Jefferson
Benj Harrison
Thos Nelson jr.
Francis Lightfoot Lee
Carter Braxton

Robt Morris
Benjamin Rush
Benj Franklin
John Morton
Geo Clymer
Jas Smith
Geo Taylor
James Wilson
Geo Ross

Caesar Rodney
Geo Read
Tho M:Kean

Wm Floyd
Phil. Livingston
Fras Lewis
Lewis Morris

Richd Stockton
Jno Witherspoon
Fras Hopkinson
John Hart
Abra Clark

Josiah Bartlett
Wm Whipple

Saml Adams
John Adams
Robt Treat Paine
Elbridge Gerry

Step Hopkins
William Ellery

Roger Sherman
Sam'el Huntington
Wm Williams
Oliver Wolcott
Matthew Thornton

N.J. STONE SC. WASH.

J'ai déposé dans le comté de Bedford, à quatre miles environ de Buford, dans une excavation ou caverne à six pieds au-dessous du sol, les choses suivantes, appartenant aux personnes dont les noms figurent sur la page ci-jointe:
Le premier dépôt, de novembre 1819, consiste en mille quatorze livres d'or, et trois mille huit cent douze livres d'argent. Le second fut fait en décembre 1821 et consiste en mille neuf cent livres d'or et mille deux cent quatre vingt huit livres d'argent; ainsi que des bijoux, échangés à Saint Louis contre l'argent pour simplifier le transport, et estimés à 13 000 dollars.
Les biens ci-dessus sont enfermés à l'abri dans des récipients de fer, munis de couvercles de fer. La caverne est grossièrement tapissée de pierres, et les récipients sont posés sur un bloc de pierre, et couverts par d'autres. La feuille n°1 décrit l'emplacement exact de la caverne, afin qu'elle puisse être trouvée sans difficulté.

J'ai déposé dans le comté de Bedford, à quatre miles environ de Buford, dans une excavation ou caverne à six pieds au-dessous du sol, les choses suivantes, appartenant aux personnes dont les noms figurent sur la page ci-jointe:
Le premier dépôt, de novembre 1819, consiste en mille quatorze livres d'or, et trois mille huit cent douze livres d'argent. Le second fut fait en décembre 1821 et consiste en mille neuf cent livres d'or et mille deux cent quatre vingt huit livres d'argent; ainsi que des bijoux, échangés à Saint Louis contre l'argent pour simplifier le transport, et estimés à 13 000 dollars.
Les biens ci-dessus sont enfermés à l'abri dans des récipients de fer, munis de couvercles de fer. La caverne est grossièrement tapissée de pierres, et les récipients sont posés sur un bloc de pierre, et couverts par d'autres. La feuille n°1 décrit l'emplacement exact de la caverne, afin qu'elle puisse être trouvée sans difficulté.

J'ai déposé dans le comté de Bedford, à quatre miles environ de Buford, dans une excavation ou caverne à six pieds au-dessous du sol, les choses suivantes, appartenant aux personnes dont les noms figurent sur la page ci-jointe:
Le premier dépôt, de novembre 1819, consiste en mille quatorze livres d'or, et trois mille huit cent douze livres d'argent. Le second fut fait en décembre 1821 et consiste en mille neuf cent livres d'or et mille deux cent quatre vingt huit livres d'argent; ainsi que des bijoux, échangés à Saint Louis contre l'argent pour simplifier le transport, et estimés à 13 000 dollars.
Les biens ci-dessus sont enfermés à l'abri dans des récipients de fer, munis de couvercles de fer. La caverne est grossièrement tapissée de pierres, et les récipients sont posés sur un bloc de pierre, et couverts par d'autres. La feuille n°1 décrit l'emplacement exact de la caverne, afin qu'elle puisse être trouvée sans difficulté.

19e siècle

- Le chiffre de Beale (1822)

19e siècle

- Le chiffre de Beale (1822)
- Motivation civile : le télégraphe (1839)

19e siècle

- Le chiffre de Beale (1822)
- Motivation civile : le télégraphe (1839)
- Motivation militaire :
  TSF - télégraphie sans fil (1896)

Première Guerre

Première Guerre

- Woodrow Wilson (président des É-U) refusait d'entrer en guerre

Première Guerre

- Woodrow Wilson (président des É-U) refusait d'entrer en guerre
- Le télégramme de Zimmermann

WESTERN UNION TELEGRAM

Read the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13805 3494 14936
98092 5905 11311 10392 10371 0302 21290 5181 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4459 5905 17166 13851 4458 17149 14471 6706
13850 13224 6929 14991 7382 15857 67893 14218 36477
[illegible] 17553 67893 5970 5454 16102 15217 22801 17138
[illegible] 17388 7116 23638 18282 6719 14331 15021 23845
[illegible] 23552 22096 21604 4707 9497 22464 20855 4377
[illegible] 18140 22260 5905 13347 20420 39689 13732 20607
[illegible] 5578 18507 52262 1340 22049 13339 11265 22295
10439 14614 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9569 22464 15674 18502 18500 15857
218[illegible] 5376 7381 98092 18127 13486 9360 9220 76036 14219
5144 2831 17920 11347 17142 11364 7667 7768 15099 9110
10482 97556 3569 3070

REPEATED

Charge German Embassy.

16 janvier 1917

TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, ~~invite~~ Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, ~~invite~~ Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

DECLASSIFIED
Letter 1-8-58
W. R. Emerson, State Dept.
By Mary E. Eckhoff Archivist
Date Oct. 22, 1958

TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, ~~invite~~ Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Deuxième Guerre

- Arthur Scherbius dès 1923 !

Patented Jan. 24, 1928. 1,657,411

UNITED STATES PATENT OFFICE.

ARTHUR SCHERBIUS, OF BERLIN-WILMERSDORF, GERMANY, ASSIGNOR, BY MESNE ASSIGNMENTS, TO CHIFFRIERMASCHINEN AKTIENGESELLSCHAFT, OF BERLIN, GERMANY; A CORPORATION OF GERMANY.

CIPHERING MACHINE.

Application filed February 6, 1923, Serial No. 617,352, and in Germany February 11, 1922.

It has already been proposed to use for ciphering of a clear text and for deciphering machines which either type the ciphered letters in a similar manner to that of a typewriting machine or which produce a ciphered perforated cable tape or operate an indicating device. The operation of machines of this type is based for instance on the interchanging of the closed circuits between the keys marked with the letters of the alphabet and the type levers or the levers of a perforator for cable tapes each time after the sending of one or more of a determined number of letters. As soon as with two machines of this type this interchange, which is per se irregular, is effected in exactly the same manner, a telegram which has been ciphered with the aid of one machine can be deciphered with the aid of a corresponding machine. A condition is however that the number of letters counted from the same starting position has remained the same. At the sending of telegrams, especially with wireless telegraphy, one must however count upon the accidental omission of certain letters or groups of letters. The machine which is used in such a case for deciphering is thus unsynchronized, so that not only the letters which have been omitted but also all the succeeding text cannot be deciphered any more.

According to the invention this defect is avoided or at least restricted greatly by providing that the machine is reversed after the repeated sending of the same letter. The device which serves for counting the length of the row of letters may continue to operate, if this should be desirable for any reason, if the same letter is repeated each time for a determined number of times. It would be still better to reverse the machine in such a manner that it types clear text, the mechanism which effects the interchange of letters being stopped, wherefrom results the advantage that in the clear text an easily recognizable message can be given and that after the sending of this message the ciphering can be continued with the machine which during this sending has not been adjusted for sending code. Such a message can consist for instance of a check member, or if desired the number of letters which have been sent up to this moment. For each series of letters a new key indication might be selected on the machine which key indication for safety's sake would be sent in the clear text several times. Service regulations might further be inserted. Clear text might further be signalized by special signs, for instance by spaced type.

In order to make the invention clearly understood I shall proceed to describe the same with reference to the accompanying drawing wherein:

Fig. 1 shows by way of example a ciphering machine according to this invention.

Figure 2 is an edge elevation of one of the

Patented Jan. 24, 1928. 1,657,411

UNITED STATES PATENT OFFICE.

ARTHUR SCHERBIUS, OF BERLIN-WILMERSDORF, GERMANY, ASSIGNOR, BY MESNE ASSIGNMENTS, TO CHIFFRIERMASCHINEN AKTIENGESELLSCHAFT, OF BERLIN, GERMANY; A CORPORATION OF GERMANY.

CIPHERING MACHINE.

Application filed February 6, 1923, Serial No. 617,352, and in Germany February 11, 1922.

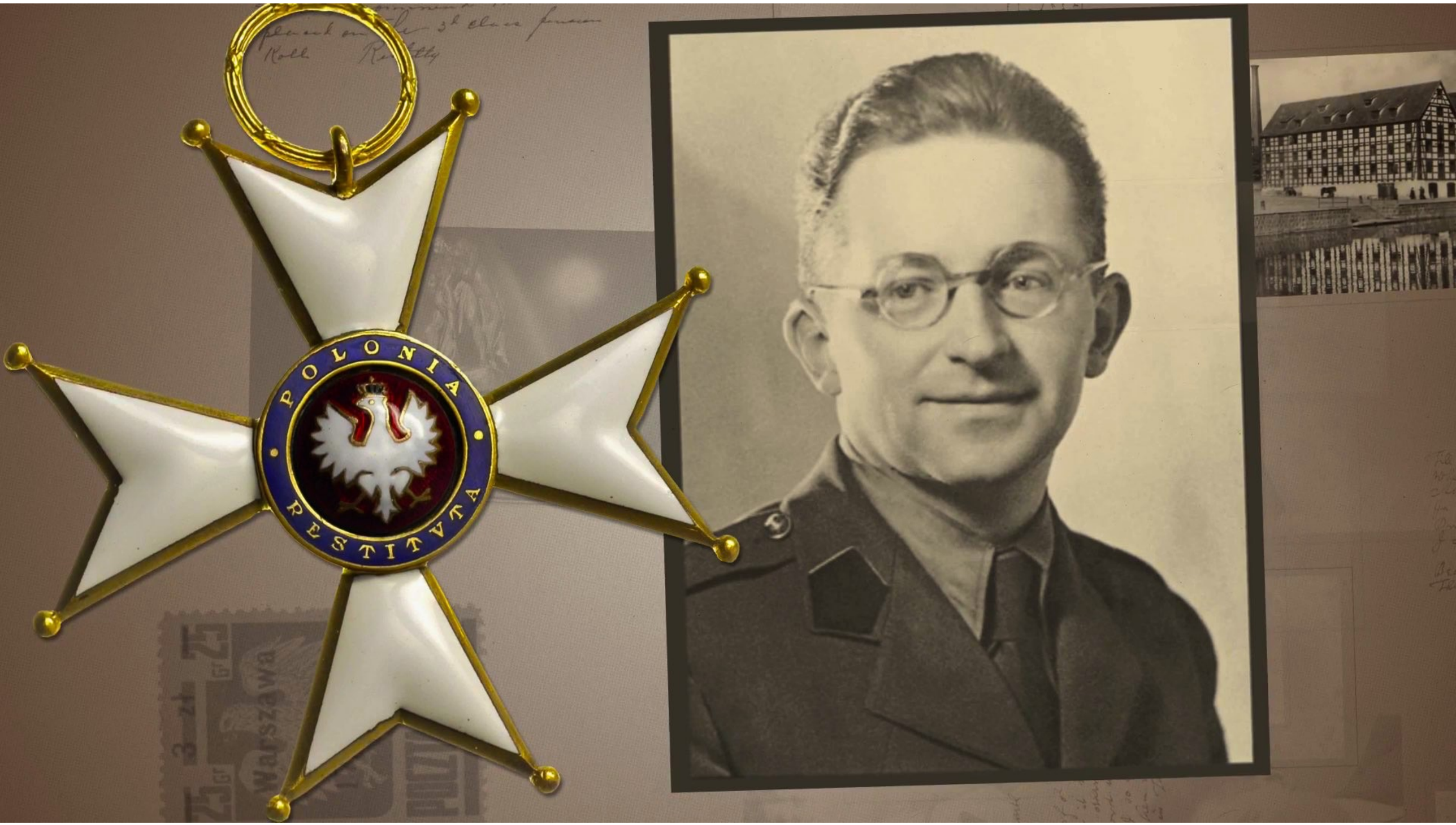

T244
Nur Glühlampen mit 12 mm Durchmesser verwenden.

Deuxième Guerre

- Arthur Scherbius dès 1923

Deuxième Guerre

- Arthur Scherbius dès 1923 !
- Marian Rejewski en Pologne



Marian Adam Rejewski

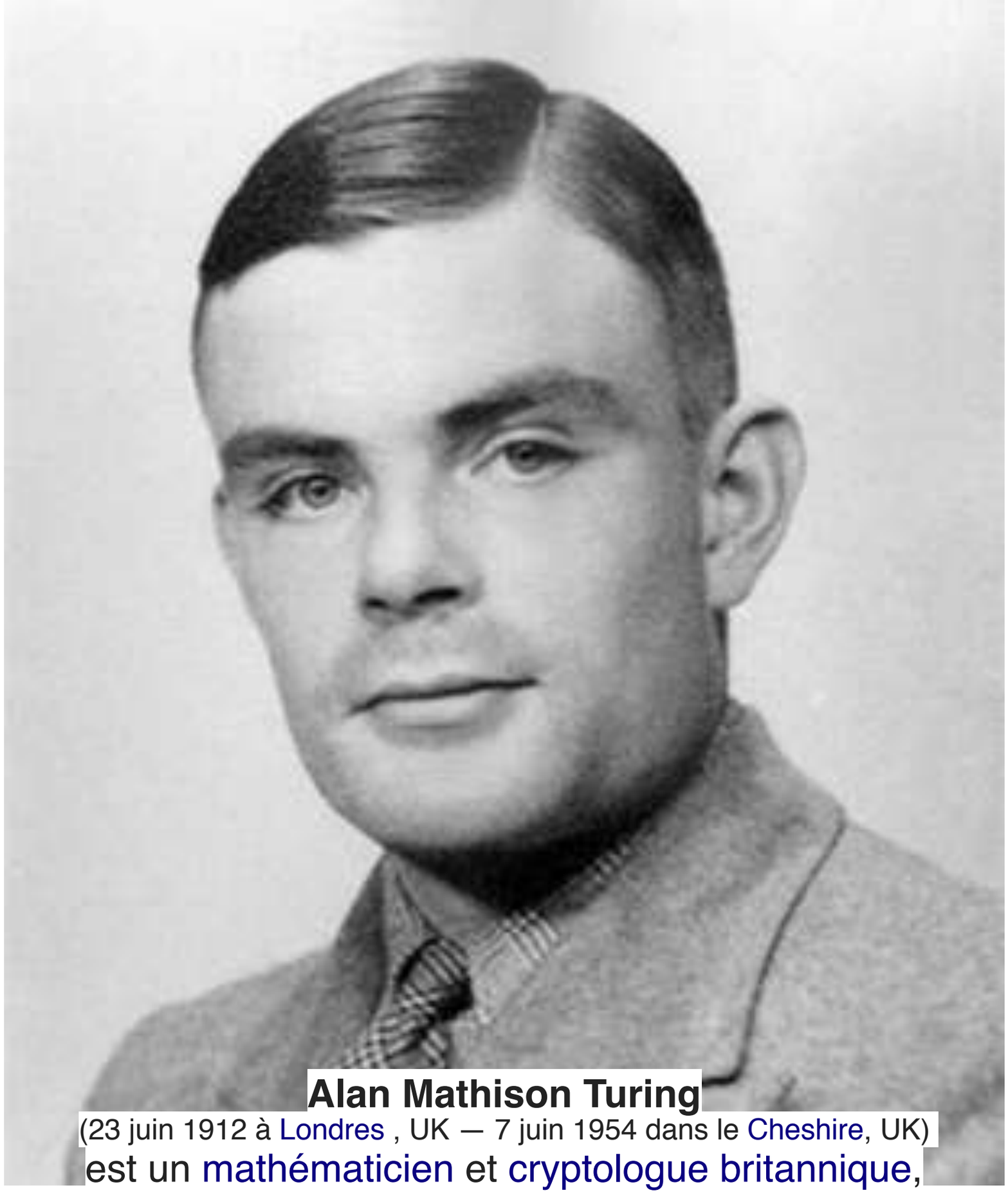
(16 août 1905 à Bydgoszcz, Pologne – 13 février 1980 à Varsovie)
est un cryptologue polonais. Il est à l'origine de la première attaque cryptanalytique sur la machine Enigma au début des années 1930.

Deuxième Guerre

- Arthur Scherbius dès 1923 !
- Marian Rejewski en Pologne

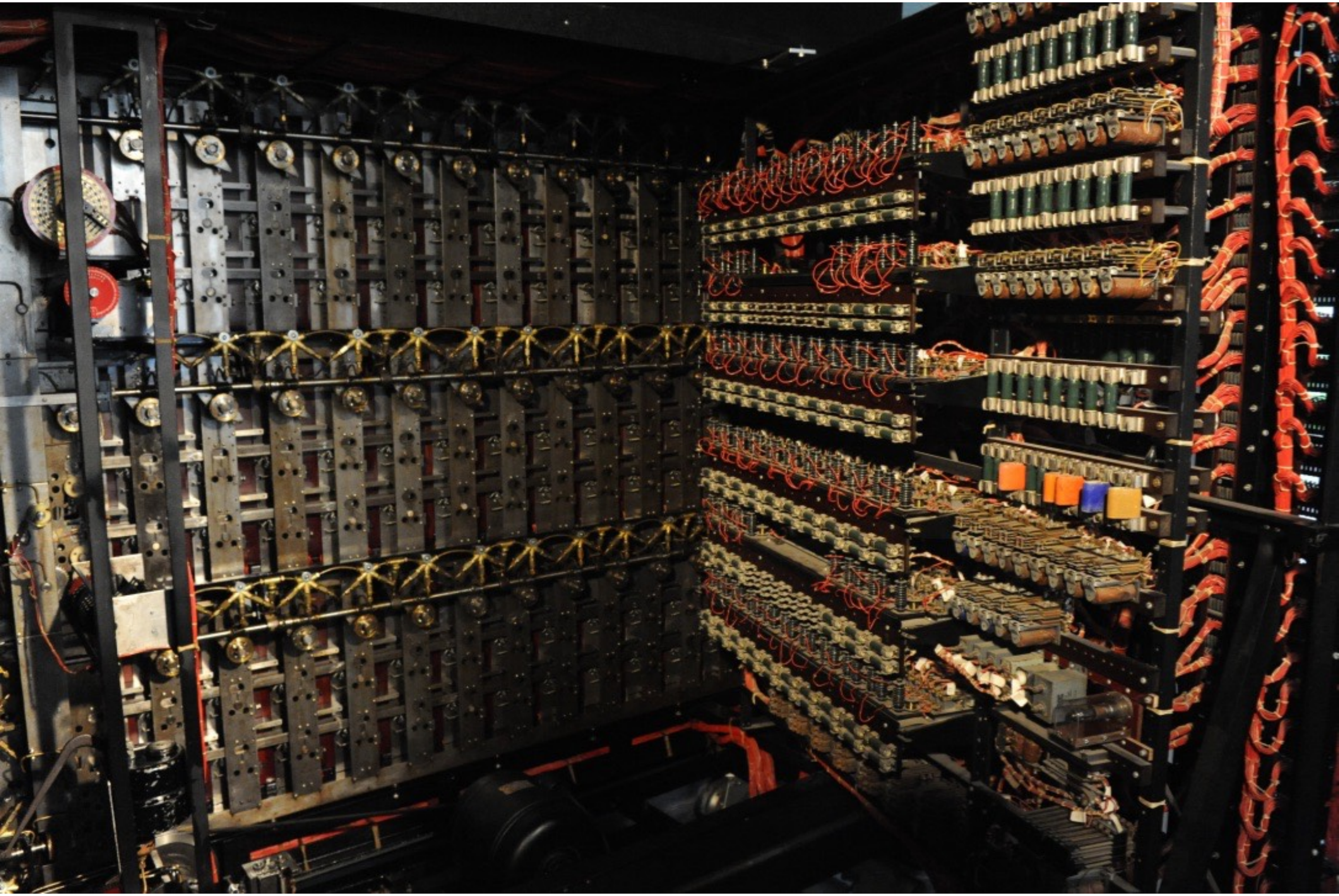
Deuxième Guerre

- Arthur Scherbius dès 1923 !
- Marian Rejewski en Pologne
- Alan Turing à Bletchley Park



Alan Mathison Turing
(23 juin 1912 à Londres , UK — 7 juin 1954 dans le Cheshire, UK)
est un mathématicien et cryptologue britannique,
auteur de travaux qui fondent scientifiquement l'informatique.


BLETCHLEY PARK,
SEPT 2017



Deuxième Guerre

- Arthur Scherbius dès 1923 !
- Marian Rejewski en Pologne
- Alan Turing à Bletchley Park

Deuxième Guerre

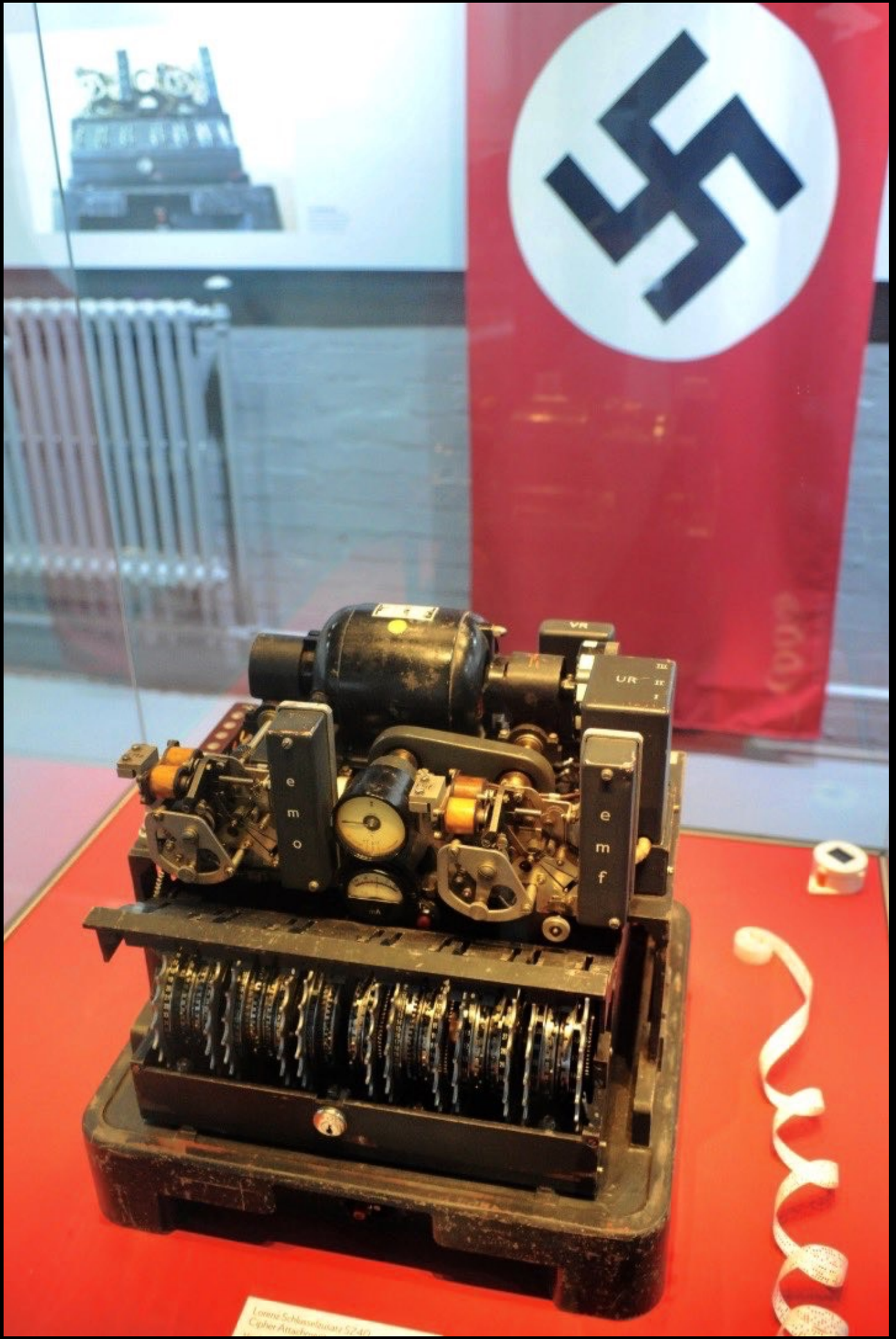
- Arthur Scherbius dès 1923 !
- Marian Rejewski en Pologne
- Alan Turing à Bletchley Park

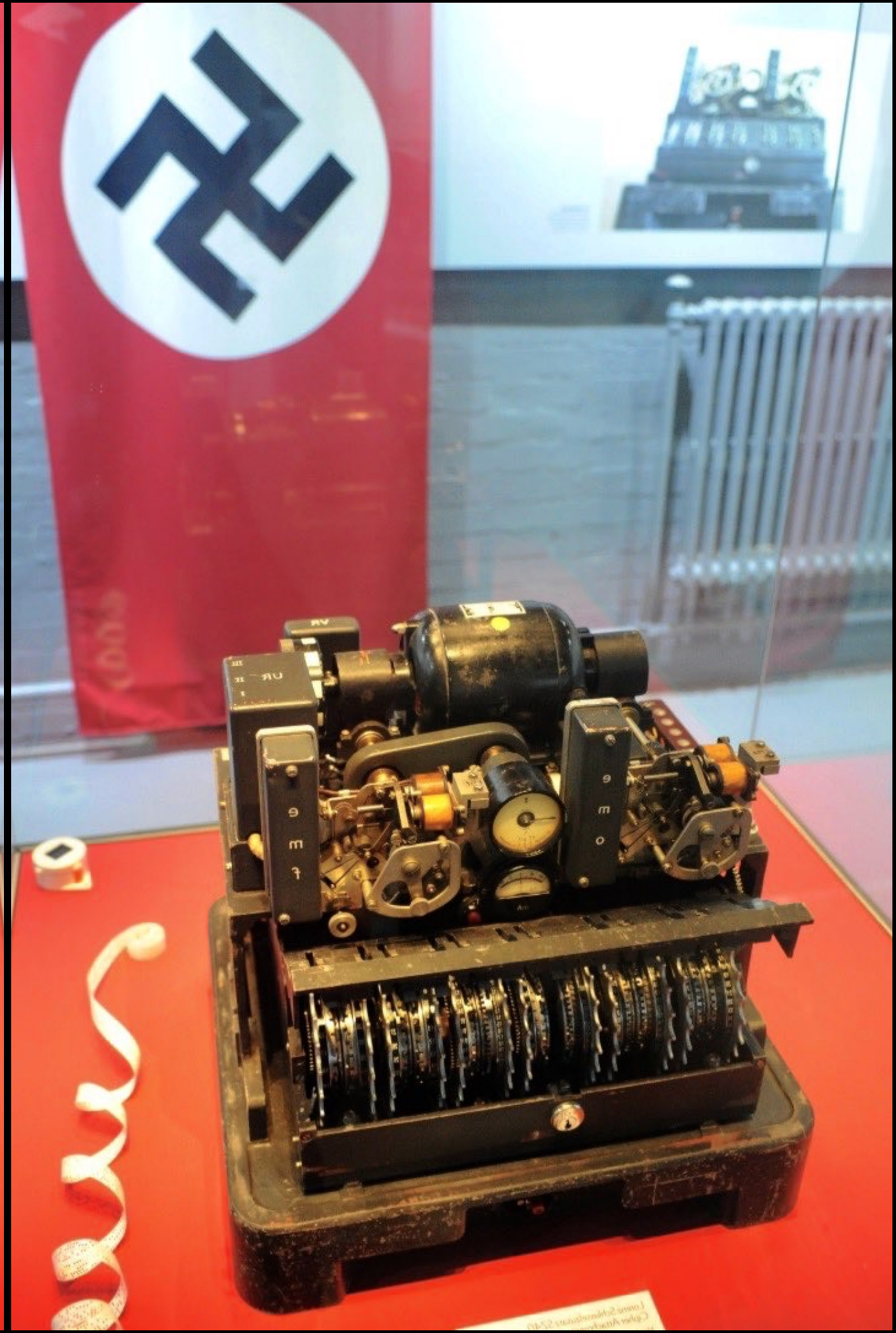
Deuxième Guerre

- Arthur Scherbius dès 1923 !
- Marian Rejewski en Pologne
- Alan Turing à Bletchley Park

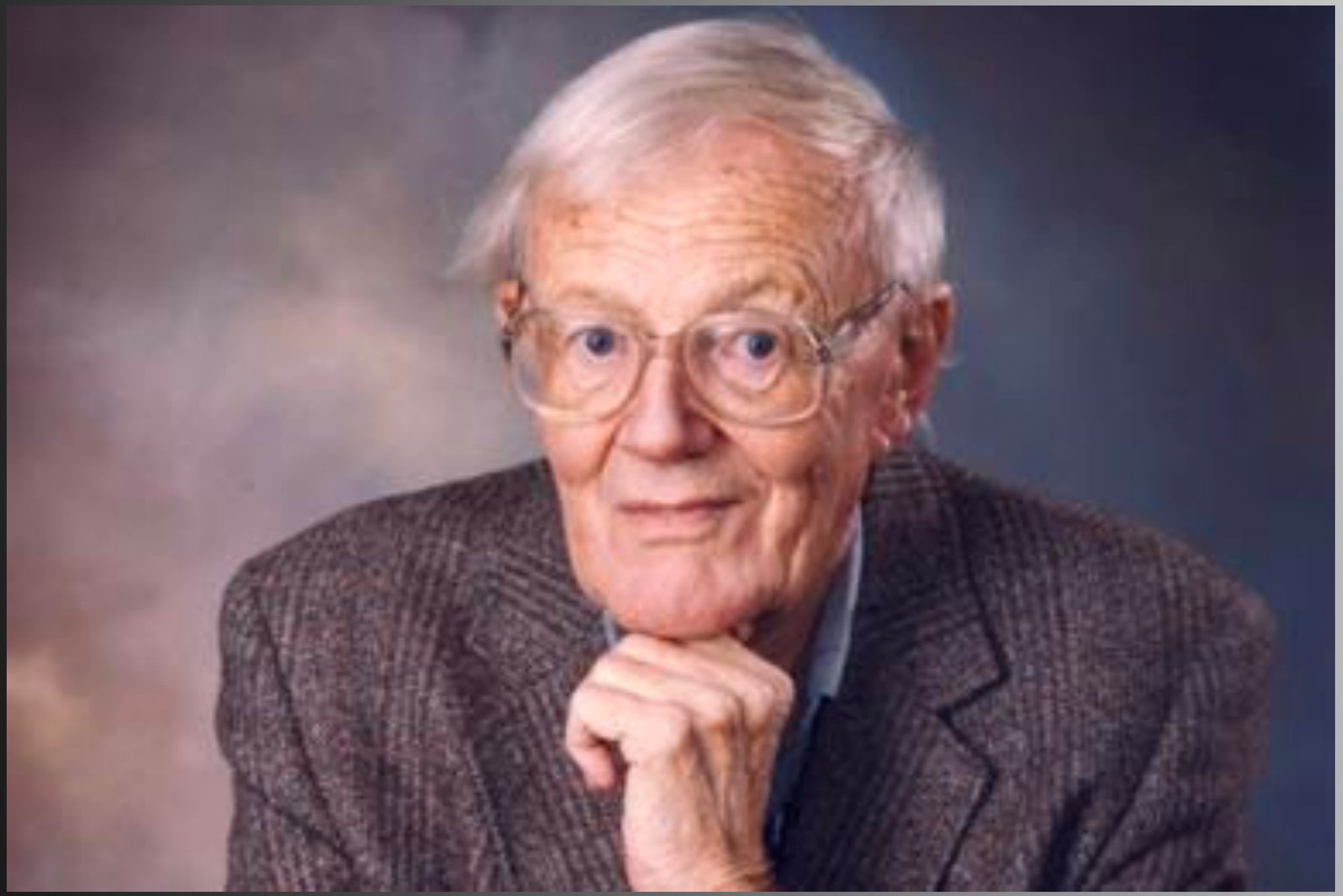
Deuxième Guerre

- Arthur Scherbius dès 1923 !
- Marian Rejewski en Pologne
- Alan Turing à Bletchley Park
- Chiffre de Lorentz


VR
UR
III
II
I
e
m
o
e
m
f


VR
UR
III
II
I
e
m
o
e
m
f

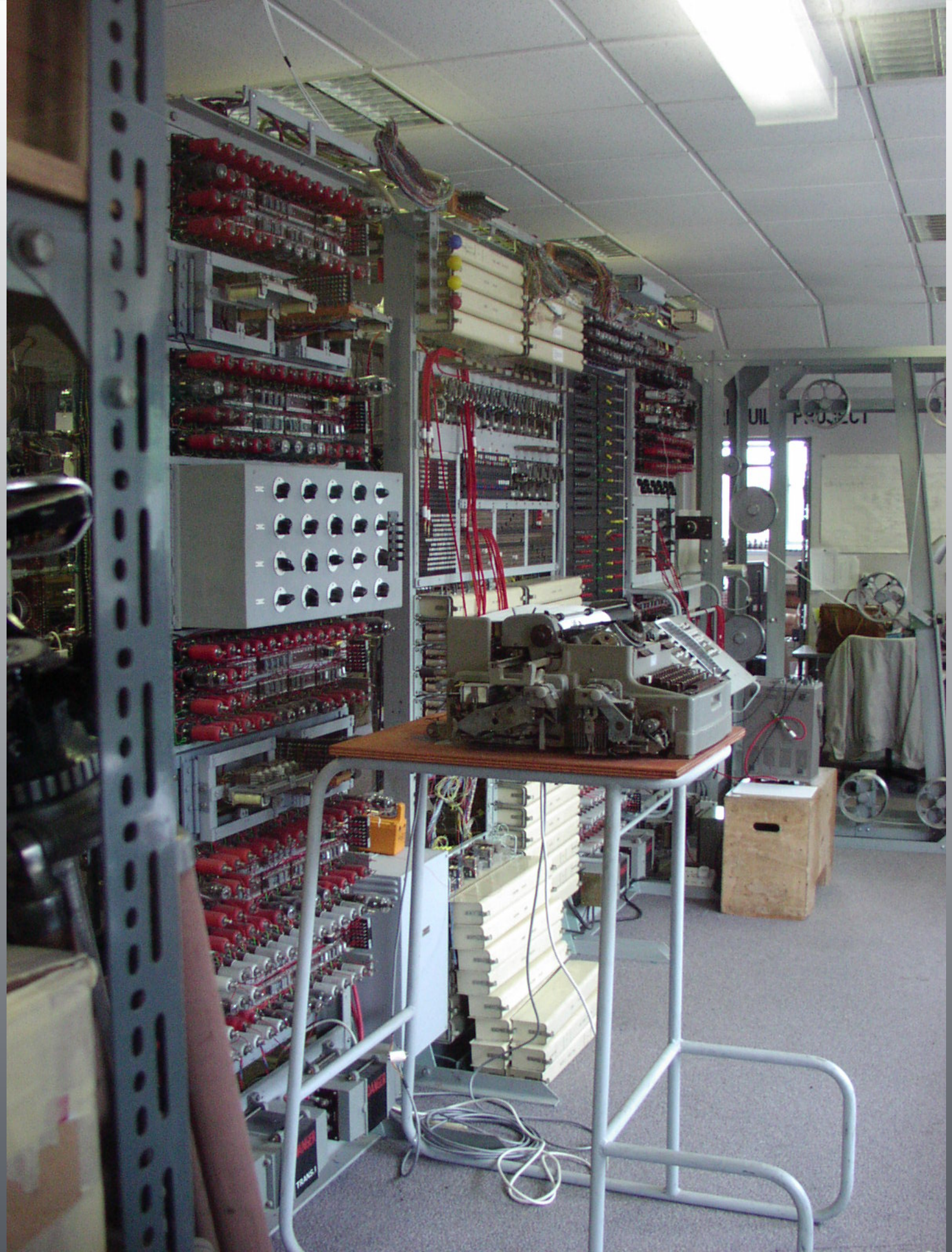

Motor
Schnell



WILLIAM TUTTE

Deuxième Guerre

- Arthur Scherbius dès 1923 !
- Marian Rejewski en Pologne
- Alan Turing à Bletchley Park
- Chiffre de Lorentz
- Colossus : Le premier ordinateur électronique programmable



Aujourd'hui ?

Advanced Encryption Standard (AES)

Devenu standard américain en 2001

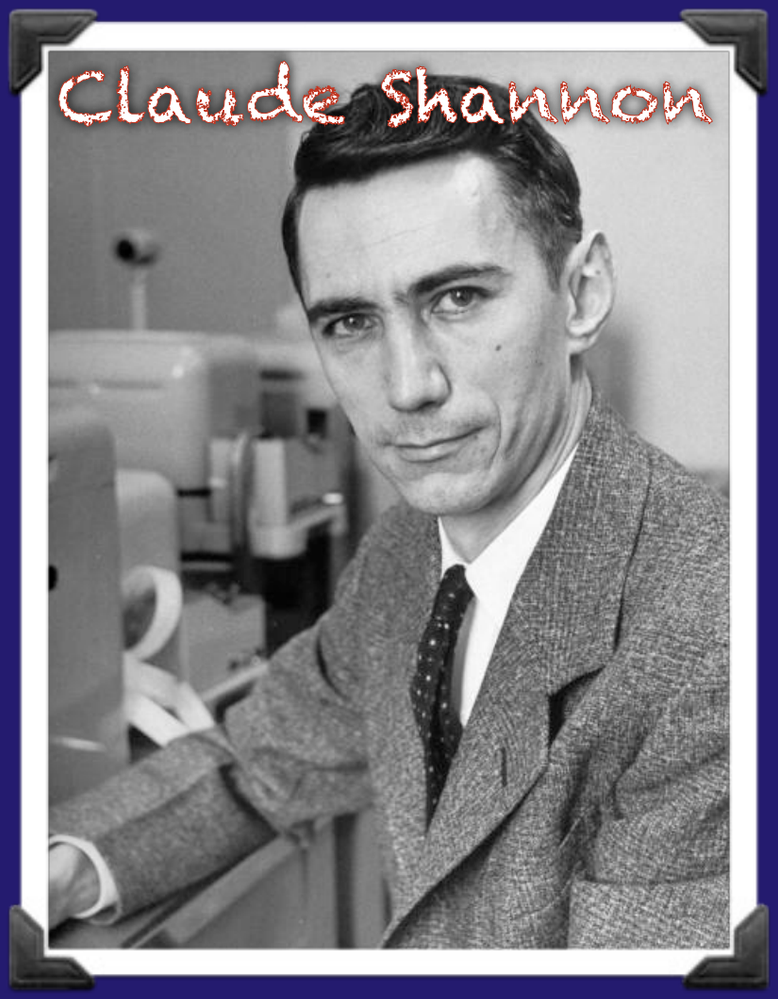
Sécuritaire ? On ne sait pas !

Masque jetable (one-time-pad)

Inventé par Frank Miller en 1882

Sécuritaire de façon parfaite !

Cryptographie



informationelle

1950

Deux questions

Comment utiliser
une clef secrète ?

Chiffrement et déchiffrement

Comment obtenir cette clef ?

Établissement de la clef

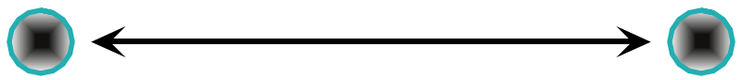
Deux questions

Comment obtenir cette clef ?

Établissement de la clef

La malédiction quadratique

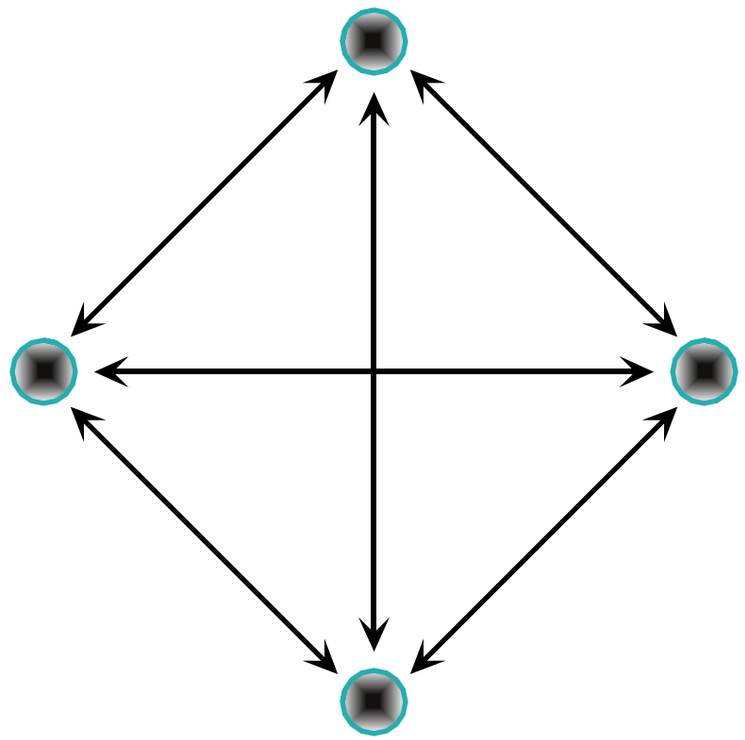
2 utilisateurs



1 clef secrète

La malédiction quadratique

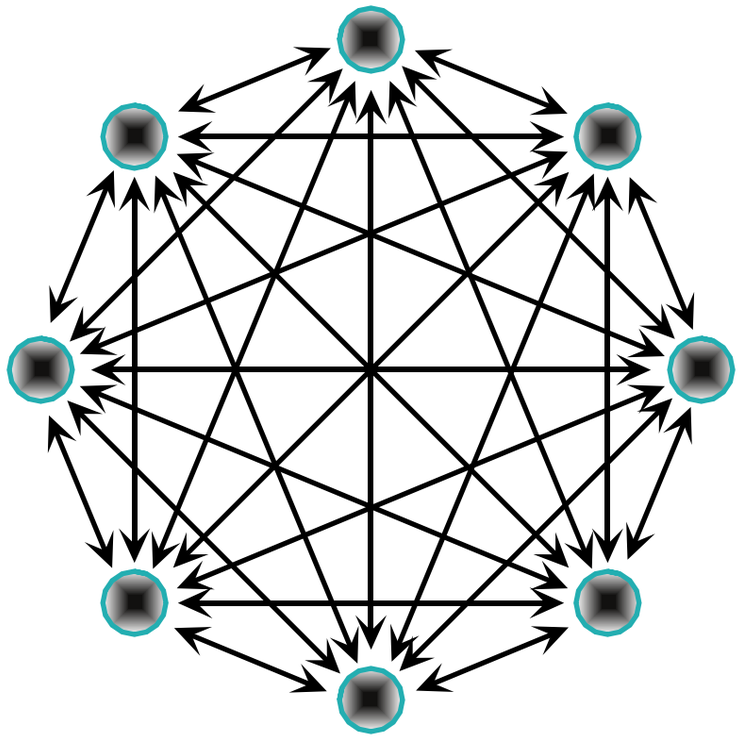
4 utilisateurs



6 clefs secrètes

La malédiction quadratique

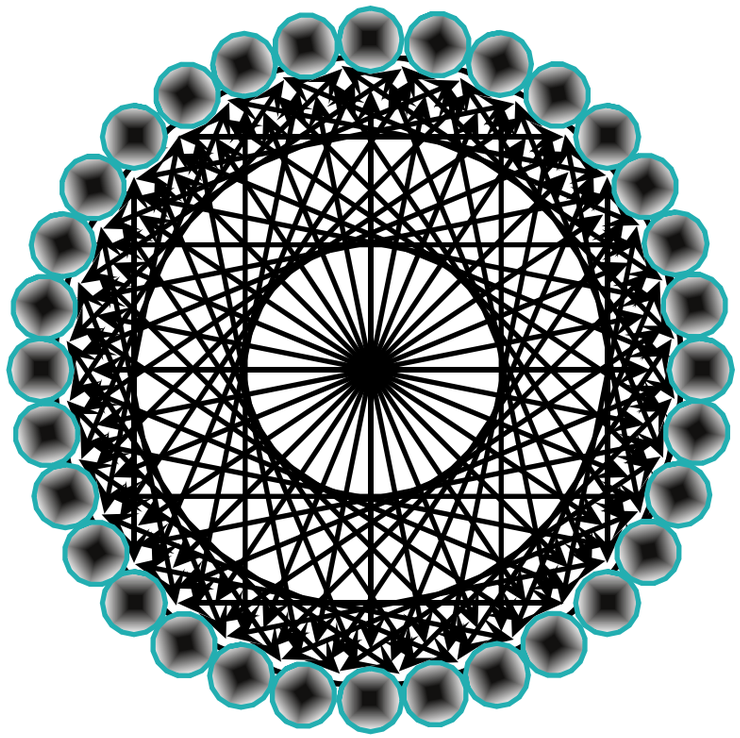
8 utilisateurs



28 clefs secrètes

La malédiction quadratique

n utilisateurs

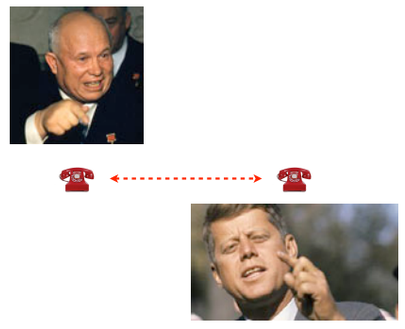


$n(n\text{-}1)/_2$ clefs secrètes

Établissement de clef

Comment peut-on établir une clef secrète ?

Tiers de confiance



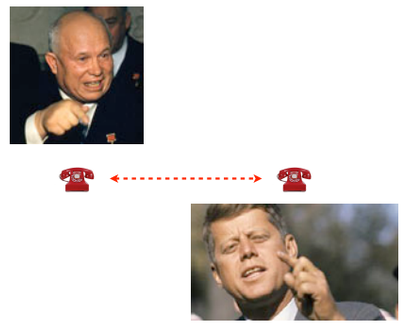
Sécurité calculatoire

Physique quantique

Établissement de clef

Comment peut-on établir une clef secrète ?

Tiers de confiance



Sécurité calculatoire

Physique quantique

Établissement de clef

Établissement de clef

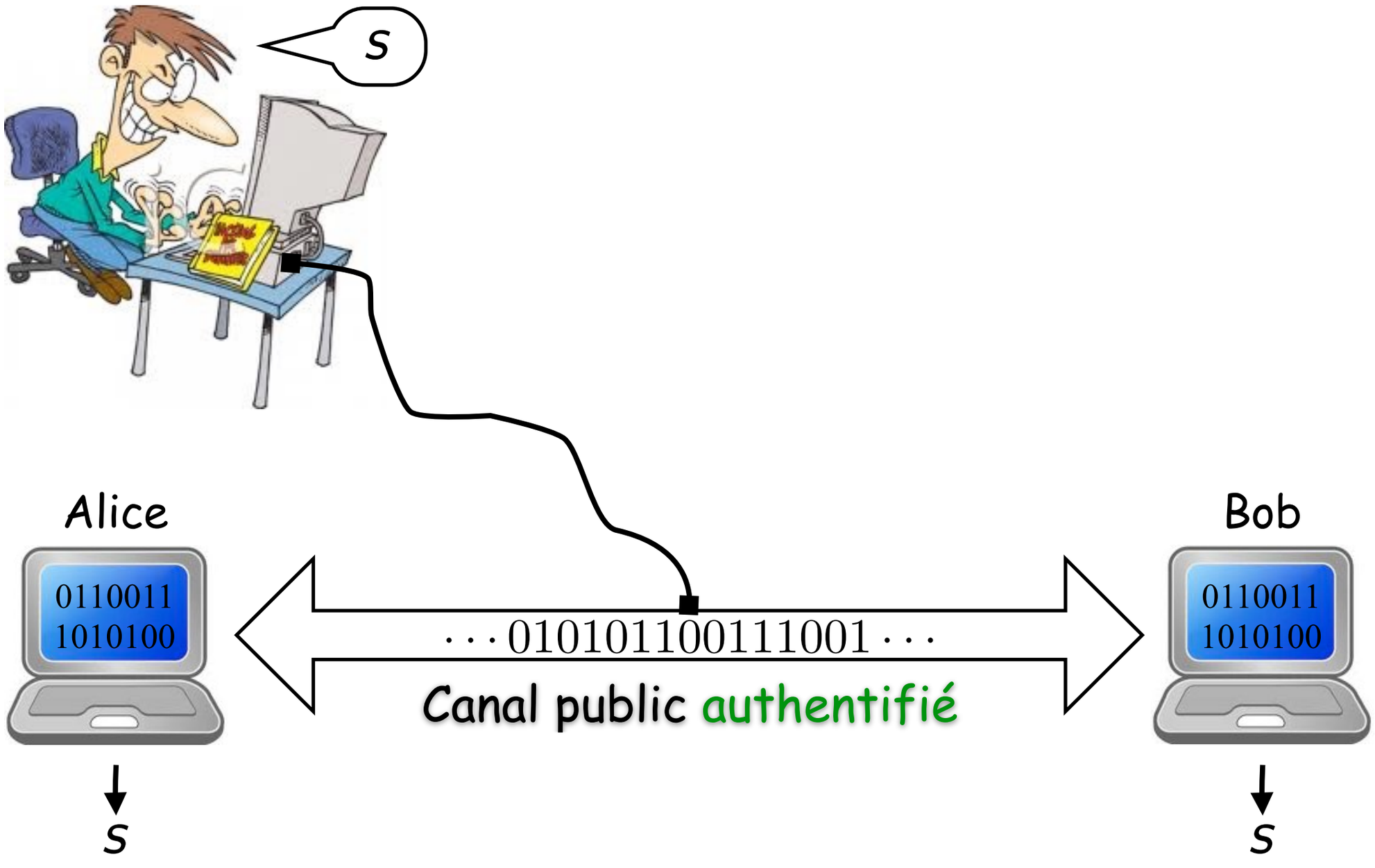
Alice

Bob

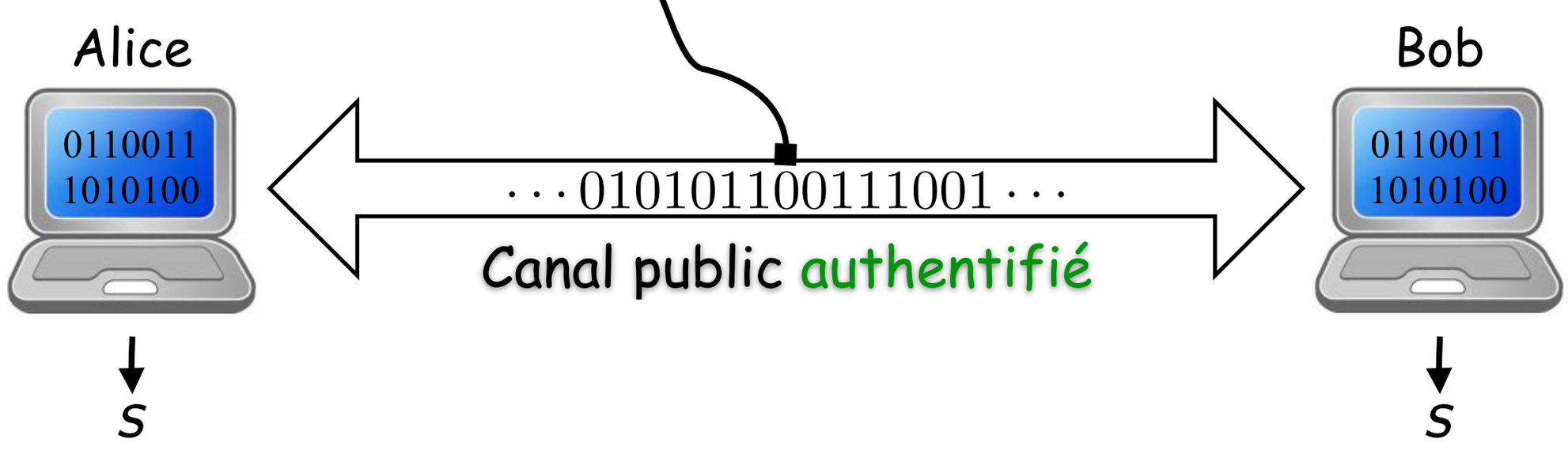
Établissement de clef

Établissement de clef

Établissement de clef

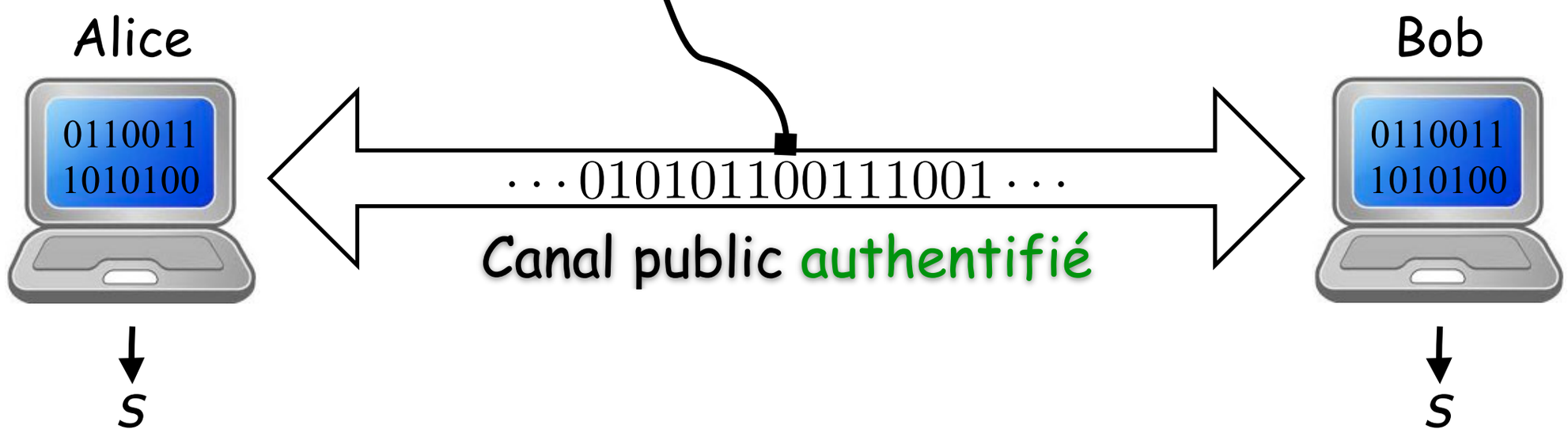


Établissement de clef



Établissement de clef

Magie noire ?

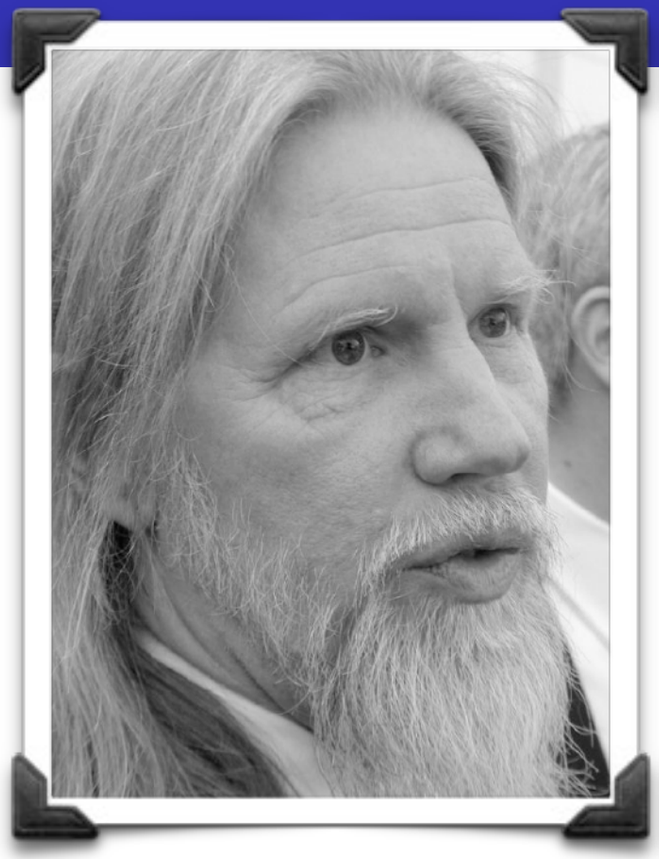


Sécurité calculatoire

Sécurité calculatoire

Diffie et Hellman (1976)

Sécurité calculatoire



Diffie et Hellman (1976)

Sécurité calculatoire

Diffie et Hellman (1976)

Sécurité calculatoire

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Sécurité calculatoire

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Sécurité calculatoire

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Sécurité calculatoire

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Sécurité calculatoire

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Sécurité calculatoire

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Sécurité calculatoire

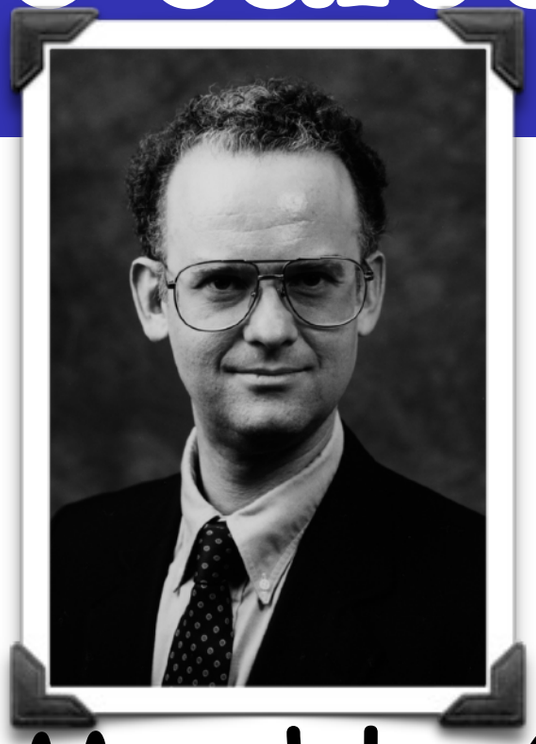
Ralph Merkle (1974)

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Sécurité calculatoire



Ralph Merkle (1974)

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Sécurité calculatoire

Ralph Merkle (1974)

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Sécurité calculatoire

Clifford Cocks (1973)

Ralph Merkle (1974)

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Sécurité calculatoire

Clifford Cocks (1973)

Ralph Merkle (1974)

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Sécurité calculatoire

Clifford Cocks (1973)

Ralph Merkle (1974)

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Sécurité calculatoire

James Ellis (1970)

Clifford Cocks (1973)

Ralph Merkle (1974)

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Sécurité calculatoire

James Ellis (1970)

Clifford Cocks (1973)

Ralph Merkle (1974)

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Sécurité calculatoire

James Ellis (1970)

Clifford Cocks (1973)

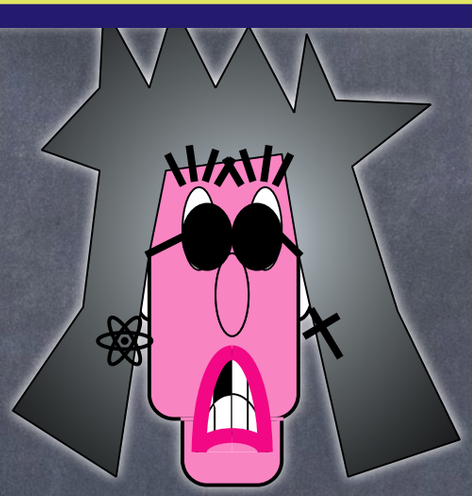
Ralph Merkle (1974)

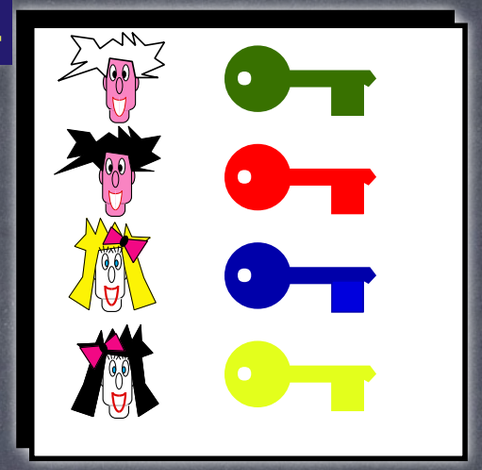
Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

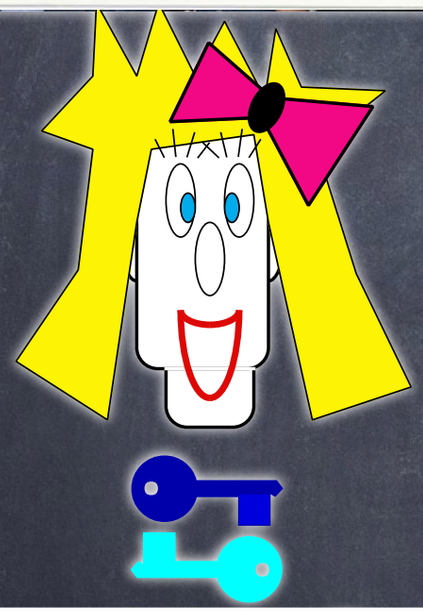
Robert McEliece (1978)

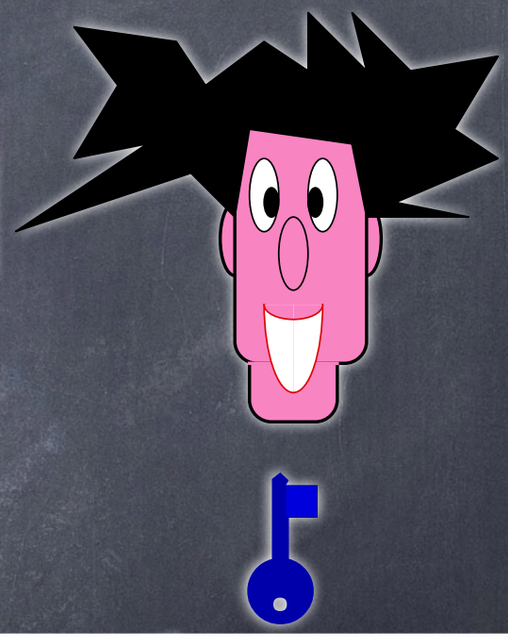
Chiffrement à clef publique



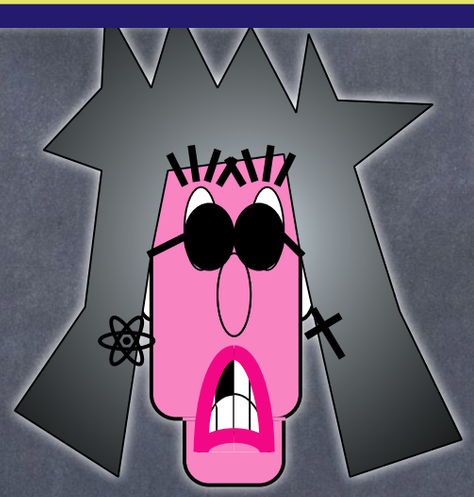


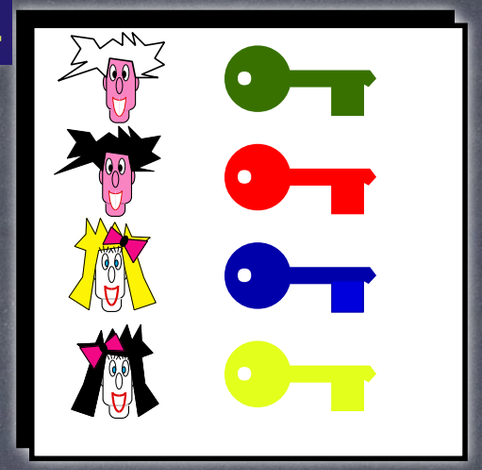
8RdewtU5qkLa$es!T9@



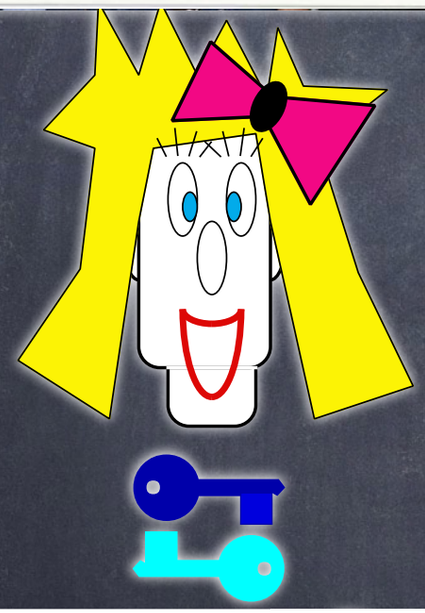


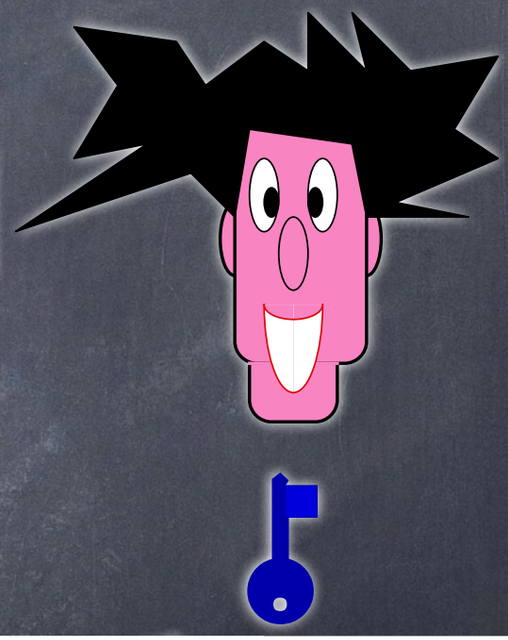
Chiffrement à clef publique





8RdewtU5qkLa$es!T9@



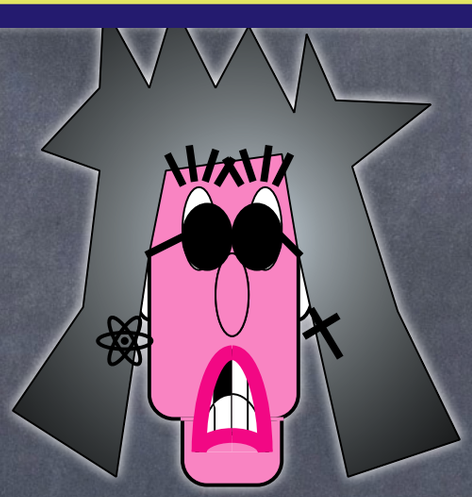


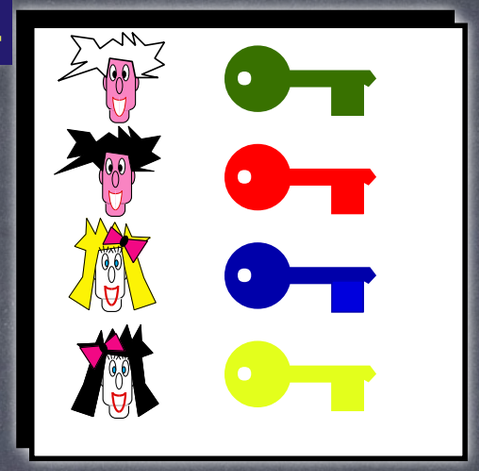
Chiffrement

8RdewtU5qkLa$

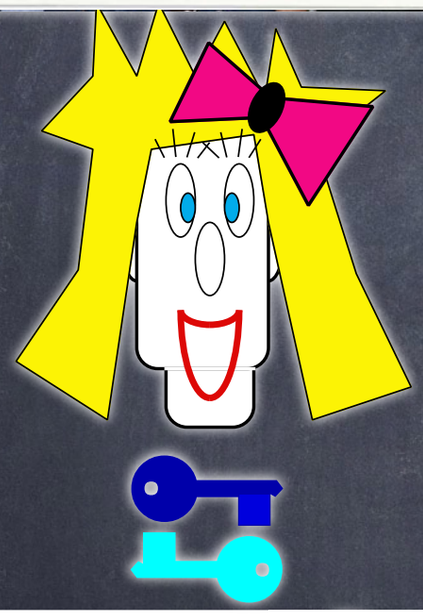
pouser?

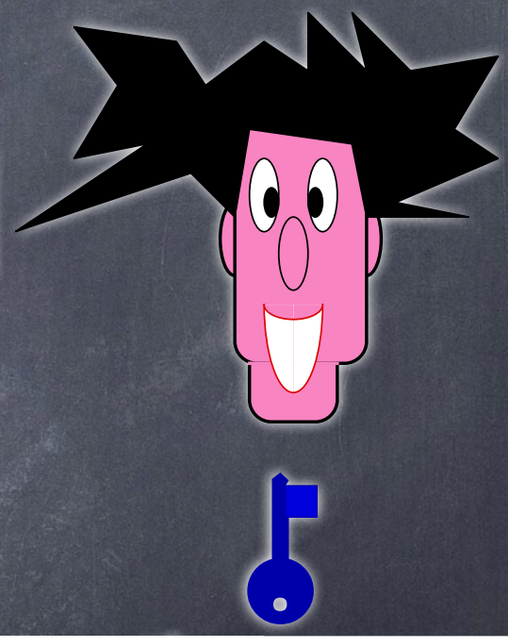
Chiffrement à clef publique



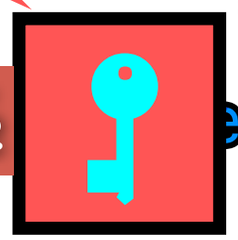


8RdewtU5qkLa$es!T9@

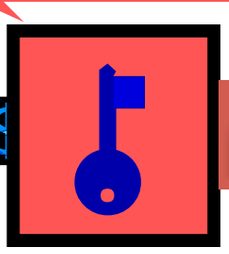




Déchiffrement

Veux-tu m'é  es!T9@

Chiffrement

8RdewtU5qkLa$  pouser?

La grande question

La grande question

Nous vivons dans un monde quantique

La grande question

Nous vivons dans un monde quantique

Est-ce une bénédiction

pour les faiseurs de codes?

La grande question

Nous vivons dans un monde quantique

Est-ce une bénédiction
ou une malédiction
pour les faiseurs de codes?

Algorithme de Shor

Algorithme de Shor

Algorithme de Shor

Factorise les grands nombres efficacement

Algorithme de Shor

Factorise les grands nombres efficacement

Extrait les logarithmes discrets efficacement

Algorithme de Shor

Factorise les grands nombres efficacement

Extrait les logarithmes discrets efficacement même dans les courbes elliptiques

Algorithme de Shor

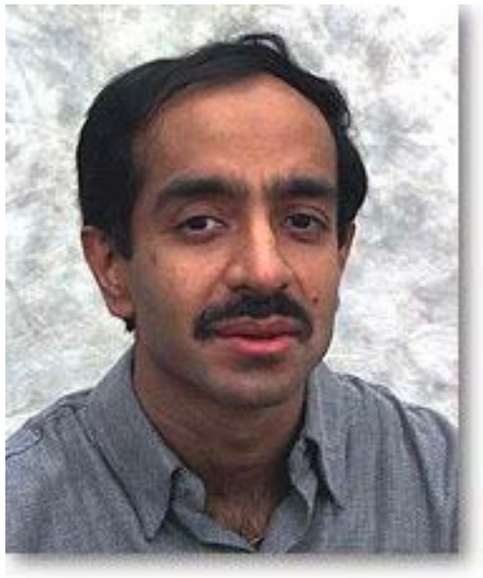
Factorise les grands nombres efficacement

Extrait les logarithmes discrets efficacement
même dans les courbes elliptiques

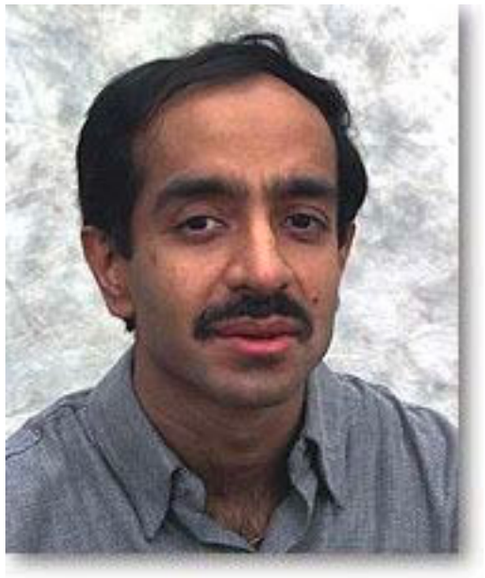
sur un ordinateur quantique

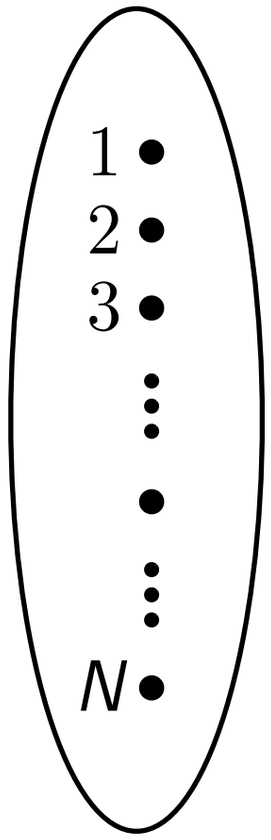
Algorithme de Grover

Algorithme de Grover

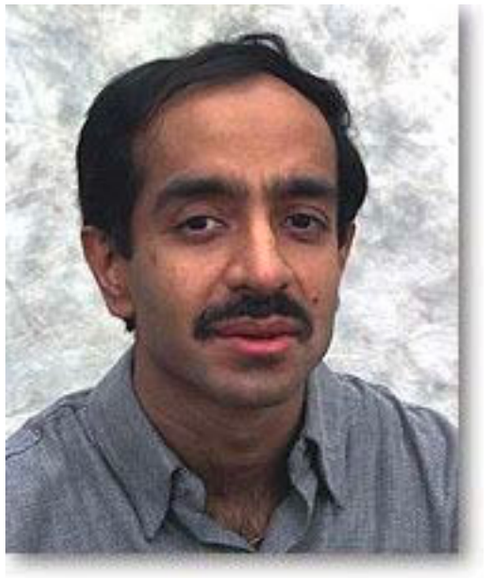


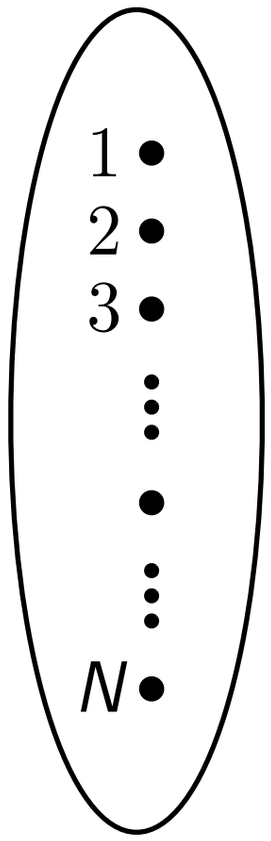
Algorithme de Grover





Algorithme de Grover

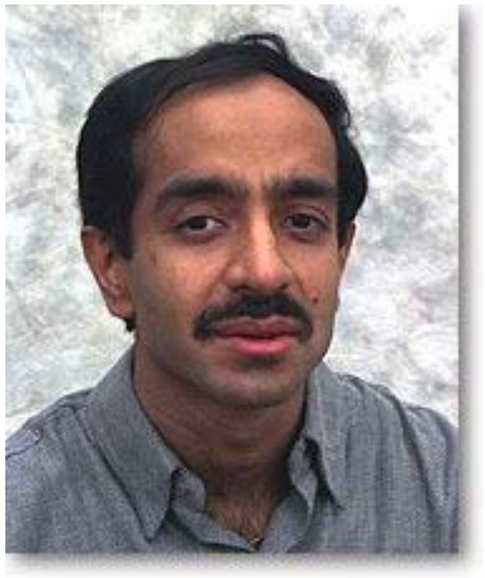


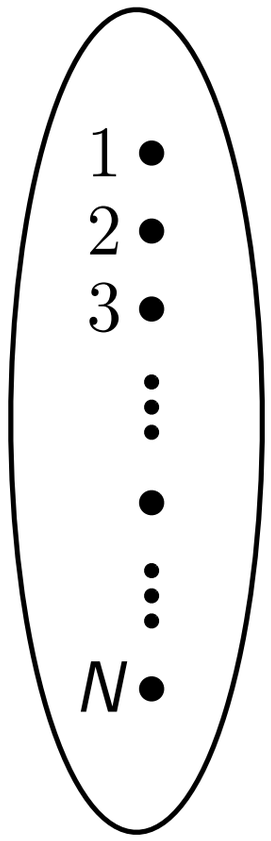


0

1

Algorithme de Grover



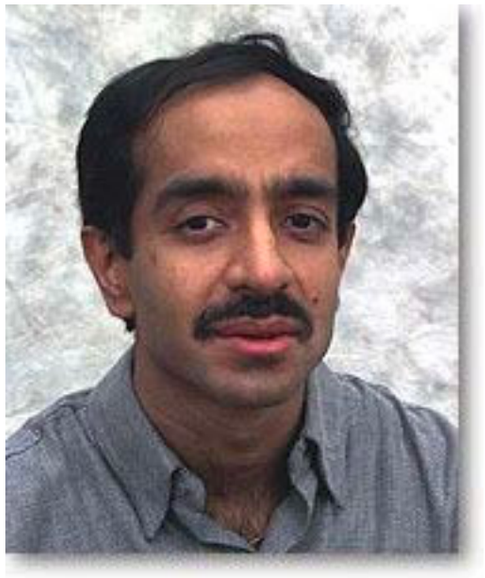


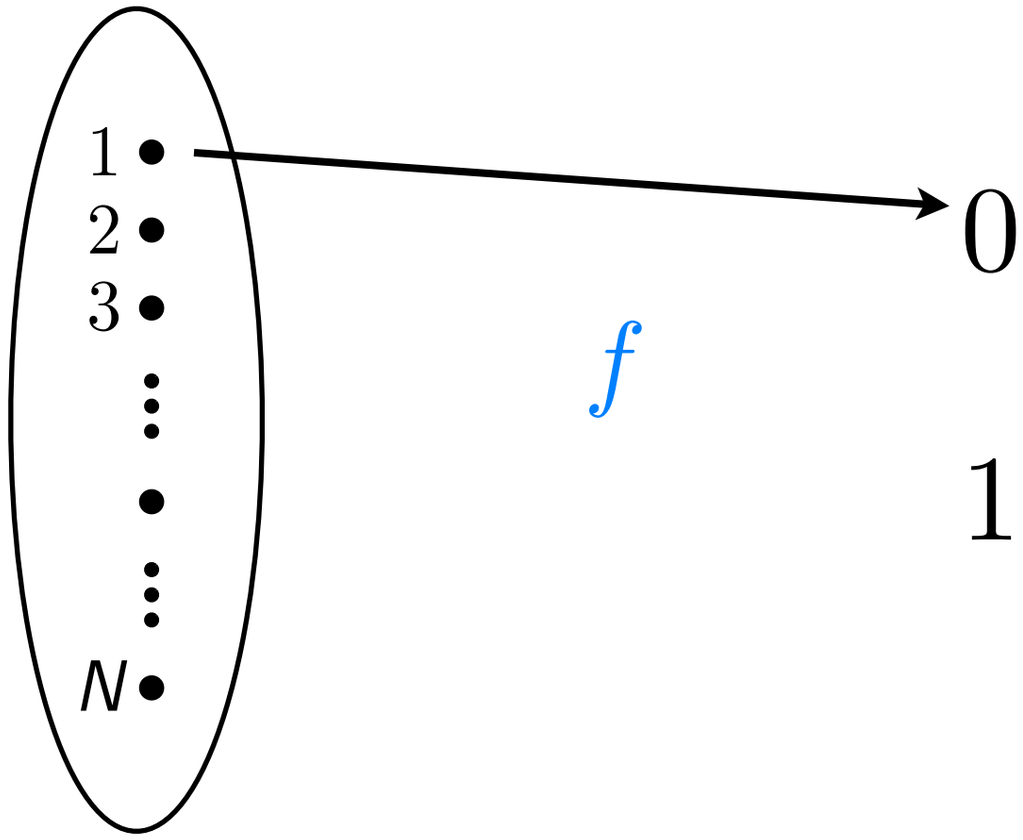
f

0

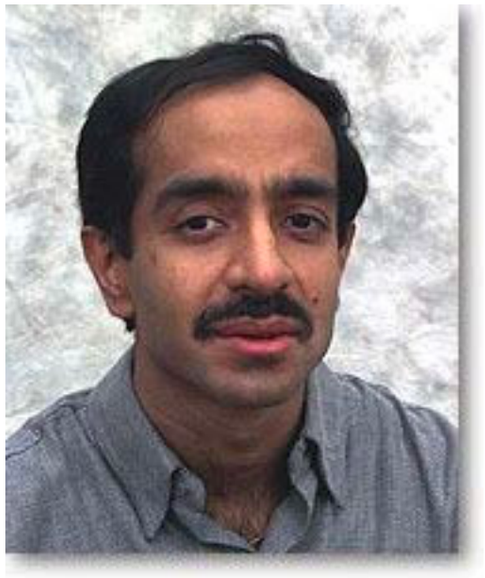
1

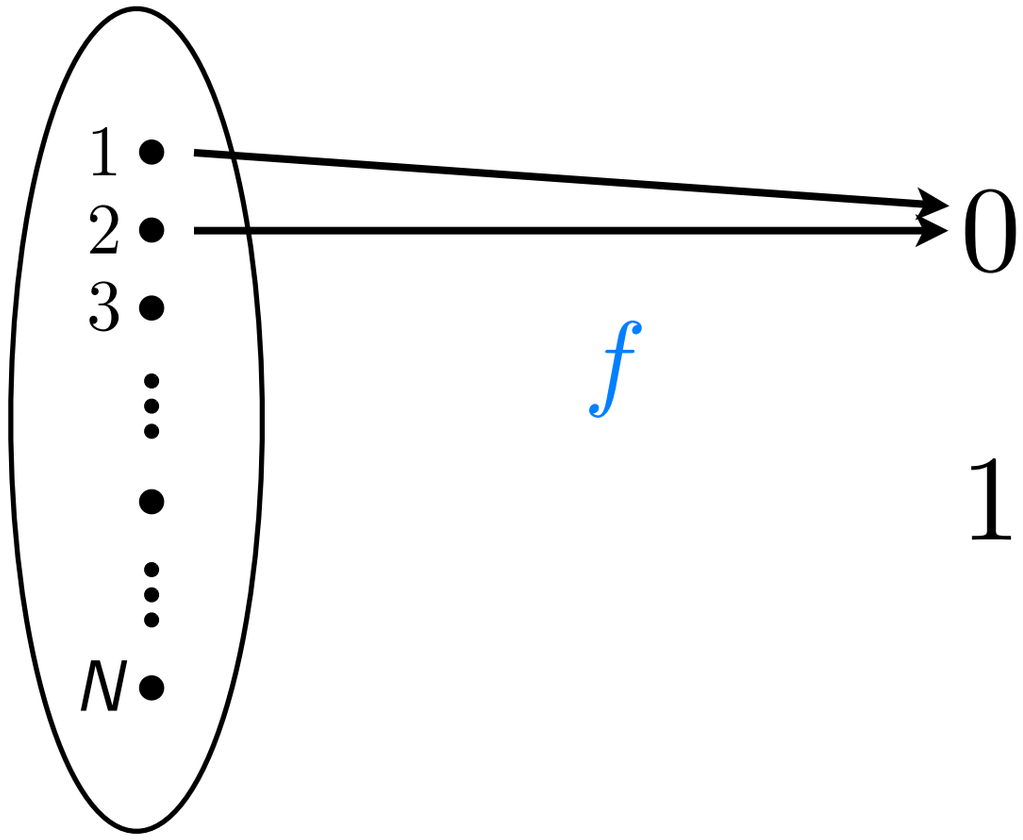
Algorithme de Grover



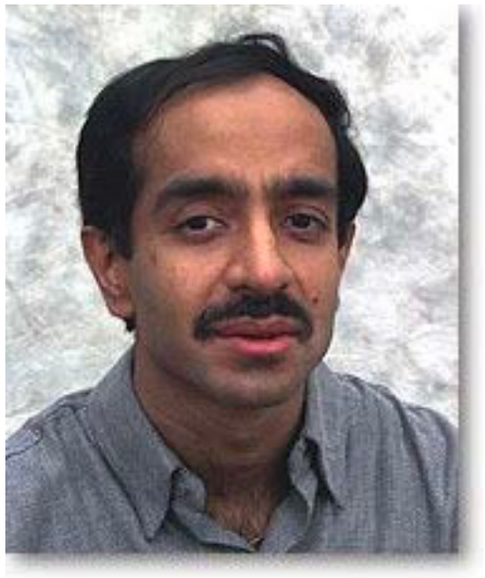


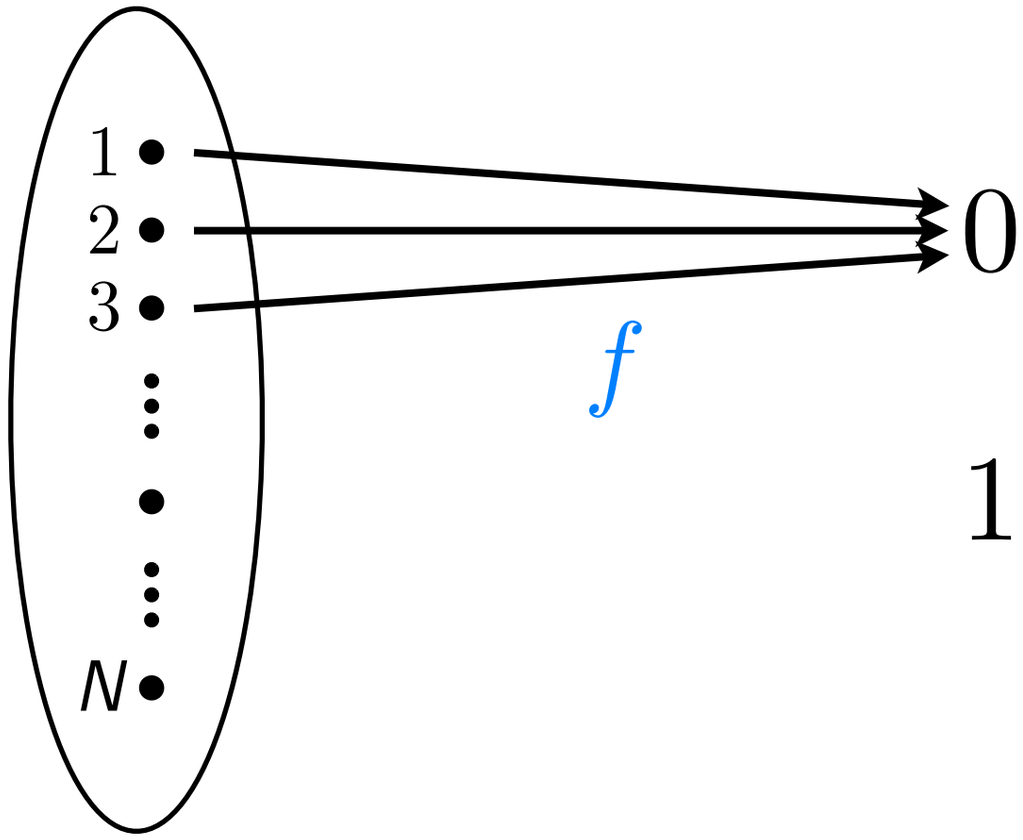
Algorithme de Grover



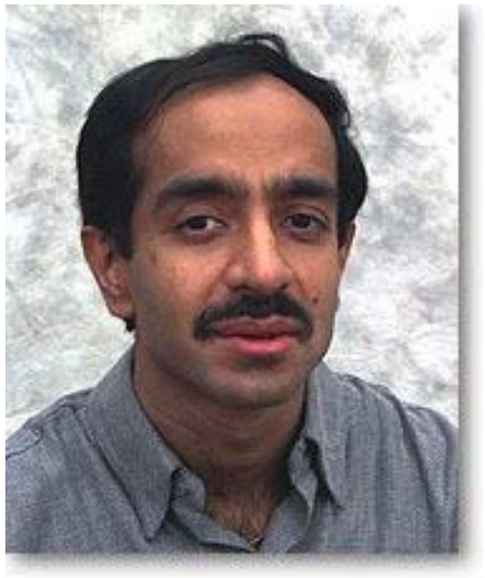


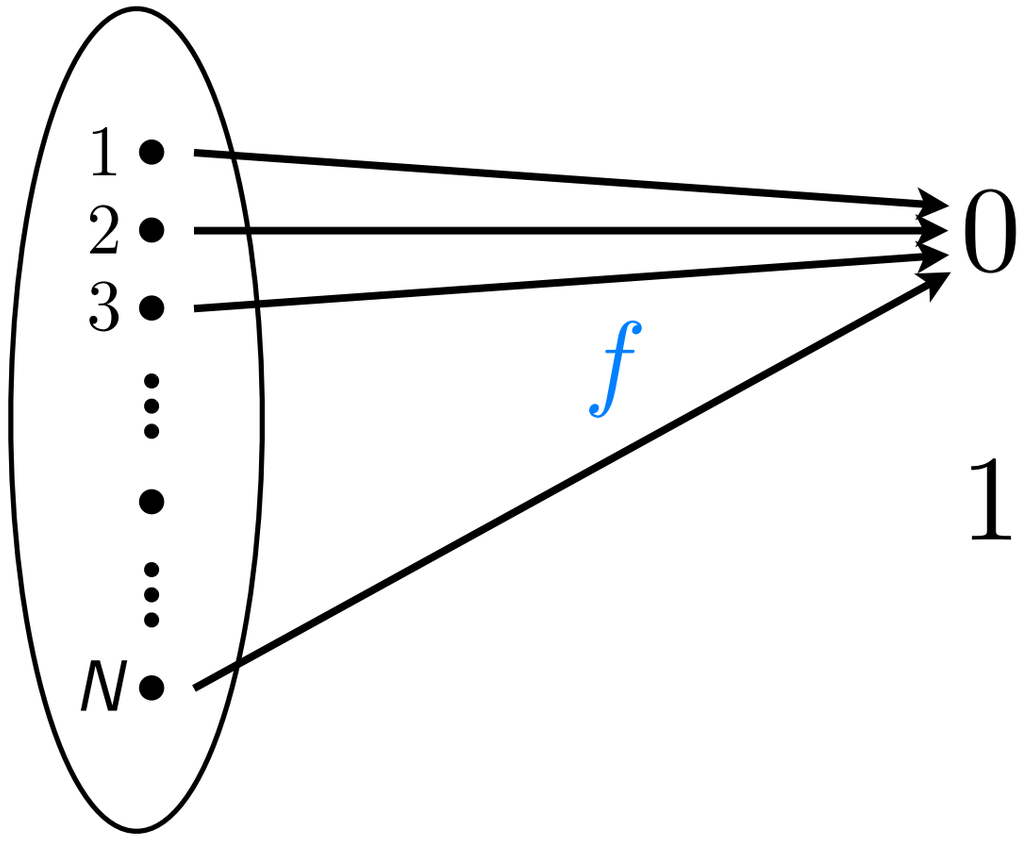
Algorithme de Grover



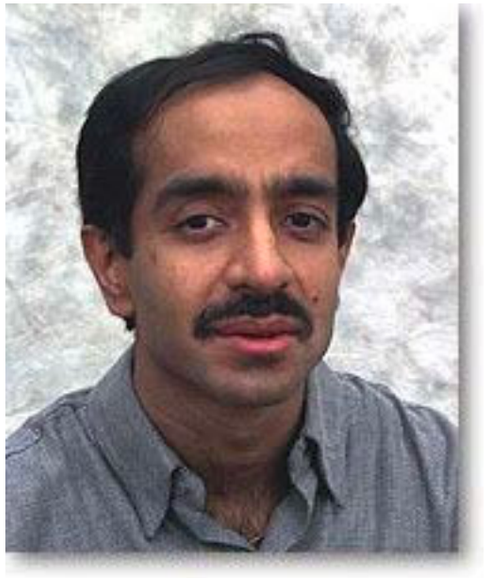


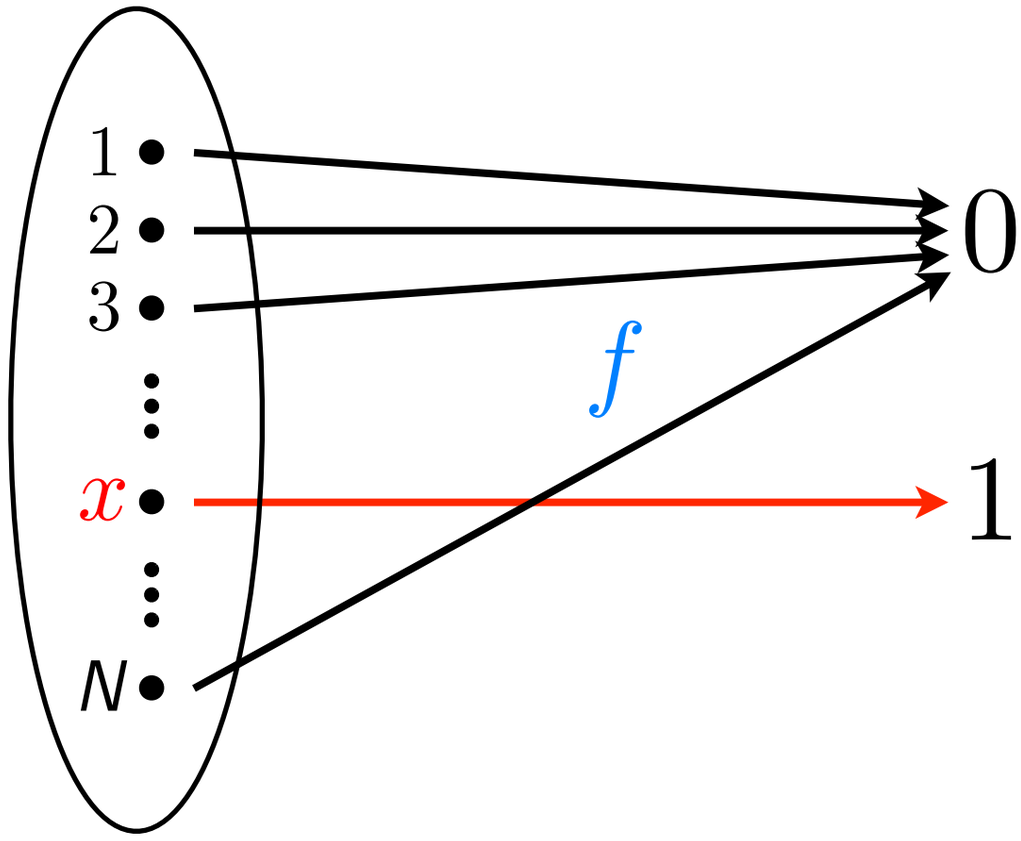
Algorithme de Grover



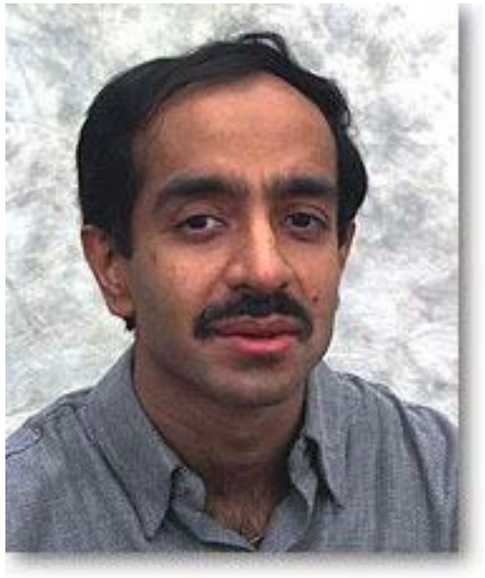


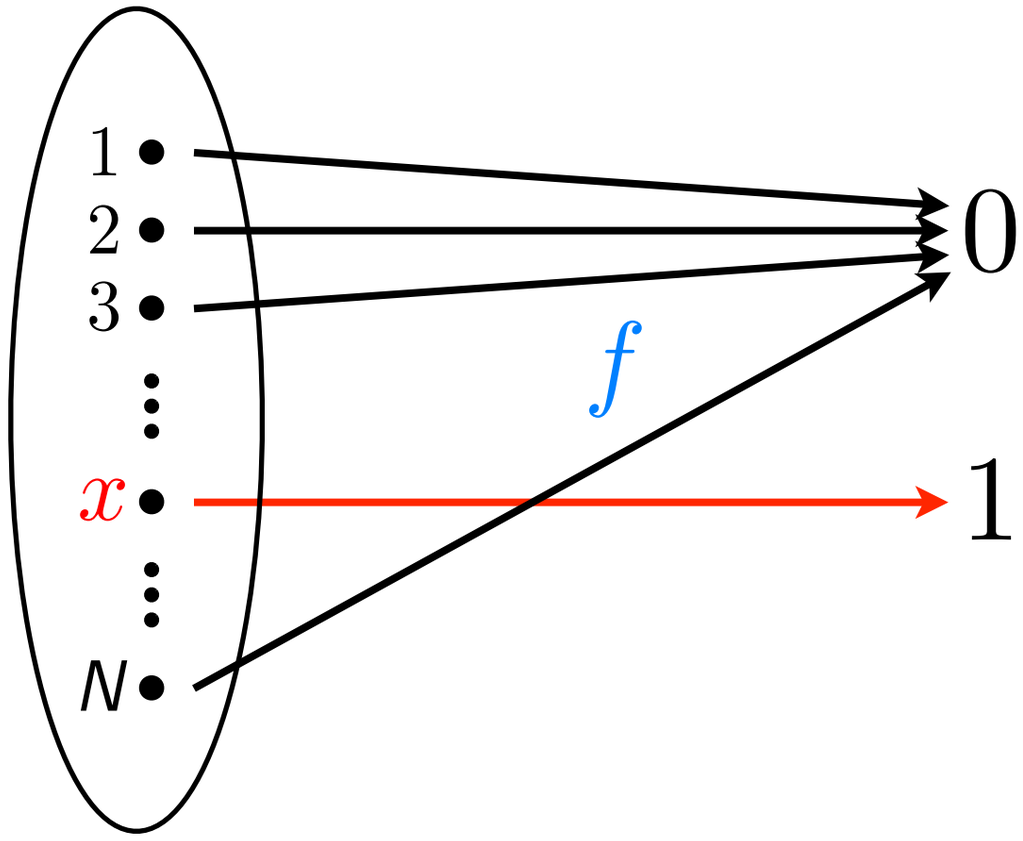
Algorithme de Grover





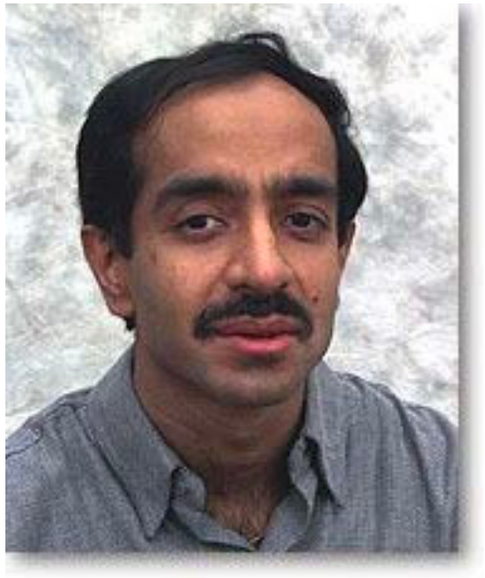
Algorithme de Grover

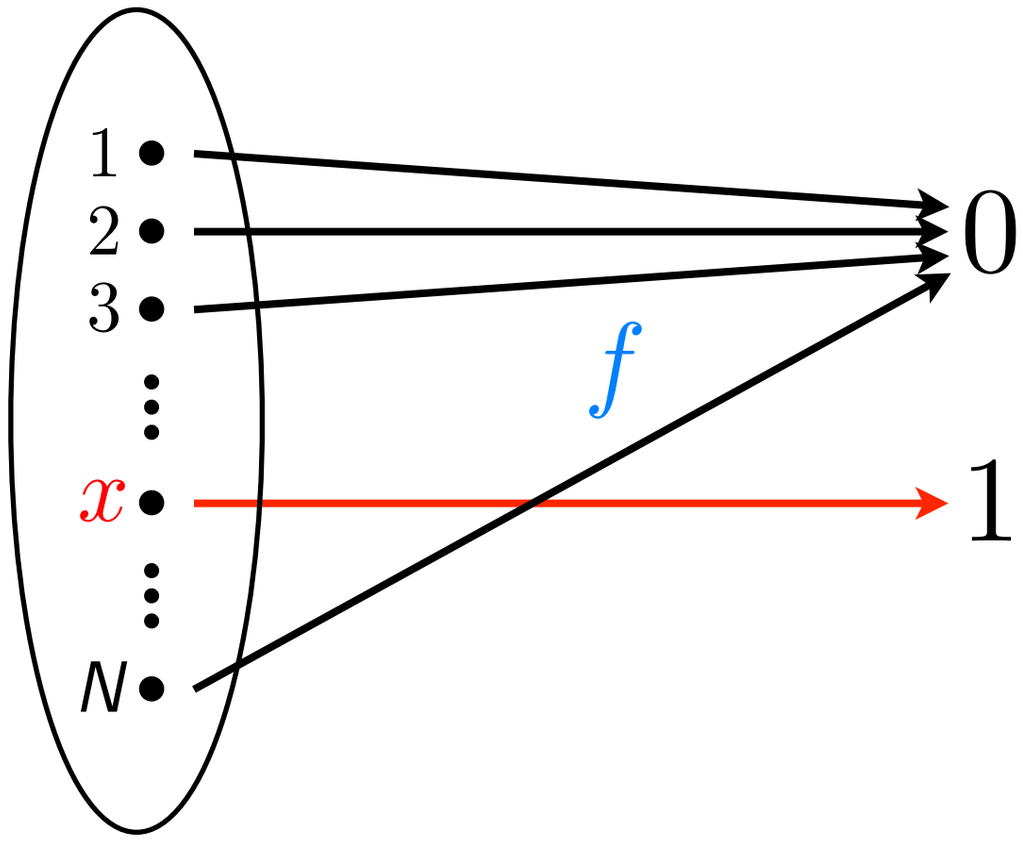




Problème : trouver x tel que $f(x) = 1$

Algorithme de Grover

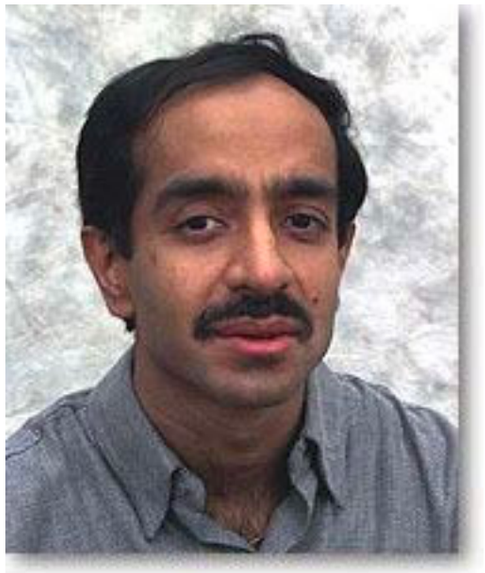


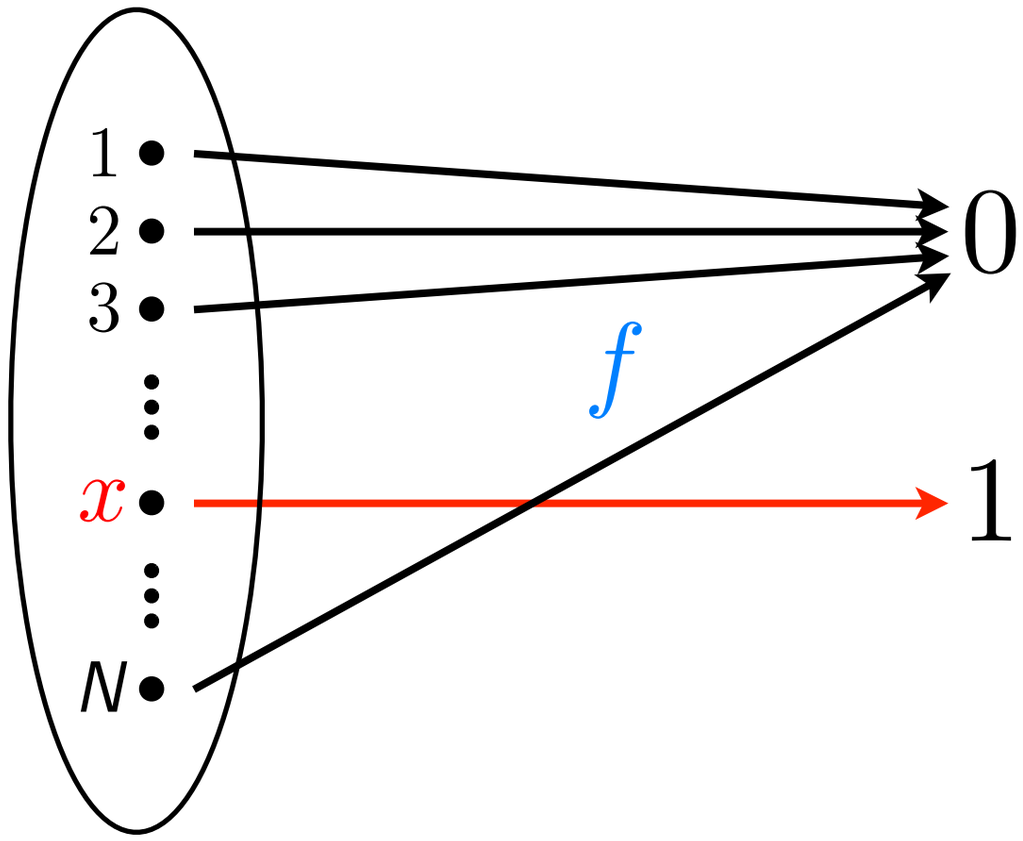


Problème : trouver x tel que $f(x) = 1$

Classique : requiert $N/2$ requêtes en moyenne

Algorithme de Grover





Problème : trouver x tel que $f(x) = 1$

Classique : requiert $N/2$ requêtes en moyenne

Grover : il suffit de $\sim\sqrt{N}$ requêtes quantiques !

Crypto post-quantique

James Ellis (1970)

Clifford Cocks (1973)

Ralph Merkle (1974)

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Crypto post-quantique

James Ellis (1970)

Clifford Cocks (1973)

~~Ralph Merkle (1974)~~

Diffie et Hellman (1976)

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Crypto post-quantique

James Ellis (1970)

Clifford Cocks (1973)

~~Ralph Merkle (1974)~~

~~Diffie et Hellman (1976)~~

Rivest, Shamir, Adleman (1977)

Robert McEliece (1978)

Crypto post-quantique

James Ellis (1970)

Clifford Cocks (1973)

~~Ralph Merkle (1974)~~

~~Diffie et Hellman (1976)~~

~~Rivest, Shamir, Adleman (1977)~~

Robert McEliece (1978)

Crypto post-quantique

James Ellis (1970)

~~Clifford Cocks (1973)~~

~~Ralph Merkle (1974)~~

~~Diffie et Hellman (1976)~~

~~Rivest, Shamir, Adleman (1977)~~

Robert McEliece (1978)

How much of a problem is quantum computing, really??

China will open a $10 billion quantum computer center and others also investing in quantum computing

brian wang | October 10, 2017

Crypto post-quantique

James Ellis (1970)

~~Clifford Cocks (1973)~~

~~Ralph Merkle (1974)~~

~~Diffie et Hellman (1976)~~

~~Rivest, Shamir, Adleman (1977)~~

Robert McEliece (1978)

Crypto post-quantique

James Ellis (1970)

~~Clifford Cocks (1973)~~

~~Ralph Merkle (1974)~~

~~Diffie et Hellman (1976)~~

~~Rivest, Shamir, Adleman (1977)~~

Robert McEliece (1978) ?

Résumé avec techniques classiques

Résumé avec techniques classiques

Dans un monde classique, RSA et Diffie-Hellman semblent sûr, mais nous n'avons pas de preuves

Résumé avec techniques classiques

Dans un monde classique, RSA et Diffie-Hellman semblent sûr, mais nous n'avons pas de preuves

Dans un monde quantique, RSA et Diffie-Hellman sont complètement brisés (même si on utilise les courbes elliptiques)

Résumé avec techniques classiques

Dans un monde classique, RSA et Diffie-Hellman semblent sûr, mais nous n'avons pas de preuves

Dans un monde quantique, RSA et Diffie-Hellman sont complètement brisés (même si on utilise les courbes elliptiques)

La mécanique quantique semble être une **malédiction** pour les faiseurs de codes

Résumé avec techniques classiques

Dans un monde classique, RSA et Diffie-Hellman semblent sûr, mais nous n'avons pas de preuves

Dans un monde quantique, RSA et Diffie-Hellman sont complètement brisés (même si on utilise les courbes elliptiques); McEliece pourrait survivre

La mécanique quantique semble être une **malédiction** pour les faiseurs de codes

Résumé avec techniques classiques

Dans un monde classique, RSA et Diffie-Hellman semblent sûr, mais nous n'avons pas de preuves

Dans un monde quantique, RSA et Diffie-Hellman sont complètement brisés (même si on utilise les courbes elliptiques); McEliece pourrait survivre ainsi que NewHope, Frodo, etc.

La mécanique quantique semble être une malédiction pour les faiseurs de codes

PQ Crypto algorithms

PQ Crypto algorithms

National Institute of Standards and Technology
U.S. Department of Commerce

BIG QUAKE	*HK17	Odd Manhattan
BIKE	HQC	Ouroboros-R
CFPKM	KCL *(pka OKCN/AKCN/CNKE)*	Picnic
Classic McEliece	KINDI	Post-quantum RSA-Encryption
Compact LWE	LAC	Post-quantum RSA-Signature
CRYSTALS-DILITHIUM	LAKE	pqsigRM
CRYSTALS-KYBER	LEDAkem	QC-MDPC KEM
DAGS	LEDApkc	qTESLA
Ding Key Exchange	Lepton	RaCoSS
DME	LIMA	Rainbow
DRS	Lizard	Ramstake
DualModeMS	LOCKER	*RankSign
*Edon-K	LOTUS	RLCE-KEM
EMBLEM and R.EMBLEM	LUOV	Round2
FALCON	McNie	RQC
FrodoKEM	Mersenne-756839	*RVB
GeMSS	MQDSS	SABER
Giophantus	NewHope	SIKE
Gravity-SPHINCS	NTRUEncrypt	SPHINCS+
Guess Again	pqNTRUSign	*SRTPI
Gui	NTRU-HRSS-KEM	Three Bears
HILA5	NTRU Prime	Titanium
HiMQ-3	NTS-KEM	WalnutDSA
* denotes algorithm has been withdrawn		***Created January 03, 2017, Updated September 04, 2018***

PQ Crypto algorithms

PQ Crypto algorithms

PQ Crypto algorithms

National Institute of Standards and Technology
U.S. Department of Commerce

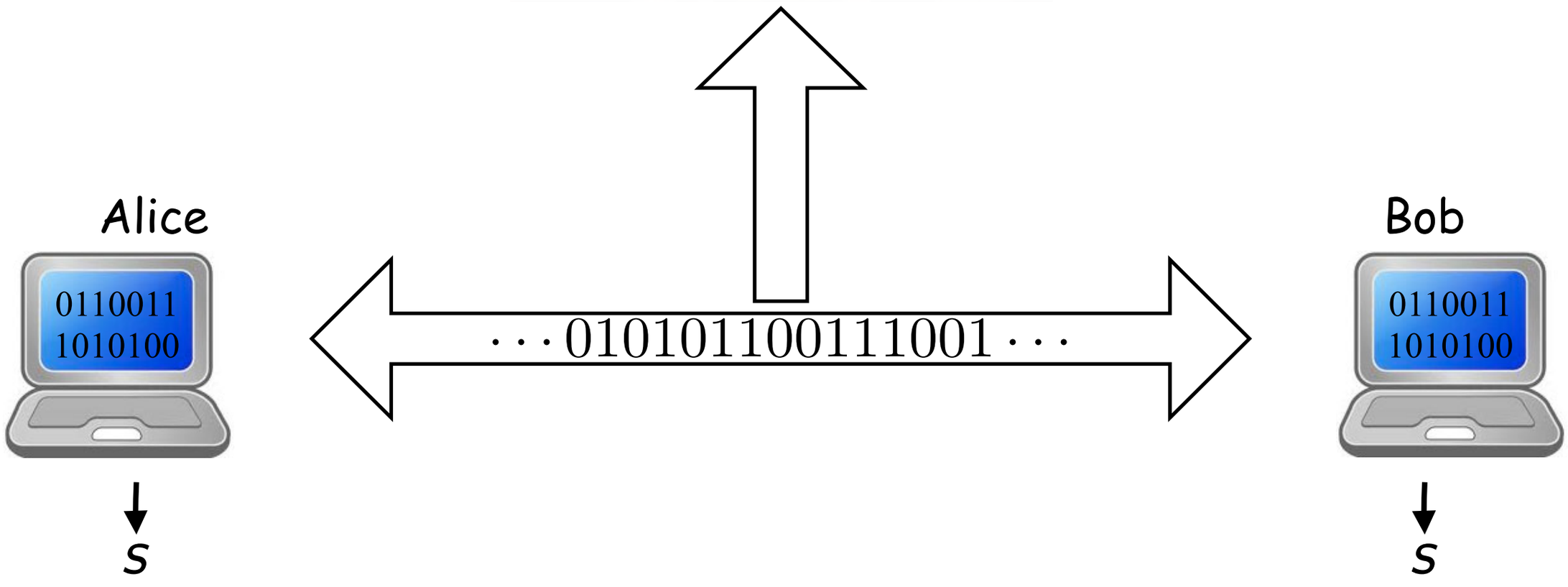
BIG QUAKE	*HK17	Odd Manhattan
BIKE	HQC	Ouroboros-R
CFPKM	KCL *(pka OKCN/AKCN/CNKE)*	Picnic
Classic McEliece	KINDI	Post-quantum RSA-Encryption
Compact LWE	LAC	Post-quantum RSA-Signature
CRYSTALS-DILITHIUM	LAKE	pqsigRM
CRYSTALS-KYBER	LEDAkem	QC-MDPC KEM
DAGS	LEDApkc	qTESLA
Ding Key Exchange	Lepton	RaCoSS
DME	LIMA	Rainbow
DRS	Lizard	Ramstake
DualModeMS	LOCKER	*RankSign
*Edon-K	LOTUS	RLCE-KEM
EMBLEM and R.EMBLEM	LUOV	Round2
FALCON	McNie	RQC
FrodoKEM	Mersenne-756839	*RVB
GeMSS	MQDSS	SABER
Giophantus	NewHope	SIKE
Gravity-SPHINCS	NTRUEncrypt	SPHINCS+
Guess Again	pqNTRUSign	*SRTPI
Gui	NTRU-HRSS-KEM	Three Bears
HILA5	NTRU Prime	Titanium
HiMQ-3	NTS-KEM	WalnutDSA
* denotes algorithm has been withdrawn		*Created January 03, 2017, Updated September 04, 2018*

2017

PQ Crypto algorithms

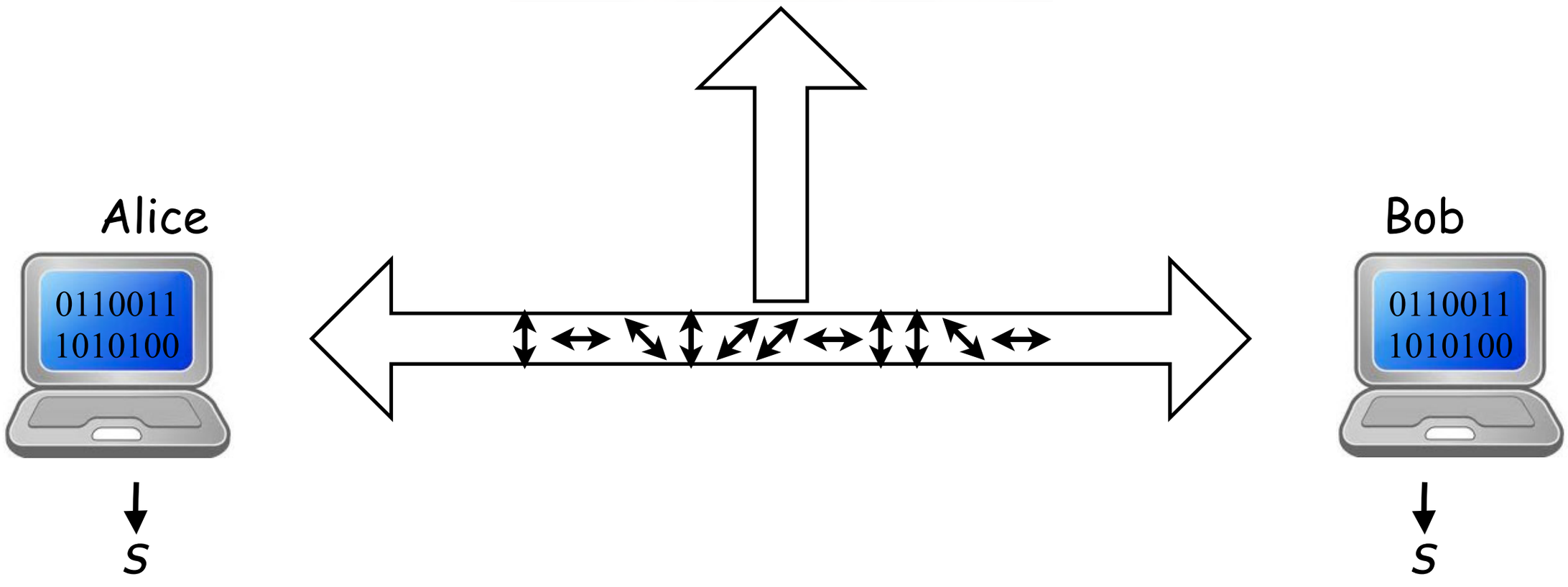
Établissement de clef dans un monde quantique

Adversaire quantique

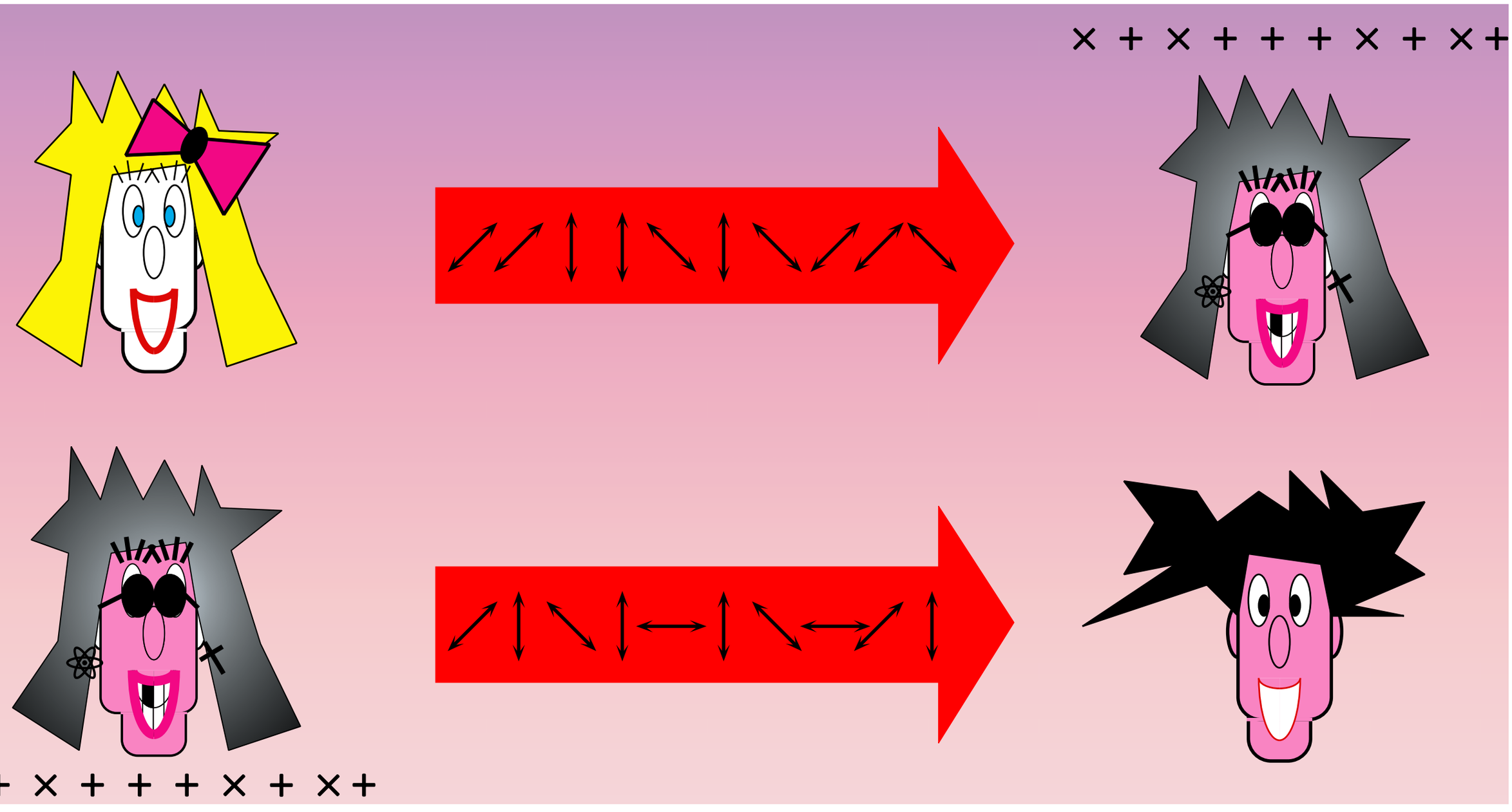


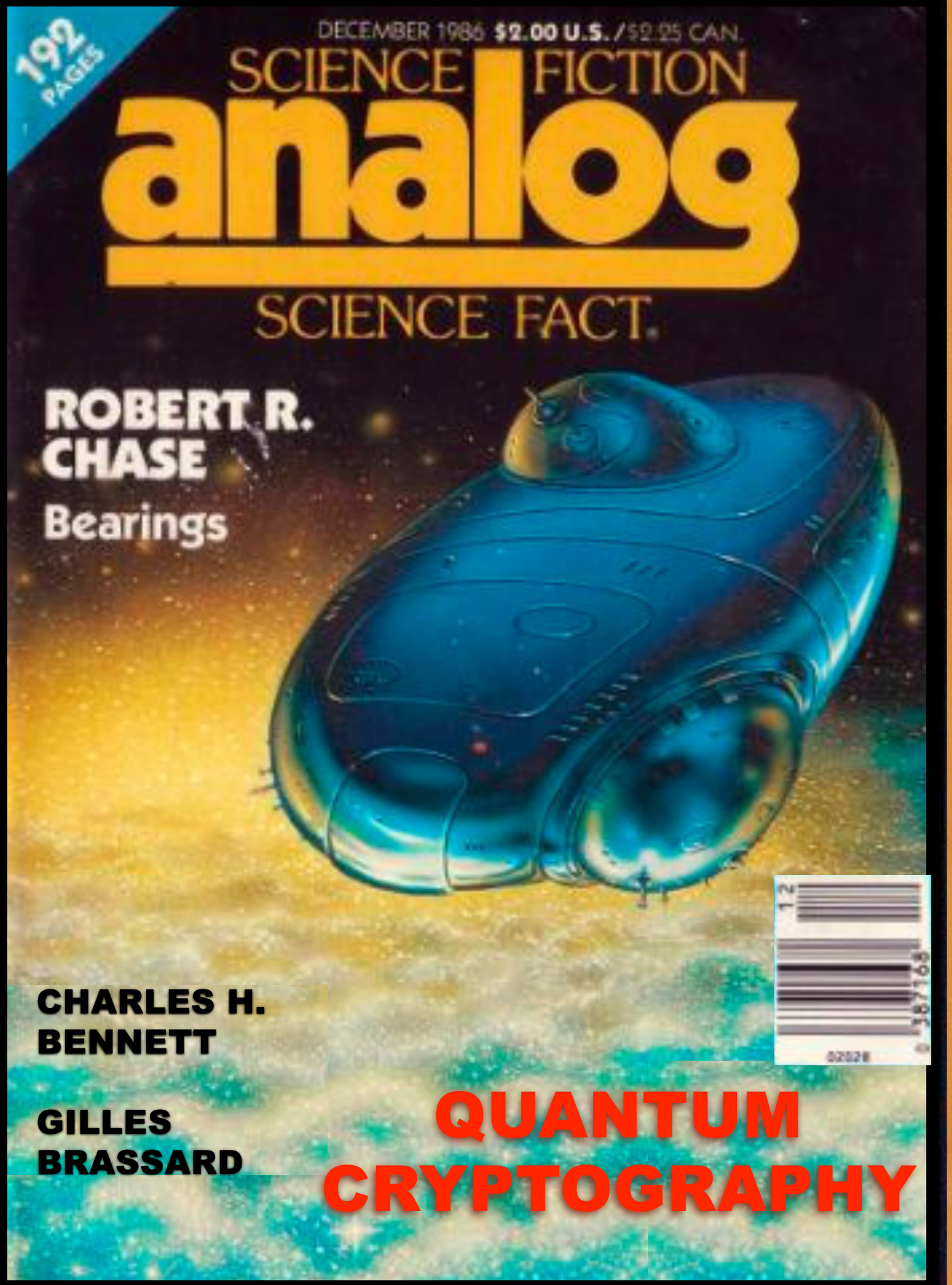
Établissement de clef dans un monde quantique

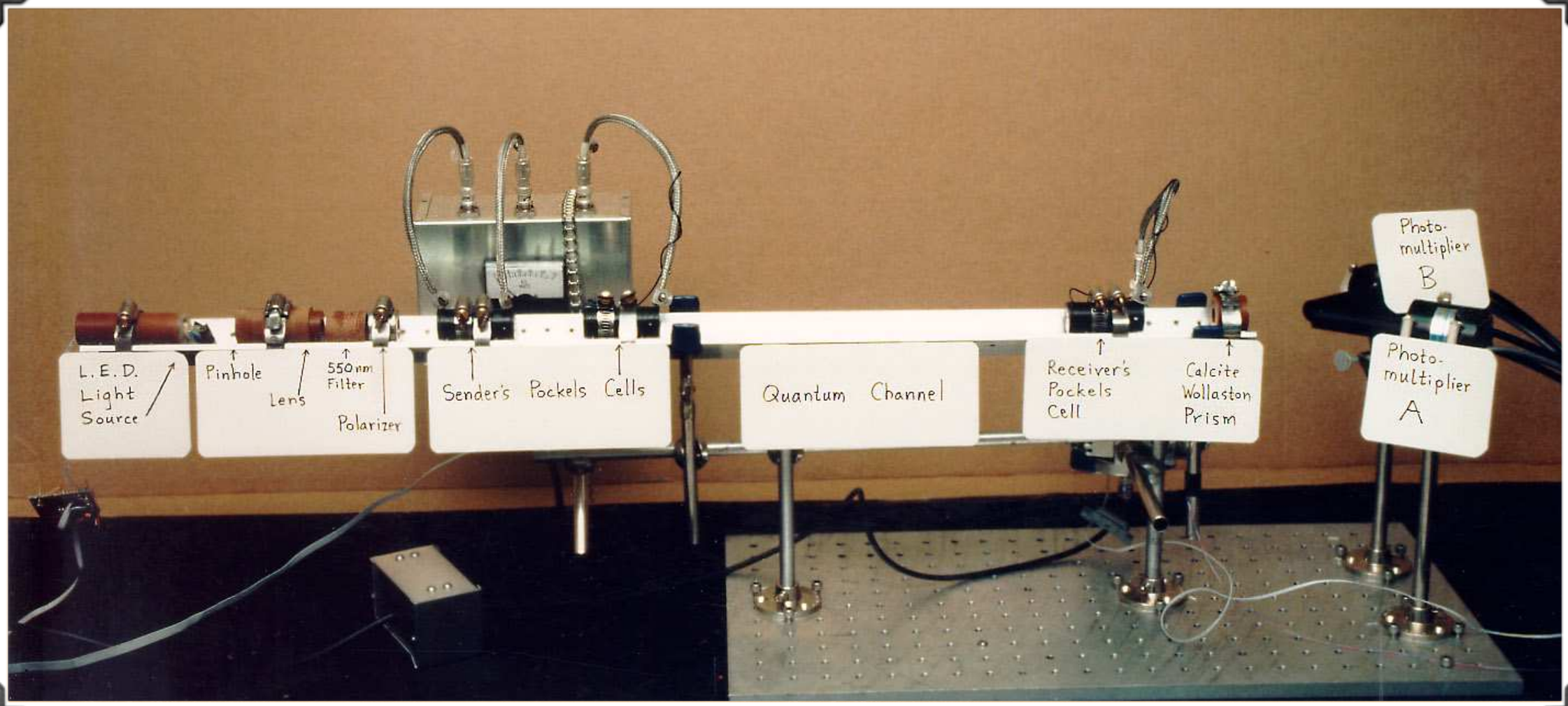
Adversaire quantique



Cryptographie quantique

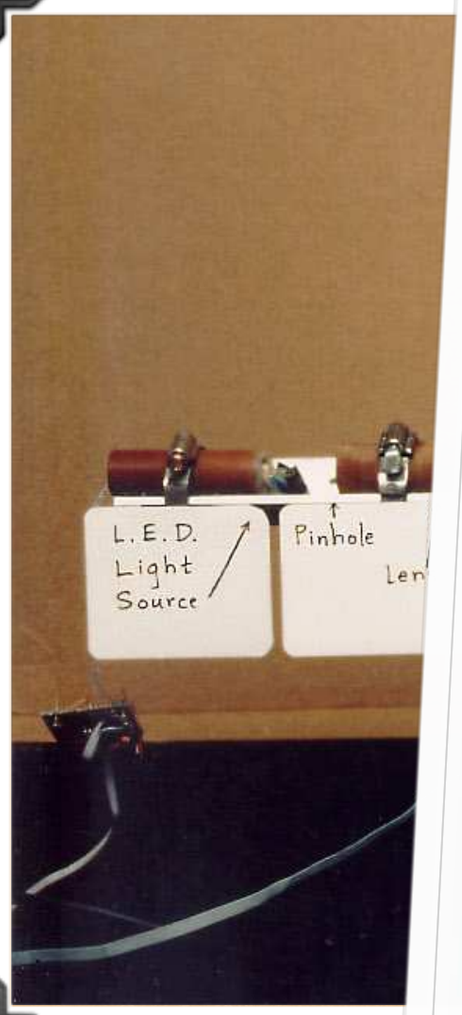



192 PAGES
DECEMBER 1986 $2.00 U.S./$2.25 CAN.
SCIENCE FICTION
analog
SCIENCE FACT.
ROBERT R. CHASE
Bearings
CHARLES H. BENNETT
GILLES BRASSARD
QUANTUM CRYPTOGRAPHY



GILLES BRASSARD

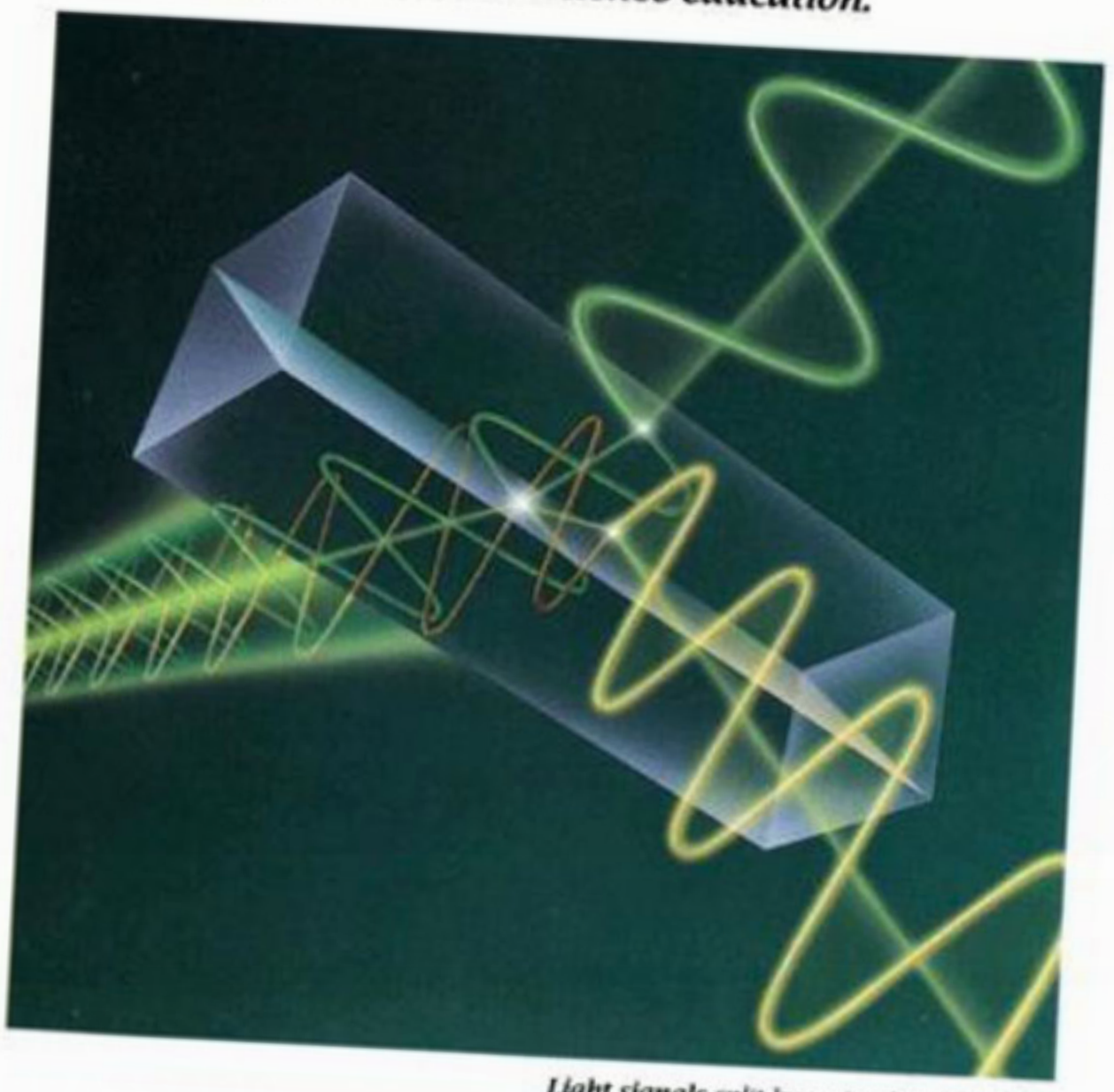
QUANTUM CRYPTOGRAPHY



SCIENTIFIC AMERICAN

OCTOBER 1992
$3.95

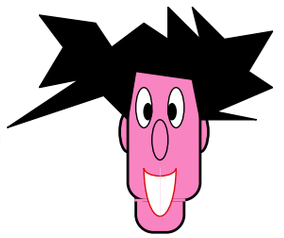
The promise of diamond semiconductors.
Was early man a heroic hunter—or a scavenger?
Raising the grades in U.S. science education.



***Light signals** split by a simple prism allow messages to be transmitted in absolute secrecy.*

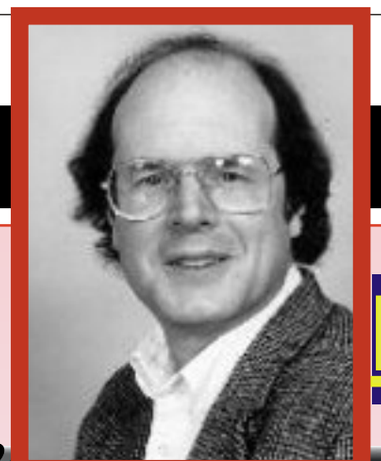
Établissement

quantique de clé



A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0	↱	↱	0	↱	1	↱	↱	1	↱	0	↱	↱	↱	↱	1	0	↱	↱	1	↱	0	0	0
B:	0			0		1			1		0					1	0			1		0	0	0
A:	0			0		1			1		0					1	1			1		0	0	0
A:	0					1					0						1							0
B:	=					=					=						≠							=
B:									1							1							0	
A:									1							1							0	

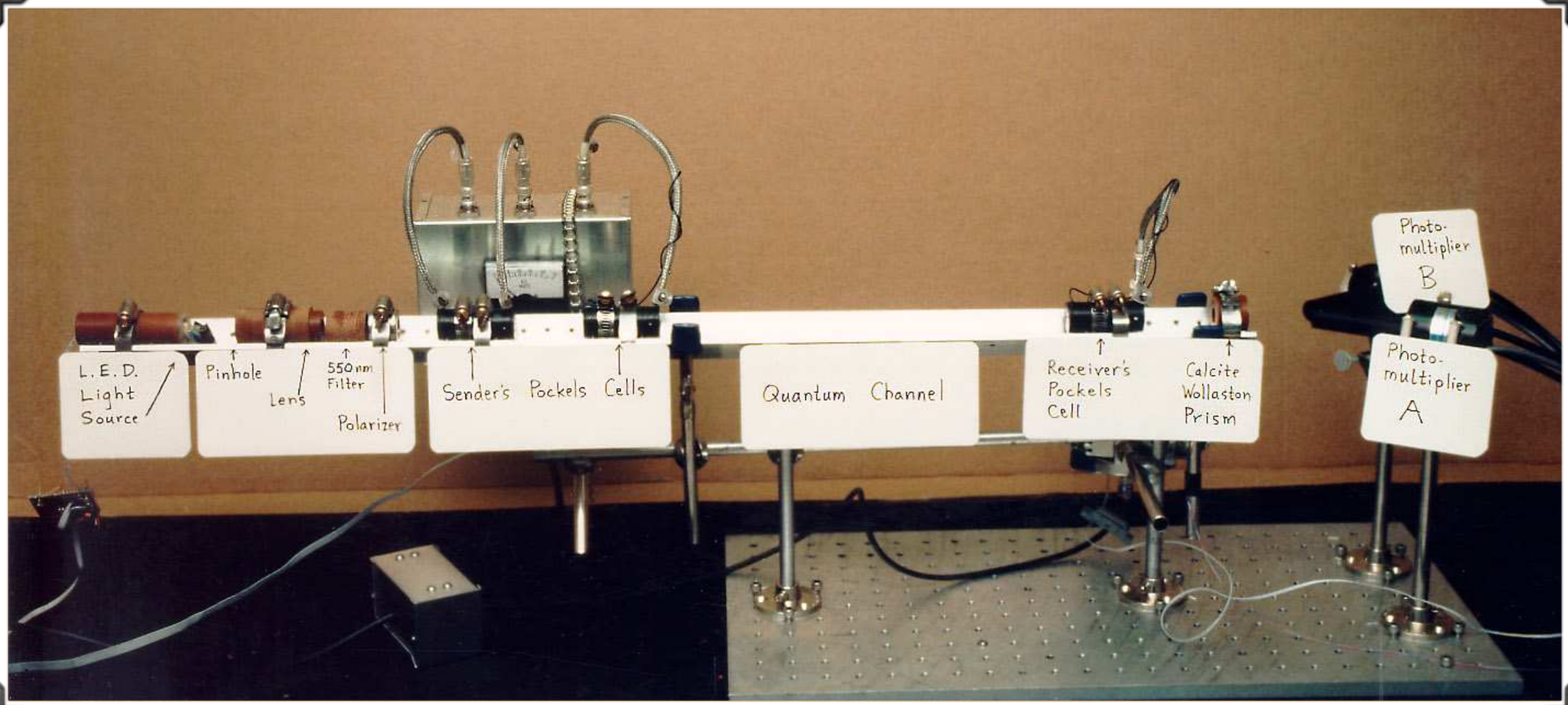
20%



Bennett- Brassard

Démonstration expérimentale

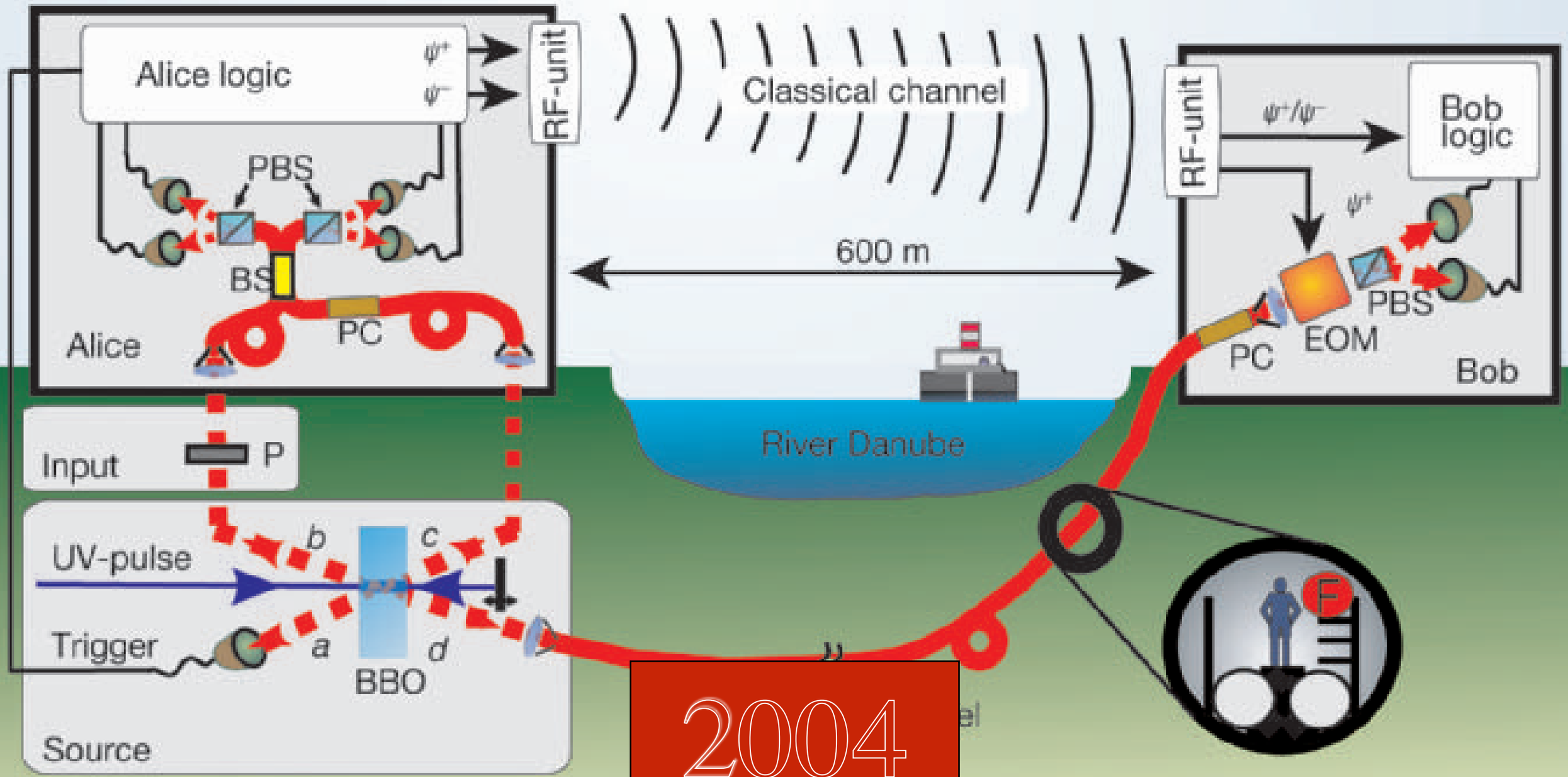
Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail and John Smolin



1989

Démonstration expérimentale

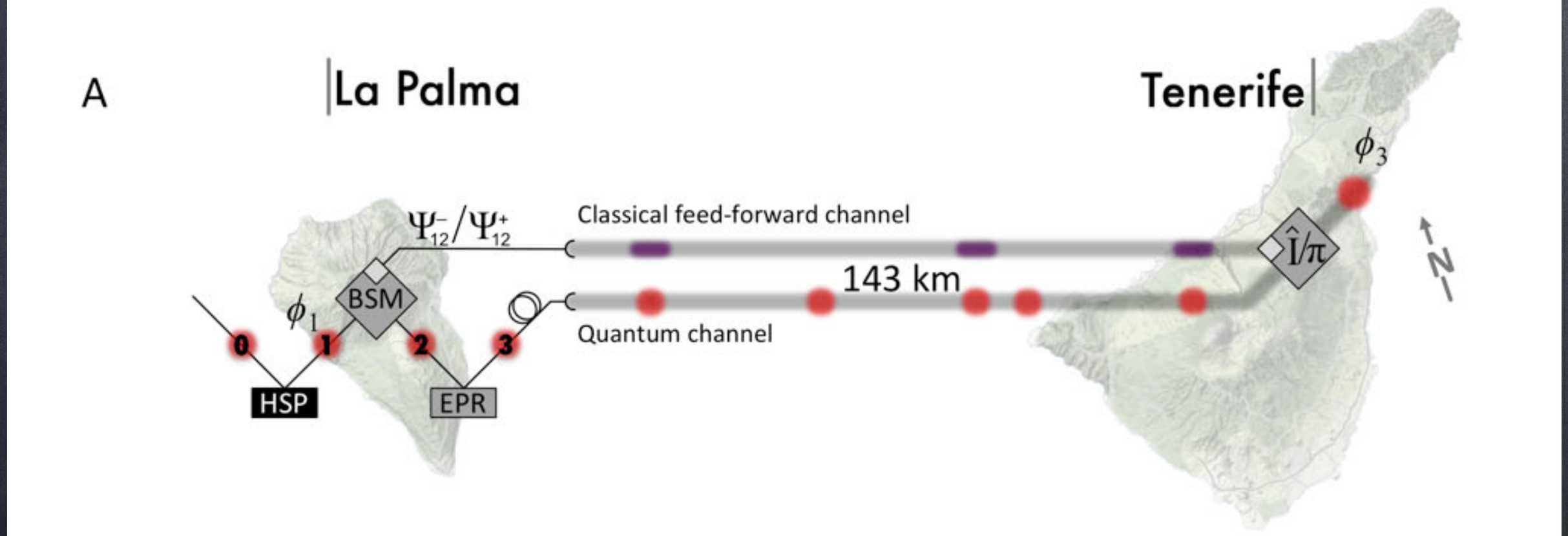
Rupert Ursin, Thomas Jennewein, Markus Aspelmeyer, Rainer Kaltenbaek, Michael Lindenthal, Philip Walther, Anton Zeilinger



NATURE | VOL 430 | 19 AUGUST 2004 | www.nature.com/nature

Démonstration expérimentale

Xiao-song Ma, Thomas Herbst, Thomas Scheidl, Daqing Wang, Sebastian Kropatschek, William Naylor, Alexandra Mech, Bernhard Wittmann, Johannes Kofler, Elena Anisimova, Vadim Makarov, Thomas Jennewein, Rupert Ursin, and Anton Zeilinger

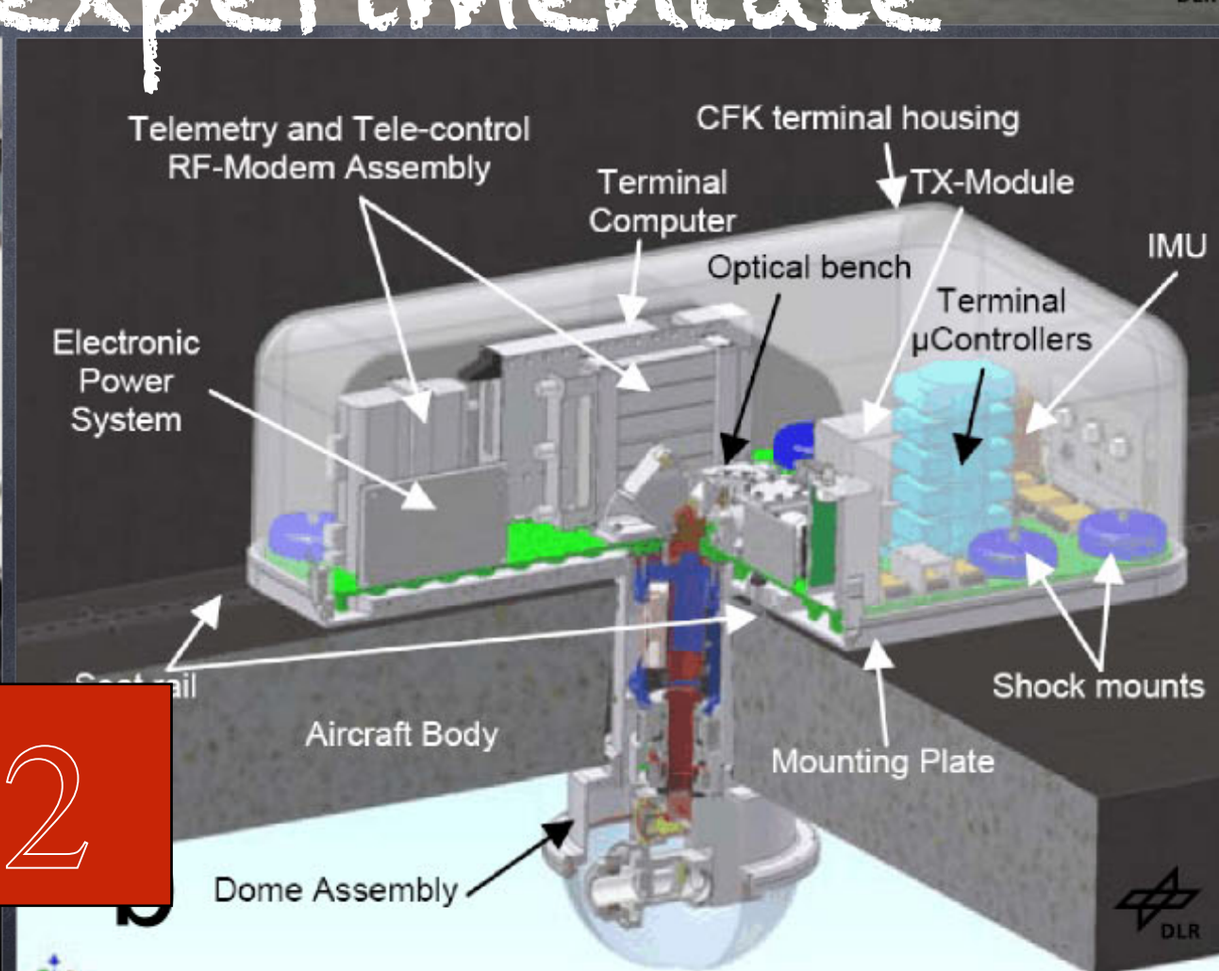


2012

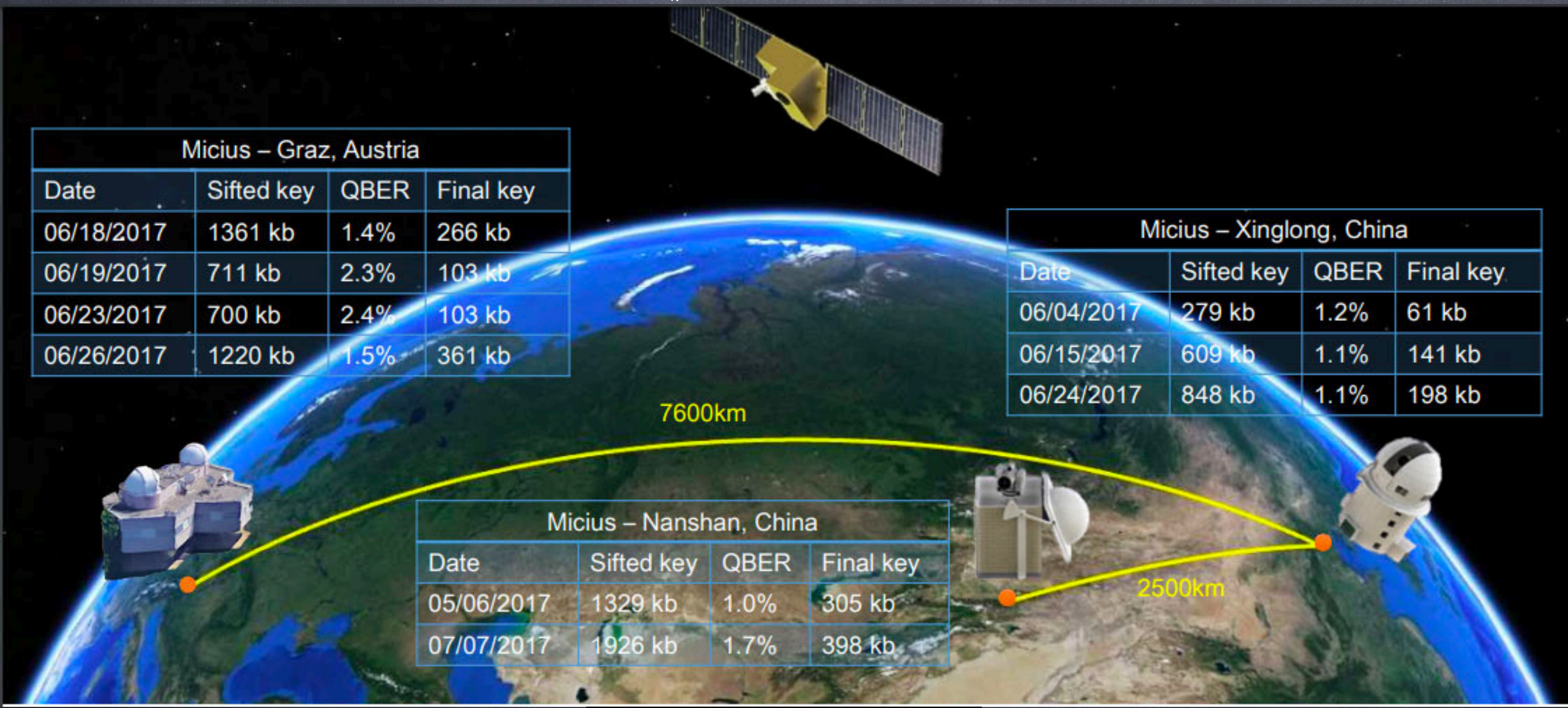
Sebastian Nauerth, Florian Moll, Markus Rau,
Christian Fuchs, Joachim Horwath & Harald Weinfurter

Démonstration expérimentale

2012



Crypto Quantique via Satellite



Micius – Graz, Austria			
Date	Sifted key	QBER	Final key
06/18/2017	1361 kb	1.4%	266 kb
06/19/2017	711 kb	2.3%	103 kb
06/23/2017	700 kb	2.4%	103 kb
06/26/2017	1220 kb	1.5%	361 kb

Micius – Xinglong, China			
Date	Sifted key	QBER	Final key
06/04/2017	279 kb	1.2%	61 kb
06/15/2017	609 kb	1.1%	141 kb
06/24/2017	848 kb	1.1%	198 kb

7600km

2500km

Micius – Nanshan, China			
Date	Sifted key	QBER	Final key
05/06/2017	1329 kb	1.0%	305 kb
07/07/2017	1926 kb	1.7%	398 kb

2017-18

China launches world's 1st quantum satellite

QUESS satellite designed to establish 'hack-proof' quantum communications

Thomson Reuters Posted: Aug 16, 2016 9:00 AM ET | Last Updated: Aug 16, 2016 11:56 AM ET

China launches revolutionary quantum satellite 0:44

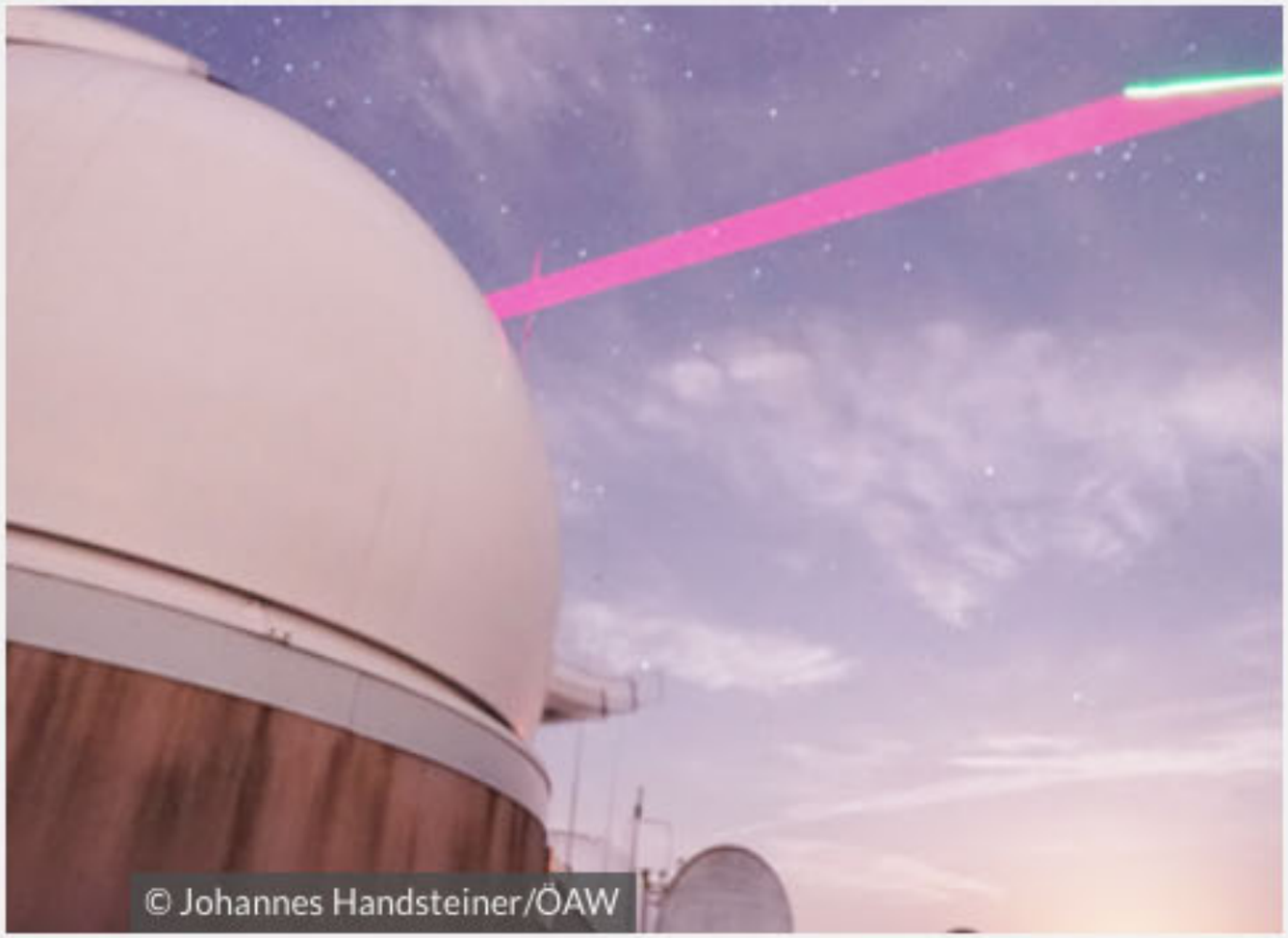
China on Tuesday launched the world's first quantum satellite, which will help it establish "hack-proof" communications between space and the ground, state media said, the latest advance in an ambitious space programme.

09/29/2017

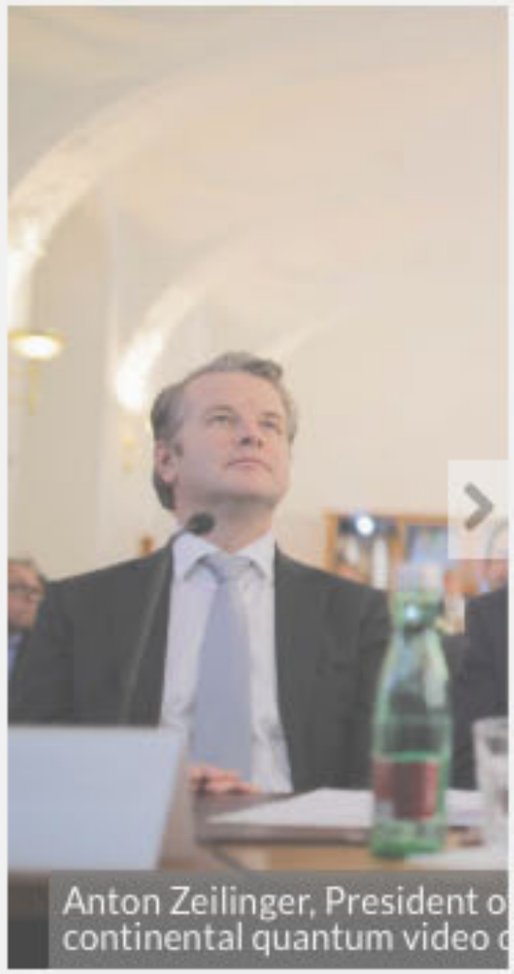
AUSTRIAN AND CHINESE ACADEMIES OF SCIENCES SUCCESSFULLY CONDUCTED FIRST INTER-CONTINENTAL QUANTUM VIDEO CALL

The two Academy presidents Chunli Bai and Anton Zeilinger tested quantum encrypted communication between Beijing and Vienna in a live-experiment. The quantum key was transmitted via the Chinese quantum satellite Micius.

cademy of Sciences. © ÖAW



© Johannes Handsteiner/ÖAW



Anton Zeilinger, President o
continental quantum video c

Crypto Quantique industrielle

IDQ

Cerberis QKD Blade

The world's first carrier-grade QKD platform

- Provably secure key exchange based on Quantum Key Distribution
- Quantum keys ensure long-term protection and forward secrecy
- Fully automated key exchange with continuous key renewal
- Integrated entropy source based on a Quantum Random Number Generator

Cryptographie Quantique industrielle

Cryptographie Quantique industrielle

Qubitekk to Receive Federal Funding to Help Protect Nation's Power Grid From Cyber Attack

San Diego startup, Qubitekk, will benefit from a $3M Department of Energy grant to speed the development of unhackable quantum encryption technology that will protect the country's power grid from cyber attack. Under the DOE's Cybersecurity for Energy Delivery Systems (CEDS) program, the nation's premier program for grid security, Qubitekk will be working in partnership [...]

READ MORE

Qui gagnera ?

FAISEURS DE CODES

ou

BRISEURS DE CODES

?

Qui gagnera ?

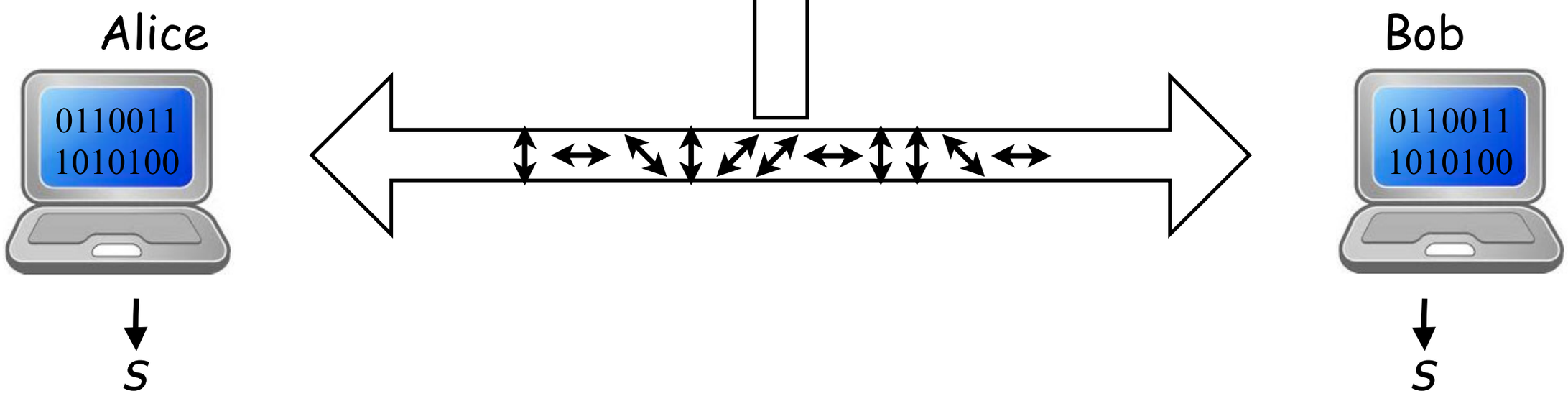
« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

Poe avait tort !

Établissement de clef dans un monde quantique

©Makarov

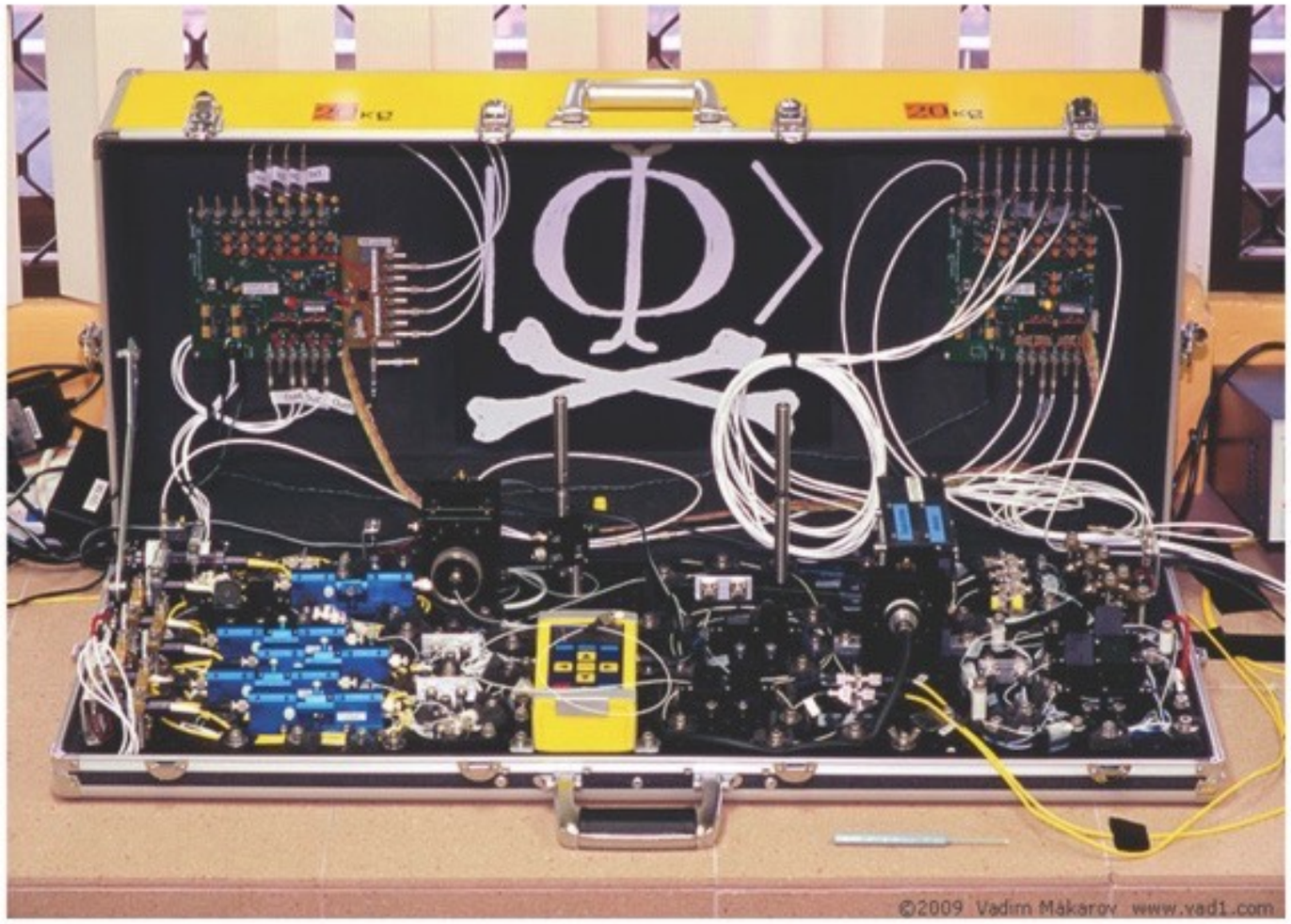
Adversaire quantique



Quantum Hacking

NTNU
Department of Electronics and Telecommunications

UNIK
UNIVERSITY GRADUATE CENTER



Qui gagnera ?

« It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve »

Poe avait-il raison après tout ??

La fabuleuse histoire des codes secrets

Prof. Claude CRÉPEAU

McGill

INTRIQ

UTA Chambly, 1981, boul. de Périgny, Chambly, Qc J3L 4C3 • • • 27 septembre 2018