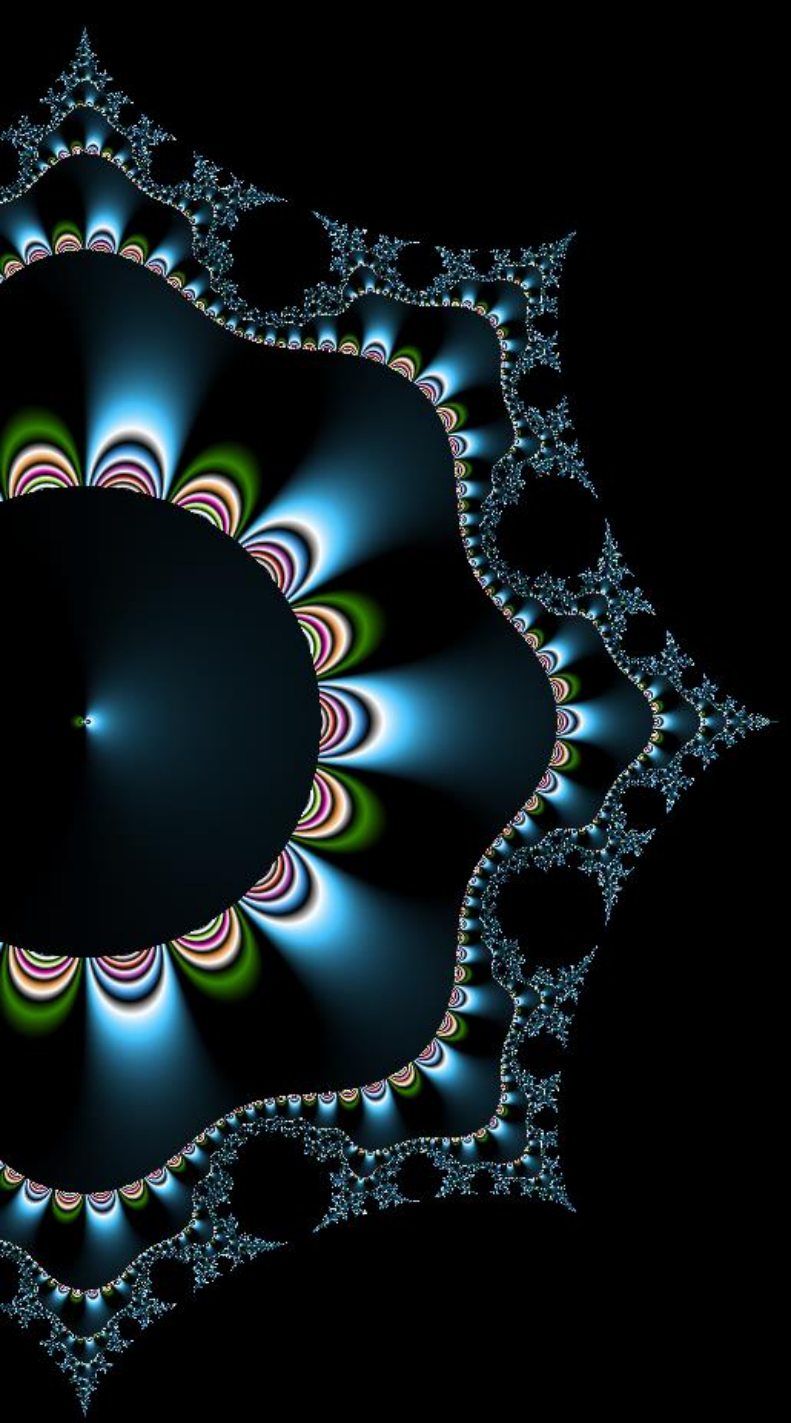


05 Cryptographie

Histoire

Corinne HENIN

www.arsouyes.org

Il était une fois …

Alice

Il était une fois …

Alice

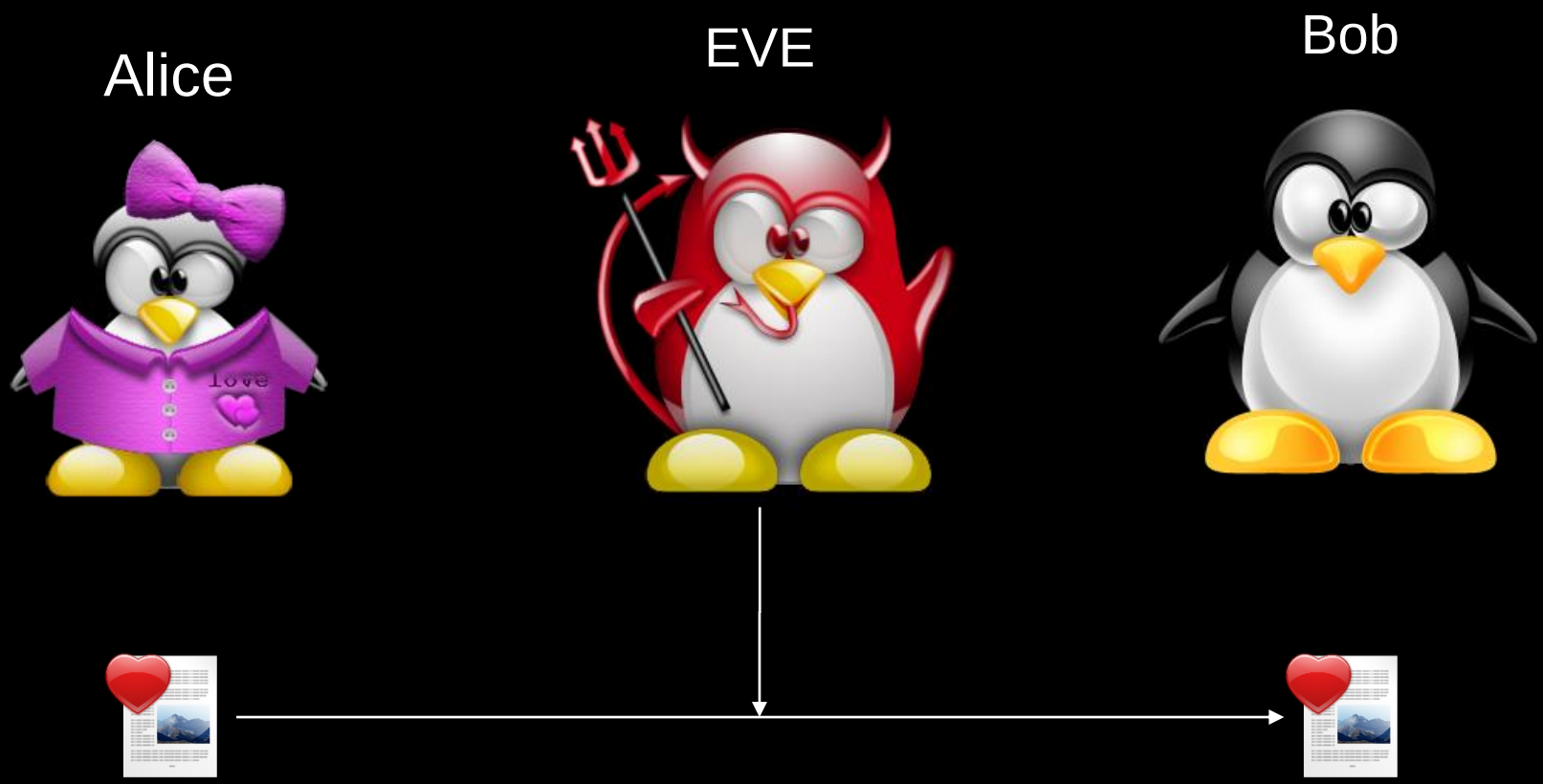
Bob

Il était une fois …

Alice

Bob

Il était une fois …



Historiquement

Garantir le secret de la communication

Scytale

Ve avant JC

Principe

Enrouler le message

Cryptanaylse

Avoir un scytale

Bruteforce

Kama-sutra Manuscrit 45

IV^{e} avant JC

Principe

Substitution mono-alphabétique

Mlecchita-vikalpà

Mélanger les lettres

Exemple

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

Clair = SECURITE INFORMATIQUE

Code = ?

Exemple

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

Clair = SECURITE INFORMATIQUE

Code = M

Exemple

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

Clair = SECURITE INFORMATIQUE

Code = MB

Exemple

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

Clair = SECURITE INFORMATIQUE

Code = MBX

Exemple

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

```
Clair = SECURITE INFORMATIQUE
Code  = MBXRHQOB QFGPHIVOQARB
```

Chiffre de César

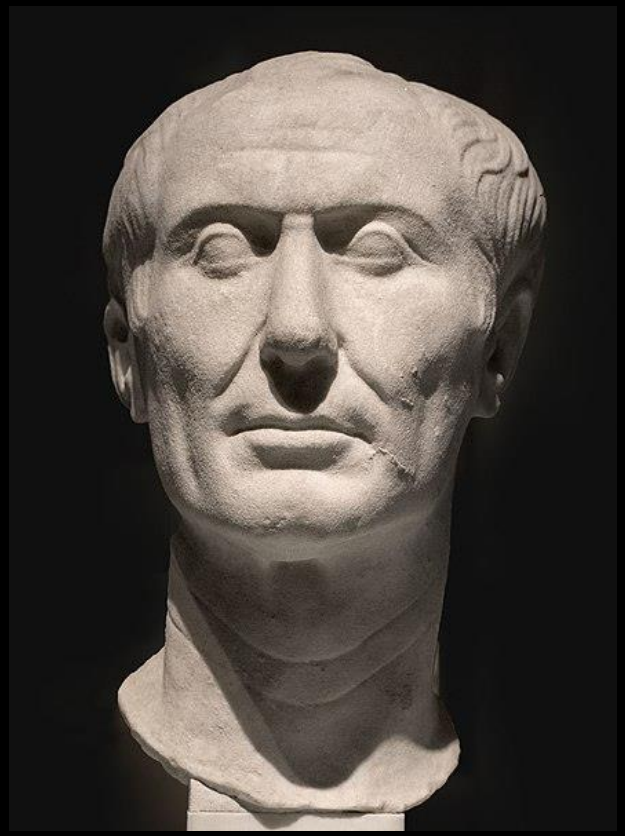
50 avant JC

Code de Cesar

50 av JC

Simplification

Décaler tout de 3 cases



Exemple

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
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

Clair = SECURITE INFORMATIQUE

Code = ?

Exemple

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
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

Clair = SECURITE INFORMATIQUE

Code = V

Exemple

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
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

Clair = SECURITE INFORMATIQUE

Code = VH

Exemple

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
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

Clair = SECURITE INFORMATIQUE

Code = VHF

Exemple

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
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

```
Clair = SECURITE INFORMATIQUE
Code  = VHFXULWH LQIRUPDWLTXH
```

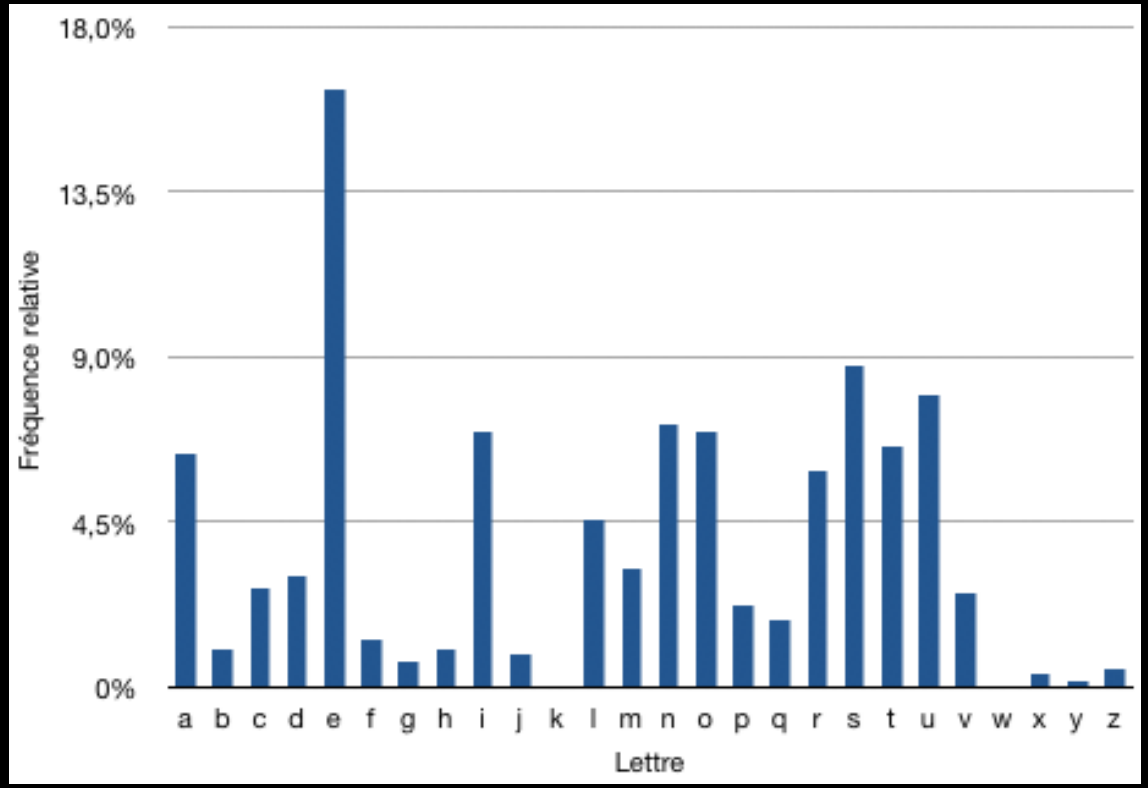
Analyse fréquentielle

IX^{e} siècle

Cryptanalyse

Les lettres ont une fréquence d’apparition

En fonction de la langue



Chiffre d’Alberti

1460

Principe

Deux alphabets désordonnés

On boucle de l’un a l’autre

Exemple

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

Clair = SECURITE INFORMATIQUE

Code = ?

Exemple

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

Clair = SECURITE INFORMATIQUE

Code = V

Exemple

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

Clair = SECURITE INFORMATIQUE

Code = VP

Exemple

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

Clair = SECURITE INFORMATIQUE

Code = VPF

Exemple

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

Clair = SECURITE INFORMATIQUE

Code = VPFI

Exemple

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

Clair = SECURITE INFORMATIQUE

Code = VPFIUCWP LKIMUQDELFXP

Chiffre de Vigenere

1586

Principe

Changer le décalage à chaque lettre

Un mot-clef

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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Exemple

```
Clef    = BAC
Clair   = SECURITE INFORMATIQUE
Chiffre =
```

A	B	C	D	…
B	C	D	E	…
C	D	E	…	…
…	…	…	…	…

Exemple

```
Clef    = BAC
Clair   = SECURITE INFORMATIQUE
Chiffre = T
```

…	…	…	S	…
B			T	
…				
…				

Exemple

```
Clef    = BAC
Clair   = SECURITE INFORMATIQUE
Chiffre = TE
```

A	…	…	E	…
…				
…				
…				

Exemple

```
Clef    = BAC
Clair   = SECURITE INFORMATIQUE
Chiffre = TEE
```

…	…	C	…	…
C		E		
…				
…				

Exemple

```
Clef    = BACBAC
Clair   = SECURITE INFORMATIQUE
Chiffre = TEEV
```

…	…	U	…	…
B		V		
…				
…				

Exemple

```
Clef    = BACBACBA CBACBACBACBA
Clair   = SECURITE INFORMATIQUE
Chiffre = TEEVRKUE KOFQSMCUISVE
```

Cryptanalyse
1863

Estimation de la longueur de la clef

détecter les répétitions

Analyse de fréquences

Clé répétée	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C	D	A	B	C
Texte en clair	M	E	S	S	A	G	E	R	T	R	E	S	M	E	S	Q	U	I	N	M	E	S	O	P	O	T	A	M	I	E	N
Texte chiffré	M	F	U	V	A	H	G	U	T	S	G	V	M	F	U	T	U	J	P	P	E	T	Q	S	O	U	C	P	I	F	P

Grand Chiffre

1691

Principe

1 syllabe

OU

1 mot

OU

1 lettre/ponctuation

OU

1 instruction

=

1 ou plusieurs codes

Cryptanalyse
1893

Déchiffrement « à vue de nez »

À partir du contexte

ADFGVX

1918

Principe

Substitution

+

Transposition

Avec une clef

Exemple - substitution

```
Clair = police
Code  =
```

	A	D	F	G	V	X
A	8	t	b	w	r	q
D	p	4	c	g	2	9
F	3	o	5	m	x	e
G	d	a	z	j	s	y
V	l	h	7	u	v	0
X	n	1	k	6	i	f

Exemple - substitution

```
Clair = police
Code  = AD
```

	A	D	F	G	V	X
A	8	t	b	w	r	q
D	p	4	c	g	2	9
F	3	o	5	m	x	e
G	d	a	z	j	s	y
V	l	h	7	u	v	0
X	n	1	k	6	i	f

Exemple - substitution

```
Clair = police
Code  = AD FD
```

	A	D	F	G	V	X
A	8	t	b	w	r	q
D	p	4	c	g	2	9
F	3	o	5	m	x	e
G	d	a	z	j	s	y
V	l	h	7	u	v	0
X	n	1	k	6	i	f

Exemple - substitution

```
Clair = police
Code  = AD FD VA XV FX
```

	A	D	F	G	V	X
A	8	t	b	w	r	q
D	p	4	c	g	2	9
F	3	o	5	m	x	e
G	d	a	z	j	s	y
V	l	h	7	u	v	0
X	n	1	k	6	i	f

Exemple - transposition

```
Clair        = police
Substitution = AD FD VA XV FX
Clef         = BAC
Chiffré      =
```

B	A	C

Exemple - transposition

```
Clair        = police
Substitution = AD FD VA XV FX
Clef         = BAC
Chiffré      =
```

B	A	C
A	D	

Exemple - transposition

```
Clair        = police
Substitution = AD FD VA XV FX
Clef         = BAC
Chiffré      =
```

B	A	C
A	D	F
D	V	A
X	V	F
X	X	X

Exemple - transposition

```
Clair        = police
Substitution = AD FD VA XV FX
Clef         = BAC
Chiffré      =
```

A	B	C
D	A	F
V	D	A
V	X	F
X	X	X

Exemple - transposition

```
Clair        = police
Substitution = AD FD VA XV FX
Clef         = BAC
Chiffré      = DAFVDAVXFXXX
```

A	B	C
D	A	F
V	D	A
V	X	F
X	X	X

Cryptanalyse
juin 1918

Tester toutes les permutations possibles

Analyse de fréquence des paires

Indice de coïncidence

Enigma

1918

Principe

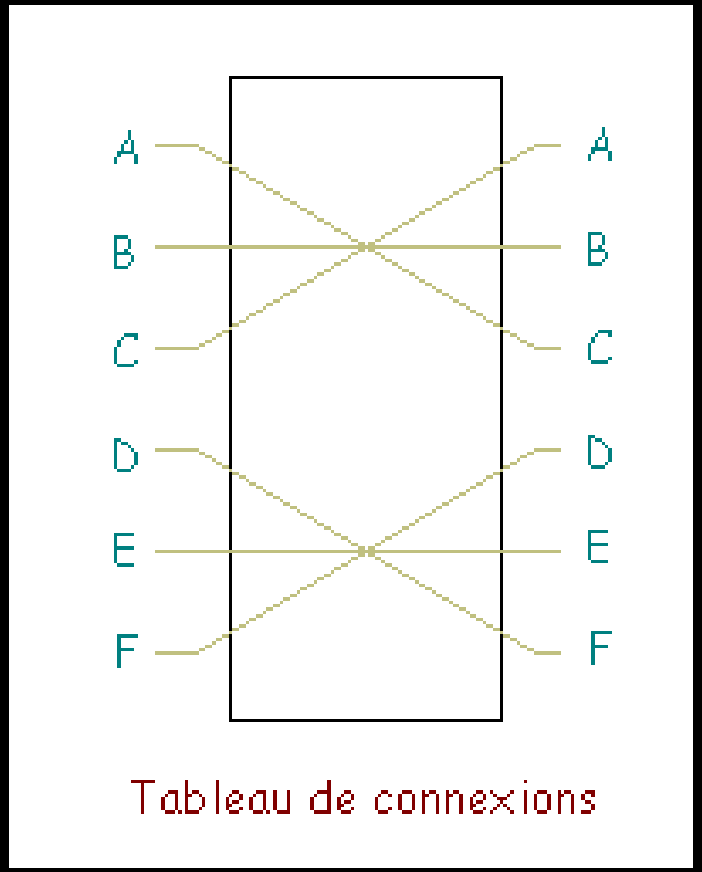
Automatisation

Substitution mono-alphabétique

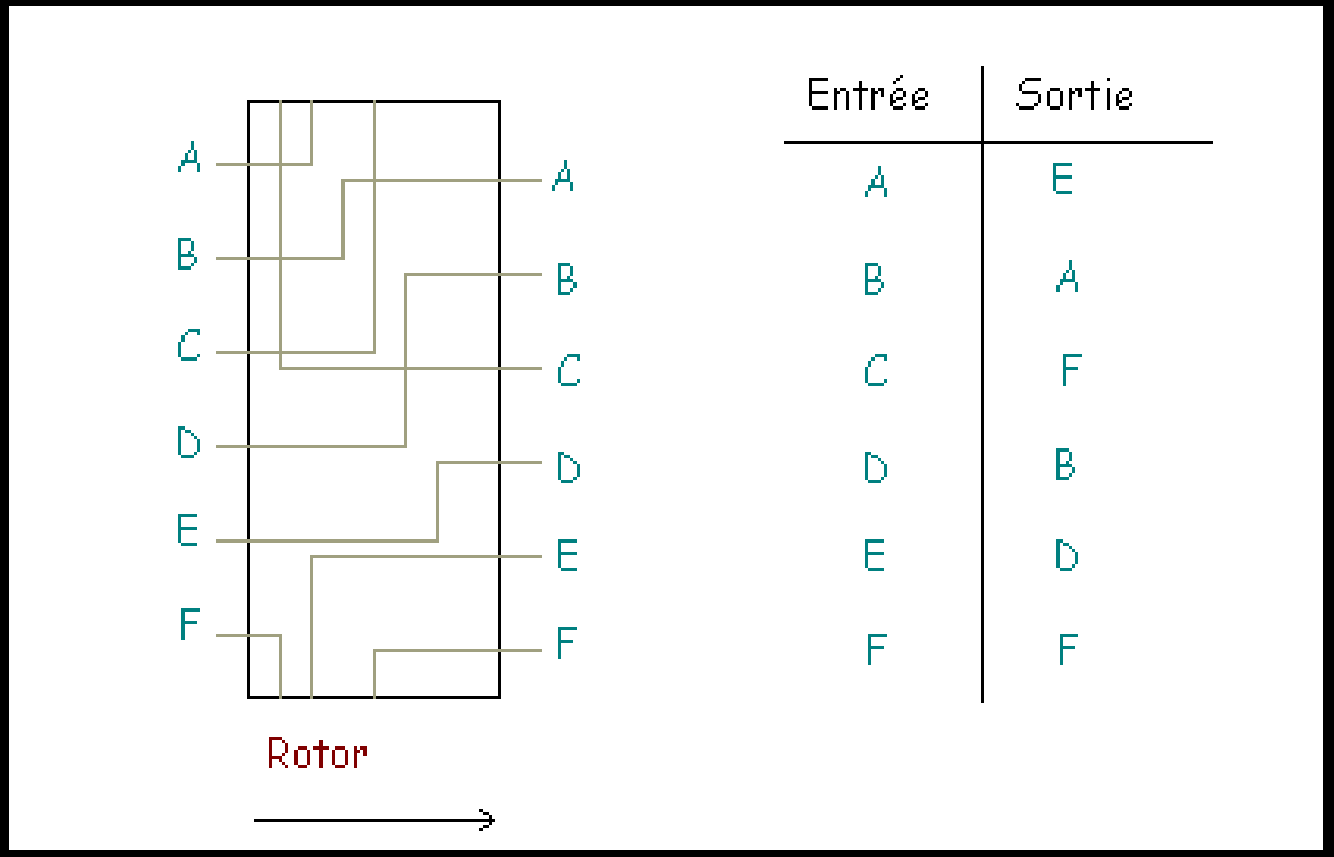
2^{62} clés possibles

Principe

Tableau de connexions

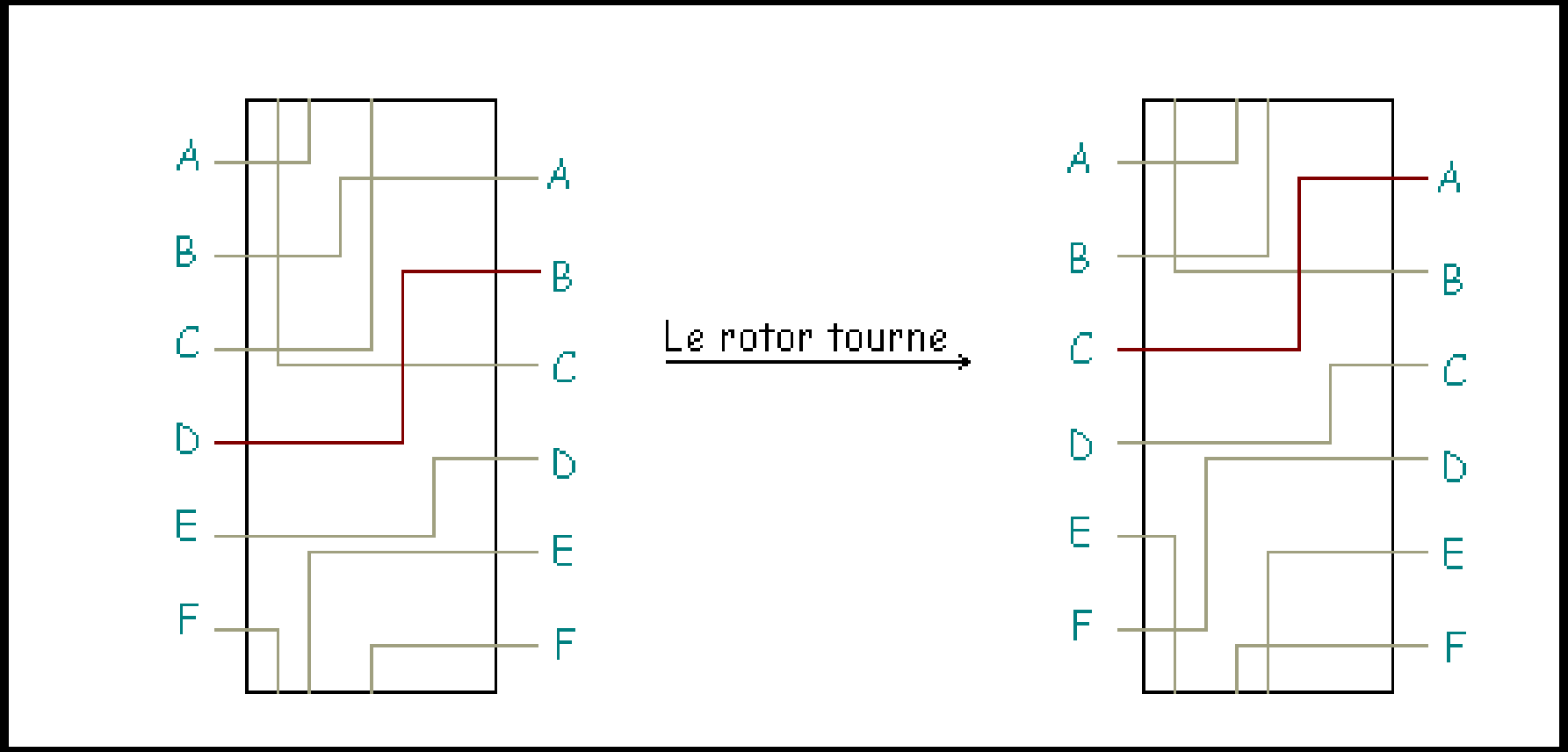


Principe
Rotors

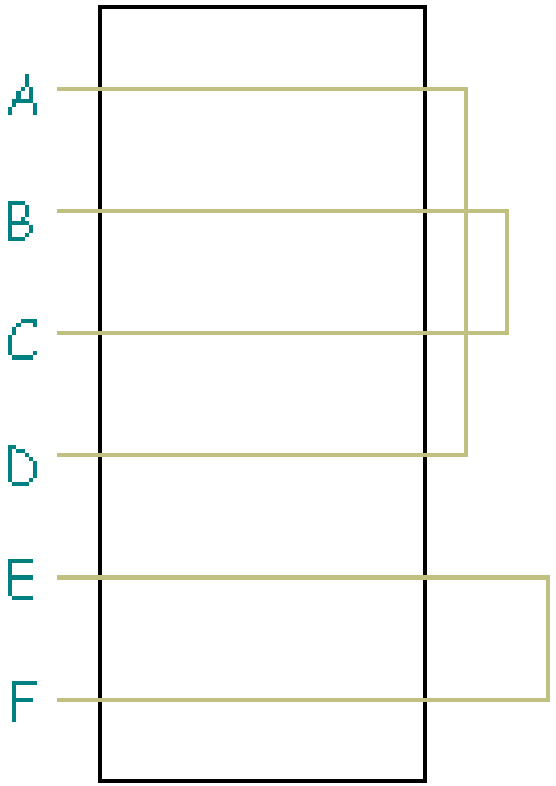


Entrée	Sortie
A	E
B	A
C	F
D	B
E	D
F	F

Principe
Décalage du rotor



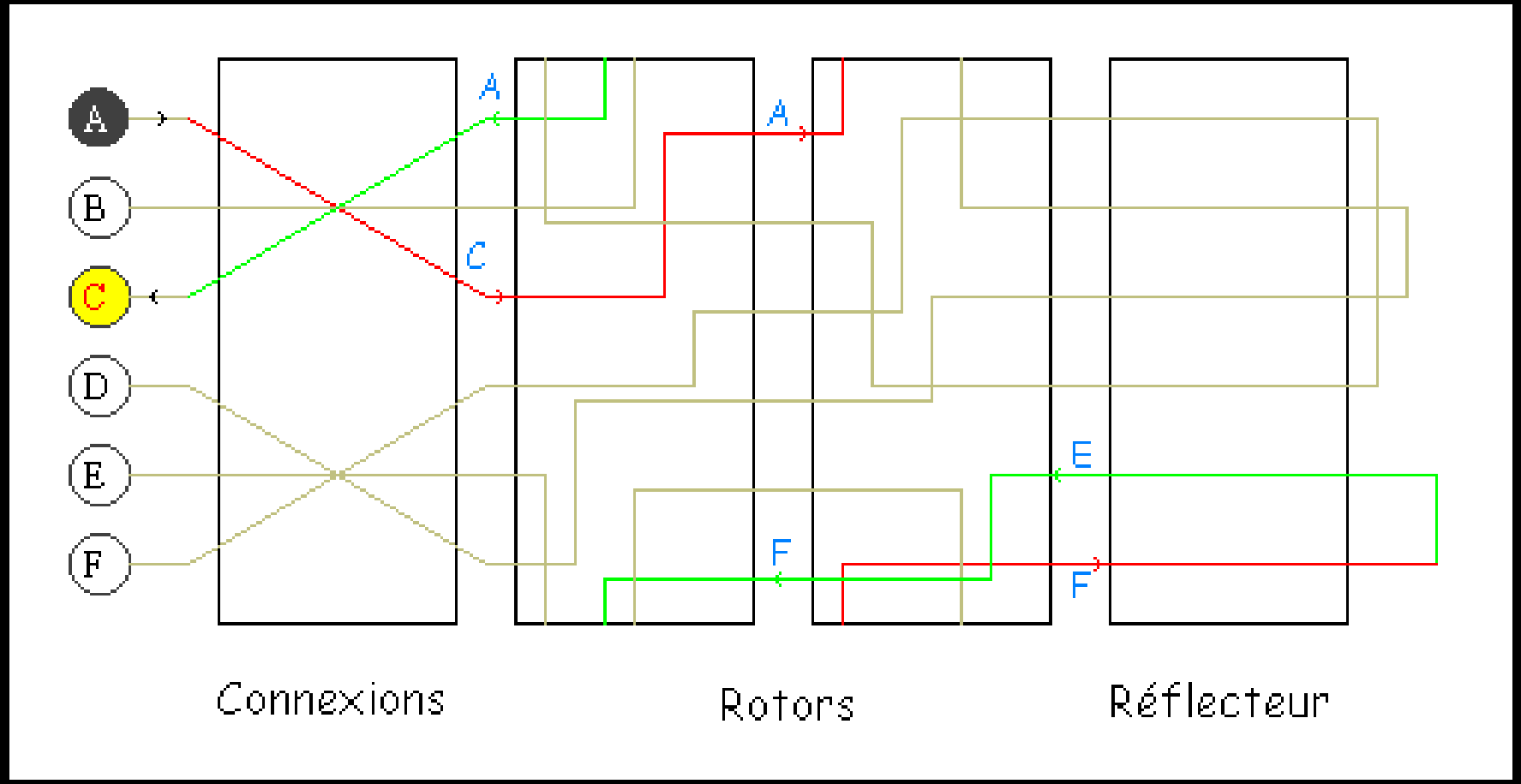
Principe
Reflecteur



A est permuté avec D, B est permuté avec C, et E avec F.

Le réflecteur

Exemple



Cryptanalyse
1940

Cribs

À 6h05 les messages contiennent le mot «wetter»

Bombes

Test exhaustif de toutes les positions de rotors

Cryptographie moderne

Chiffre de Vernam

1890 - 1960

Principe

Combinaison message/clef

Longueur clef = longueur message

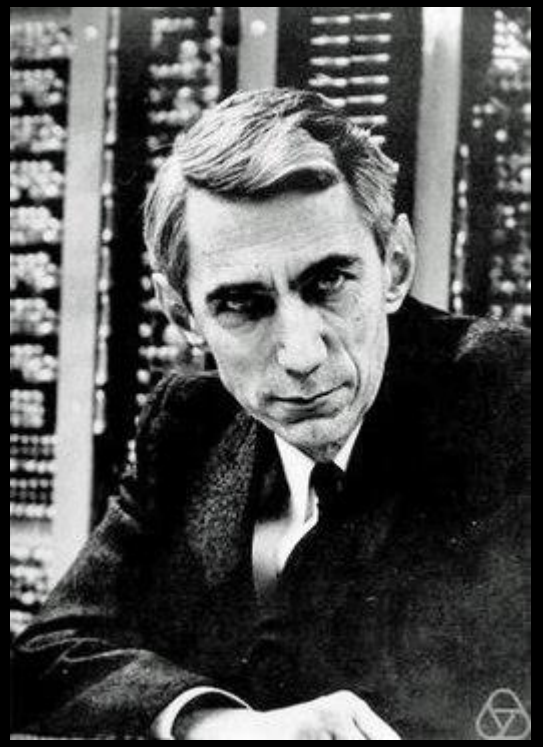
Clef aléatoire

Clef a usage unique

Preuve

1949

Cryptographiquement sûr



Et après ?

Depuis 1960

Standardisation

NIST

AES, RSA, SHA…

La sécurité

Confidentialité	Eve ne peut pas lire le message
Intégrité	Eve ne peut pas modifier le message
Disponibilité	Bob peut lire le message
Authenticité	Bob sait que c'est ce qu'Alice a voulu dire, qu'elle est l'auteur
Anonymat	Eve ne sait pas qui communique avec qui
Non-répudiation	Bob sait que le message a été envoyé
Déni-plausible	Eve ne sait pas si le message est un faux

Quelques définitions

Cryptologie	Art, puis science du secret
Cryptographie	Protéger l'accès à un message
Cryptanalyse	Contourner la cryptographie
Stéganographie	Cacher un message
Stéganalyse	Contourner la stéganographie
Chiffrer	Changer la forme pour rendre illisible.
Crypter / coder	
Déchiffrer	Opération inverse : obtenir la version lisible
Décrypter / décoder	
Hacher	Calculer une empreinte d'une donnée plus grande

Définition légale

- **Art. 29 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique**
  - On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.
  - On entend par prestation de cryptologie toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie.

Définition légale

- **Art. 29 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique**
  - On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.
  - On entend par prestation de cryptologie toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie.

Principe de Kerckhoffs (1835 – 1903)

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

(Journal des sciences militaires, vol. IX, 1883)