

05 Cryptographie

Histoire

Corinne HENIN

www.arsouyes.org

Il était une fois ...

Alice

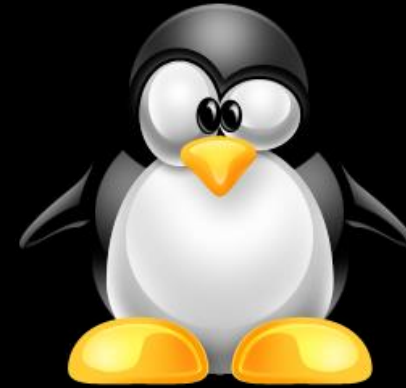


Il était une fois ...

Alice



Bob

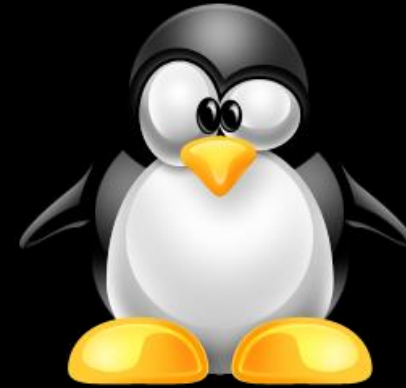


Il était une fois ...

Alice



Bob



Il était une fois ...

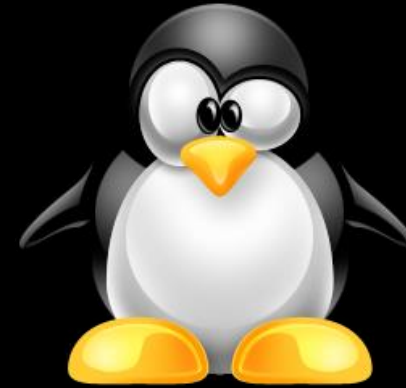
Alice



EVE



Bob



Historiquement

Garantir le secret de la communication

Scytale

Ve avant JC

Principe

Enrouler le message



Cryptanalyse

Avoir un scytale

Bruteforce

Kama-sutra Manuscrit 45

IV^e avant JC

Principe

Substitution mono-alphabétique

Mlecchita-vikalpà

Mélanger les lettres

मंयोवनेतादाचित्वाइश्चावि पधमोमाङ्गावनेनसत विषयत्
तिर्कवितेयोमतिननुचक्षिवइत्यनियतकालत्वात्त्याद्यानु
अप्रचार्येचकारमाहत्याश्चासत्वाप्रतिष्ठावत्वाइधमोदिनि
निष्ठाहतिवक्त्रुतस्वीयितासदशनीतयाषाययोरमितिय
कामावुमानसा मध्यवत्वावती अश्लिकसवायामसयवःउ

उ।मङ्गलपणोपपमतापङ्कडानवादिनाचवर्षःपुत्रवाधीअमिद्वक्त्रातितेपथाद्या
वैतनासिततेत्यासवतेयस्यभक्तितायेवितेयामावुववातावातिपेयुष्वेधमथुतो
यमथ्यतयोवालेतुधमादिषुस्यमातपुयद्यपिसुसंगदितारावैतानेवतुनादापुयु
इत्तापयद्यतितवसासवैत्रात्पथिममपिाषोदनेकोनेधमोधीवपि।इतिविपधमथु
उयोवेत्याथासवततिःपुनवेनेरवेस्मात्वाडावकादवीअमद्यात्विआयहपाधसव



याःकालवेषमिसेनवानिभमयति।यावश्चिदानुगृह्यातमावत्कामे
ःअथ्यनुविद्यायत्तएवईयाएत्तयाद्येनेनसेनेवतिअतस
मथ्यतावातावात्यपिधमार्थकामोनस।वतत्तत्तमवृष्टानव
स्वइयाविवदितस्वत्यत्वावलोकिकायद्योदयशदुविशिष्ट
फलस्यादरीतमायइइष्टकलोःसात्राअलाकिवाःनतवइ
नसवतअप्रथमधमःतद्वहणविद्याताविद्याताविद्यायेनानावस्य।प्रमार्थःननुनतिमय
यक्षिन्तइस्वत्वांश्वमासासति।वाक्येययावितुअप्योअनिअमिन्नितीगशाषाडसुवर्धइई
वाकापिसुयपिजानेनश्चेत्येयतशयिज्ञानेनतुनयमथाहाअलाकिक्त्वाविद्यादिनातेला
अयुएवमातिकत्वादिदितस्वइयाःककमन्तोकिकाइत्यासअइष्टातीवितेनयामनेतु
वशिइष्टसमख्याधवतभवनेतस्तिअयइनाःआदिशहात्रुपश्वपणादयःतमामवइतीनी

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 = SEURITE 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

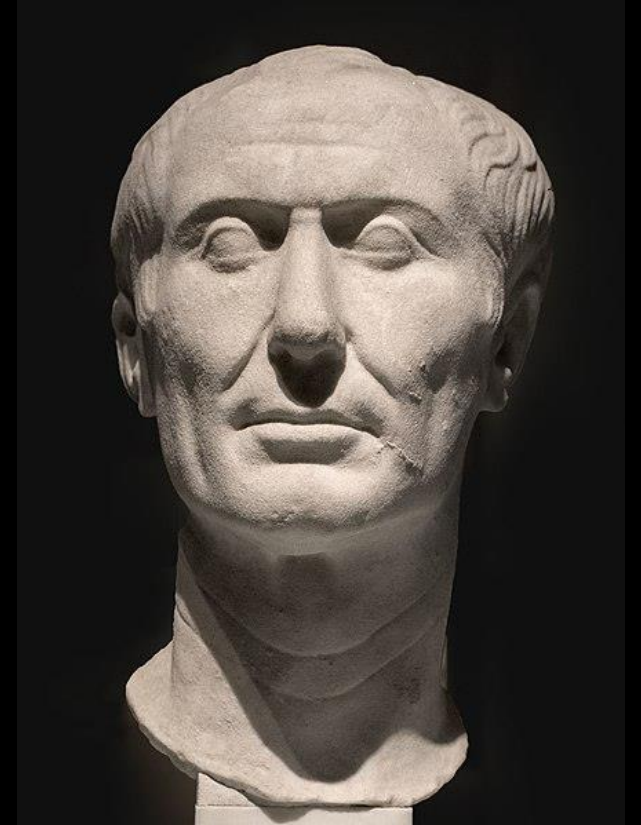
50 avant JC

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 = SEURITE 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

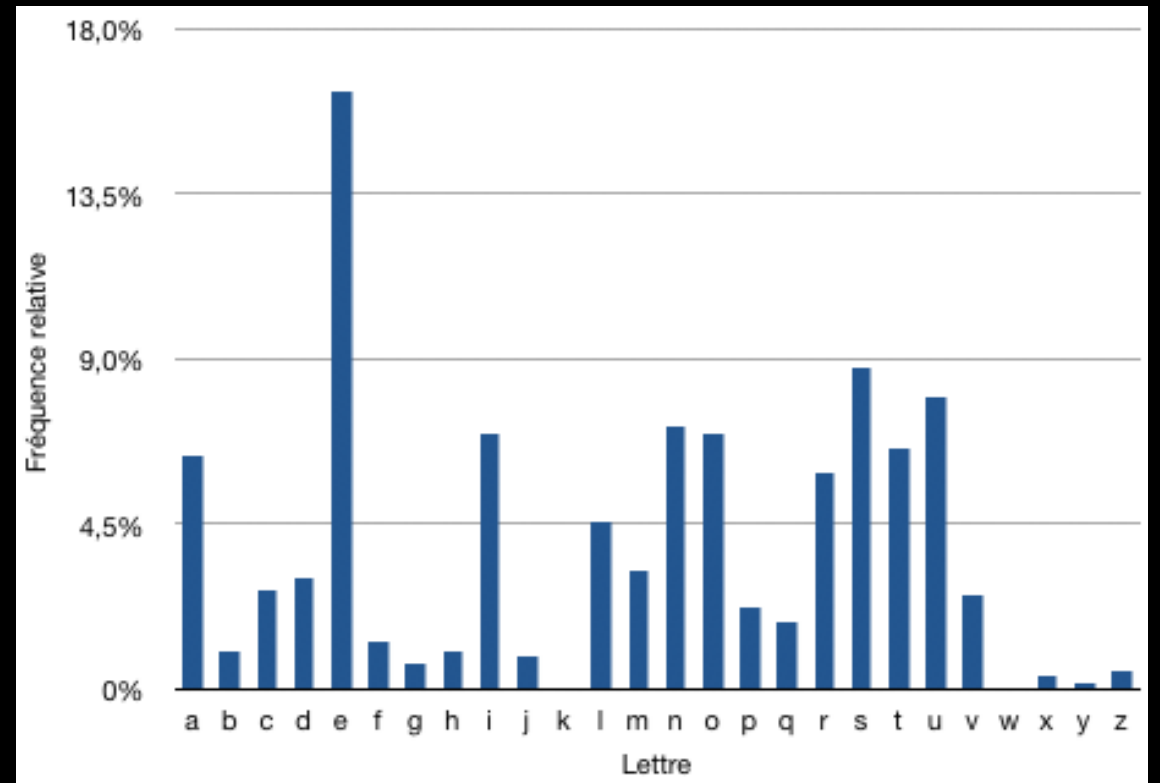
Analyse fréquentielle

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 = VP**F**

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~~I~~

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 = SEURITE 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 KOFQSMCUIISVE

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				
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



N	O	P	Q	R	S	T	V	X	Y	Z	&
811	117 238	219	407	511	555	340	141 163	205	518	820	279 448
702	359 500	338	595	733	527	618	284 164	436	639		615 827
genera, l. uax.	35		lieu, x.		668	Ob.		19	presque.		801
gens.	55		limites.		708	obei.		59	preterit, dre. tion.		30
ger.	575	95	liore		728	objet, s.		69	pretexte.		841
ges.		115	le Roy de.		758	oblig, er, ation.		89	pri.		881
gla.		155	le Prince, de		798	observ, er, ation.		129	principal, uax.		52
gle.		215	le Duc de.		838	obstacle, s.		179	prisonnier, s.		132
gli.		275	le Marquis de.		858	obtenir.		220	pro.		162
glo, ire.		335	le Baron de.		898	oc, casion.		249	prochain.		202
gna.		375	le Sieur de.		49	ocup, er.		289	profit, er.		262
gne.	845	435	loin.		79	of.		349	projet, s.		282
gni.		485	lon.		119	office, ier, s.		429	propos, ition, s.		382
gno.		505	lors.		189	offre, s.		449	provision, s.		422
gouvern, er, ment.	16		luy.	848	239	oient.		499	prouv.		442
gra, ce.	405		Ma 865			298	oir.		529	pru.	462
grand.	525		me.	779	339	oite.		559	publi, er, c.		512
gre.	585		mi.		379	oit.		629	puis, sance.		572
gri.	625		mo.		439	ol.		669	QU		
gro.	665		mu.		489	om.		729	qua.		642
gua.	695		magasin, s.		519	on, s.		759	qualite.		722
gue.	735		main, s.		549	ont,		739	quand.		742
guerre.	825		mais.	159	579	op, pose, ition.		819	quantite.		762
gui, de, s.	895		maitre, s.		609	or.		849	quarente.		782
ha			mal, ade, s, je, s.		639	ordinaire, s.		899	quart, ier, s.		822
be.	56		mand, er,		679	ordonn, er.		20	quatre.		842
bi.	156		maniere, s.		719	ordre, s.		60	que.		862
bo.	216		manque, r.		739	or, s, t.		100	quel, le, s.		882
bu.	266		marche, s.		769	os, t.		130	question, s.		25
baut.	326		marqu, e, r.		799	ou, r.		160	qui.	50	53
babi, t, le, tant.	486		marecha, f, uax.		829	ouvr.		240	qu'il.		75
keur, e, s.	656		mauvais.		859	La			quinze.		153
bier.	796		meilleur.		879			270	quo, n.	390	153

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

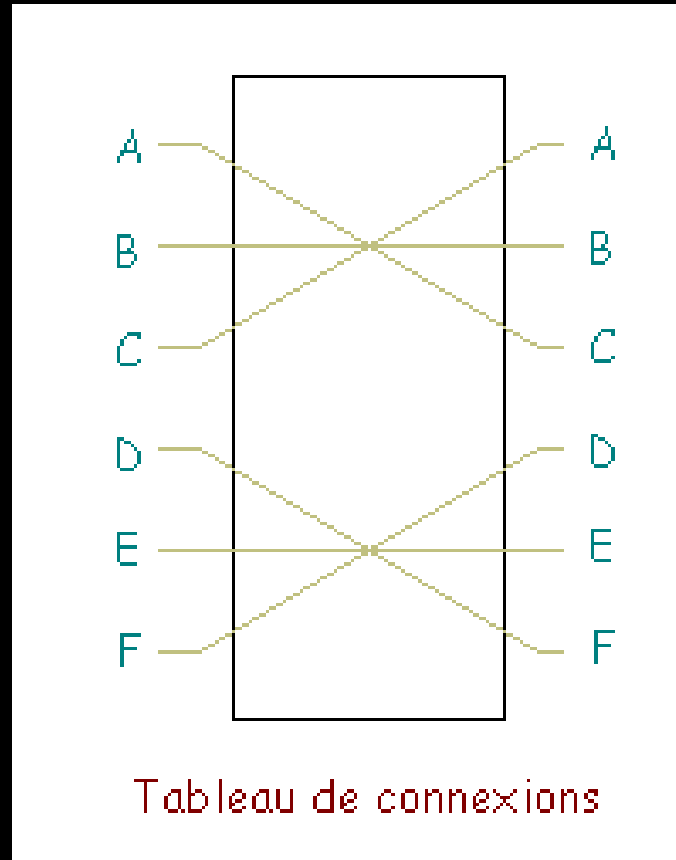
Substitution mono-alphabétique

2^{62} clés possibles

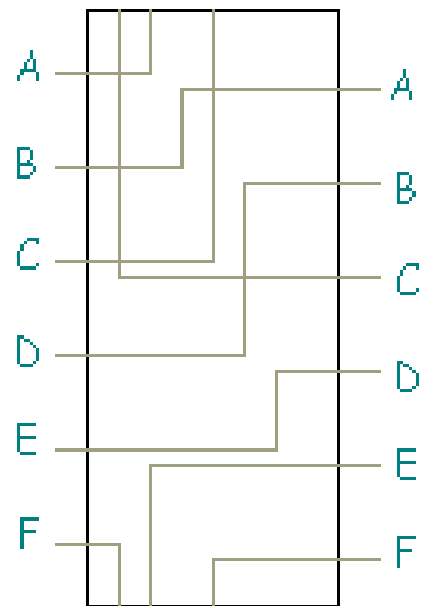


Principe

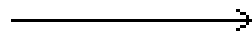
Tableau de connexions



Principe Rotors



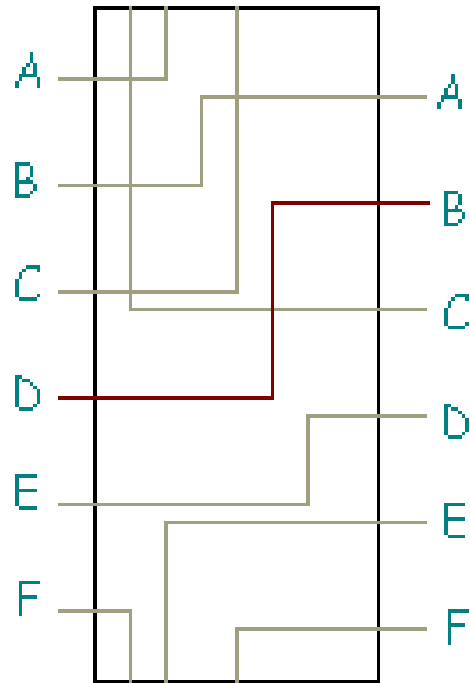
Rotor



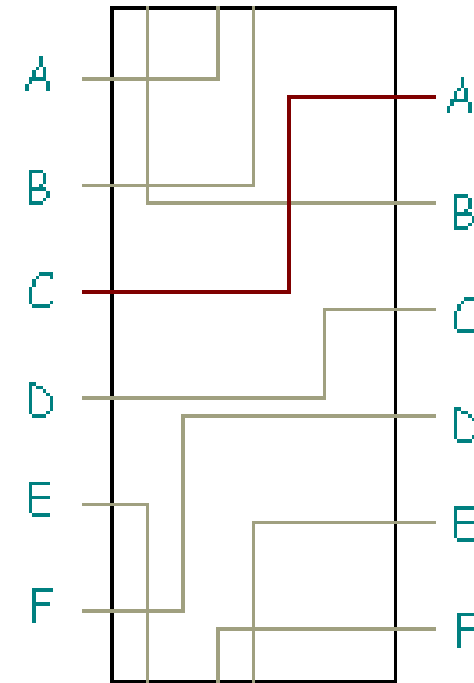
Entrée	Sortie
A	E
B	A
C	F
D	B
E	D
F	F

Principe

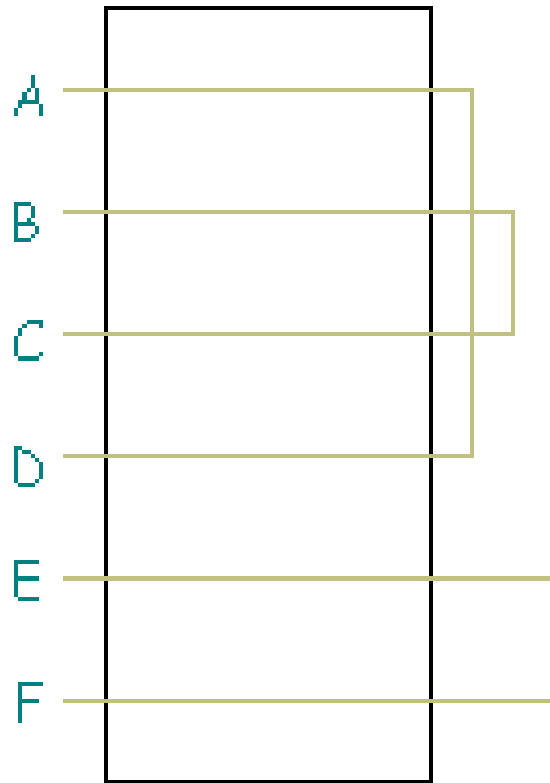
Décalage du rotor



Le rotor tourne →



Principe Reflecteur



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

Le réflecteur

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

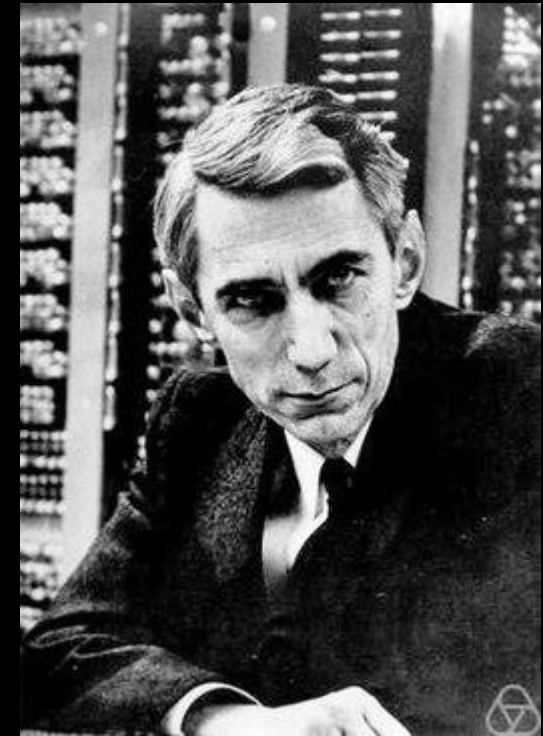
Clef a usage unique



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)