Cryptographie et Cryptanalyse

Christophe Bidan

Références

- Historique *:*
  - *Histoire des codes secrets : de l'Égypte des pharaons à l'ordinateur quantique*, Simon Singh.
- Introduction :
  - *Cryptographie appliquée : protocoles, algorithmes, et code source en C*, Bruce Schneier.
- Approfondir :
  - *Handbook of Applied Cryptography*, A. Menezes, P. van Oorschot and S. Vanstone.

    `http://www.cacr.math.uwaterloo.ca/hac/index.html`

Introduction

- Stéganographie : (στεγανο - γραφην)
  écriture couverte.

- Cryptographie : (κρυπτο - γραφην)
  écriture cachée / brouillée.

Stéganographie

Information non-chiffrée

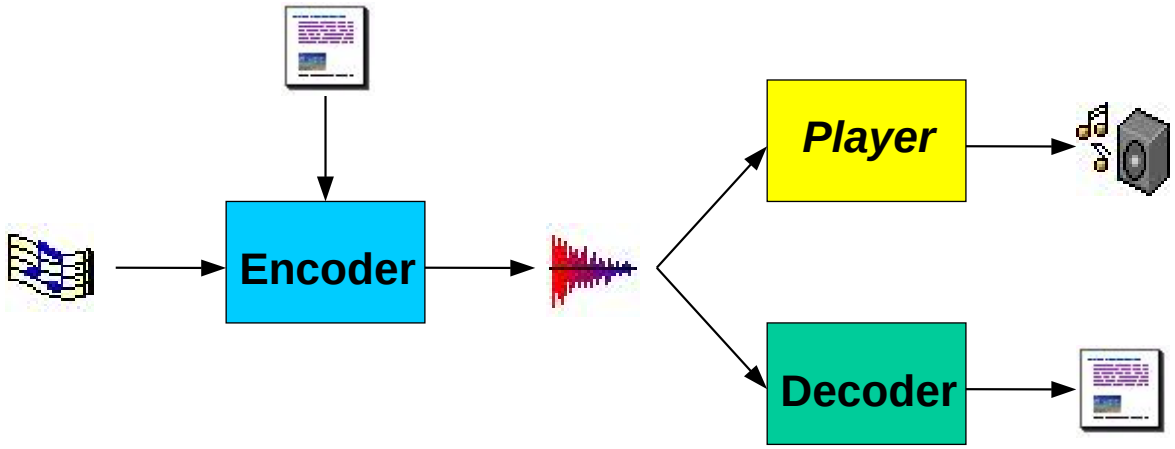
Connaissance de l'existence de l'information
=
connaissance de l'information

Exemples de stéganographie

- Message *couvert* :
  - Tablette couverte de cire
  - Crane du messager
- Message *invisible* :
  - Encre invisible (Pline - 1er siècle avant JC)
- Message *illisible* :
  - Micro-film sous la forme d'un point.

Exemple de MP3Stegano ...

Inclusion de texte dans un fichier MP3



Stéganographie

- Faible niveau de sécurité :
  - R. Anderson and F. Petitcolas. *On The Limits of Steganography*. IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998.

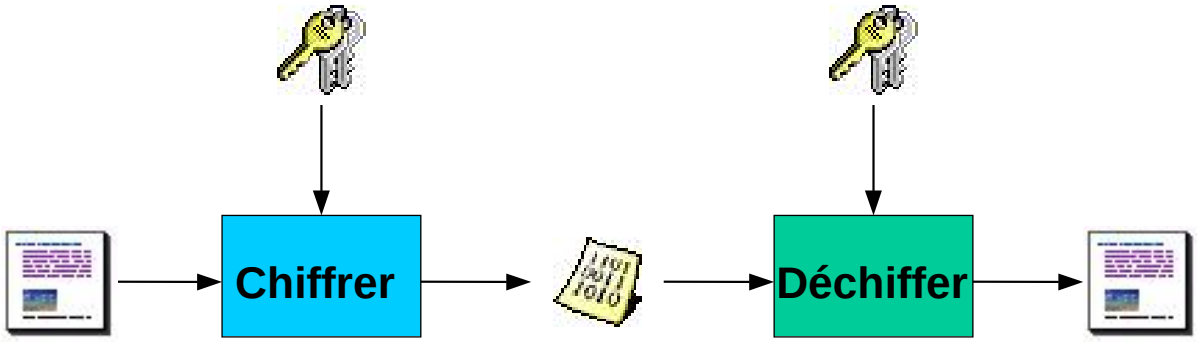
- Utilisation pour le *watermarking* :
  - Images JPEG, Fichiers MP3 ...

Cryptographie

Information chiffrée

Connaissance de l'existence de l'information
≠
connaissance de l'information

Algorithme de cryptographie

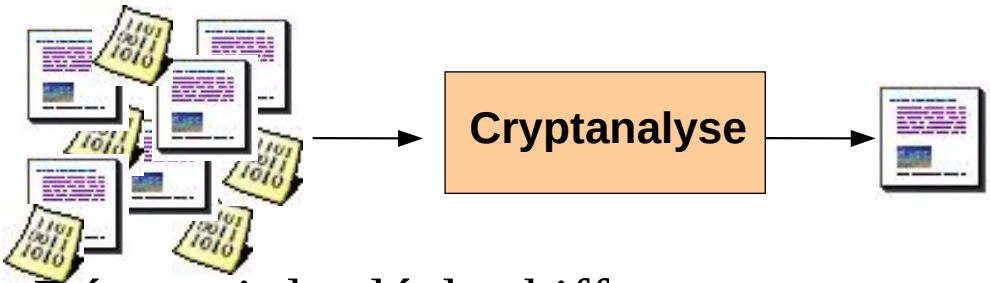


Principes de la cryptographie

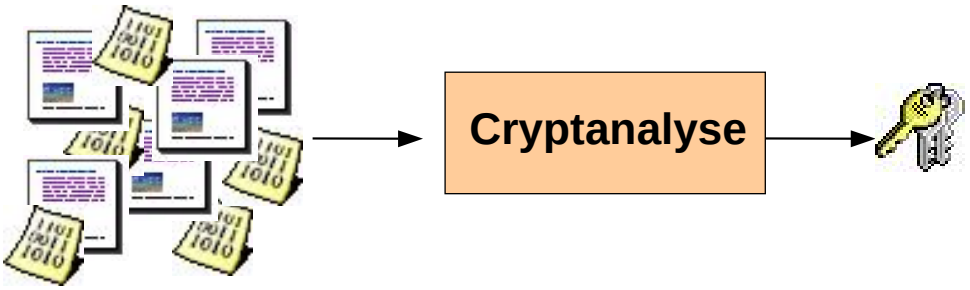
- Principe de Kerckhoffs : la sécurité repose sur le secret de la clé, et non sur le secret de l'algorithme (19ème siècle).
- Le déchiffrement sans la clé est impossible (*à l'échelle humaine*).
- Trouver la clé à partir du clair et du chiffré est impossible (*à l'échelle humaine*).

Cryptanalyse

- Déchiffrer les messages sans connaître la clé.



- Découvrir la clé de chiffrement.



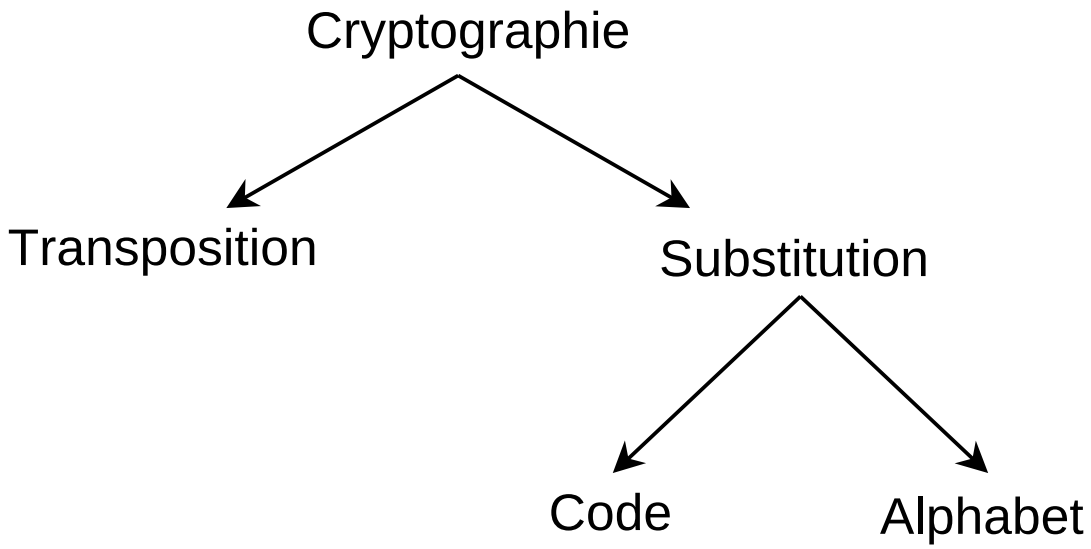
Objectifs de ce cours

- Introduire les bases de la cryptographie moderne.
- Introduire les bases de la cryptanalyse moderne.
- Comprendre les principes de bases de la cryptographie.

Plan

- **Histoire de la cryptographie et de la cryptanalyse**
- Outils moderne de la cryptographie
- Cryptographie symétrique
- Cryptographie asymétrique

Histoire de la cryptographie

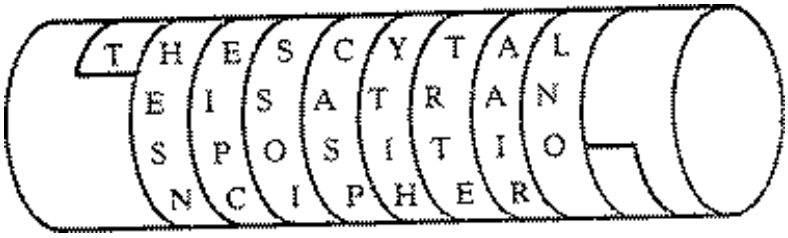


Transposition

- Chiffrement type *anagramme.*
- Niveau de sécurité *théorique* :
  - Message de 35 lettres : 35! chiffrés possibles.
- Problème :
  - Nécessite un système *rigoureux* pour aider le déchiffrement (i.e., une clé).

Exemple de transposition

La *scytale* spartiate (5ème siècle av. JC) :



Exemple de transposition

Ecriture *en dents de scie* :

LA TRANSPOSTION PERMET EN THEORIE D'AVOIR UN HAUT DEGRE DE SECURITE

L	R	S	S	I	P	M	E	H	R	D	O	U	A	D	R	E	C	I
A	A	P	I	O	E	E	N	E	I	A	I	N	U	E	E	S	U	T
T	N	O	T	N	R	T	T	O	E	V	R	H	T	G	D	E	R	E

LRSSIPMEHRDOUADRECIAAPIOEENEIAINUEESUTTNOTNRTTOEVRHTGDERE

Cryptanalyse de la transposition

- Découvrir le système *rigoureux* de déchiffrement (i.e., la clé).
  - Très difficile en général, mais …
- Gestion et distribution des clés difficiles.

Peu utilisé seul !

Substitution

- Chiffrement en changeant d'alphabet.
  - Kama Sutra : *mlecchita-vikalpà* ou art de l'écriture secrète (4ème siècle av JC).
- Niveau de sécurité *théorique* :
  - Alphabet à 26 lettres : 26! alphabets possibles.
- Problème :
  - Chaque lettre du message conserve sa place d'origine.

Exemple de substitution

Chiffrement de *Caesar*

Alphabet clair : abcdefghijklmnopqrstuvwxyz

Alphabet chiffré : DEFGHIJKLMNOPQRSTUVWXYZABC

Texte clair :

errare humanum est, perseverare diabolicum

Texte chiffré :

HUUDUH KXPDQXP HVW, SHUVHYHUDUH GLDEROLFXP

Substitution monoalphabétique

Alphabet clair : abcdefghijklmnopqrstuvwxyz

Alphabet chiffré : MOTSECRUVWXYZABDFGHIJKLNPQ

Texte clair :

l'erreur est humaine, y persévérer est diabolique

Texte chiffré :

Y'EGGEJG EHI UJZMVAE, P DEGHEKEGEG EHI SVMOBYVFJE

Cryptanalyse de la substitution monoalphabétique

- Principe (Al-Kindi - 9ème siècle) :

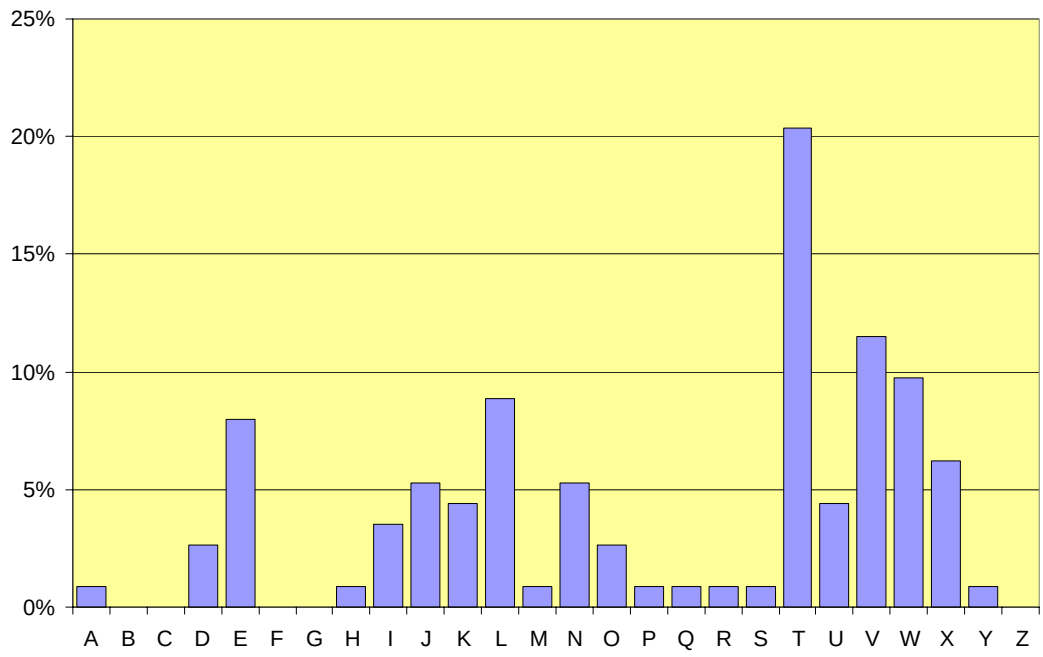
Lettre	Fréquence %
A	**9.42**
B	**1.02**
C	**2.64**
D	**3.39**
E	**15.87**
F	**0.95**
G	**1.04**
H	**0.77**
I	**8.41**
J	**0.89**
K	**0.00**
L	**5.34**
M	**3.24**

Lettre	Fréquence %
N	**7.15**
O	**5.14**
P	**2.86**
Q	**1.06**
R	**6.46**
S	**7.90**
T	**7.26**
U	**6.24**
V	**2.15**
W	**0.00**
X	**0.30**
Y	**0.24**
Z	**0.32**

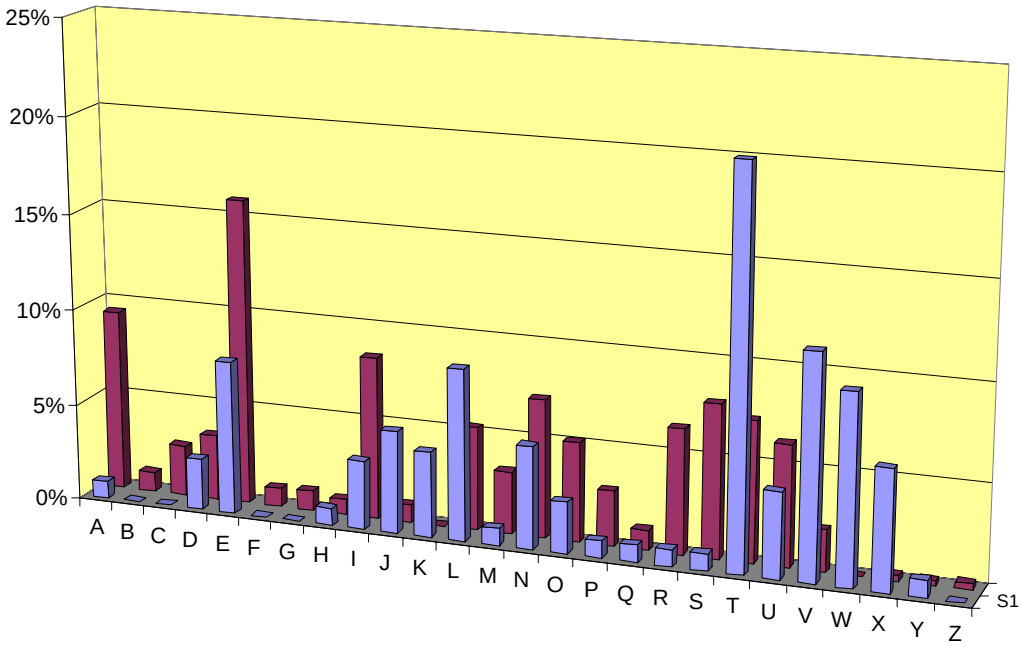
Exemple de cryptanalyse de la substitution monoalphabétique

JTVMNKKTVLDEVVTLWTWITKTXUTLWJ
ERUTVTWTHDXATLIUNEWV.
JTVIEVWELOWENLVVNOEDJTVLTPTXYT
LWTWUTSNLITTVQXTVXUJXWEJEWTON
KKXLT.

Analyse de fréquences



Comparaison des fréquences



Début du déchiffrement ...

JeVMNKKeVLDE*VV*eLWeWIeKeXUeLWJ
ERUeVeWeHDXAeLIUNEWV.
JeVIEVWELOWENL*VV*NOEDJeVLePeXYe
LWeWUeSNLIeeVQXeVXUJXWEJEWeON
KKXLe.

… suite du déchiffrement ...

lesMNKKesLDEsseLtetIeKeureLtlERreseteH
DuAeLIrNEts.
lesIEstELOtENLssNOEDlesLePeuYeLtetreS
NLIeesQuesurlutElEteONKKuLe.

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
				T							J	K	L				U	V	W	X	Y	Z	A	B	C

… suite du déchiffrement ...

les MNmmes nDEssent et Iemeurent
lERres et eHDux en IrNEts.
Les IEstEnOtENns sNOEDles ne Peuvent etre
SNLIees Que sur lutElEte ONmmune.

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
				T							J	K	L				U	V	W	X	Y	Z	A	B	C

… fin du déchiffrement.

« Les hommes naissent et demeurent
libres et égaux en droits.
Les distinctions sociales ne peuvent être
fondées que sur l'utilité commune. »

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

Limite de l’analyse de fréquence

- «De Zanzibar à la Zambie et au Zaïre, des zones d ’ozone font courir les zèbres en zigzags zinzins.»

- *La disparition*, de Georges Perec.

Variante de la substitution monoalphabétique

- Utilisation de caractères *nuls*.
- Mauvaise orthographe.
- Utilisation de *mots de code* : *nomenclature*.
- Alphabet chiffré tenant compte des fréquences.
- Substitution homophonique.

Code et nomenclature

- Substitution à l'aide de code :

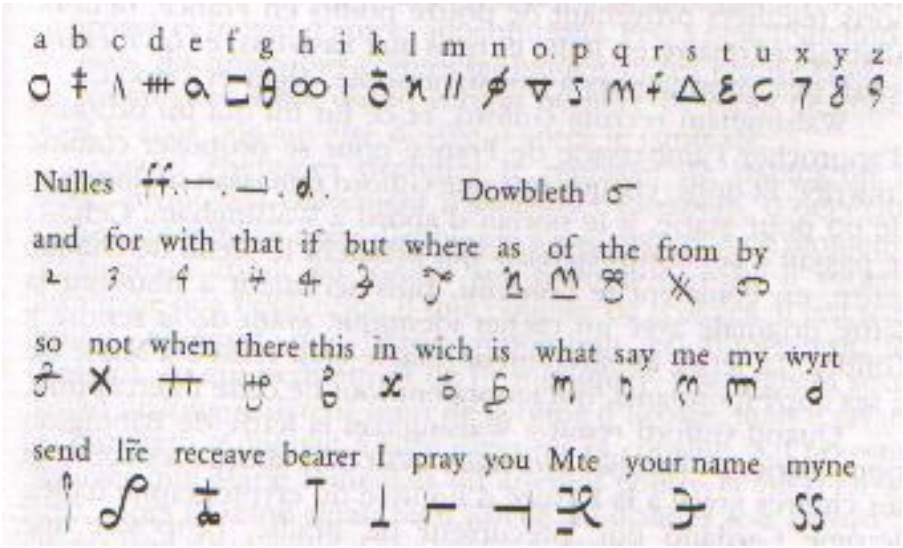
  «Les sanglots longs des violons de l'automne bercent mon cœur d 'une langueur monotone.»

  Verlaine.

- Niveau de sécurité *théorique* : *infini*.
- Problème :
  - Définition et gestion du dictionnaire.

Code et *nomenclature*

- Substitution monoalphabétique et codes :
  - Marie Stuart, reine d'Ecosse (16ème siècle).



Code et *nomenclature*

- Niveau de sécurité *théorique* :
  - Dépend du nombre de codes utilisés.

- Cryptanalyse :
  - Idem à substitution monoalphabétique.
  - Codes déduits du contexte.

Substitution monoalphabétique fréquencielle

- Alphabet chiffré tenant compte des fréquences :

Lettre	%	Chiffre
A	**9**	**09 12 33 47 48 53 67 78 92**
B	**1**	**81**
C	**3**	**13 41 62**
D	**3**	**01 03 45**
E	**16**	**06 10 14 16 23 24 44 46 54 55 57 74 79 82 87 98**
F	**1**	**31**
G	**1**	**25**
H	**1**	**39**
I	**8**	**32 50 56 70 73 83 88 93**
J	**1**	**15**
K	**0**	**04**
L	**5**	**26 37 51 65 84**
M	**3**	**22 27 68**

Lettre	%	Chiffre
N	**7**	**18 58 59 66 71 91 99**
O	**5**	**00 05 07 54 72**
P	**3**	**38 90 95**
Q	**1**	**94**
R	**6**	**29 35 40 42 77 80**
S	**8**	**11 19 21 36 76 86 96 97**
T	**7**	**17 20 30 43 49 69 75**
U	**6**	**02 08 61 63 85 90**
V	**2**	**34 52**
W	**0**	**60**
X	**0**	**28**
Y	**0**	**24**
Z	**0**	**01**

Substitution monoalphabétique fréquencielle

- Niveau de sécurité *théorique* :
  - Supérieur à la substitution monoalphabétique.
- Cryptanalyse :
  - Idem à substitution monoalphabétique sur les digrammes.

Substitution homophonique

- Chiffrer les homophones.
- Niveau de sécurité *théorique* :
  - Supérieur à la substitution monoalphabétique.
- Cryptanalyse :
  - Idem à substitution monoalphabétique sur les homophones.

Résumé sur la substitution monoalphabétique

- Cryptanalyse basée sur l'analyse de fréquences.
- Niveau de sécurité faible *en général* :
  - *Impossibilité* de déchiffrer certaines substitutions (*à l'échelle humaine*).

Exemple de substitution monoalphabétique *indéchiffrable*

- Chiffre de Beale ou chiffre du livre :
  - Utilisation d'un texte *quelconque*.
  - Numérotation des 1$^{\text{ères}}$ lettres de chaque mot pour définir l'alphabet de chiffrement.
- Cryptanalyse :
  - Trouver le texte (e.g., Déclaration d'Indépendance) ou bien … ?

Extensions à la substitution monoalphabétique

- Faiblesse de la substitution :
  - Une lettre / un digramme est toujours chiffré(e) *de la même manière*.
- Idée :
  - Faire évoluer l'alphabet chiffré en cour de chiffrement.

Extensions à la substitution monoalphabétique

- Substitution polyalphabétique :
  - Utilisation de deux ou plusieurs alphabets de chiffrement.
- Combiner transposition et substitution :
  - Base de la cryptographie moderne.

Substitution polyalphabétique

Alphabet clair : abcdefghijklmnopqrstuvwxyz

Alphabet chiffré 1: MOTSECRUVWXYZABDFGHIJKLNPQ

Alphabet chiffré 2: QPNLKJIHGFDBAZYXWVURCESTOM

Texte clair :

vinum et musica laetificant cor

Texte chiffré :

KGACZ KI AJUVNM BMKIGCGTQAR TYG

Chiffre de Vigenère

(16ème siècle)

- Définition du carré de Vigenère :
  - 26 alphabets : chiffrement de *Caesar*.
- Définition de la clé de chiffrement :
  - *Mot-clé* identifiant les alphabets à utiliser.

Carré de Vigenère

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
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

Exemple d'utilisation du carré de Vigenère

- Choix du mot-clé : *key*.
- Alphabets de chiffrement :

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
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
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
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

- Chiffrement d'un message :

m	e	n	s	s	a	n	a	i	n	c	o	r	p	o	r	e	s	a	n	o
K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y
W	I	L	C	W	Y	X	I	G	X	G	M	B	T	M	B	I	Q	K	R	M

Cryptanalyse de la substitution polyalphabétique

C. Babbage (19ème siècle)

- Principe en deux étapes :
  - Trouver la longueur du mot-clé.
  - Analyse fréquencielle sur chacun des alphabets.
- Longueur du mot clé :

e	t	e	t	e	t	e	t
K	E	Y	K	E	Y	K	E
O	X	C	D	I	R	O	X

h	i	v	e	r	h	i	v	e	r	h	i	v	e	r	h	i	v	e	r
K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E
R	M	T	O	V	F	S	Z	C	B	L	G	F	I	P	R	M	T	O	V

Exemple de cryptanalyse de la substitution polyalphabétique

NLPKMVGNSOXYPTGCEMQYHGDTGY
WGPWGEHGDSRTRKZRUPWVFRFPWFC
SKEWNPWRWYUAVGNMGFBFPPJZQOP
XQFXETXQJIPAIWEHQYGRLVNPVGNV
KCIKXTTTQGCPKMVGXIPEWCFJCCIRZ
RFCIFPPCMYUOIEPXVPPKMITEIFLRUW
IUNEUOIVPVOTRGDTCCPCWSK.

Début de la cryptanalyse ...

Longueur du mot-clé = ?

NLPKMVGNSOXYPTGCEMQYHGDTGY
WGPWGEHGDSRTRKZRUPWVFRFPWFC
SKEWNPWRWYUAVGNMGFBFPPJZQOP
XQFXETXQJIPAIWEHQYGRLVNPVGNV
KCIKXTTTQGCPKMVGXIPEWCFJCCIRZ
RFCIFPPCMYUOIEPXVPPKMITEIFLRUW
IUNEUOIVPVOTRGDTCCPCWSK.

… suite de la cryptanalyse ...

Longueur du mot clé = 3

Séquence	Espace	Facteurs premiers
HGD	12	2 – 3
PW	6	2 – 3
	9	3
FP	24	2 – 3

… suite de la cryptanalyse ...

Message chiffré avec alphabet 1 :

NKGOPCQGGGGGRKUVFFKNRUGGFJOQEQPWQRNG
KKTGKGPCCRFFCUEVKTFUUUVOGCCK

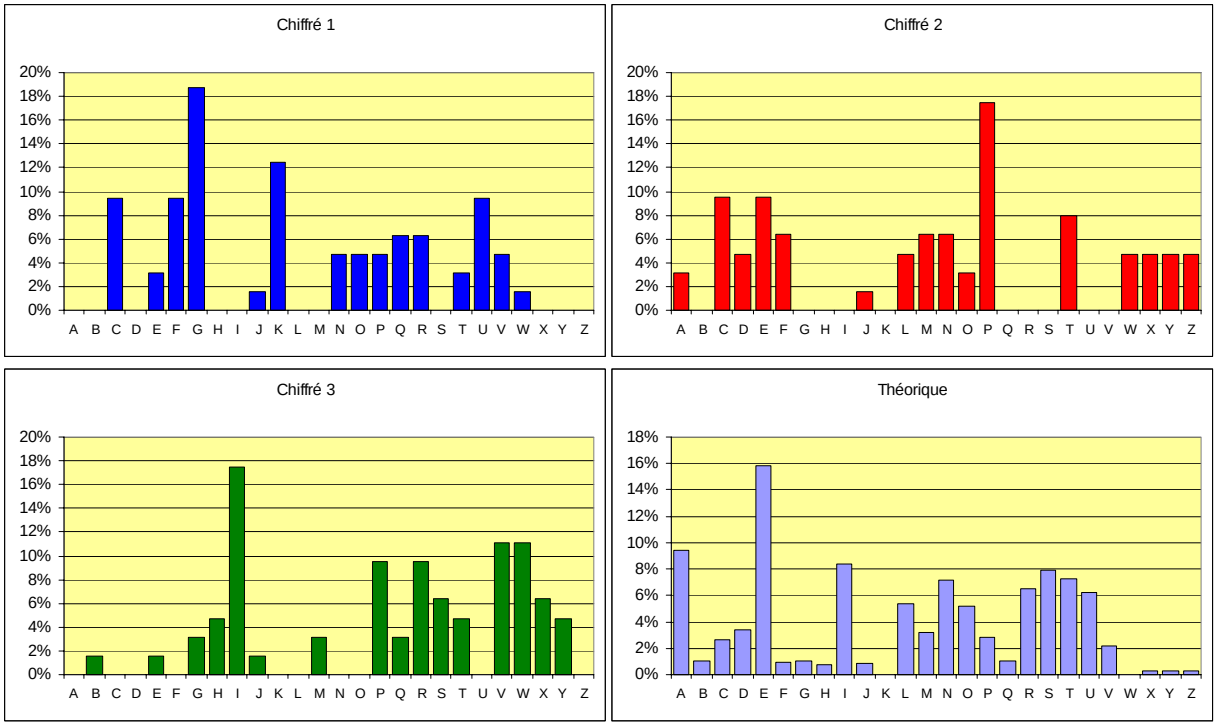
Message chiffré avec alphabet 2 :

LMNXTEYDYPEDTZPFPCEPWANFPZPFTJAEYLPNCX
TCMXEFCZCPMOPPMELWNOPTDCW

Message chiffré avec alphabet 3 :

PVSYGMHTWWHSRRWRWSWWYVMBPQXXXIIHGV
VVITQPVIWJIRIPYIXPIIRIEIVRTPS

… suite de la cryptanalyse ...



… fin de la cryptanalyse.

« La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme ; tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi. »

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
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
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
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

Résumé sur la substitution polyalphabétique

- Cryptanalyse basée sur l'analyse de fréquences.
- Niveau de sécurité équivalent à la substitution monoalphabétique.

Extension à la substitution polyalphabétique

- Faiblesse de la substitution :
  - Taille du mot-clé : un digramme peut être chiffré plusieurs fois *de la même manière*.
- Idée :
  - Choisir des mot-clés plus grand (i.e., utilisation de plus d'alphabets de chiffrement).

Vers la définition d'un chiffrement *parfait* ...

- Longueur du mot-clé = longueur du message :
  - Garantie *a priori* un niveau de sécurité maximal mais …
- Cryptanalyse possible si :
  - Réutilisation du mot-clé.
  - Mot-clé *trivial*.

Exemple de cryptanalyse sur le mot-clé

?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
K	V	Q	I	K	O	T	J	M	J	Z	Q	G	C	Z	C	H	W	E	E	E	Y	L	W	W

C	*R*	*Y*	?	?	?	?	*Y*	*I*	*R*	?	?	?	?	*R*	*Y*	*P*	?	?	?	?	?	*A*	*S*	*E*
l	*e*	*s*	?	?	?	?	*l*	*e*	*s*	?	?	?	?	*l*	*e*	*s*	?	?	?	?	?	*l*	*e*	*s*
K	V	Q	I	K	O	T	J	M	J	Z	Q	G	C	Z	C	H	W	E	E	E	Y	L	W	W

C	R	Y	O	T	H	E	R	A	P	I	E	?	?	*R*	*Y*	*P*	?	?	?	?	?	?	*E*	*S*
l	*e*	*s*	*u*	*r*	*h*	*p*	*s*	*m*	*u*	*r*	*m*	?	?	*l*	*e*	*s*	?	?	?	?	?	?	*e*	*s*
K	V	Q	I	K	O	T	J	M	J	Z	Q	G	C	Z	C	H	W	E	E	E	Y	L	W	W

Exemple de cryptanalyse sur le mot-clé

C	R	Y	P	T	O	G	R	A	P	H	I	E	?	*R*	*Y*	*P*	?	?	?	?	?	*E*	*S*
l	*e*	*s*	*t*	*r*	*a*	*n*	*s*	*m*	*u*	*s*	*i*	*c*	?	*l*	*e*	*s*	?	?	?	?	?	*e*	*s*
K	V	Q	I	K	O	T	J	M	J	Z	Q	G	C	Z	C	H	W	E	E	E	Y	L	W	W

C	R	Y	P	T	O	G	R	A	P	H	I	E	*C*	*R*	*Y*	*P*	*T*	*A*	*N*	*A*	*L*	*Y*	*S*	*E*
l	e	s	t	r	a	n	s	m	u	s	i	c	a	*l*	*e*	*s*	d	e	r	e	n	n	*e*	*s*
K	V	Q	I	K	O	T	J	M	J	Z	Q	G	C	Z	C	H	W	E	E	E	Y	L	W	W

C	R	Y	P	T	O	G	R	A	P	H	I	E	C	R	Y	P	T	A	N	A	L	Y	S	E
l	e	s	t	r	a	n	s	m	u	s	i	c	a	l	e	s	d	e	r	e	n	n	e	s
K	V	Q	I	K	O	T	J	M	J	Z	Q	G	C	Z	C	H	W	E	E	E	Y	L	W	W

Le chiffrement idéal : *One-time-pad*.

- Longueur du mot-clé = longueur du message.
- Mot-clé choisi *aléatoirement*.
- Mot-clé *jamais* réutilisé.

Sécurité *mathématiquement* prouvée !

Sécurité du *One-time-pad.*

?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
H	Z	S	G	O	P	K	B	X	E	H	A	Q	W	J	I	L	G	H	M	D	S	C	V	Y

W	*V*	*A*	*N*	*X*	*P*	*X*	*J*	*L*	*K*	*P*	*S*	*O*	*W*	*Y*	*E*	*T*	*D*	*D*	*V*	*Z*	*F*	*P*	*R*	*G*
l	e	s	t	r	a	n	s	m	u	s	i	c	a	l	e	s	d	e	r	e	n	n	e	s
H	Z	S	G	O	P	K	B	X	E	H	A	Q	W	J	I	L	G	H	M	D	S	C	V	Y

W	*V*	*A*	*B*	*X*	*P*	*X*	*Z*	*J*	*Z*	*T*	*P*	*I*	*S*	*R*	*X*	*L*	*P*	*T*	*K*	*W*	*O*	*R*	*K*	*U*
l	e	s	f	r	a	n	c	o	f	o	l	i	e	s	l	a	r	o	c	h	e	l	l	e
H	Z	S	G	O	P	K	B	X	E	H	A	Q	W	J	I	L	G	H	M	D	S	C	V	Y

Utilisation du *One-time-pad.*

- Problème :
  - Définition de clés *aléatoires*.
  - Gestion et distribution du dictionnaire des clés.
- Utilisation réelle :
  - Ligne directe entre présidents russe et américain.
  - *One-time-password*.

Plan

- Histoire de la cryptographie et de la cryptanalyse
- **Outils moderne de la cryptographie**
- Cryptographie symétrique
- Cryptographie asymétrique

Outils modernes de la cryptographie

- Evolution :
  - Mécanisation de la cryptographie.
  - Informatisation de la cryptanalyse.
  - Informatisation de la cryptographie.
- Concepts de base :
  - Substitution et transposition.
  - Propriétés mathématiques.

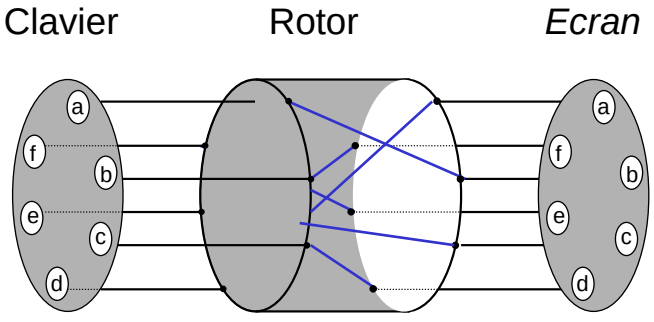
Mécanisation de la cryptographie

Enigma (Scherbius - 1920).

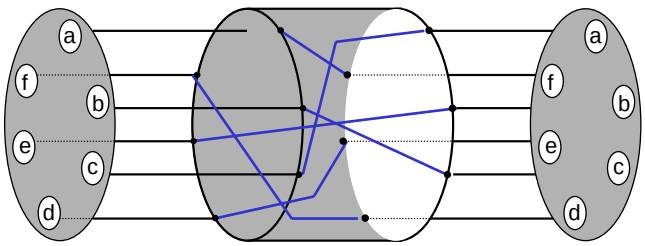
- Principes de base :
  - Substitution polyalphabétique.
  - Transposition élémentaire.
- Techniques utilisées :
  - Rotors = substitutions poly-alphabétiques.
  - Connector = transposition.

Enigma - Rotor

Substitution polyalphabétique



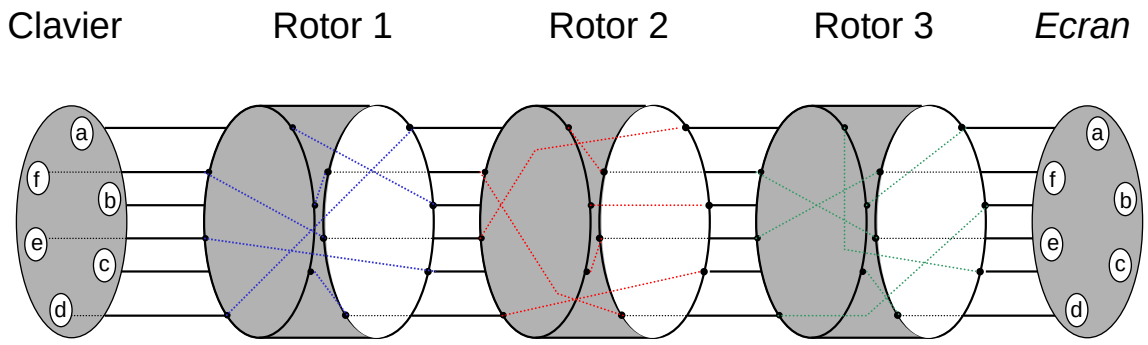
a	b	c	d	e	f
B	F	D	A	C	E



a	b	c	d	e	f
F	C	A	E	B	D

Enigma - Rotors

Substitutions polyalphabétiques

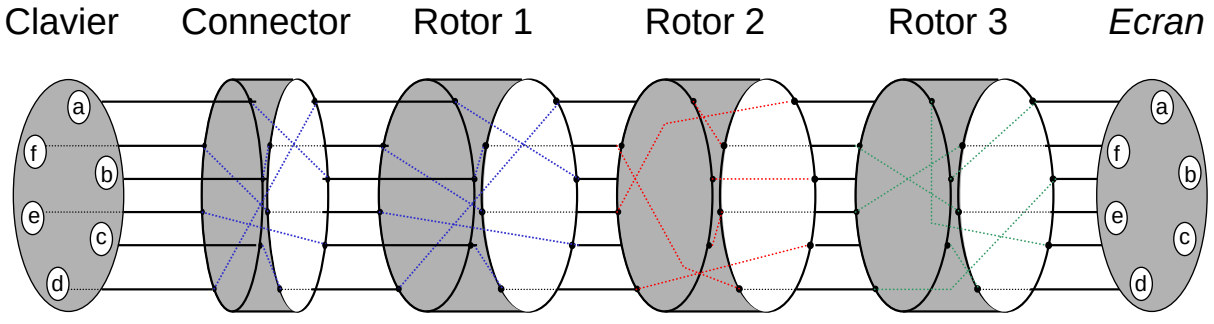


Complexité de la substitution :

– 26 x 26 x 26 = 17 576 alphabets de chiffrement.

Enigma - Connector

Transposition

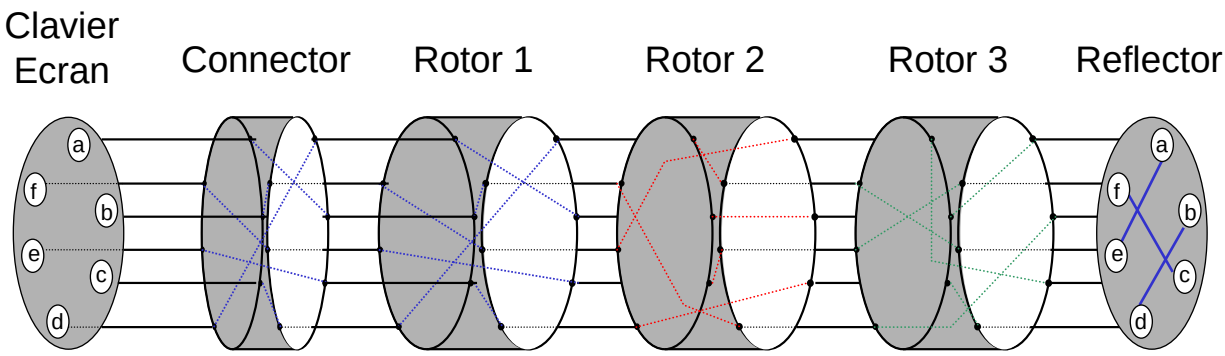


Complexité de la transposition :

– 6 connexions possibles : 100 391 791 500 branchements possibles.

Enigma

Chiffrement *et* déchiffrement



Enigma

Algorithme et clé.

- Algorithme :
  - Substitutions des rotors.
- Clé de chiffrement :
  - Disposition des rotors.
  - Orientation initiale des rotors.
  - Connexions entre lettres de l’alphabet.

Enigma

Complexité / niveau de sécurité *théorique*

- Orientation des rotors :
  - 26 x 26 x 26 alphabets.
- Dispositions des rotors :
  - 6 dispositions.
- Connexions :
  - 100 391 791 500 branchements.

$\approx 2^{50}$ clés (i.e., alphabets de chiffrement).

Cryptanalyse de *Enigma* :

Faille dans le mode d'utilisation.

- Utilisation de *Enigma* :
  - Notion de clé de session :

    PDG | PDG | LEMESSAGEACHIFFRER

- Analyse du chiffré :

  XAT | UMF | RERFFIHCAEGASSEMAL

  - Relations dépendant de la clé : X et U, A et M, T et F.

Cryptanalyse de *Enigma* :

Signature de la clé (Rejewski).

- Analyse d'un ensemble de chiffrés :

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

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

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

- *Signature* de la clé :

A H B Z T V F P L Q M W N J E O I X U Y R D G K **(23 liens)**

C S C **(2 liens)**

Cryptanalyse de *Enigma* :

Propriétés de la *signature*.

- Indépendant des connections :

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

A S A **(2 liens)**

B Z T V F P L Q M W N J E O I X U Y R D G K C H B **(23 liens)**

- Complexité de l'attaque :
  - Référencer toutes les *signatures* :

26 x 26 x 26 x 6 = 105456 *signatures*.

Cryptanalyse de *Enigma* :
Mécanisation de la cryptanalyse : la *Bombe*.

- 6 machines *Enigma* en parallèle :
  - une par disposition des rotors.
- Sur chaque machine :
  - essai successif des 17546 possibilités.

Recherche exhaustive de la clé.

Cryptanalyse de *Enigma* :
Limite de la *Bombe* de Rejewski.

- Introduction de 2 nouveaux rotors :
  - Disposition des rotors : 60 possibilités.
- 20 connexions possibles :
  - $\approx 2^{50}$ branchements possibles.
- Clé de session non dupliquée.

- Complexité / niveau de sécurité *théorique :*

  $\approx 2^{72}$ clés (i.e., alphabets de chiffrement).

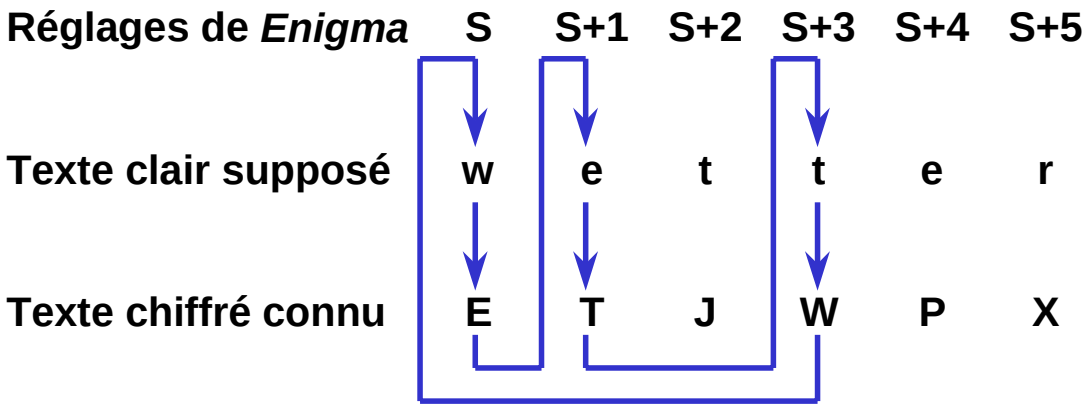
Cryptanalyse de *Enigma* :

Informatisation de la cryptanalyse (Turing).

- Principe de base :
  - Identifier une propriété dépendant exclusivement des rotors.
- Technique utilisée :
  - Messages *à clair connus*.

Cryptanalyse de *Enigma* :

Mots probables ou *cribs*.

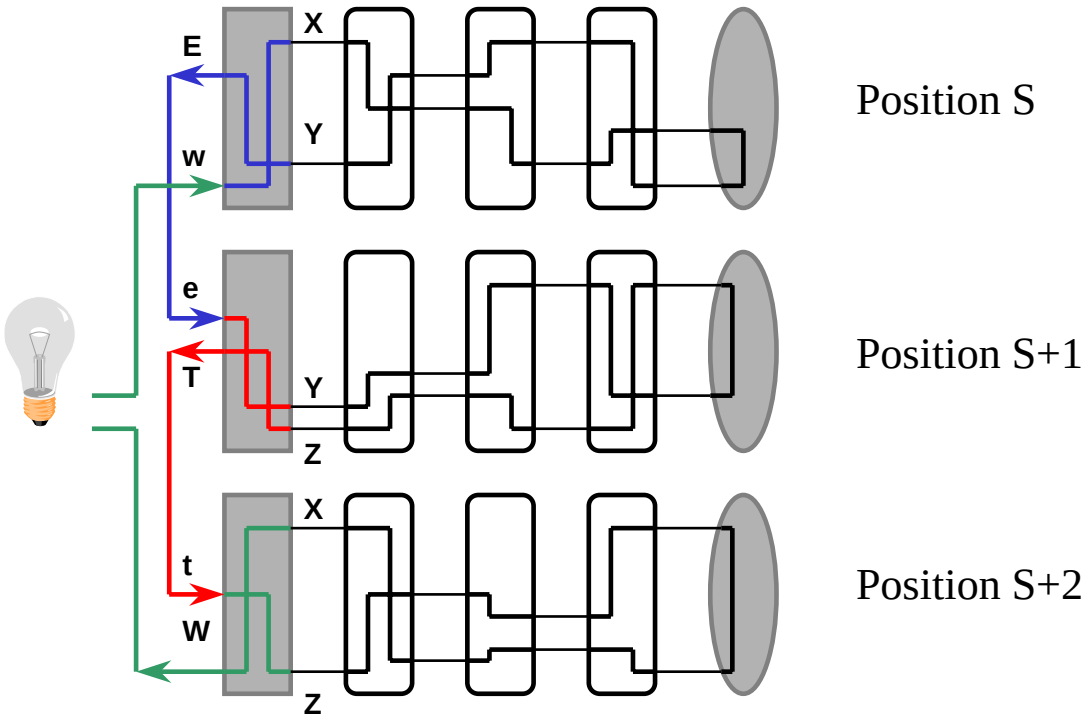


Cryptanalyse de *Enigma* :
Propriétés des mots probables.

- Indépendant des connections :
  - Dépend uniquement du réglage initial des rotors.
- Complexité de l'attaque :
  - Nombre de positions initiales possibles :

$$26 \times 26 \times 26 \times 60 = 1054560 \approx 2^{20}.$$

Cryptanalyse de *Enigma* :
La *Bombe* de Turing.



Cryptanalyse de *Enigma* :
La *Bombe* de Turing.

Cryptanalyse de *Enigma* :
Résultat de la *Bombe* de Turing.

- Performance :
  - Clé trouvée en 1 heure.
- Limite de la *Bombe* :
  - Utilisation de plus de 5 rotors.
  - Pas de structure dans message.

Décisif dans la victoire des alliers.

Informatisation de la cryptographie

- En réponse à l'*informatisation* de la cryptanalyse.
- Nécessité de chiffrer toujours plus d'informations.

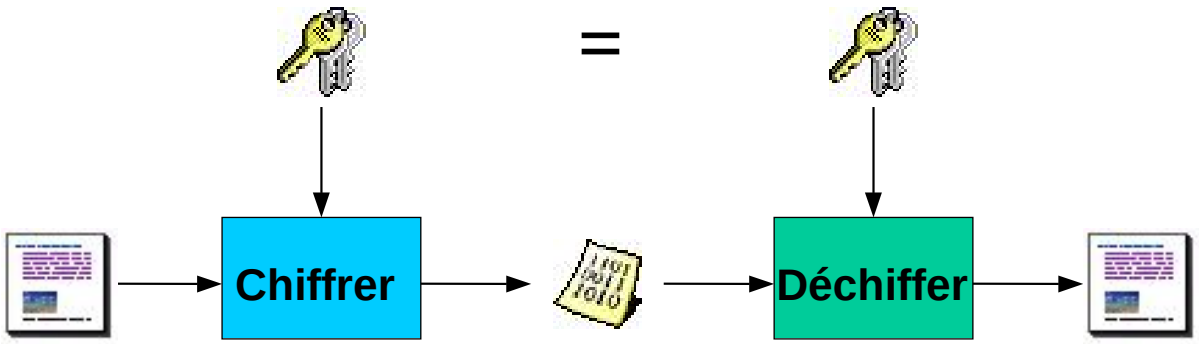
Atteindre un haut niveau de sécurité.

Outils informatique de la cryptographie

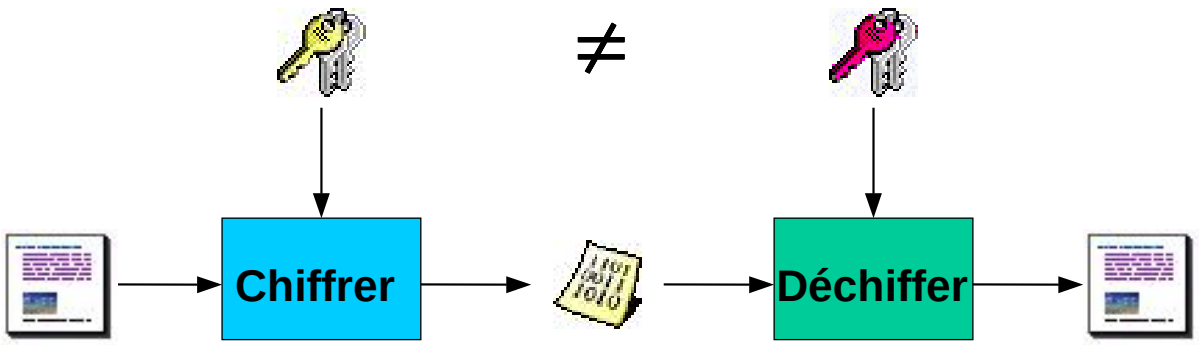
- Substitution et transposition :
  - Faiblesse de *Enigma* : possibilité de dissocier substitution et transposition.
- Outils mathématiques modernes :
  - Problèmes *NP-Complets*.

Cryptographie symétrique et asymétrique.

Cryptographie symétrique.



Cryptographie asymétrique.

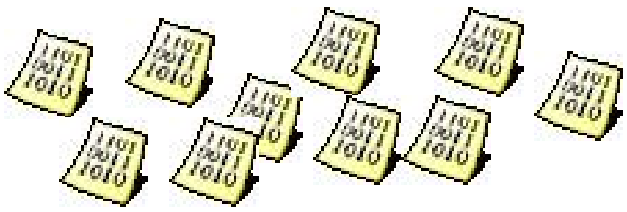


Cryptanalyse moderne :
Classification des attaques.

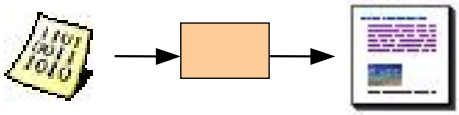
- Attaque en aveugle.
- Attaque à clairs connus.
- Attaque à clairs choisis.
- Attaque à clairs choisis adaptatifs.
- Attaque à chiffrés choisis.
- Attaque à clé choisie.

Cryptanalyse moderne :
Attaque en aveugle.

- Connu : un ensemble de chiffrés.



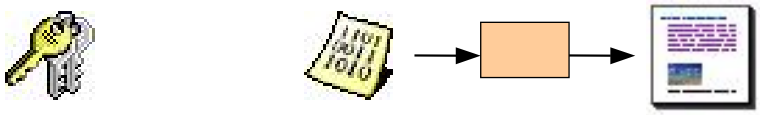
- Résultat :



Cryptanalyse moderne :
Attaque à clairs connus.

- Connu : un ensemble de *(clair, chiffré).*

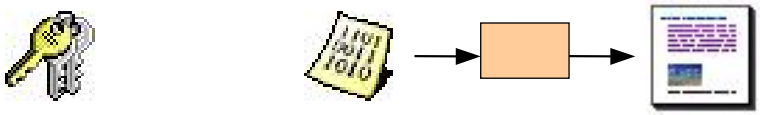
- Résultat :



Cryptanalyse moderne :
Attaque à clairs choisis.

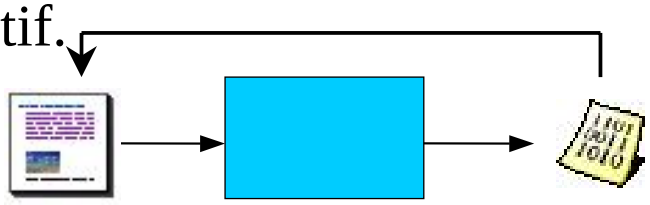
- Accès à une *machine* de chiffrement.

- Résultat :

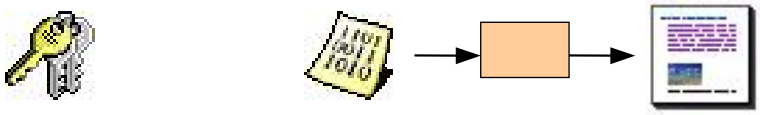


Cryptanalyse moderne :
Attaque à clairs choisis adaptatif.

- Accès à une *machine* de chiffrement adaptatif.



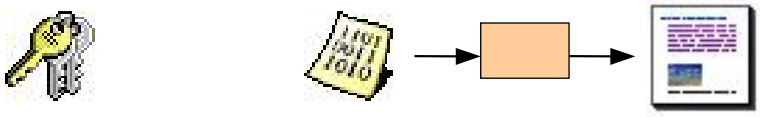
- Résultat :



Cryptanalyse moderne :
Attaque à chiffrés choisis.

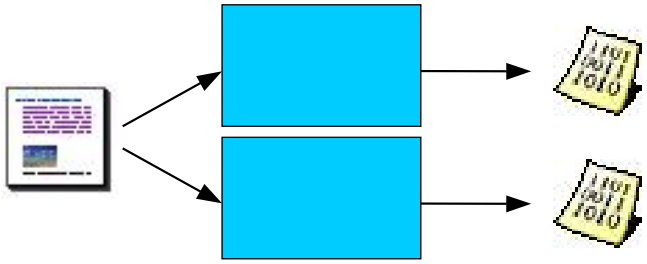
- Accès à une *machine* de déchiffrement.

- Résultat :

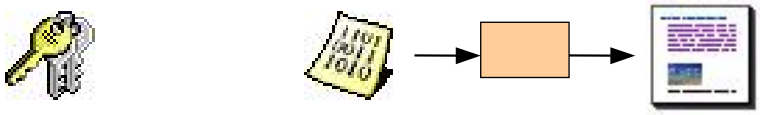


Cryptanalyse moderne :
Attaque à clés choisis.

- Accès à plusieurs *machines* de chiffrement.



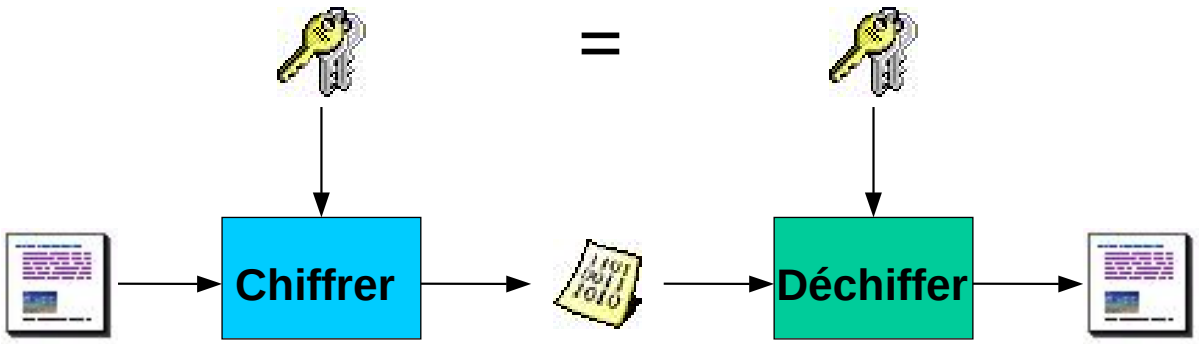
- Résultat :



Plan

- Histoire de la cryptographie et de la cryptanalyse
- Outils moderne de la cryptographie
- **Cryptographie symétrique**
- Cryptographie asymétrique

Cryptographie symétrique



Informatisation de ...

- Alphabet binaire : $\mathsf{A} = \{0,1\}$.
- Espace des messages (en clair) :

  $\mathsf{M} = \{m=(m_1 \ldots m_n) \mid \forall\, i, m_i \in \mathsf{A}$ *et m a un sens*$\}$.
- Espace des (messages) chiffrés :

  $\mathsf{C} = \{c=(c_1 \ldots c_n) \mid \forall\, i, c_i \in \mathsf{A}\}$.
- Espace des clés :

  $\mathsf{K} = \{k=(k_1 \ldots k_n) \mid \forall\, i, k_i \in \mathsf{A}\}$.

… la cryptographie symétrique

- Fonctions de chiffrement :
  - $E : \mathsf{M} \times \mathsf{K} \rightarrow \mathsf{C}$.
  - $E(..,k) = E[k](..) = E_k(..)$.
- Fonctions de déchiffrement :
  - $D : \mathsf{C} \times \mathsf{K} \rightarrow M$.
  - $D(..,k) = D[k](..) = D_k(..)$.

$$\forall\, m \in \mathsf{M}, \forall\, k \in \mathsf{K}, D_k(\, E_k(m)\,) = m$$

Outils informatiques

- Transposition :
  - Permutation.
  - Opérations mathématiques : $x^3 \bmod pq$, …
- Substitution :
  - Tableaux indexés.
  - Opérations binaires : XOR, ...

Théorie de l'information

- Entropie ou incertitude :

$$H(X) = \sum_{i=1}^{n} p_i \, log_2(\frac{1}{p_i})$$

  - $0 \leq H(X) \leq log_2(n)$
  - $H(X) = 0 \Leftrightarrow \exists!\ i \mid p_i = 1$
  - $H(X) = log_2(n) \Leftrightarrow \forall i,\ p_i = 1/n$

Confusion et Diffusion

- Confusion :
  - *Eliminer* la *syntaxe* du texte clair.
  - Substitution polyalphabétique.
- Diffusion :
  - *Eliminer* la *sémantique* du texte clair.
  - Tranposition.

Augmenter l'entropie du message chiffré.

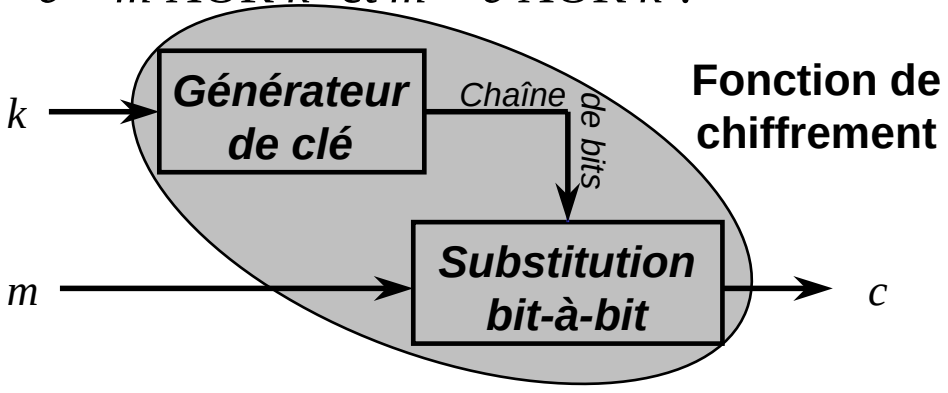
Type de chiffrement

- Chiffrement en chaîne :
  - Principe : chiffrement *bit-à-bit*.
- Chiffrement par block :
  - Principe : chiffrement *block par block*.

Chiffrement en chaîne

Stream cipher

- Chiffrement *à la One-Time-Pad* :
  - Taille du message $m = n$.
  - k permet de générer k' de taille n.
  - $c = m$ XOR k' et $m = c$ XOR k'.



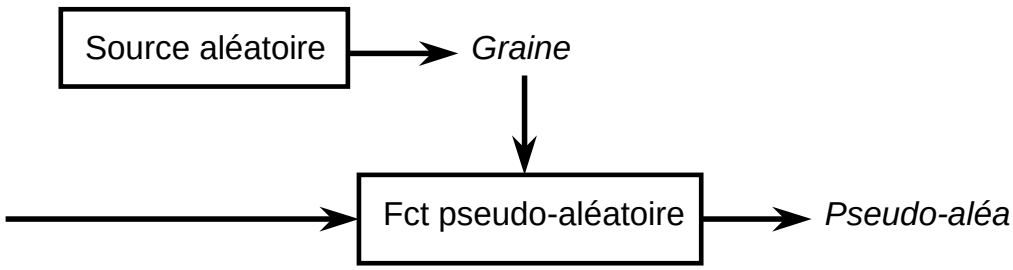
Sécurité du chiffrement en chaîne

- Fonction de substitution :
  - Connue et (généralement) trivial.
- Fonction de génération de clé :
  - Fonction *pseudo-aléatoire* : impossible *à l'échelle humaine* à prédire.

La sécurité repose sur le générateur de clé.

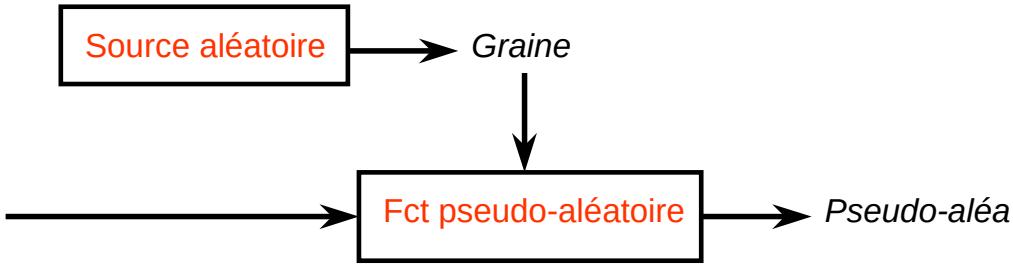
Générateur de clé

- Fonction *pseudo-aléatoire* :
  - Basée sur une source *aléatoire*.



Sécurité du générateur de clé

- Sécurité de la source *aléatoire*.
- Fonction *pseudo-aléatoire*.



Sécurité de la source aléatoire

- Source aléatoire *logicielle* :
  - Horloge système.
  - Clavier ou mouvement de souris.
  - Buffers.
- Source aléatoire *matérielle* :
  - Emission de particules
  - Son d'un microphone ou video d'une camera.

Sécurité de la fonction pseudo-aléatoire.

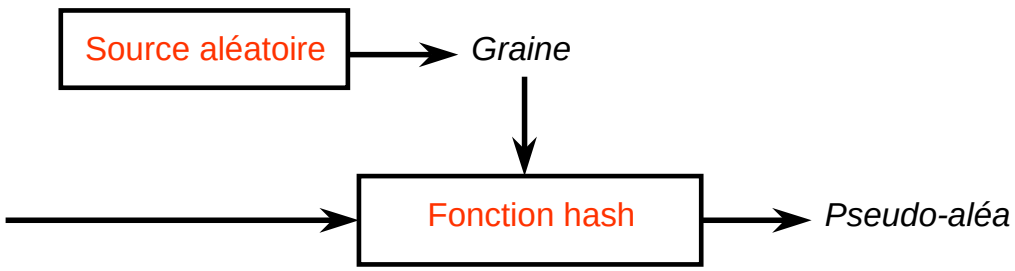
- Fonction *hash* :

$$h : \{0,1\}^* \rightarrow \{0,1\}^n$$

  – Impossible *à l'échelle humaine* de trouver *m* et *m'* tels que : $h(m) = h(m')$.

Attaque sur le générateur de clé

- Attaque sur la source *aléatoire* :
  – Rendre la source prédictible.
- Attaque sur la fonction *hash*.



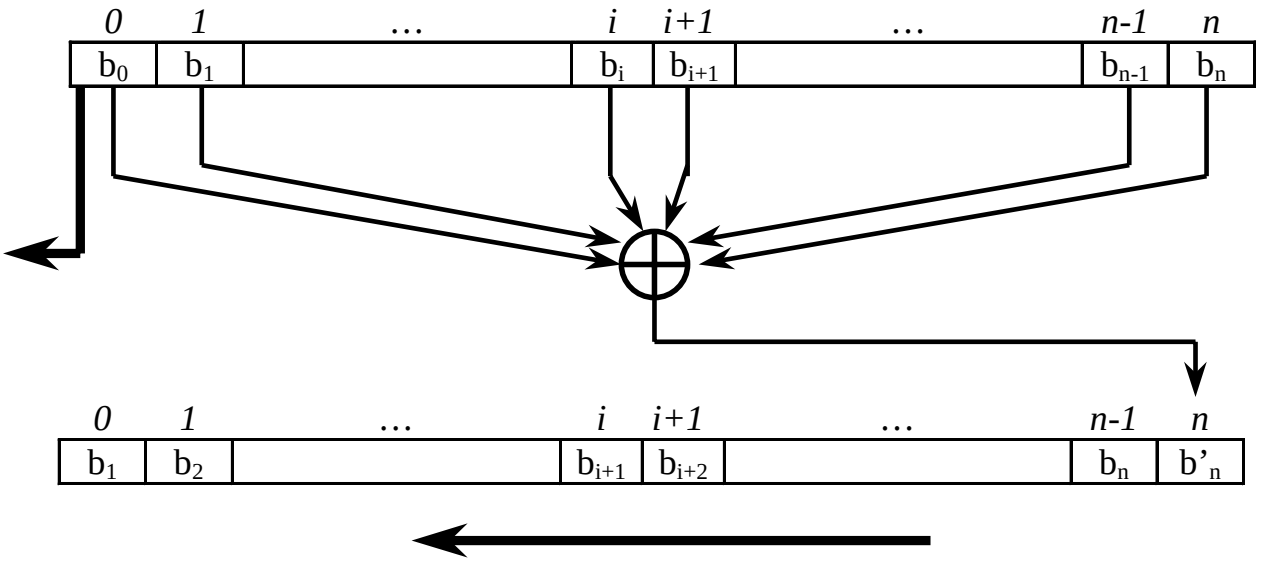
Attaque sur la fonction *hash*.

$$h : \{0,1\}^* \rightarrow \{0,1\}^n$$

- Principe :
  - Etant donné η, trouver *m* tel que *h*(*m*) = η.
- Paradoxe des anniversaires :
  - Probabilité *0.5* de trouver *m* et *m'* tel que *h*(*m*) = *h*(*m'*) en $2^{n/2}$ messages

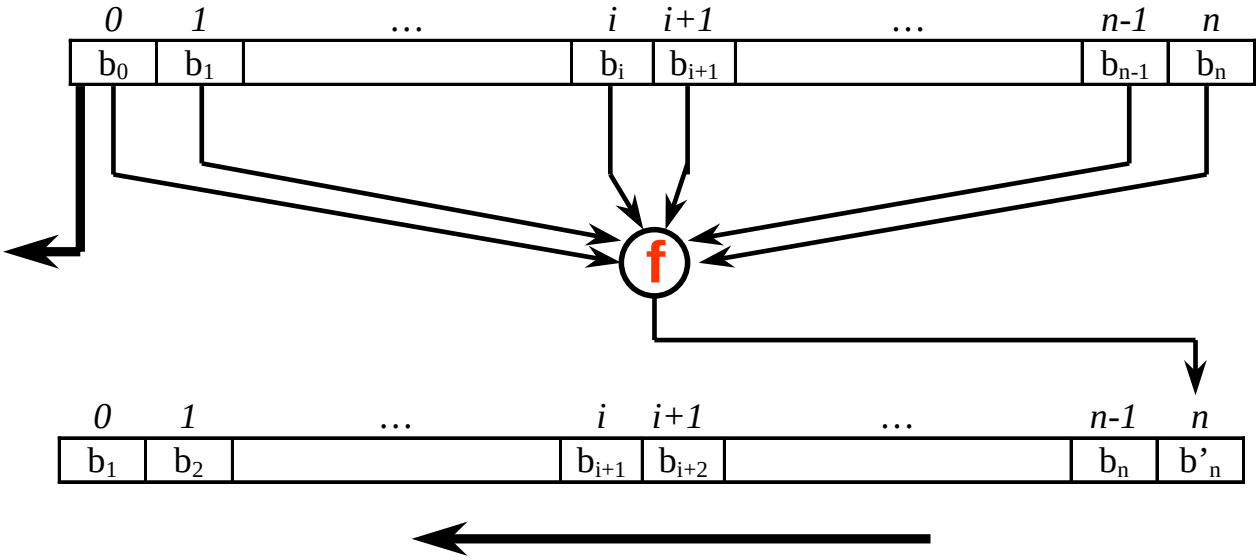
Registres linéaires de décalage

Linear Feedback Shift Registers



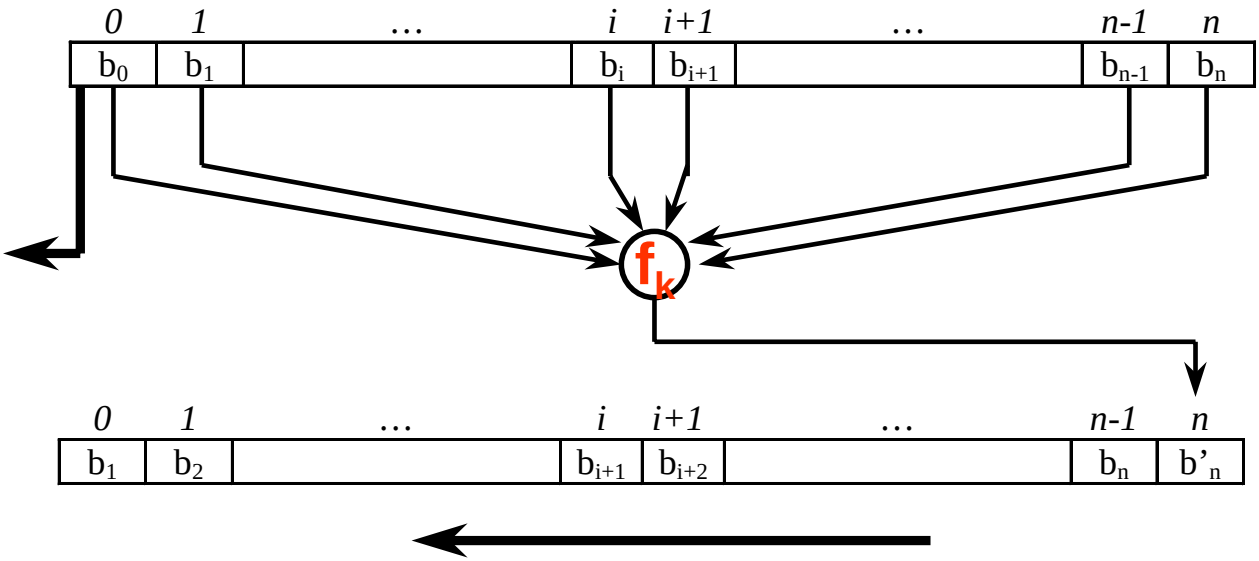
Registres non-linéaires de décalage

Non-linear Feedback Shift Registers



Registres non-linéaires de décalage

Chiffrement / Déchiffrement



Utilisation de LFSRs

- Implémentation facile en *hardware*.
- Utilisation généralement d'une fonction f_k secrète.
- Niveau de sécurité : confiance limitée.

Algorithme RC4

Rivest Cipher ou Ron Code

- Générateur de clé :
  - Permutation sur un *tableau de substitution* (*S-box*).
  - Permutation fonction de la clé de chiffrement.
- Fonction de substitution :
  - XOR entre la clé générée et le message en clair.

Algorithme secret
propriété de RSA Data Security, Inc.

Algorithme RC4

Secret jusqu'en 1994 ...

- Initialisation :

```
S0 = 0, … , S255 = 255
K0, …, K255
for i = 0 to 255
     j = (j + Si + Ki) mod 256
     swap Si and Sj
```

- Génération :

```
i = (i+1) mod 256
i = (i+1) mod 256
swap Si and Sj
t = (Si + Sj) mod 256
K = St
```

Utilisation de RC4

- Intérêts :
  - Très bonne performance.
  - Code facile à retenir.
- Lotus Notes, Apple Computer, Oracle Secure SQL …
- Niveau de sécurité : bonne confiance.

Intérêts du chiffrement en chaîne

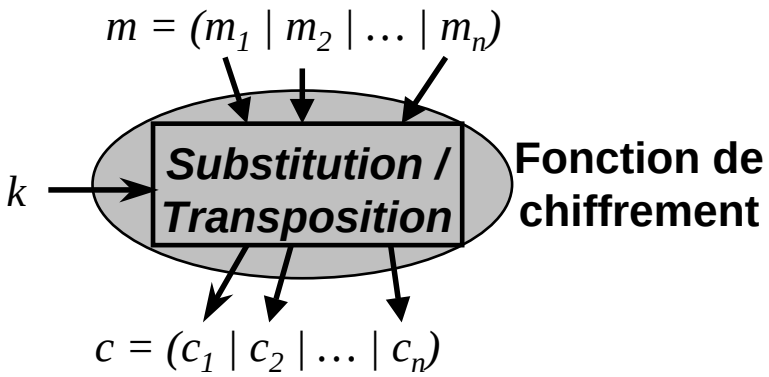
- Rapidité de chiffrement / déchiffrement.
- Codage généralement simple.
- Pas de propagation des erreurs.

Problème : attaques par rejoue de message.

Chiffrement par block

Block cipher

- Principe de base :
  - Message $m = (m_1 \mid \ldots \mid m_n)$, *n blocks* de *x* bits.
  - Transposition et substitution *block par block* .



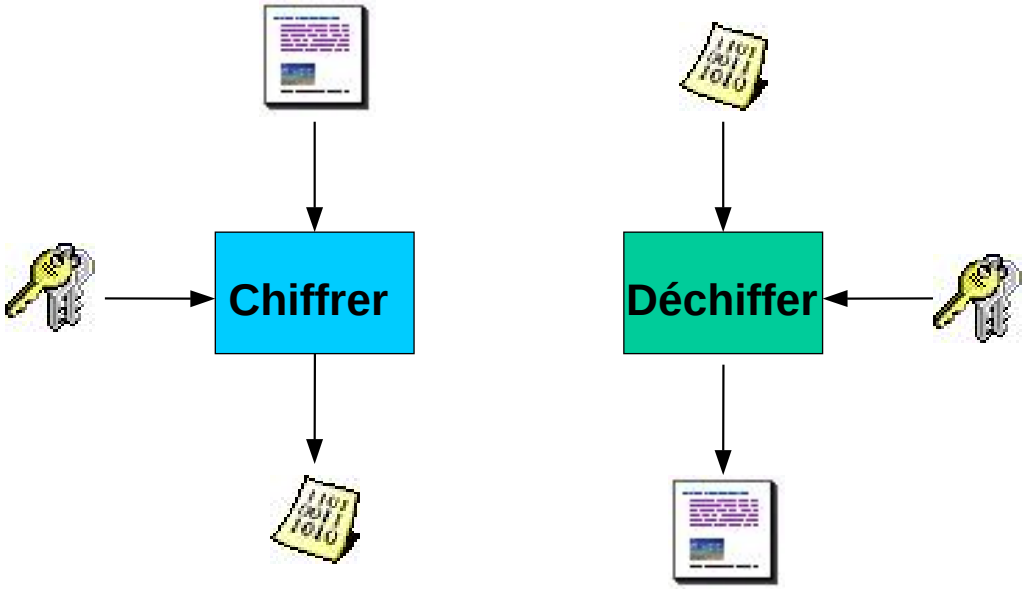
Sécurité du chiffrement par block

- Substitution polyalphabétique.
  - Utilisation de tableaux ou *S-boxes*.
- Transposition :
  - Agit sur les *S-boxes*.

La sécurité repose sur la combinaison substitution/transpostion.

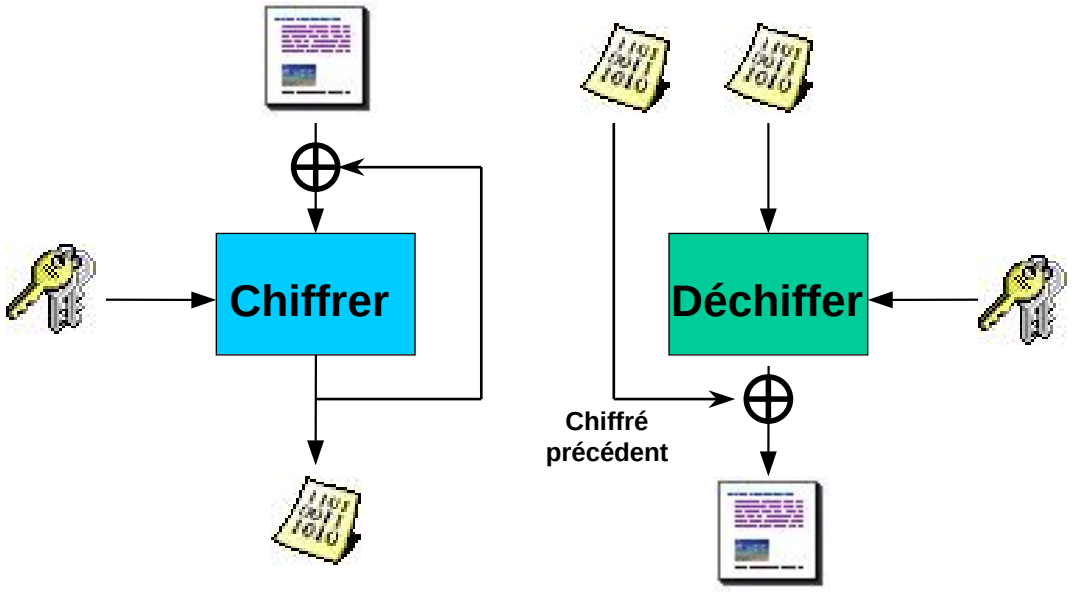
Modes de chiffrement

Mode ECB (*Electronic CodeBook*)



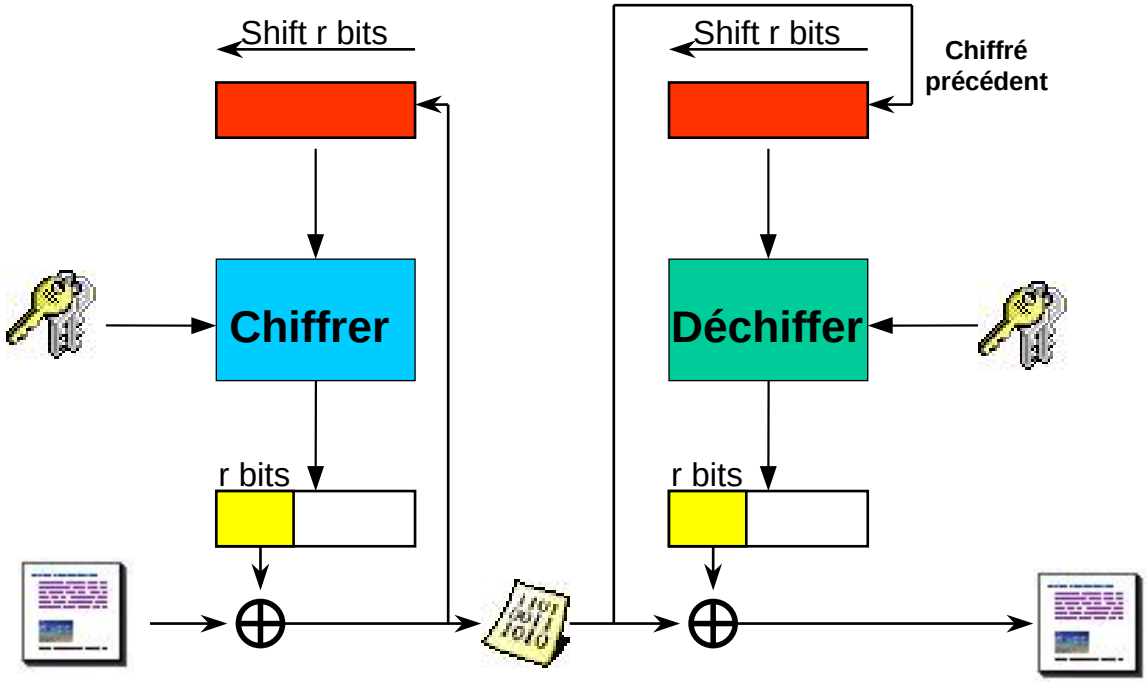
Modes de chiffrement

Mode CBC (*Cipher Block Chaining*)



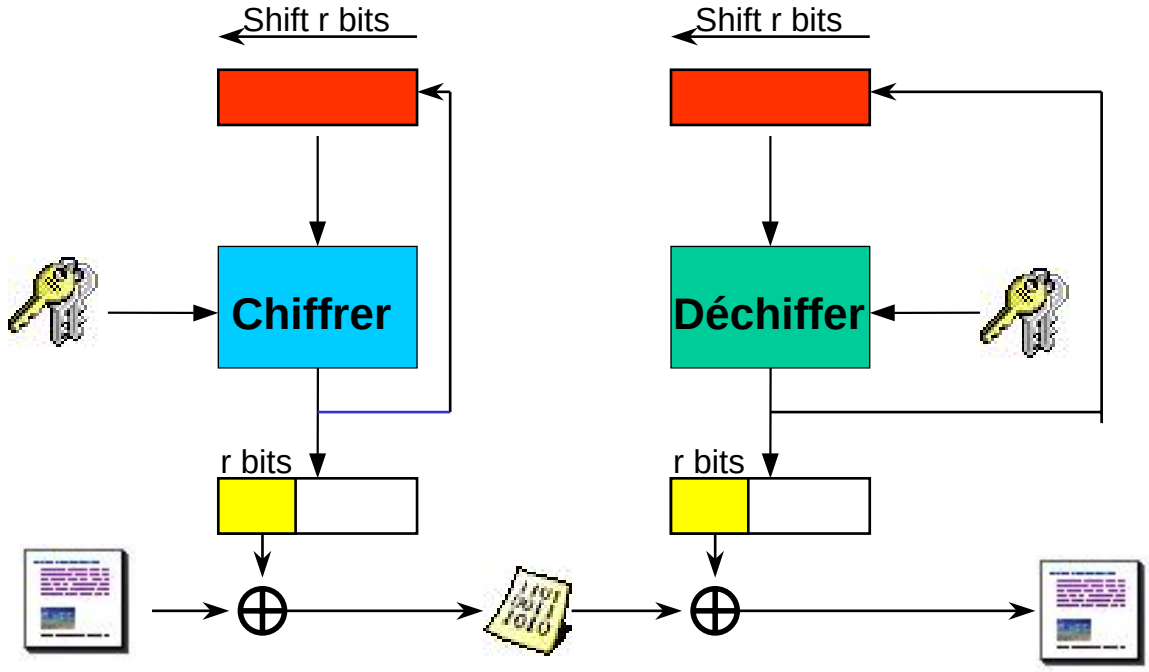
Modes de chiffrement

Mode CFB (*Cipher FeedBack*)



Modes de chiffrement

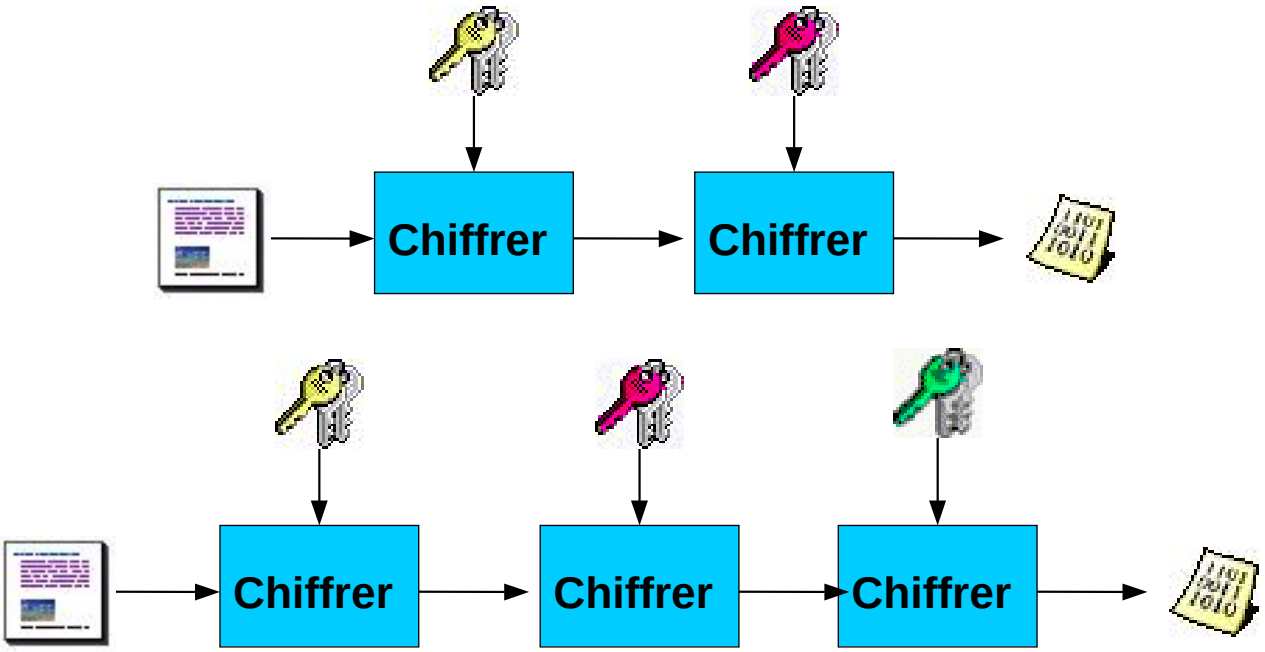
Mode OFB (*Output FeedBack*)



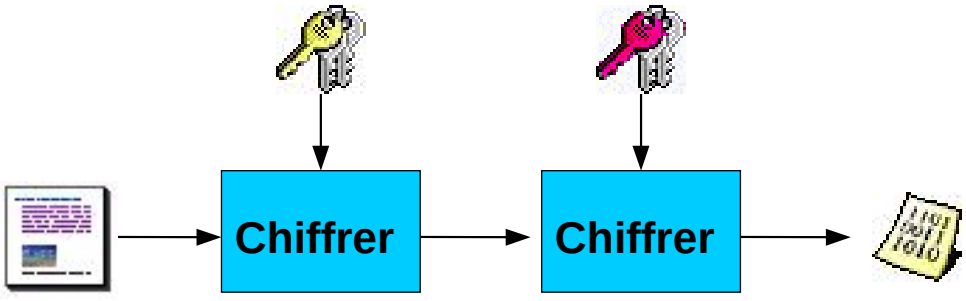
Propriétés des modes de chiffrement

- Mode ECB :
  - Chiffrement *statique* et pas de propagation d'erreur.
- Mode CBC :
  - Chiffrement *chaîné* et propagation d'erreur limitée à 1 block.
- Modes CFB et OFB :
  - Chiffrement *chaîné* et propagation d'erreur.

Combinaison/Produit de chiffrement par block

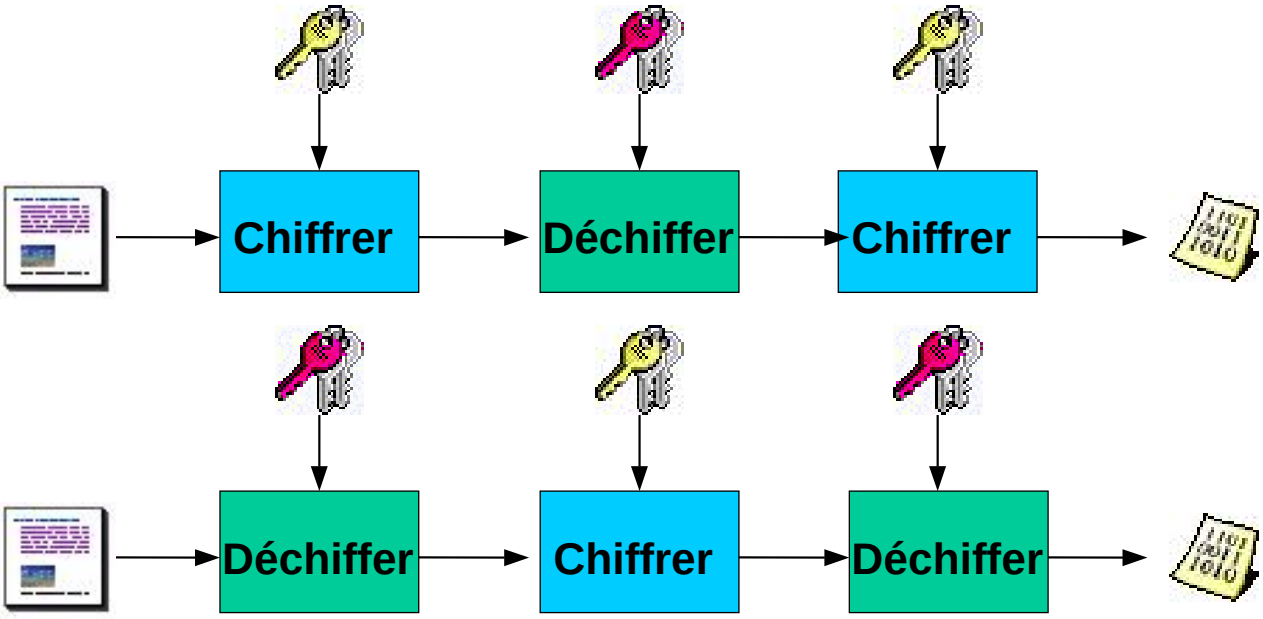


Sécurité du double chiffrement



- Clé identique :
  - si taille de clé 2^k, attaque en 2^k.
- Clé différentes :
  - si taille de clé 2^k, attaque en 2^{k+1}.

Triple chiffrement/déchiffrement



DES

Data Encryption Standard

- Historique :
  - Milieu des années 70.
  - 1er algorithme de chiffrement pour l'industrie.
  - Standard américain FIPS 46-2.
- Principes de base :
  - Produit de substitutions/transpositions.
  - Chiffrement à la Feistel : itération de la fonction de chiffrement.

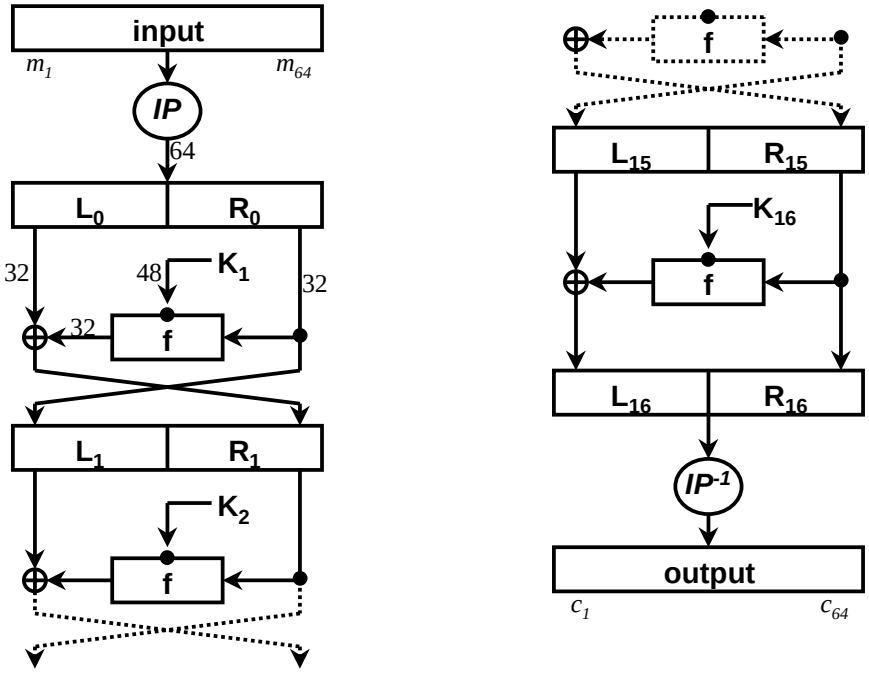
DES

Informations techniques

- Taille des block : 64 bits.
- Taille de la clé : 56 bits.
- Structure globale :
  - Permutation initiale.
  - Fonction itérée : expansion, substitution, permutation
  - Nombre d'itérations : 16.
  - *Key schedule* : 16 sous-clé de 48 bits.

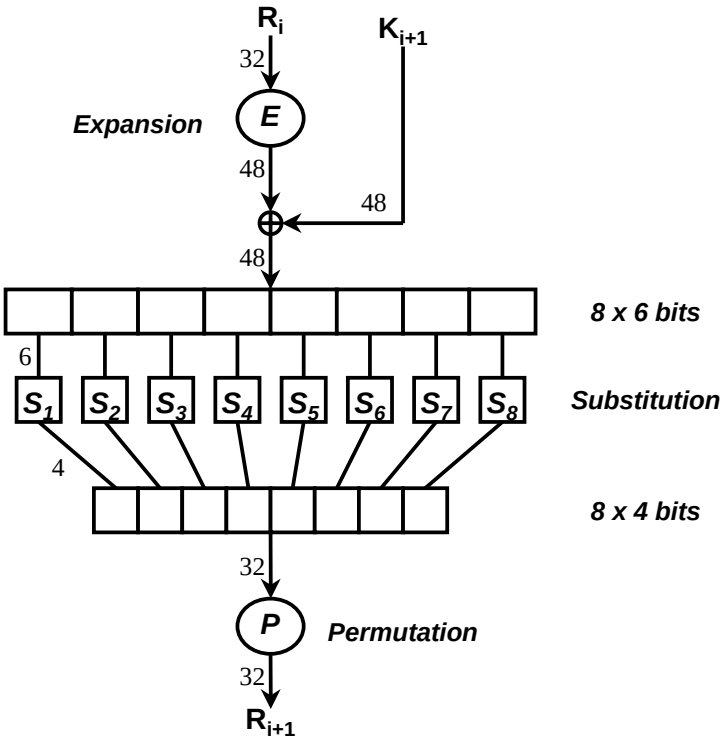
DES

Algorithme global



DES

Fonction itérative



DES

Propriétés et sécurité

- Propriété de *complémentarité* :

$$y = DES_k(x) \qquad \underline{y} = DES_{\underline{k}}(\underline{x})$$

- Clés faibles : 4 clés + 6 pairs de clés.

$$k \mid \forall\, x,\ DES_k(DES_k(x)) = x$$

$$k1,k2 \mid \forall\, x,\ DES_{k1}(DES_{k2}(x)) = x$$

  - Points fixes importants pour les clés faibles.

DES

Propriétés et sécurité

- DES n'est pas un groupe :

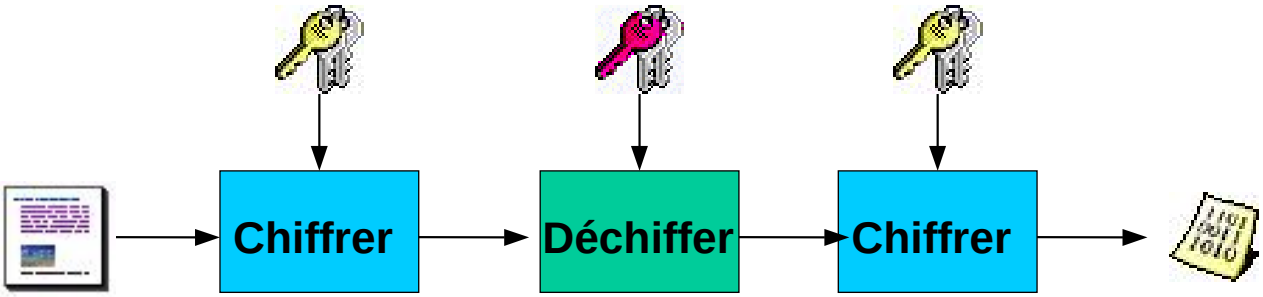
  $\forall$ k1,k2, $\nexists$ k3 | $\forall$ *x*, $DES_{k1}(DES_{k2}(x)) = DES_{k3}(x)$

- Cryptanalyse linéaire :
  - Meilleure attaque *théorique* connue.
- Cryptanalyse différentielle :
  - Résiste *en partie* à l'attaque.

DES et attaques

Méthode d'attaque	Texte connu	Texte choisi	Complexité de stockage	Complexité de calcul
Précalcul exhaustif		1	256	1 tableau
Recherche exhausive	1			2^{55}
Cryptanalyse linéaire	2^{43}		*pour les textes*	2^{43}
	2^{38}		*pour les textes*	2^{50}
Cryptanalyse différentielle		2^{47}	*pour les textes*	2^{47}
	2^{55}		*pour les textes*	2^{55}

Triple DES



- Compatibilité ascendante.
- Rapidité.
- Algorithme bien connu / étudier.

AES

Advanced Encryption Standard

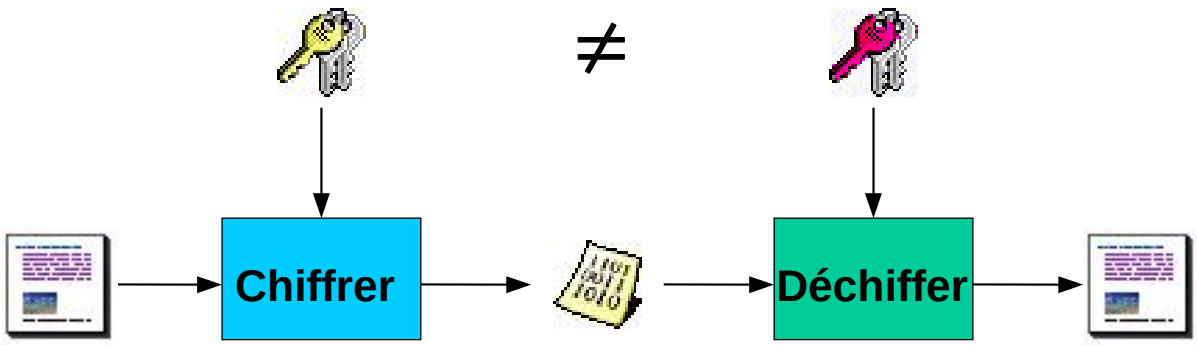
- Processus de sélection :
  - 1/1997 : Appel à candidature.
  - 8/1998 : Fin des candidatures.
  - 8/1998 - 8/2000 : Analyse des candidats.
  - 8/2000 : Sélection de l'AES.

Rjindael

Plan

- Histoire de la cryptographie et de la cryptanalyse
- Outils moderne de la cryptographie
- Cryptographie symétrique
- **Cryptographie asymétrique**

Cryptographie asymétrique



Cryptographie asymétrique
Histoire

- Cryptographie symétrique :
  - Pas de signature digitale.
- Diffie-Hellman (1976) :
  - Introduction du concept de signature digitale et de la cryptographie à clé publique.
- Rivest-Shamir-Adleman (1978) :
  - Premier algorithme de cryptographie asymétrique.

Cryptographie asymétrique
Histoire ou légende ...

- NSA affirme connaître la cryptographie asymétrique depuis 1966.
  - Pas de preuve mais …
- L'équivalent anglais connaissait la cryptographie asymétrique depuis 1971.
  - Preuve depuis 1999.

Informatisation de ...

- Alphabet clair : $\mathsf{A} = \{0,1\}$.
- Espace des messages (en clair) :

  $\mathsf{M} = \{m=(m_1 \ldots m_n) \mid \forall\, i,\, m_i \in \mathsf{A}$ *et m a un sens*$\}$.
- Espace des (messages) chiffrés :

  $$\mathsf{C} = \{c=(c_1 \ldots c_n) \mid \forall\, i,\, c_i \in \mathsf{A}\}.$$
- Espace des clés :

  $$\mathsf{K} = \{(k_p, k_s) \mid k_p \leftrightarrow k_s\}.$$

… la cryptographie asymétrique …

- Fonctions de chiffrement :
  - $E : \mathsf{M} \times \mathsf{K}_p \rightarrow \mathsf{C}$.
  - $E(..,k_p) = E[k_p](..) = E_{kp}(..)$.
- Fonctions de déchiffrement :
  - $D : \mathsf{C} \times \mathsf{K}_s \rightarrow M$.
  - $D(..,k_s) = D[k_s](..) = D_{ks}(..)$.

$$\forall\, m \in \mathsf{M},\, \forall\, (k_p,k_s) \in \mathsf{K},\, D_{ks}(\, E_{kp}(m)\,) = m$$

… et signature digitale.

- Fonctions de signature :
  - $S : \mathsf{M} \times \mathsf{K}_s \rightarrow \mathsf{C}$.
  - $S(..,k_s) = S[k_s](..) = S_{ks}(..)$.
- Fonctions de vérification :
  - $V : \mathsf{C} \times \mathsf{K}_p \rightarrow M$.
  - $V(..,k_p) = V[k_p](..) = V_{kp}(..)$.

$\forall\, m \in \mathsf{M}, \forall\, (k_p,k_s) \in \mathsf{K}, V_{kp}(\, S_{ks}(m)\,) = m$

Outils mathématiques

- Théorie de la complexité :
  - Problèmes P, NP, NP-Complets …
- Théorie des nombres :
  - Nombreux problèmes NP *à sens uniques*.

Théorie des nombres

- Interprétation des messages :
  - Ecriture en base 2.
- Chiffrement :
  - Opérations mathématiques sur les nombres.
- Déchiffrement :
  - Opérations inverses au chiffrement.

Exemple simple.

- Problème *difficile* : $x^{1/3}$.
  - Fonction *à sens unique* : x^3.
- Chiffrement :

$$E(m) = m^3 = c.$$

- Déchiffrement (à l ’aide d’un *Oracle*) :

$$D(c) = c^{1/3} = m.$$

Théorie des nombres

Problèmes de référence

- Factorisation de nombres entiers :
  - Trouver les facteurs premiers n.
- Racines e$^{\text{ième}}$ dans un corps finis :
  - Trouver x tel que $x^e \equiv c \bmod n$.
- Logarithme discret :
  - Trouver x tel que $a^x \equiv b \bmod p$.

Théorie des nombres

Problèmes de référence

- Résidu quadratique :
  - Décider si a est un résidu quadratique modulo n (i.e., J(a,n) = 1).
- Logarithme discret *généralisé* (Diffie-Hellman) :
  - étant donnés $a^x \bmod p$ et $a^y \bmod p$, trouver $a^{xy} \bmod p$.

Algorithmes de cryptographie asymétrique

- RSA (Rivest-Shamir-Adleman, 1978) :
  - Racine eième dans un corps finis.
- Rabin (Rabin, 1979) :
  - Racines carrées dans un corps finis.
- ElGamal (ElGamal, 1985) :
  - Logarithme discret généralisé.
- Courbes elliptiques (Koblitz et Miller, 1985).

Algorithme RSA

Initialisation

1- p et q deux grands nombres premiers.

2- $n = pq$ et $\phi(n) = (p-1)(q-1)$.

3- Entier e tq $1 < e < \phi(n)$ et $\gcd(e,\phi(n))=1$

4- Calculer d tq $1 < d < \phi(n)$ et $ed \equiv 1 \bmod \phi(n)$

(Algorithme d'Euclide).

5- Clé publique : (e,n). Clé privée : d.

Algorithme RSA
Chiffrement

1- Obtenir la clé publique (e,n) du destinataire.

2- Représenter le message comme un entier m tel que $1 < m < n$.

3- Calculer $c \equiv m^e \bmod n$.

Algorithme RSA
Déchiffrement

1- A l'aide de la clé privée d, calculer

$$m \equiv c^d \bmod n.$$

Preuve :

$$c^d \equiv (m^e)^d \bmod n \equiv m^{ed} \bmod n = m \bmod n.$$

Algorithme RSA

Signature digitale

1- Représenter le message comme un entier m tel que $1 < m < n$.

2- A l'aide de la clé privé d, calculer

$$s \equiv m^d \bmod n.$$

Algorithme RSA

Vérification d'une signature

1- Obtenir la clé publique (e,n) du signataire.

2- Calculer $m \equiv s^e \bmod n$.

Preuve :

$$s^e \equiv (m^d)^e \bmod n \equiv m^{ed} \bmod n \equiv m \bmod n.$$

Algorithme RSA
Propriétés

- Propriétés multiplicatives :

  $(m_1 m_2)^e \equiv m_1^e \, m_2^e \bmod n \equiv c_1 \, c_2 \bmod n.$

- Existence de points fixes :

  $\exists \, m$ tel que $m^e \equiv m \bmod n$.

Algorithme RSA
Attaques classiques

- Factorisation de n :
  - Taille de n ; choix de e et d.
- Chiffrement et signature :
  - Signer avant de chiffrer.
- Propriétés multiplicatives :
  - Choix du padding.

Algorithme Diffie-Hellman

Génération de clés de session

1- p un grand nombre premier ; α un générateur de Z_p^*.

2- A choisit a, et calcule $\alpha_a = \alpha^a \bmod p$.

3- B choisit b, et calcule $\alpha_b = \alpha^b \bmod p$.

4- A et B s'échange α_a et α_b.

5- A calcule $\alpha_b{}^a \bmod p$ et B calcule $\alpha_a{}^b \bmod p$.

Cryptographie asymétrique

Problèmes génériques

- Performances médiocres :
  - Utilisation de clé de session.
  - Utilisation de fonctions *hash*.
- Certification des clés publiques :
  - Garantir/vérifier la relation clé/utilisateur.
  - PKI : *Public Key Infrastructure*.

Conclusion

- Historique de la cryptographie.
- Cryptographie symétrique.
- Cryptographie asymétrique.

Comparaison cryptographie symétrique/asymétrique

- Cryptographie symétrique :
  - Rapide mais nécessité de partager un secret.
- Cryptographie asymétrique :
  - Lent mais pas de partage de secret et signature digitale

Combinaison cryptographie symétrique/asymétrique

- Cryptographie asymétrique :
  - Génération de clés de session.
  - Signature digitale (utilisation d'une fonction *hash*).
- Cryptographie symétrique :
  - Chiffrement à l'aide de la clé de session.

Sécurité des algorithmes.

- Cryptographie symétrique :
  - au moins 128 bits.
- Fonction *hash* :
  - au moins 160 bits.
- Cryptographie asymétrique :
  - Type RSA : au moins 768 bits.
  - Courbes elliptiques : 180 bits.

A retenir ...

- Algorithme secret ≠ sécurité élevée.
  - Au contraire ...
- Rien n’est acquis en cryptographie.
  - Taille de clé variable.
- « Seuls les paranoïaques survivent »...
  - … et encore !