

Introduction à la cryptologie

Arithmétique et cryptographie



Sommaire

1. Petit lexique.
2. Bref historique.
3. Les deux types de cryptographie.
4. Applications modernes.



1. Petit lexique.

1. Petit lexique.

Définitions de base

- **Cryptologie** : science des messages secrets, se décomposant en cryptographie et cryptanalyse.
 - **Cryptographie** : ensemble des techniques et méthodes utilisées pour transformer un message clair en un message inintelligible.
 - **Cryptanalyse** : ensemble des techniques et méthodes utilisées pour retrouver le texte en clair à partir du texte crypté.

1. Petit lexique.

Notion de chiffre

- **Chiffre** : système de cryptage où l'on remplace chaque lettre du message d'origine par une autre (ou par un symbole) en suivant un algorithme bien défini.
- Deux types de chiffre :
 - **Chiffre de substitution** : chaque lettre est remplacée par une autre mais garde sa place d'origine.
 - **Chiffre de transposition** : chaque lettre reste inchangée mais est mise à une autre place (principe de l'anagramme).

1. Petit lexique.

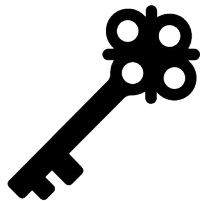
Les différents chiffres de substitution

- Chiffre de **substitution monoalphabétique** : chaque lettre du message d'origine est toujours remplacée par une même autre lettre.
- Chiffre de **substitution polyalphabétique** : une même lettre du message d'origine peut être remplacée par plusieurs lettres différentes.
- Chiffre de **substitution polygrammique** : les lettres ne sont pas remplacées une par une mais par blocs de plusieurs (deux ou trois généralement).

1. Petit lexique.

Algorithme de chiffrement et clé : définitions

- **Algorithme de chiffrement** : suite d'opérations à effectuer pour obtenir le chiffrement d'un message. Il doit être lié à une clé qui précise son fonctionnement.
- **Clé** : paramètre (nombre, mot, phrase...) qui permet, connaissant un algorithme de chiffrement, de chiffrer un message.



1. Petit lexique.

Algorithme de chiffrement et clé : exemple

- Si on chiffre un message en remplaçant chaque lettre par la lettre venant 3 places après elle dans l'alphabet, l'algorithme est le décalage vers la droite et la clé le nombre 3.



1. Petit lexique.

Alternative (anecdotique) au chiffre

- Un **code** est un système de cryptage où l'on remplace chaque mot du message d'origine par un symbole ou ensemble de symboles.
- L'exemple typique de code est le **rébus** :



1. Petit lexique.

Cryptanalyse

- On distingue deux types d'opérations, selon que la personne voulant retrouver le message d'origine soit le destinataire ou un ennemi ayant intercepté le message :
 - **déchiffrement** : opération par laquelle à partir d'un message chiffré on retrouve le message d'origine, connaissant l'algorithme de chiffrement et la clé.
 - **décryptement** : même chose que le déchiffrement mais sans connaître la clé.

1. Petit lexique.



2. Bref historique.

2. Bref historique.

Les débuts de la cryptographie : la scytale

- 2000 avant J.C. : en Egypte un scribe utilise des hiéroglyphes non usuels sur une pierre tombale, c'est la première trace de cryptographie.
- 450 avant J.C. : à Sparte, utilisation d'une scytale, bâton entouré d'une lanière de cuir sur laquelle on écrivait le message à chiffrer. La lanière déroulée porte les mêmes lettres que le message d'origine, mais dans un ordre différent. Pour déchiffrer le message, le destinataire n'avait qu'à enrouler la lanière sur un bâton de même diamètre que celui de l'expéditeur.

2. Bref historique.

Les débuts de la cryptographie : la scytale

- Reconstitution d'une scytale



- C'est le premier exemple connu de chiffre de transposition.

2. Bref historique.

Les débuts de la cryptographie : premiers chiffres monoalphabétiques

- 400 avant J.C : les hébreux utilisent des chiffres de substitution monoalphabétique, par exemple dans l'ancien testament.
 - Chiffre Atbash :

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

2. Bref historique.

Les débuts de la cryptographie : premiers chiffres monoalphabétiques

- Chiffre Albam :

clair	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
chiffré	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

- Chiffre Atbah :

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

2. Bref historique.

Les débuts de la cryptographie : premiers chiffres monoalphabétiques

- 50 avant J.C. : Jules César utilise lui aussi un chiffre de substitution monoalphabétique très simple pour transmettre des messages militaires. Chaque lettre du message est remplacée par la lettre venant 3 places après elle dans l'alphabet.

clair	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
chiffré	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

2. Bref historique.

Les débuts de la cryptographie : analyse des fréquences

- 9ème siècle après J.C. : le savant arabe Abu Yusuf Ya'qub ibn Is-haq ibn as-Sabbah Oòm-ran ibn Ismaïl Al-Kindi écrit le premier traité de cryptanalyse, “manuscrit sur le déchiffrement des messages cryptographiques”. Il y présente une technique appelée “analyse des fréquences”, permettant de casser tout chiffre de substitution. Il remarque en effet que dans une langue, chaque lettre n’a pas la même fréquence d’apparition, et que d’un texte à l’autre on retrouve sensiblement les mêmes fréquences. En étudiant ainsi les occurrences des lettres du message chiffré on peut donc le décrypter.

2. Bref historique.

La renaissance de la cryptographie : chiffre de Vigenère

- 1460 : Léon Battista Alberti invente le principe de chiffrement polyalphabétique. C'est un chiffre de substitution où chaque lettre ne sera pas remplacée par une même autre lettre, car on va utiliser plusieurs alphabets de chiffrement. Cette idée est fondamentale dans l'histoire de la cryptographie, car cette méthode permet d'échapper à l'analyse des fréquences.
- 1585 : Blaise de Vigenère écrit son "traicté des chiffres ou secrètes manière d'escrire". Il y présente un chiffre longtemps considéré comme incassable. Il utilise un tableau de Trithème, appelé parfois improprement carré de Vigenère.

2. Bref historique.

La renaissance de la cryptographie

- Tableau de Trithème :

	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

2. Bref historique.

La renaissance de la cryptographie : chiffre de Vigenère

- Le chiffre de Vigenère nécessite un mot clé, qu'expéditeur et destinataire ont convenu par avance.
- On va par exemple chiffrer le message « la Touraine est une belle région » avec le mot clé « SUPINFO ».



2. Bref historique.

La renaissance de la cryptographie : chiffre de Vigenère

- On commence par répéter en boucle la clé au-dessus du texte. Ensuite, pour coder la première lettre, 'l', on regarde la lettre de la clé correspondante, 'S', et on se place dans le carré de Vigenère à l'intersection de la ligne commençant par 'S' et de la colonne commençant par 'l'. On trouve 'D'. Etc.

Clé	S	U	P	I	N	F	O	S	U	P	I	N	F	O	S	U	P	I	N	F	O	S	U	P	I	N	F
clair	l	a	t	o	u	r	a	i	n	e	e	s	t	u	n	e	b	e	l	l	e	r	e	g	i	o	n
chiffré	D	U	I	W	H	W	O	A	H	T	M	F	Y	I	F	Y	Q	M	Y	Q	S	J	Y	V	Q	B	S

2. Bref historique.

La renaissance de la cryptographie : chiffre de Vigenère

- A l'exposé de la méthode, on comprend que ce chiffre fut longtemps considéré comme incassable.
- Il l'est d'ailleurs si l'on utilise une clé aussi longue que le texte à chiffrer, et que l'on change de clé à chaque message.
- Cette méthode est appelée masque jetable et fut élaborée par Vernam en 1917. Son inviolabilité a été démontrée par Shannon en 1949.

2. Bref historique.

La renaissance de la cryptographie : chiffre de Playfair

- 1854 : chiffre de substitution polygrammique utilisé par exemple par les Britanniques lors de la guerre des Boers.
- On commence par découper le message d'origine en bigrammes.
- Si le nombre de lettres est impair on rajoute arbitrairement un 'x' à la fin.



2. Bref historique.

La renaissance de la cryptographie : chiffre de Playfair

- On exclut de l'alphabet le 'w', que l'on remplacera si besoin est par 'vv'.
- On dispose les 25 autres lettres dans un carré, qui constitue la clé de ce chiffre :

s	e	v	m	a
t	k	p	y	n
l	x	z	b	h
d	q	i	c	u
j	f	o	r	g

2. Bref historique.

La renaissance de la cryptographie : chiffre de Playfair

- Si deux lettres sont sur les sommets d'un rectangle, les lettres chiffrées correspondantes seront sur les deux autres sommets :

s	e	v	m	a
t	k	p	y	n
l	x	z	b	h
d	q	i	c	u
j	f	o	r	g

Par exemple 'eb' sera chiffré en 'MX' et 'be' en 'XM'.

2. Bref historique.

La renaissance de la cryptographie : chiffre de Playfair

- Si deux lettres sont sur une même ligne (*resp.* colonne), on prend comme lettres chiffrées les deux lettres situées juste à leur droite (*resp.* en dessous) :

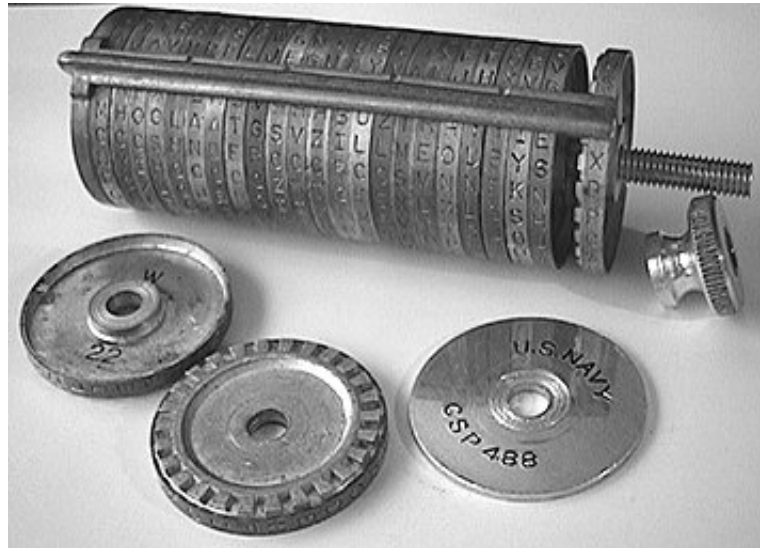
s	e	v	m	a
t	k	p	y	n
l	x	z	b	h
d	q	i	c	u
j	f	o	r	g

Par exemple 'ea' sera chiffré en 'VS' et 'yc' en 'BR'.

2. Bref historique.

La mécanisation de la cryptographie : cylindre de Jefferson

- 1800 : Thomas Jefferson met au point le “cylindre de Jefferson”, composé d’une série de disques pivotant autour d’un axe, et sur lesquels sont inscrits des alphabets désordonnés.



2. Bref historique.

La mécanisation de la cryptographie : cylindre de Jefferson

- Ici, la clé est l'ordre dans lequel les disques sont insérés sur l'axe.
- Pour chiffrer un message, on fait tourner les disques de façon à ce qu'il apparaisse sur une ligne du cylindre. Le message chiffré sera alors le contenu de la ligne suivante.
- Le destinataire, après avoir ordonné les disques selon la clé, reconstituera sur une ligne le message chiffré. Il n'aura plus ensuite qu'à lire le texte intelligible sur la ligne précédente.

2. Bref historique.

La mécanisation de la cryptographie : machine ENIGMA

- 1918 : Arthur Scherbius dépose le brevet de sa machine à chiffrer appelée “ENIGMA” qui réalise un chiffre de substitution polyalphabétique.
- Elle ressemble à une machine à écrire. À chaque lettre tapée, une impulsion électrique est émise, parcourt divers circuits dépendants de la position de rotors, et éclaire finalement une ampoule correspondant à la lettre chiffrée. Entre chaque lettre, la position des rotors changent, modifiant ainsi la substitution opérée.
- La clé de chiffrement de cette machine est la position initiale des rotors. Le nombre de clés est gigantesque.

2. Bref historique.

La mécanisation de la cryptographie : machine ENIGMA



2. Bref historique.

La mécanisation de la cryptographie : machine ENIGMA

- À partir de 1926, les différents secteurs de l'armée allemande vont s'équiper en machines ENIGMA.
- Environ 100 000 exemplaires seront ainsi utilisés.
- Les services secrets britanniques créeront pendant la deuxième guerre une cellule chargée de déchiffrer les messages issus de machines ENIGMA.
- La réussite de cette opération, la plus vaste de l'histoire de la cryptanalyse, permit selon les historiens d'écourter la guerre d'environ deux ans.

2. Bref historique.

La cryptographie contemporaine

- 1976 : Whitfield Diffie et Martin Hellman publient “new directions in cryptography”, un article dans lequel ils décrivent un protocole afin de s’échanger secrètement une clé de chiffrement. C’est une avancée majeure car la communication des clés a toujours été un problème fondamental. Dans cet article ils introduisent également le concept de clé publique.
- 1976 : algorithme de chiffrement à clé secrète D.E.S., Data Encryption Standard. Longtemps il fut un des chiffres les plus utilisés au monde.

2. Bref historique.

La cryptographie contemporaine

- 1977 : algorithme R.S.A., conçu par Ron Rivest, Adi Shamir et Leonard Adleman.
- 1991 : logiciel PGP “Pretty Good Privacy” mis au point par Phil Zimmermann. Il s’agit d’un freeware destiné principalement aux particuliers afin qu’ils chiffrent leurs emails.
- 2000 : algorithme A.E.S., Advanced Encryption Standard, mis au point par Joan Daemen et Vincent Rijmen, remplaçant de l’algorithme D.E.S.

2. Bref historique.

La cryptographie contemporaine

- Les dernières recherches se portent sur ce que l'on appelle la cryptographie quantique.
- L'échange de clés se ferait par un canal quantique, ou une information interceptée et lue par un tiers y introduit des erreurs.
- On peut donc détecter si une clé a été interceptée par un ennemi potentiel, et par conséquent l'utiliser ou pas.

2. Bref historique.



3. Les deux types de cryptographie.

3. Les deux types de cryptographie.

Cryptographie symétrique : définition

- Un système de chiffrement est dit **symétrique** si la clé utilisée lors du chiffrement est aussi celle utilisée lors du déchiffrement.
- Un tel système est aussi qualifié de **système de chiffrement à clé secrète**.



3. Les deux types de cryptographie.

Cryptographie symétrique : exemples

- Scytale : on utilise des bâtons de même diamètre pour chiffrer et déchiffrer.
- Chiffre de César : le décalage est de trois lettres que ça soit pour chiffrer ou déchiffrer (seul le sens du décalage change).
- Chiffre de Vigenère : on utilise le même mot clé pour chiffrer et déchiffrer.
- Machine Enigma : la position des rotors est la même lors du chiffrement ou du déchiffrement.

3. Les deux types de cryptographie.

Cryptographie symétrique : le problème de l'échange des clés

- Les correspondants doivent convenir par avance d'une clé avant de commencer leurs échanges de messages.
- La communication des clés est ainsi le problème majeur des systèmes symétriques car elle doit se faire confidentiellement.
- D'autant plus que pour résister aux attaques des cryptanalistes, il faut changer régulièrement de clé.

3. Les deux types de cryptographie.

Cryptographie asymétrique : définition

- Un système de chiffrement est dit **asymétrique** si la clé utilisée lors du chiffrement est différente de celle utilisée lors du déchiffrement.
- Un tel système est aussi qualifié de **système de chiffrement à clé publique**.



3. Les deux types de cryptographie.

Cryptographie asymétrique : principe

- Les correspondants ont chacun une clé qu'ils gardent secrète et une clé dite publique qu'ils communiquent à tous.
- Pour envoyer un message, on le chiffre à l'aide de la clé publique du destinataire.
- Celui-ci utilisera sa clé secrète pour le déchiffrer.



3. Les deux types de cryptographie.

Cryptographie asymétrique : analogie

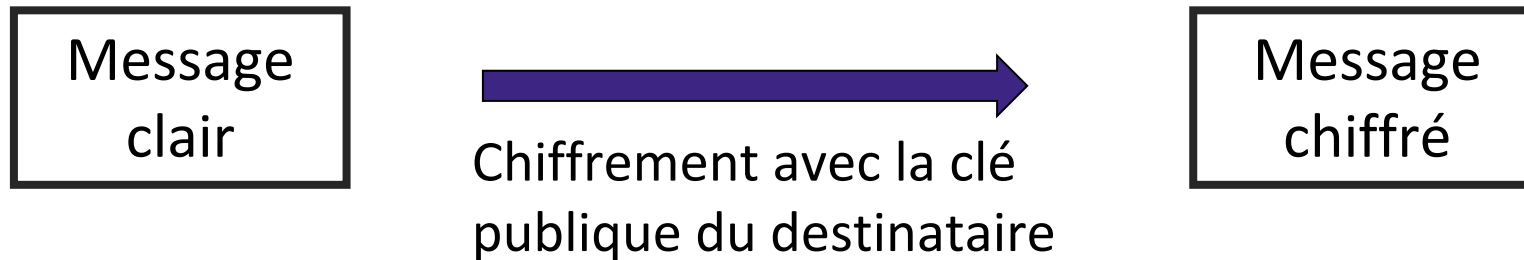
- C'est comme si le destinataire mettait à disposition de tous des cadenas ouverts dont lui seul a la clé.
- Quand on lui écrit, on insère le message dans un coffre que l'on ferme avec un tel cadenas, et on lui adresse le tout.



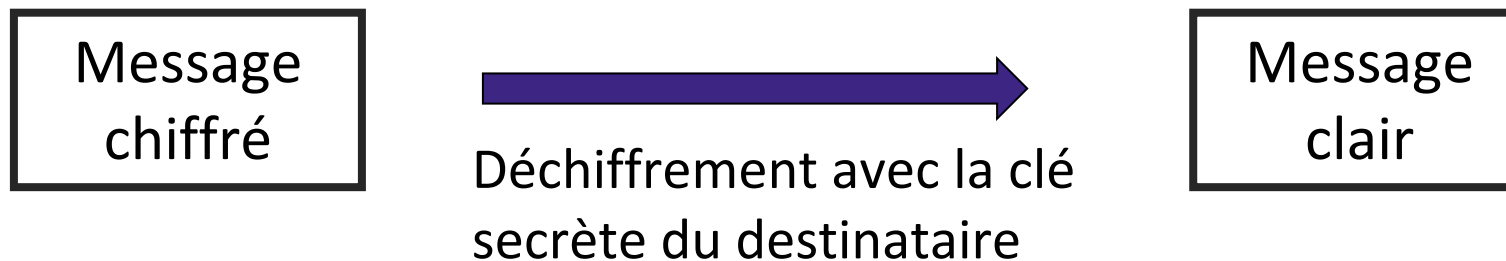
3. Les deux types de cryptographie.

Cryptographie asymétrique : schématisation

- Du côté de l'expéditeur :



- Du côté du destinataire :



3. Les deux types de cryptographie.

Comparatif

Cryptographie symétrique	Cryptographie asymétrique
Problème majeur d'échange des clés	Pas de clés à échanger
Relative simplicité d'implémentation	Relative complexité d'implémentation
Peu coûteux en ressources matérielles	Très coûteux en ressources matérielles
Relativement rapide	Très lent

3. Les deux types de cryptographie.

Comparatif

- Le logiciel PGP (Pretty Good Privacy) pallie en partie à ces problèmes en combinant les deux systèmes.
- A chaque message, il génère une clé secrète à usage unique et il :
 - chiffre le message avec un algorithme de chiffrement symétrique et cette clé.
 - chiffre la clé avec un algorithme de chiffrement de type R.S.A.
- L'expéditeur envoie enfin message et clé chiffrés au destinataire.

3. Les deux types de cryptographie.



4. Applications modernes.

4. Applications modernes.


Applications diplomatiques

- À l'origine, la cryptologie a été utilisée à des fins diplomatiques et militaires (cf. historique).
- Cette application est cependant encore d'actualité.
- Citons par exemple le fameux “téléphone rouge”, ligne reliant le Kremlin et la maison blanche.
- L'algorithme utilisé était celui de Vigenère, avec une clé aussi longue que le message à chiffrer. Cette clé était échangée par la valise diplomatique.

4. Applications modernes.

Applications diplomatiques

- Fidel Castro et Ernesto Guevara utilisèrent ce même procédé dans les années soixante.



03288	88767	08762	63183	76487	06267	67068	
61866	68432	46051	87931	78292	03033	46993	
69140	10399	44713	40019	44679	09280	05754	
23797	68277	65867	08709	58395	76588	72397	← clair
62773	41168	42357	47453	62133	71390	45511	← clé
85680	09338	07119	45854	10428	47828	17823	← chiffré
63095	87089	58672	71528	72843	93707	49876	
48794	07888	48128	80098	62982	48696	87716	
01989	84869	96997	51516	34722	71395	28786	
38726	50833	82088	28727	68626	31833	73111	
84880	19471	78213	76699	88830	42540	62630	
16276	69204	50291	94311	56956	73373	35741	
72722	28366	58976	46760	97613	05867	63237	
12764	35601	94508	52040	57871	52509	78693	
89751	53567	42474	98720	44484	57361	31872	
21773	78208	76926	39376	32616	03746	41483	
61818	00621	07408	75573	67230	67808	81792	
80001	78829	73324	03881	99806	60744	28175	
15439	76858	98767	26796	59377	93987	62946	
23892	30542	38091	40169	48423	46825	73171	
31221	06310	26758	61895	97790	39702	35027	
58728	73333	08077	15832	85850	65872	88728	
06389	25061	32247	88411	82783	32321	22788	
154082	98332	32214	92293	67933	97153	00523	

4. Applications modernes.

Signature numérique : objectif

- Le but ici n'est pas de chiffrer un message, mais de vérifier l'intégrité de celui-ci et d'authentifier l'identité de son expéditeur.
- Par intégrité on entend non-altération du message, c'est-à-dire que l'on se demande si le message aurait pu être intercepté et modifié.



4. Applications modernes.

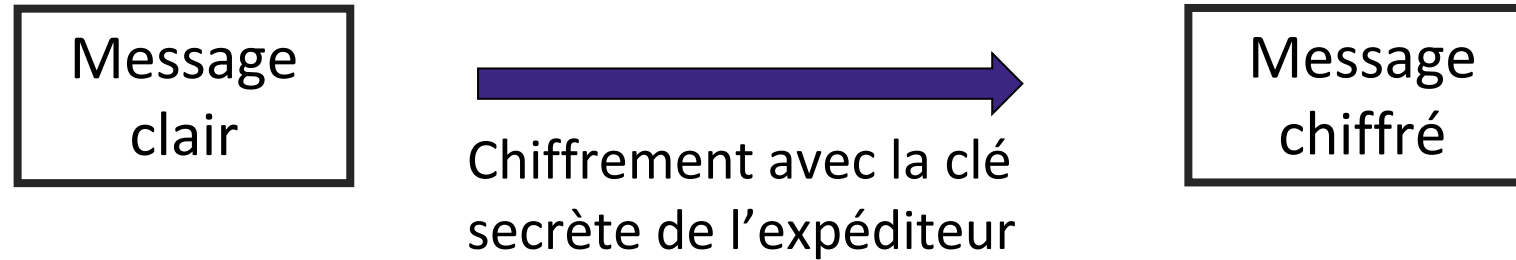
Signature numérique : principe

- Pour implémenter une signature numérique on utilise un système de chiffrement à clé publique :
 - L'expéditeur "chiffre" son message à l'aide de sa clé secrète et il envoie alors message chiffré et message en clair à son destinataire.
 - Le destinataire déchiffre le message chiffré à l'aide de la clé publique de l'expéditeur et compare ce qu'il obtient avec le message en clair.
 - Une différence entre les deux prouverait que soit le message a été altéré, soit l'expéditeur n'est pas celui qu'il prétend être.

4. Applications modernes.

Signature numérique : schématisation

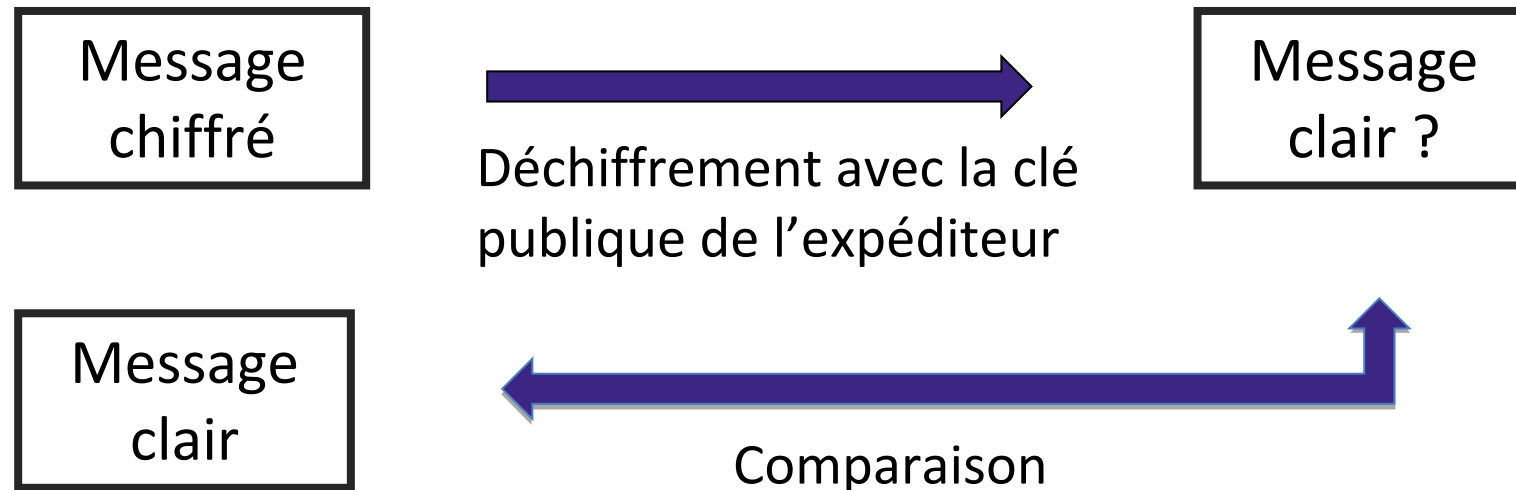
- Du côté de l'expéditeur :



4. Applications modernes.

Signature numérique : schématisation

- Du côté du destinataire :



4. Applications modernes.

Sécurité des cartes bancaires : trois facteurs

1. Code confidentiel à 4 chiffres.
2. Authentification hors ligne (signature R.S.A.) : chaque carte a une V.S., Valeur de Signature, nombre calculé lors de sa fabrication à partir des informations personnelles du propriétaire. Ce calcul s'effectue à l'aide d'un algorithme R.S.A. et de la clé secrète du groupement des cartes bancaires. Déchiffré à l'aide de la clé publique du groupement, il est alors comparé aux informations personnelles du propriétaire.

4. Applications modernes.

Sécurité des cartes bancaires : trois facteurs

3. Authentification en ligne (par D.E.S.) : le centre de paiement envoie à la carte une valeur aléatoire. Celle-ci chiffre cette valeur à l'aide d'une clé secrète contenue dans sa puce et de l'algorithme D.E.S. Le centre de paiement fait ce même calcul et compare les deux valeurs. À noter que cela nécessite que le centre de paiement connaisse les clés secrètes de toutes les cartes bancaires.



4. Applications modernes.



