

# Introduction

---

Le passage de la préhistoire à l'Histoire s'est fait dès la création de l'écriture. En effet à partir du moment où l'on a pu conserver les grands faits de l'homme, elle a débuté. Sans l'écriture la cryptologie n'aurait jamais existé. Cependant son élaboration ne s'est pas faite au hasard du temps. On peut penser comme David Kahn l'a dit que ce doit être dès que la culture a atteint un certain niveau, mesuré par sa littérature, que la cryptographie apparaît spontanément (comme ses parents l'écriture et le langage, l'ont probablement fait). Les besoins multiples de l'homme demandant de la confidentialité entre deux ou plusieurs personnes, au milieu de la société conduit inévitablement à la cryptographie.

Dans le monde actuel, le décryptement, opération qui consiste à rétablir le texte clair d'un document chiffré dont on ne connaît pas la clé, est la source la plus importante de renseignements secrets. Les informations qu'il procure, beaucoup plus nombreuses et plus sûres que celles fournies par l'espionnage, exercent une influence sur la politique des gouvernements. Cependant l'édification de cette science qu'est la cryptologie ne s'est pas faite en un jour. Elle regroupe la cryptographie et la cryptanalyse. Le mot "*cryptologie*" du grec *kruptos* (caché) et *graphein* (écrire) peut être assimilé à "étude des écritures secrètes". La cryptographie, c'est l'art de dissimuler ses intentions ou ses instructions à ses ennemis et pourtant de les transmettre à ses amis au moyen d'un texte chiffré. En face, chez l'adversaire, il s'agit de briser le code, de trouver le système qui préside à son élaboration : c'est la cryptanalyse.

La cryptologie est apparue dans de nombreux domaines tels que l'armée, le commerce, la religion... Elle a donc énormément influencé le cours de l'histoire même si elle est restée dans l'ombre. Mais quels sont les principaux faits historiques que la cryptologie a bouleversé jusqu'à nos jours et par quels moyens ?

Cette étude portera sur la naissance de celle-ci jusqu'au deuxième conflit mondial puis nous aborderons l'état des techniques actuelles.

[G. PAIRE](#)

[\(partie suivante ...\)](#)

## Les 4000 premières années

### 1 De la naissance de la cryptologie jusqu'au moyen-âge

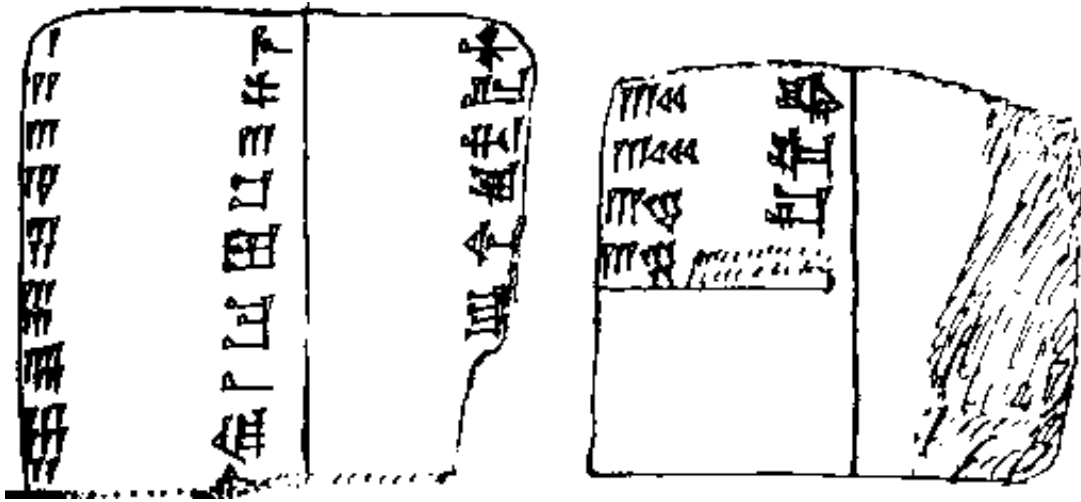
Un jour, il y a environ 4000 ans, dans une ville nommée Menet Khufu, au bord du Nil, un scribe traçait des hiéroglyphes qui racontaient la vie de son maître. Cela n'avait rien à voir avec une écriture secrète au sens que l'on donne de nos jours mais cet homme grava sur la pierre funéraire des hiéroglyphes inusités. Le but n'était pas de rendre le texte incompréhensible mais plutôt de lui conférer un caractère plus solennel. C'est comme si on lisait à la place de "1863", "*l'an de grâce mil huit cent soixante trois*". Ainsi l'inscription contenait le premier élément essentiel de la cryptographie : une modification volontaire de l'écriture. Dès lors apparut en Egypte un engouement pour la modification des hiéroglyphes. Les scribes rédigeaient délibérément leurs écritures de façon obscure sur les pierres funéraires pour soit disant attirer l'attention des lecteurs. Cela ne fut pas le cas, car aucun dictionnaire n'était disponible. Ces inscriptions possédaient le deuxième élément essentiel de la cryptologie : le secret. Cependant cette méthode échoua complètement car au lieu de raviver les intérêts, elle éteignit jusqu'au moindre désir de lire l'introduction d'une sorte de cryptographie.

Alors que l'on peut douter d'une véritable cryptologie égyptienne, il est sûr que la Chine antique pratiquait cette technique. Ils utilisaient plus précisément la stéganographie qui vise à dissimuler le message secret. Les Chinois employaient généralement du papier ou de la soie pour le message qu'ils roulaient en boule et recouvraient de cire. Le porteur dissimulait la sphère de cire sur lui ou avalait celle-ci.

Cependant la Chine n'a jamais vraiment pratiqué la cryptographie, science appliquée englobant à la fois les techniques de chiffrement et la cryptanalyse. Pourquoi cela, sachant que ce pays a longtemps surclassé les autres civilisations ? On peut répondre par la remarque du professeur Owen Lattimore de l'université de Leeds : "*Bien que l'écriture soit très ancienne dans la culture chinoise, sa pratique fut toujours limitée à une si petite minorité que l'écriture elle-même était un code*". Ainsi il n'y avait aucune notion de confidentialité nécessaire pour un émetteur quelconque de message.

Chez le grand voisin de l'Ouest de la Chine, l'Inde, dont la civilisation atteignit pendant de nombreuses années un niveau élevé, plusieurs sortes de communications secrètes étaient connues. Notamment dans le célèbre ouvrage érotique le "*Kama Sutra*", l'écriture secrète figure parmi les soixante-quatre arts que les femmes doivent connaître. Mais aussi dans un ouvrage classique de science politique, "*l'Artha-Sastra*" de Kautilya, écrit entre 321 et 300 avant Jésus-Christ où il recommandait de faire appel à la cryptanalyse pour recueillir des renseignements : "*...il peut essayer de se renseigner ( pour savoir l'état de la loyauté du peuple ) en écoutant les bavardages des mendiants, des ivrognes ou des fous [...], ou en prenant connaissance des graffitis écrits sur les lieux de pèlerinage ou dans les temples, ou bien en déchiffrant les inscriptions ou les écritures secrètes*". Kautila en faisant voisiner la cryptanalyse avec de telles sources voulait-il en faire l'éloge ou la discréditer ? Néanmoins bien qu'il ne donne aucune indication sur la manière de décrypter, le fait qu'il en connaisse la possibilité suggère un embryon de science cryptologique. Cela a été la première mention dans l'histoire d'une cryptanalyse à but politique.

La Mésopotamie, autre grande civilisation de l'antiquité, atteignit un niveau cryptologique étonnamment moderne. On retrouva à Suse (Iran actuelle) des fragments de tablettes où à des nombres (barres sur le schéma ) correspondaient des mots.



Cependant, du fait de l'usure du temps, ces tablettes ne se sont pas conservées entièrement. Et on n'a pu savoir s'il s'agit vraiment du premier répertoire dans l'histoire de la cryptologie, mais beaucoup de chercheurs s'accordent sur cette hypothèse.

Autre grande civilisation de l'antiquité, la Grèce, avec Sparte la plus guerrière des cités grecques, a conçu le premier procédé de chiffrement militaire. Dès le 5ème siècle avant Jésus Christ elle employait un instrument appelé "*scytale*", le premier utilisé en cryptographie et fonctionnant selon le principe de transposition (les lettres sont mélangées). Il consistait en un axe de bois autour duquel on enroulait, en spires jointives, un ruban de papyrus, cuir ou parchemin. Le texte était écrit (en lignes droites successives parallèles à l'axe) sur le ruban qui était ensuite déroulé tel quel par le destinataire. Ce dernier réenroulait la bande sur le bâton de même diamètre que le premier. Les mots chevauchaient alors les spires et le texte se reformait. Des historiens grecs tels que Thucydide ou Plutarque mentionne l'utilisation de ce procédé par les Spartes vers 475 avant Jésus Christ pour ordonner à un général trop ambitieux de s'allier ou même 100 ans plus tard quand un général spartiate répond à une accusation d'insubordination.

Les Grecs sont aussi à l'origine de procédés stéganographiques tels que des trous représentant les lettres de l'alphabet sur un disque. Le chiffrement consistait à passer un fil de façon aléatoire dans les différents trous. Un autre procédé stéganographique était de marquer d'une piqûre d'épingle dans un livre ou tout autre document les lettres dont la succession fournit le texte secret (notamment utilisé par les Allemands pendant le premier conflit ). Polybe, écrivain grec, est à l'origine du premier procédé de chiffrement par substitution. C'est un système de transmission basé sur un carré de 25 cases :

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Chaque lettre peut être ainsi représentée par un groupe de deux chiffres : celui de sa ligne et celui de sa colonne. Ainsi e=15, v=51,...

Polybe proposait de transmettre ces nombres au moyen de torches. Une dans la main droite et cinq dans la main gauche pour e par exemple. Cela permettait donc de transmettre des messages sur de longue distance. Les cryptologues modernes ont vu dans le "carré de 25" plusieurs caractéristiques extrêmement intéressantes :

- la conversion de lettres en chiffres
- la réduction de nombres, de symboles
- la représentation de chaque lettre par deux éléments séparés

Malheureusement, Polybe ne relate aucune utilisation de son procédé révolutionnaire. Les premières utilisations confirmées du principe de substitution se sont vues dans les opérations militaires avec notamment les romains et le plus grand d'entre eux : César. Il écrivait à Cicéron en remplaçant chaque lettre claire par celle située 3 rangs plus loin dans l'alphabet.

Durant le moyen-âge la cryptologie évolue faiblement car peu la pratique. Seul les moines en Europe utilisent cette science plus par jeu que par nécessité. Ils ont été probablement influencés par les Saintes écritures de "l'ancien testament" chapitre 25 verset 36 où la ville de Babylone (Babel) apparaît sous la forme de sheshak. Il s'agit d'un système de substitution traditionnelle appelé "Atbash", c'est l'équivalent de l'alphabet hébreu de a=z, b=y, c=x, d=w,...

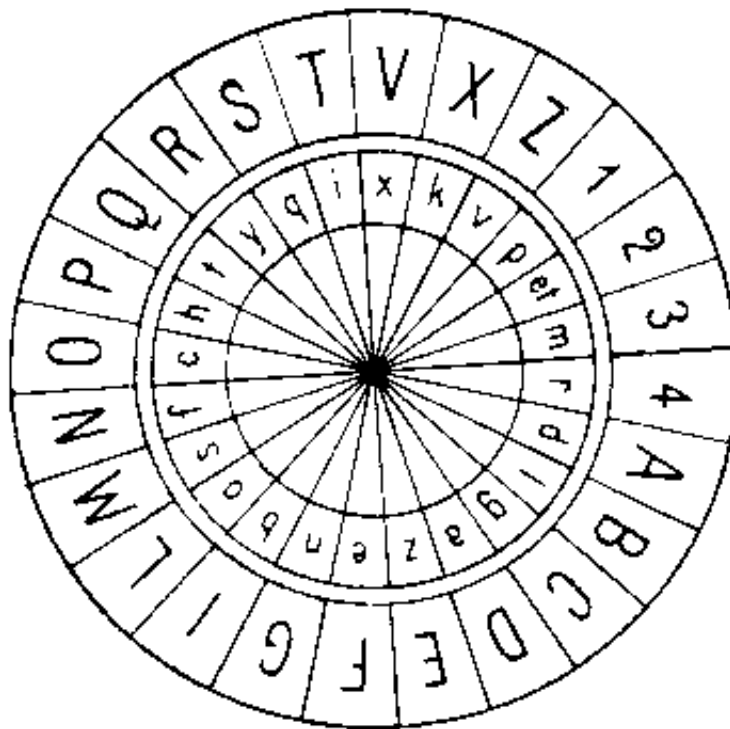
De plus, jusqu'au moyen-âge, il n'y a eu aucune recherche suivie en matière de cryptanalyse. Celle-ci naquit chez les Arabes. Ils découvrirent les méthodes de décryptement et les consignèrent par écrit. Cet intérêt pour la cryptologie se manifesta dès 855 avec le savant Abu Bakar ben Wahshiyya qui mentionne

plusieurs alphabets secrets traditionnels. Dans son livre "*Kitab shank almustahann fi ma'arifat rumus al aklan*" (livre de la connaissance longuement désirée des alphabets occultes enfin dévoilé). Le titre de son ouvrage démontre le côté magique que les gens se faisaient de la cryptologie. En effet, dès l'aube de son existence, elle a été employée pour dissimuler les fragments essentiels des écrits traitant de cet inquiétant sujet qu'est la magie. Des procédés stéganographiques comme les encres sympathiques, leur paraissaient peut-être inexplicables. Loin de s'inquiéter à propos de cela, les Arabes utilisèrent qu'en de rares occasions, leurs moyens de chiffrement. Cependant la science arabe en matière de cryptologie est exposée dans la "*subh al-a sha*", encyclopédie en 14 volumes. Elle fut achevée en 1412. Cet œuvre annonce de nouvelles méthodes de transposition et substitution, avec notamment plusieurs représentations cryptographiques pour une même lettre. Mais ces innovations sont éclipsées par une autre bien plus importante : un traité de cryptanalyse, le premier de l'histoire.

## 2 L'éveil de l'occident

Alors que la féodalité du moyen-âge n'avait que peu fait avancer la cryptologie européenne, l'Italie en 1467 a réussi avec un homme d'un génie exceptionnel, Leon Batista Alberti, à faire fortement évoluer la science des écritures secrètes. Il inventa la substitution polyalphabétique, procédé permettant la correspondance de nombreux alphabets cryptés en un seul clair.

Le grand disque est fixe tandis que le second est mobile. Chacun d'eux est divisé en 24 secteurs. Il possède les 24 lettres de l'alphabet latin. Ce sont les lettres en majuscule de l'alphabet normal sans h, k, y, j, u, w et avec en plus les chiffres 1, 2, 3 et 4.



*Cadran chiffrant d'Alberti*

Il faut convenir d'une lettre indice dans le cercle interne, k, avec le correspondant puis l'on peut débiter le cryptogramme par la lettre de l'anneau placée en face de la lettre indice. Mais là où Alberti engage la cryptographie sur la voie de la complexité, est quand il écrit : "Après avoir écrit 3 ou 4 mots, je peux changer la position de la lettre indice en tournant le disque de façon que k soit, par exemple, sous le D. Donc dans un message, j'écrirai un D majuscule et à partir de ce point k ne signifiera plus B mais D et toutes les lettres du disque fixe auront de nouveaux équivalents."

La substitution polyalphabétique est née. Mais où Alberti va plus loin, est quand il complète sa découverte par une autre invention déterminante dans l'histoire de la cryptologie : le surchiffrement codique. En effet il constitua un répertoire de 336 groupes de mots représentés par toutes les combinaisons allant de 11 à 4444. Mais le génie d'Alberti était trop en avance sur son temps et ce n'est que 400 ans plus tard que les puissances mondiales utiliseront ce procédé de surchiffrement codique mais bien plus simplement.

Un moine bénédictin en 1518 conçut aussi un système de substitution polyalphabétique, Jean Trithème. Il utilisait un tableau qu'il appela "*tabula recta*".

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

Il chiffrait la première lettre avec le premier alphabet, la deuxième lettre avec le deuxième alphabet, et ainsi de suite.

Mais la substitution polyalphabétique évolua encore sous l'impulsion de Giovanni Batista Belaso, homme si ordinaire que l'on ne sait presque rien de lui. Il inventa la notion de clé littérale qu'il appela "mot de passe".

*Clé littérale* : BEL ASOBELA SOB ELASOB

*Texte clair* : LES ITALIENS ONT TROUVE

Si la clé est "belaso", le cryptogramme est créé par l'association entre B et L pour cet exemple. Il suffit de regarder dans un tableau comme ci-dessus pour mettre un caractère crypté et ainsi de suite pour les autres lettres. Cependant l'invention revînt à un jeune prodige, futur fondateur de la première société scientifique, Giovanni Batista Porta, qui utilisait cette notion de clé littérale avec la première substitution

## bigrammatique de l'histoire de la cryptologie

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	Z
Y	9	Y	9	∇	H	∅	X	∅	X	X	∅	H	∅	∅	∅	∅	∅	∅	A
∅	P	∆	P	∆	H	∅	X	∅	X	X	∅	∅	∅	∅	∅	∅	∅	∅	B
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	C
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	D
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	E
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	F
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	G
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	H
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	I
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	L
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	M
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	N
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	O
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	P
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	Q
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	R
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	S
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	T
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	V
∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	∅	Z

*Le premier système bigrammatique connu: chaque paire de lettres était remplacée par le symbole situé à l'intersection de la colonne de l'une et de la ligne de l'autre*

Il écrit en 1563 un livre "De Furtivis Literarum Notis" résumant les éléments existants en cryptologie. Il y parle d'un objet du même type que celui qu'avait conçu Alberti, de la facilité de changement de clé littérale du système Belaso et du chiffrement lettre à lettre de Trithème.

Il y aura encore des améliorations de la substitution polyalphabétique au 16ème siècle par l'utilisation d'un procédé "autoclave" (le message lui-même est la clé). C'est Cardan, médecin et mathématicien

milanais qui invente ce procédé. Malgré sa brillante idée, l'application qu'il en faisait était défectueuse.

L'inventeur du second procédé "*autoclave*", valable celui là, est un français du nom de Blaise de Vigenère. C'est à Rome qu'il a eut son premier contact avec la cryptologie. Il y fera d'autres séjours pour renouer avec les experts cryptologues. Parmi les nombreux systèmes exposés par Vigenère, comme la façon de dissimuler un message dans l'image d'un champ d'étoiles, figure la substitution polyalphabétique. Il utilise un tableau du type Trithème : c'est le "*carré de Vigenère*" :

	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

*Tableau carré, dit « Carré de Vigenère »*



Jusqu'en 1917 ce procédé semblait indécryptable, notamment par des revues scientifiques américaines.

Cependant les gens utiliseront plus les répertoires par rapport à la substitution polyalphabétique qui nécessite plus de précision. En dépit du mythe de son inviolabilité, elle fut parfois décryptée. Mais il s'agissait de cas isolés, très espacés dans le temps, si peu fréquents que les ouvrages classiques de cryptologie ne les mentionnent même pas. Du fait de sa faible utilisation, les méthodes de décryptement étaient inexistantes.

Très vite les cryptologues insistent sur l'importance de la cryptanalyse dans la politique. Un homme, Antoine Rossignol intervient pour la royauté contre les huguenots assiégeant la ville de Réalmont en 1628. Il décrypte un message destiné aux huguenots en une heure annonçant la fin de munitions très proche des huguenots. Surprise l'armée royale fit capituler la ville malgré les remparts imposant. Avec ce haut fait, commença la carrière de celui qui allait devenir le premier cryptologue professionnel de France. Il se fit très vite une place de choix auprès du Roi. En 1630, ses décryptements l'ont rendu suffisamment riche pour construire un château à Juvisy. Le travail de Rossignol lui donnait accès à certains des plus importants secrets de l'Etat et, de ce fait, faisait de lui un homme brillant et respecté de la cour de Louis XIV. En 1682 il décède et son fils qu'il avait formé prit sa succession. Bonaventure hérita de 12000 livres et passa en 1688 de conseiller du parlement à président aux requêtes du palais. Une des plus grandes contributions des Rossignols fut de démontrer de façon éclatante à ceux qui gouvernaient la France l'importance du décryptement dans la détermination de leur politique.

Cela aboutit à la création d'un bureau spécialisé au 18ème, le Cabinet Noir. D'autres s'édifièrent dans toute l'Europe. Celui de Vienne en Autriche passait pour être le meilleur d'Europe. Les cryptanalystes utilisaient la sténographie pour plus de rapidité, ils connaissaient toutes les langues européennes. Si une était inconnue alors un fonctionnaire l'apprenait. Dix personnes travaillaient et déchiffraient 80 à 100 courriers par jour. Ils commirent que peu d'erreurs. En effet pour plus d'efficacité, une personne travaillait une semaine sur deux. L'Autriche possédait alors une très bonne politique extérieure du fait de leur puissance dans le domaine de la cryptologie.

L'Angleterre possédait aussi son Cabinet Noir. C'est sous l'impulsion de Wallis, passionné par la science des écritures secrètes, que de nombreux décryptements sur répertoire et substitution mono-alphabétique furent possible, notamment des cryptogrammes américains à destination de l'Europe. C'est le père de la cryptologie anglaise comme Rossignol l'était en France.

Sans aucun doute les succès des cryptanalystes étaient dus, dans une large mesure, à leur habileté. Cependant, selon François de Callière : "Les déchiffreurs célèbres ne doivent leur considération qu'à la négligence de ceux qui donnent de méchants chiffres, et à celle des négociateurs et de leurs secrétaires qui s'en servent mal.". Sa remarque est juste dans le sens où il y avait une mauvaise utilisation du chiffre facilitant ainsi la tâche du cryptanalyste. Les tourments politiques de 1840 renversèrent la plus grande partie de ce qui restait en Europe d'absolutisme. Le renouveau de la liberté ne tolérait plus l'ouverture des lettres par les gouvernements. En Angleterre, une formidable clameur publique et parlementaire contre l'ouverture clandestine du courrier obligea à interrompre leur Cabinet Noir. En France, il n'a cessé de

dépérir depuis la révolution pour totalement disparaître. Mais simultanément allait naître une invention qui révolutionnera la cryptographie : le télégraphe.

Cette nouvelle innovation dans les flux d'information suscita de nouvelles vocations à la cryptologie. Les hommes d'affaires utilisaient des codes commerciaux pour leurs transactions. Ils remplaçaient des mots ou des phrases par de simples groupes codiques qui offraient une sécurité suffisante. Mais les commerçants et courtiers réalisèrent que le principal avantage de ces codes était quand même l'économie financière qu'ils procuraient.

Dans le domaine militaire, le télégraphe allait offrir aux généraux et autres officiers l'occasion d'exercer un contrôle continu et instantané des forces armées. Le chef militaire, installé dans un poste de commandement loin à l'arrière et informé par le télégraphe, suivait sur des cartes l'évolution de la bataille, mieux qu'il n'aurait pu le faire sur le terrain. Le temps des généraux à cheval, surveillant la bataille du sommet d'une colline comme Napoléon, était révolu.

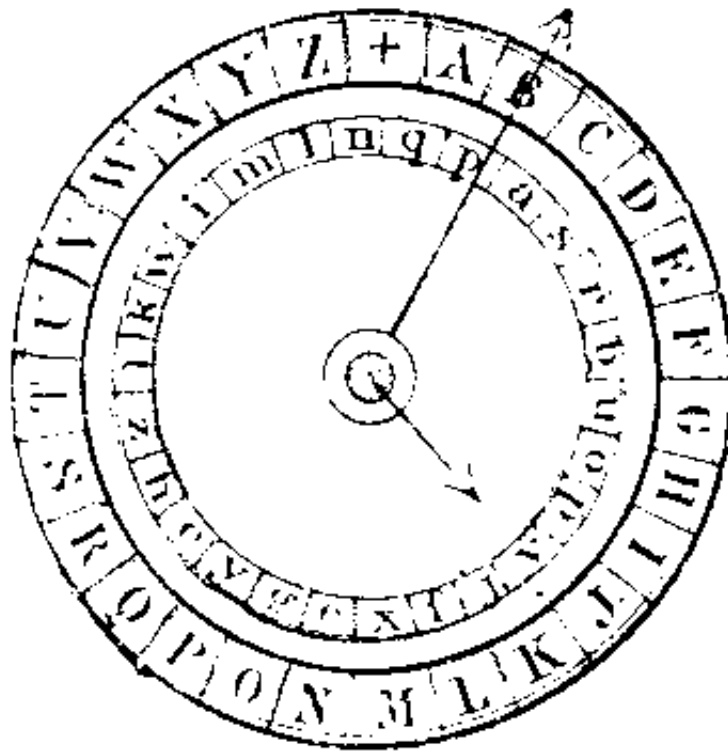
Une situation nouvelle demandait de nouvelles théories, une nouvelle approche. C'est alors qu'un ouvrage fondamental ouvrit la cryptologie aux influences extérieures : "la cryptographie militaire" d'Auguste Kerckhoffs von Nieuvenhof. Il naquit en Hollande mais fit ses études à Aix-la-Chapelle. Il s'inscrivit à l'université de Liège où il obtint un diplôme de lettres es sciences. Kerckhoffs mettait en relief le changement apporté aux communications militaires par le télégraphe. Les chefs des armées désiraient que le chiffrement militaire possède les qualités suivantes : sécurité, rapidité et donc simplicité. Kerckhoffs avait reçu ce nouvel ordre de chose et souligna l'importance de la cryptanalyse mettant à l'épreuve les procédés de chiffrement. De ces principes de sélection d'un système de chiffrement opérationnel, il déduisit six conditions fondamentales :

- le système doit être matériellement, sinon mathématiquement, indécryptable
- il faut qu'il n'exige pas le secret et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi
- la clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée et modifiée au gré des correspondants
- il faut qu'il soit applicable à la correspondance télégraphique
- il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes
- le système doit être d'un usage facile ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer

Par sa clarté, la qualité de ses sources, la valeur inestimable des nouvelles techniques qui y sont

exposées, mais avant tout par la maturité, la sagacité et l'acuité des vues de son auteur, "la cryptographie militaire" se place au premier rang parmi les ouvrages fondamentaux de la cryptologie.

Pendant quand France Kerckhoffs dégagait, avec une extraordinaire lucidité, les principes fondamentaux qui, encore de nos jours, guident les travaux des cryptologues, un illustre savant anglais, Wheatstone, sans doute plus pragmatique, enrichissait la cryptographie d'un nouveau procédé. Il s'agissait d'un cryptographe de type Alberti mais avec deux aiguilles semblables à celles d'une montre.



*Le cryptographe de Wheatstone (alphabet clair à l'extérieur, cryptographique à l'intérieur)*

Le fonctionnement était pratiquement identique sauf qu'il y avait le caractère spécial "+" permettant la séparation des mots. Ainsi en gardant le même angle entre les deux aiguilles, le cryptogramme apparaissait de façon continue, sans espace.

A l'aube du 20ème siècle, le savoir en cryptographie et cryptanalyse est important. C'est dans le domaine militaire que l'on verra le plus cette science des écritures secrètes. Beaucoup de cryptologues ont découvert des procédés très complexes cependant l'utilisation par les militaires sera simplifiée car des erreurs ont été faites dans le passé pour le cryptage ou le décryptage. La France, meilleure nation cryptologique, aborde le premier conflit mondial avec de l'avance sur l'Allemagne qui pense toujours être la nation suprême par excellence et qui reste sur ses acquis. En effet, ils ne se sont pas rendu compte de l'importance de la cryptanalyse mettant à l'épreuve la cryptographie. Des hauts faits historiques ont été

imprégnés par la cryptologie comme la résolution de l'affaire Dreyfus mais elle allait être décisive pour le destin du monde en raison de l'utilisation qu'elle a connue pendant les deux guerres mondiales.

[G. PAIRE](#)

[\(partie suivante ...\)](#)

## La première guerre mondiale

### **Bureau 40**

Le bureau 40 a été créé suite au désir de décrypter les messages allemands. C'est un organisme composé de plusieurs professionnels passionnés de cryptologie, installé en Angleterre. Leur première découverte fut la méthode de la substitution simple, qui consiste à remplacer chaque même lettre en clair par une seule unité cryptographique, toujours la même (c'est en fait un symbole).

L'un des moyens utilisés pour le décryptement fut le repérage radiogoniométrique. Ils déchiffrèrent les messages des *U-boote*, (sous-marins), qui étaient chiffrés avec un code à quatre lettres de la flotte de surface et surchiffrés par une transposition à tableau.

Les Allemands appelaient "*Gamma epsilon*" le surchiffrement pour les sous-marins classiques et "*Gamma-u*" celui des sous-marins à grand rayon d'action. Le mot clé était différent. Environ quinze mille télégrammes secrets allemands furent décryptés par le Bureau 40 d'octobre 1914 à février 1919. Cet organisme se divisait en deux sections de décryptement : la section navale et la section politique. Les Anglais décryptaient les messages diplomatiques allemands mais aussi espagnols (codés à l'aide de la méthode du surchiffrement).

Le meilleur code inventé à l'époque fut le Chiffre SA, conçu par J.C.F DAVIDSON en 1918 (qui remplaça le chiffre W). Les informations militaires transmises au consul d'Allemagne étaient chiffrées avec un dictionnaire-code et deux systèmes de langage convenu :

- 1er système : les noms de famille étaient utilisés pour les messages concernant les bateaux et les ports.
- 2ème système : pour les mêmes messages étaient utilisés les noms des produits pétroliers.

En 1917, le bureau 40 fit plusieurs découvertes. Tout d'abord ils ont découvert un long message codé, chiffré avec un code diplomatique connu sous l'appellation de code 0075, code désordonné qui était désigné, par le ministère allemand, au moyen d'un nombre de deux chiffres précédé de deux zéros (la différence arithmétique entre les deux chiffres était toujours égale à 2. D'autres codes comme le 0097, 0086, ou encore le 0064 (entre Berlin et Madrid) ont également été découverts.

Le télégramme de ZIMMERMANN suscita beaucoup de réflexion. En effet, il était chiffré, et particulièrement long, de mille groupes trouvés dans les dossiers du département de l'Etat. Quant au déchiffrement partiel, il posait problème sur l'exactitude du décodage (authenticité du message) Enfin le décryptement, par le bureau 40, d'un message ennemi contribua à l'entrée des Etats-Unis dans la première guerre mondiale. Pendant cette période l'Histoire fut entre les mains des décrypteurs.

### **Première guerre mondiale**

La première Guerre Mondiale fut une suite de véritables batailles sur le plan technique. Dans les deux camps, négligences et atermoiements caractérisèrent la période du début. Bientôt cependant, une activité fébrile marque l'intérêt des belligérants pour la cryptographie. Cette période est féconde et d'une influence décisive. Elle est à l'origine de la création, dans tous les pays, de services organisés de chiffre et de décryptement.

En août 1914, nul ne pouvait prévoir l'ampleur que devait prendre le chiffre dans une campagne que chacun, pour des raisons différentes, présumait courte. Sauf pour les Anglais, les précautions prises, dans les armées belligérantes, pour assurer le secret des correspondances furent insuffisantes. En France le commandant CARTIER avait réuni un certain nombre d'officiers qui avaient pour rôle d'assurer la confidentialité des correspondances et d'attaquer celles de l'ennemi. Les Allemands prirent conscience des dangers de l'interception de leurs messages et perfectionnèrent leur méthode, ce qui ne fut pas un obstacle pour les cryptologues.

La radio fut l'un des moyens le plus utilisé pour faire passer des messages. Les généraux s'en emparèrent rapidement comme instrument de guerre car elle multipliait l'avantage essentiel de la télégraphie militaire et accélérât la communication entre les quartiers généraux. Mais la probabilité d'interception était grande et la facilité d'écoute trop importante. (La cryptanalyse devint un moyen d'action opérationnelle. C'était une source valable d'informations et donc une véritable arme).

La radio fut utilisée de façon intensive au cours de la première Guerre Mondiale. C'est elle qui amena la cryptologie à maturité. Les Français réussirent à décrypter un système utilisé, par les Allemands, appelé *l'ÛBCHI*, qui était un système à double transposition.

Les Allemands ne changeaient leurs clés que très rarement, ce qui permit, entre autre, aux Français de bombarder THIELT (Belgique). Le 18 novembre 1915, les Allemands mirent en service un nouveau système, mais ce dernier fut rapidement décrypté par le lieutenant A..THEVENIN vers le 10 décembre. Un mois plus tard, on proposa une nouvelle méthode simplifiée pour le décryptement, appelée l'ABC mais qui fut abandonnée en mai 1915.

Les méthodes de décryptage et les clés étaient le plus fréquemment fournies par la section de Paris, aux sections du chiffre. Au début de l'année 1916, on assista à la reprise de l'activité de la radio. Les Allemands prirent connaissance de la phraséologie et des procédures de transmission, qui furent d'un grand secours acquis pendant les premiers jours de la Guerre.

Les Français continuaient leur chasse systématique aux mots-clés afin de décrypter un maximum de messages. On assista par la suite à l'apparition de nouveaux systèmes fondés exclusivement sur la substitution. Ils devinrent de plus en plus compliqués, mais cette évolution étant progressive, à aucun moment les Français ne se trouvèrent cryptologiquement distancés.

A la fin de 1916, des messages de transposition firent à nouveau leur apparition dans leur trafic militaire.

En janvier 1917, les cryptanalystes français identifièrent le procédé utilisé à cette période, comme étant celui des grilles tournantes, dont les seules caractéristiques communes avec la grille de Cardan était le nom et l'existence de fenêtres dans le cache. La grille tournante était généralement constituée par un carré de carton divisé en cases.

Le plus difficile problème auquel furent confrontés les cryptologues fut le système Für God, ainsi nommé parce que tous les messages chiffrés par ce moyen portaient cette mention pour indiquer qu'ils étaient destinés à la station radio dont l'indicatif d'appel était GOD. Ces messages étaient émis, de façon irrégulière, environ trois fois par semaine, par la puissante station de Nauen, située près de Berlin et dont l'indicatif était POZ. Le *Für God* apparut en 1916 et dura jusqu'à l'automne 1918, ce qui en fait le système allemand ayant eu la plus grande longévité. C'est un anglais, le capitaine Brooke-Hunt qui décrypta le *Für God* au début de 1917.

A l'arrière des lignes, les Français correspondaient au moyen d'un code surchiffré à quatre chiffres. Entre le 1er août 1914 et le 15 janvier 1915, ils en changèrent trois fois. Sur le front, les Français utilisaient parfois une substitution polyalphabétique par alphabets désordonnés et clé périodique. Mais le procédé auquel ils accordèrent leur confiance pendant trois ans était une transposition simple améliorée qui, paradoxalement, était théoriquement plus faible que la double transposition allemande. Mais tous leurs messages n'ont pas été décryptés car durant les deux premières années de la guerre, l'Allemagne n'avait pas de cryptanalyste sur le front ouest. Elle était entrée dans la guerre sans aucun service militaire de décryptement. Au fur et à mesure que la guerre se développait, les Français firent de plus en plus usage de la radio. En février 1916, le commandant de l'armée de Lorraine, réclama une sorte de code téléphonique en raison des interceptions qui avaient attiré des bombardements sévères et nombreux sur ses réserves. La Section de chiffre réalisa alors un *carnet de chiffres*. Les mots importants des messages téléphonés devaient être épelés sous une forme chiffrée où les lettres étaient remplacées par des bichiffres pris dans le carnet. Ces carnets étaient remplacés périodiquement.

Chaque édition avait un nom (Olive, Urbain...) et la lettre initiale de ce nom, répétée trois fois, indiquait le carnet utilisé pour le chiffrement. Plus tard, un avion d'état-major porta ces résultats au bureau de décryptement britannique et Berthold les télégraphia aux Français en utilisant un code spécial, réservé aux cryptanalystes. Ce fut la pierre de Rosette pour le décryptement du nouveau système, le *Schlüsselheft* (système américain de 1917).

Le 5 août 1918, une station d'interception capta un message de 456 lettres, adressé au ministère des Affaires étrangères et émanant du Kress von Kressenstein. Le lieutenant J.Rives Childs, qui était à la tête du petit groupe qui travaillait sur les systèmes littéraux, fit un relevé des fréquences, constata avec satisfaction que celle de la lettre b, particulièrement élevée, signifiait nécessairement qu'elle représentait le e clair dans une substitution mono-alphabétique et, en une heure, il avait décrypté le message. Mais le cryptage d'un tel message était jugé médiocre.

Mackensen, autre homme célèbre dans le domaine de la cryptanalyse, envoya une dépêche chiffrée en *ADFGVX*, probablement le chiffre de campagne le plus célèbre. Il était nommé ainsi parce que ces six

lettres seulement apparaissaient dans les cryptogrammes. Toutefois, lorsque le système fut mis en service le 5 mars 1918, cinq lettres seulement étaient utilisées : le V n'y figurait pas. A ce moment, la guerre apparaissait comme une sorte de match nul par épuisement des adversaires.

La première Guerre Mondiale marque l'un des principaux tournants de l'histoire de la cryptologie. Avant, son importance était secondaire ; après, elle était primordiale. Avant, c'était une science dans son enfance ; après, elle avait atteint la maturité. La cause directe de ce développement était l'accroissement énorme du volume des communications radio. L'accession de la cryptanalyse au rang de moyen d'information essentiel et permanent était le signe le plus frappant de la maturité récente de la cryptologie.

Mickaëlle LEBEL

[\(partie suivante ...\)](#)



## La seconde guerre mondiale

### **La cryptographie américaine**

En 1919, un organisme de recherche en matière de codes et chiffres appelé American Black Chamber (Cabinet noir) s'est installé à New York à l'initiative de Herbert Osbourne Yardley, un des plus célèbres cryptologues de l'histoire américaine. Son rôle était de décrypter les codes du Japon. Ce Cabinet noir fut considéré comme une activité d'espionnage et de surveillance dans le domaine de la politique étrangère. Quelques années plus tard, l'armée américaine décida de fondre en un seul organisme les fonctions de chiffres et de cryptanalyse et créa donc le "Signal Intelligence Service" (S.I.S) et plaça un homme dénommé William Frederick Friedman d'origine russe à sa tête qui deviendra quelques temps plus tard un cryptologue renommé. A l'approche de la guerre, le développement du S.I.S. s'accéléra et Friedman continua d'assurer, pour le compte du S.I.S, les fonctions de directeur de recherches pour les communications. Il prit sa retraite en 1955 tout en continuant de jouer un rôle de conseiller.

### **La cryptographie russe**

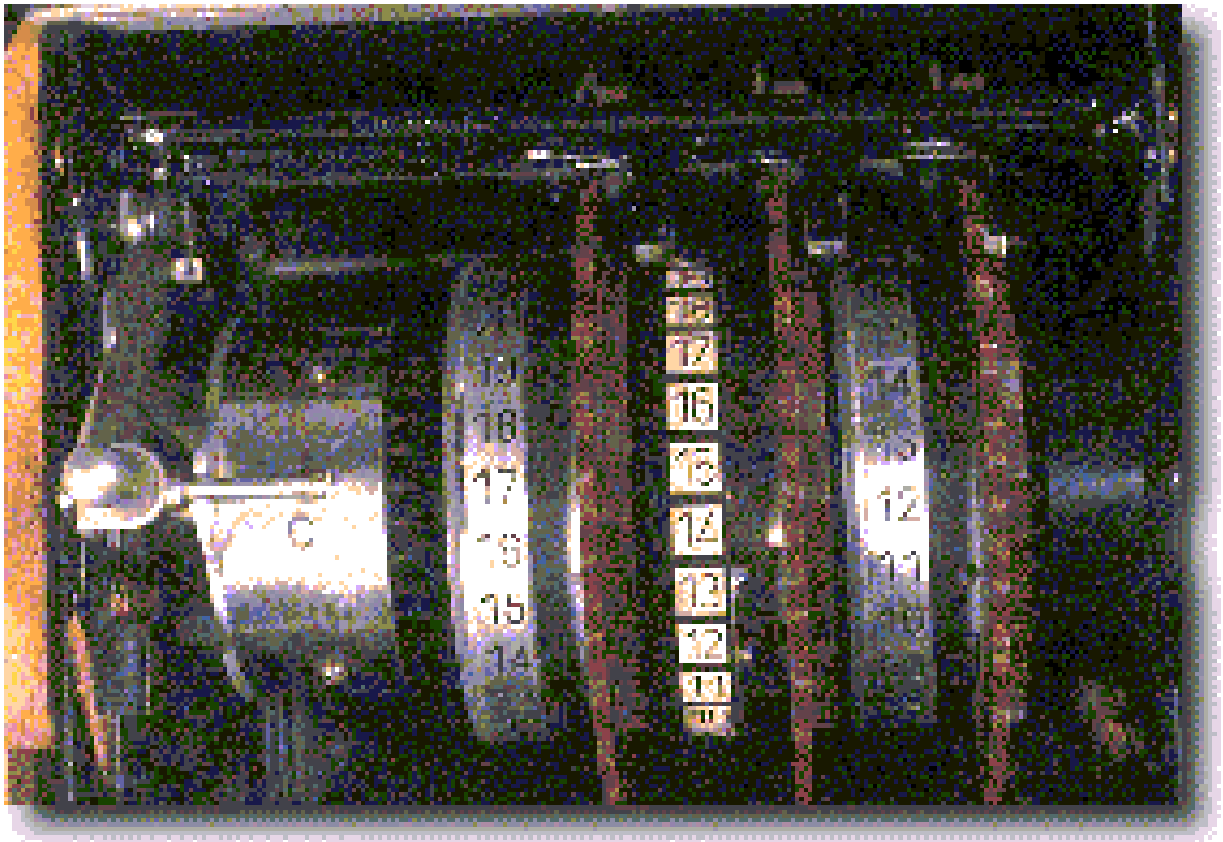
L'U.R.S.S. a marqué un certain intérêt aux codes et aux chiffres des autres pays, notamment les services de la police secrète et les renseignements militaires. La police secrète créée par Lénine a connu des appellations successives qui témoignent des mauvaises organisations. Après Staline, elle fut scindée en deux agences : le K.G.B. qui s'occupait d'espionnage et de contre espionnage et le M.V.D. ministère des affaires intérieures qui s'occupait du maintien de l'ordre. La principale organisation russe de cryptologie s'appelait le "Spets Otdel", quasi-indépendante, son activité consistait à décrypter les messages chiffrés des autres pays. C'est la police secrète qui alimentait cet organisme. Cette organisation fut dirigée par Vladimir M.Petrov. En 1929-1930, les agents du "Spets Otdel" établissait une synthèse hebdomadaire des télégrammes étrangers décryptés et la transmettait aux dirigeants de l'O.G.P.U. (police secrète) et au Comité central. Vers 1938 la diffusion devînt quotidienne. Au cours de la Seconde Guerre Mondiale, les systèmes cryptographiques de l'Armée Rouge faisaient appel à des codes surchiffrés, c'est à dire que le texte déjà chiffré subit une deuxième opération de chiffrement. Les méthodes de surchiffrement sont basés sur le principe de substitution et de transposition. A la même époque, les Russes obtinrent quelques machines Hagelin M.209 qu'ils ont utilisés comme modèle pour fabriquer leur propres machines, mais personne n'a su où ont été employées ces machines.

### **La Seconde Guerre Mondiale**

En 1939, peu avant la seconde Guerre Mondiale, le Capitaine Baudoin, un français, fait paraître son ouvrage marquant la transition entre la cryptologie classique et la cryptologie moderne. Durant la Seconde Guerre Mondiale, la cryptographie connût un développement considérable notamment avec l'utilisation de la machine ENIGMA.

### **La machine ENIGMA**

L'histoire débute en 1923 lorsque la Chiffriemaschinen Aktien Gesellschaft (Cipher Machine Corporation) montre pour la première fois au Congrès Postal International à Bern en Suisse, la machine de codage ENIGMA, modèle A. Le modèle A d'ENIGMA est lourd et volumineux, un clavier de machine à écrire (de type allemand QWERTY) est utilisé pour la saisie des messages. Dans les faits, la machine pouvait être utilisée comme une machine à écrire standard et cela même en plein milieu de l'encodage d'un texte. ENIGMA A ne connut pas un très grand succès malgré la publicité faite à cette époque. Par la suite, trois autres modèles apparurent, soit les modèles B, C, D. Le modèle B est similaire au modèle A à l'exception des rotors qui ont maintenant 26 contacts au lieu de 28 pour le modèle A. Les modèles C et D étaient portables et cryptographiquement différents des modèles précédents. Ces derniers fonctionnent selon des principes identiques à ceux des machines de Hebern, mais avec néanmoins quelques différences importantes.



**Machine ENIGMA**

### **Son utilisation**

L'ensemble mécanique de la machine ENIGMA est composé d'un clavier, 3 tambours (ou rotors) ainsi que d'un système d'entraînement des tambours. (voir image ci-dessus) Chaque touche du clavier est directement reliée à un système de levier portant un axe sur lequel peuvent pivoter trois doigts d'entraînement dont les extrémités supérieures sont terminées par un bec. Les doigts servent à entraîner les tambours et les faire avancer d'un pas. Il existe des tambours mobiles qui sont constitués chacun d'un noyau et d'une couronne crantée à 26 secteurs portant les 26 lettres de l'alphabet normal. Chaque

couronne alphabétique peut occuper 26 positions relatives par rapport au noyau.

L'ensemble électrique comprend une alimentation, 26 circuits et 26 lampes correspondant aux 26 touches du clavier. Le courant est fourni soit par des piles soit par le secteur au moyen d'un transformateur. Les 26 circuits correspondent à l'entrée et à la sortie aux lettres du clavier, ils comportent une partie fixe et une partie variable. Rapidement un grand nombre de gouvernements achètent ENIGMA pour l'étudier. Parmi les intéressés, on retrouve la marine allemande et les japonais. La marine allemande décide de mettre en fonction une machine ENIGMA dès l'année suivante. L'armée allemande redessine la machine et c'est en juin 1930 que la version standard finale, nommée ENIGMA I commence à être utilisée par l'armée. C'est de ce modèle que seront dérivées diverses variations d'ENIGMA utilisées par la marine allemande à partir d'octobre 1934 et par l'aviation à partir d'août 1935. Les changements qui seront apportés à ENIGMA se poursuivront pendant toute la durée de la guerre. Les allemands misent énormément sur l'efficacité d'ENIGMA pour vaincre. Tous les niveaux du gouvernement et de la défense utilise ENIGMA pour communiquer. Ils sont tellement convaincus que leur codes ne peuvent être brisés, qu'ils transmettront au vu et su de tous.

Malgré le haut niveau de cryptage, les secrets transmis via ENIGMA furent régulièrement et dans le détail, déchiffrés par les cryptanalystes alliés. Notons le rôle important que Alan Turing a joué dans l'accomplissement de cette tâche. La résolution de ces secrets militaires qui contenaient des informations stratégiques capitales a permis de sauver la vie de centaines de personnes mais par le fait même a mis fin prématurément à la vie de bien d'autres. Durant la Seconde Guerre Mondiale, Alan Turing, un anglais, a fortement contribué au décryptement des messages allemands. Il travaillait pour le Government Code Cypher School à Bletchley (Buckinghamshire) dans un bâtiment secret. En matière de cryptologie la France était un peu en dehors du mouvement. C'est surtout la Grande Bretagne qui était le principal moteur du décryptement durant la guerre. La cryptologie aux Etats-Unis connût un développement considérable notamment grâce à leurs relations avec des cryptologues et cryptanalystes britanniques.

L'équipe de décryptement d'Alan Turing a eu quelques difficultés à casser les codes allemands d'Enigma car les allemands effectuaient régulièrement des mises au point technologiques sur cette machine. Mais Alan Turing et ses collègues ont réussi à rattraper les allemands et finalement devancer presque chaque attaque allemande et par conséquent sauver des vies humaines. Il apparaît ainsi que la cryptographie a détenu un rôle primordial lors des ces conflits mondiaux, notamment concernant les communications des alliés

Fanny GENETÉY

[\(partie suivante ...\)](#)

## La Cryptologie actuelle

### 1 Les besoins actuels en cryptographie

De tous temps, les services secrets ont utilisé toutes sortes de codages et de moyens cryptographiques pour communiquer entre agents et gouvernements, de telle sorte que les "ennemis" ne puissent pas comprendre les informations échangées. La cryptologie a alors évolué dans ces milieux fermés qu'étaient les gouvernements, les services secrets et les armées. Ainsi, très peu de gens, voire personne n'utilisait la cryptographie à des fins personnelles. C'est pourquoi, pendant tant d'années, la cryptologie est restée une science discrète.

De nos jours en revanche, il y a de plus en plus d'informations qui doivent rester secrètes ou confidentielles. En effet, les informations échangées par les banques ou un mot de passe ne doivent pas être divulgués et personne ne doit pouvoir les déduire. C'est pourquoi ce genre d'informations est crypté. L'algorithme de cryptographie DES par exemple, est utilisé massivement par les banques pour garantir la sécurité et la confidentialité des données circulant sur les réseaux bancaires. Le système d'exploitation Unix, lui aussi, utilise ce procédé pour crypter ses mots de passe.

Finalement, la cryptologie est de plus en plus utilisée sur le réseau mondial Internet. Avec l'apparition du commerce en ligne, c'est-à-dire la possibilité de commander des produits directement sur Internet, la cryptographie est devenue nécessaire. En effet, si les différents ordinateurs branchés sur Internet sont sécurisés par des mots de passe, c'est-à-dire à priori inaccessibles par un ennemi, les transactions de données entre deux ordinateurs distants via Internet sont, quant à elles, facilement interceptibles. C'est pourquoi lorsque l'on commande un produit sur Internet en payant avec notre carte bancaire, il est beaucoup plus sûr d'envoyer notre numéro de carte bancaire une fois crypté, celui-ci ne pourra à priori, être décrypté que par la société à laquelle on a commandé ce produit.

C'est pour ces mêmes raisons d'insécurité sur Internet, et par un besoin humain d'intimité que la cryptographie à des fins purement personnelles s'est développée sur le réseau : pour la messagerie électronique. En effet lorsque l'on envoie un message électronique par Internet, on peut préférer qu'il reste discret vis à vis de la communauté Internet, voire qu'il ne soit compréhensible que par le destinataire du message. En d'autres termes, la cryptographie peut servir si l'on veut envoyer un message confidentiel, ou un message intime à quelqu'un. Cela est aujourd'hui possible grâce à la formidable distribution de logiciels gratuits permettant d'utiliser de la cryptographie "forte" très facilement. C'est le cas du logiciel PGP (Pretty Good Privacy = "assez bonne confidentialité") qui est distribué gratuitement sur Internet, développé par Philip R. Zimmerman seul, en 1991. Ce sont pour toutes ces raisons que tout d'abord la cryptologie s'est énormément renforcée, et que finalement elle est passé d'un monde fermé comme les armées ou les services secrets à un monde ouvert à tout utilisateur.

### 2 Les méthodes de cryptographie actuelle

#### 2.1 Le chiffrement actuel

Le chiffrement est l'action de transformer une information claire, compréhensible de tout le monde, en une information chiffrée, incompréhensible. Le chiffrement est toujours associé au déchiffrement, l'action inverse. Pour ce faire, le chiffrement est opéré avec un algorithme à clé publique ou avec un algorithme à clé privée.

#### 2.2 Les algorithmes à clé privé ou à clé secrète

Les algorithmes à clé privée sont aussi appelés algorithmes symétriques. En effet, lorsque l'on crypte une information à l'aide d'un algorithme symétrique avec une clé secrète, le destinataire utilisera la même clé secrète pour décrypter. Il est donc nécessaire que les deux interlocuteurs se soient mis d'accord sur une clé privée auparavant, par courrier, par téléphone ou lors d'un entretien privé. La cryptographie à clé publique, quant à elle, a été inventée par Whitfield Diffie et Martin Hellman en 1976 pour éviter ce problème d'échange de clé secrète préalable.

#### 2.3 Les algorithmes à clé publique

En effet, les algorithmes à clé publique sont aussi appelés algorithmes asymétriques. C'est à dire que pour crypter un message, on utilise la clé publique (connue de tous) du destinataire, qui sera à priori le seul à pouvoir le décrypter à l'aide de sa clé privée (connue

de lui seul).

## 2.4 La préparation au cryptage

Une information de type texte, ou n'importe quel autre type d'information a besoin d'être codée avant d'être cryptée à l'aide d'un algorithme à clé publique ou privée. En d'autres termes, il faut fixer une correspondance entre une information et un nombre, puisque les algorithmes à clé (publique ou privée) ne peuvent crypter que des nombres. Le problème se résout facilement, puisque la plupart du temps, ce type de cryptographie est essentiellement utilisé sur des machines. Et comme de toute façon les informations sur une machine sont une suite de nombres, le problème est déjà très simplifié.

### 2.4.1 La préparation au cryptage avec DES

L'algorithme DES ne crypte que des blocs de 64 bits. Il nous suffira donc de diviser nos informations à crypter en blocs de 8 octets.

### 2.4.2 La préparation au cryptage avec RSA

L'algorithme RSA, lui, ne crypte que des nombres inférieurs au nombre  $n$  qui est un élément de sa clé publique. On pourra utiliser le standard ASCII, plus communément appelé "table ASCII" qui code chaque octet (ou chaque caractère) de 000 à 255, pour transformer partie par partie l'information à crypter en nombres (tous inférieurs à  $n$ ).

## 3 L'algorithme DES

### 3.1 Histoire de DES

D.E.S., pour Data Encryption Standard ("standard de cryptage de données"), est un algorithme très répandu à clé privée créée à l'origine par IBM en 1977. Il sert à la cryptographie et l'authentification de données. Il a été jugé si difficile à percer par le gouvernement des Etats-Unis qu'il a été adopté par le ministère de la défense des Etats-Unis qui a contrôlé depuis lors son exportation. DES a été pensé par les chercheurs d'IBM pour satisfaire la demande des banques. Il a été conçu pour être implémenté directement en machine. En effet puisque les étapes de l'algorithme étaient simples, mais nombreuses, il était possible à IBM de créer des processeurs dédiés, capables de crypter et de décrypter rapidement des données avec l'algorithme DES. Cet algorithme a donc été étudié intensivement depuis les 15 dernières années et est devenu l'algorithme le mieux connu et le plus utilisé dans le monde à ce jour.

Bien que DES soit très sûr, certaines entreprises préfèrent utiliser le "triple-DES". Le triple-DES n'est rien d'autre que l'algorithme DES appliqué trois fois, avec trois clés privées différentes.

### 3.2 Description de l'algorithme DES

L'algorithme DES est un algorithme de cryptographie en bloc. En pratique, il sert à crypter une série de blocs de 64 bits (8 octets).

#### 3.2.1 Le cryptage avec l'algorithme DES

DES utilise une clé secrète de 56 bits, qu'il transforme en 16 "sous-clés" de 48 bits chacune. Le cryptage se déroule sur 19 étapes.

##### 1ère étape

La première étape est une transposition fixe (standard) des 64 bits à crypter.

##### 16 étapes suivantes

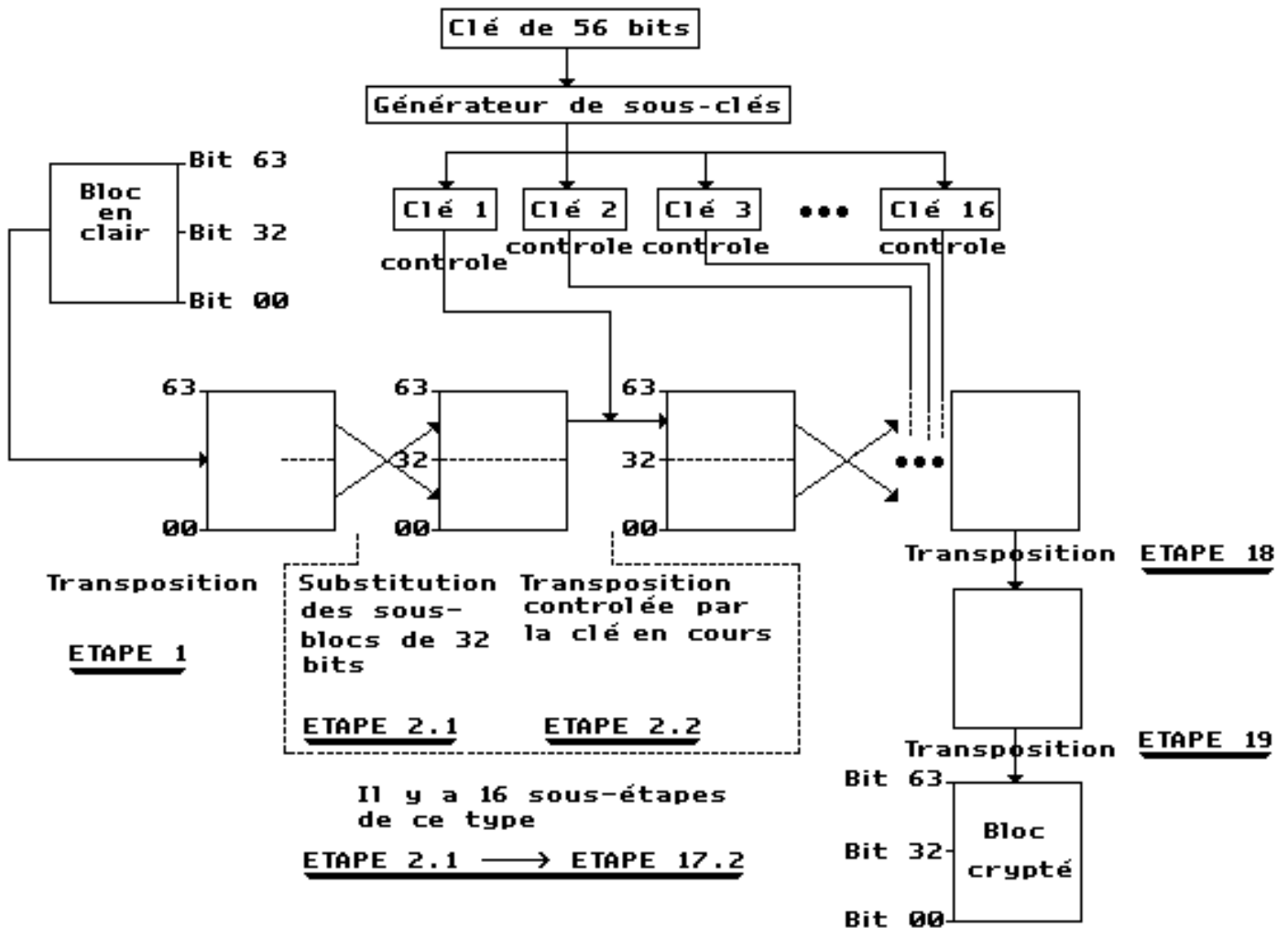
Les 16 étapes suivantes peuvent être divisées en 2 "sous-étapes" chacune. Dans un premier temps, Le bloc de 64 bits est découpé en 2x32 bits, et une substitution est effectuée entre ces deux blocs, en fait, ces deux blocs seront tout simplement échangés l'un avec

l'autre. Dans un second temps, le bloc de 32 bits ayant le poids le plus fort (le bloc qui va du bit n°32 au bit n°63) subira une transposition contrôlée par la sous-clé correspondant à l'étape en cours.

Etape 18 et 19

Les deux dernières étapes sont deux transpositions.

**SCHEMA REPRESENTANT L'ALGORITHME DES**



**3.2.2 Le décryptage avec l'algorithme DES**

Pour décrypter un document auparavant crypté avec DES, il suffit d'effectuer l'algorithme à l'envers avec la bonne clé. En effet, il n'est pas nécessaire d'utiliser un algorithme différent ou une clé différente puisque DES est comme nous l'avons vu un algorithme symétrique. Il est donc totalement et facilement réversible, si l'on possède la clé secrète.

**3.2.3 Les modes opérationnels utilisés avec DES**

Comme nous l'avons vu, l'algorithme DES ne permet que de crypter des blocs de 64 bits. Pour crypter ou décrypter un document complet, il faut donc utiliser DES en série dans un "mode opérationnel". Il existe beaucoup de modes opérationnels, nous n'allons voir que le mode ECB et le mode CBC.

### 3.2.3.1 Le mode opérationnel ECB

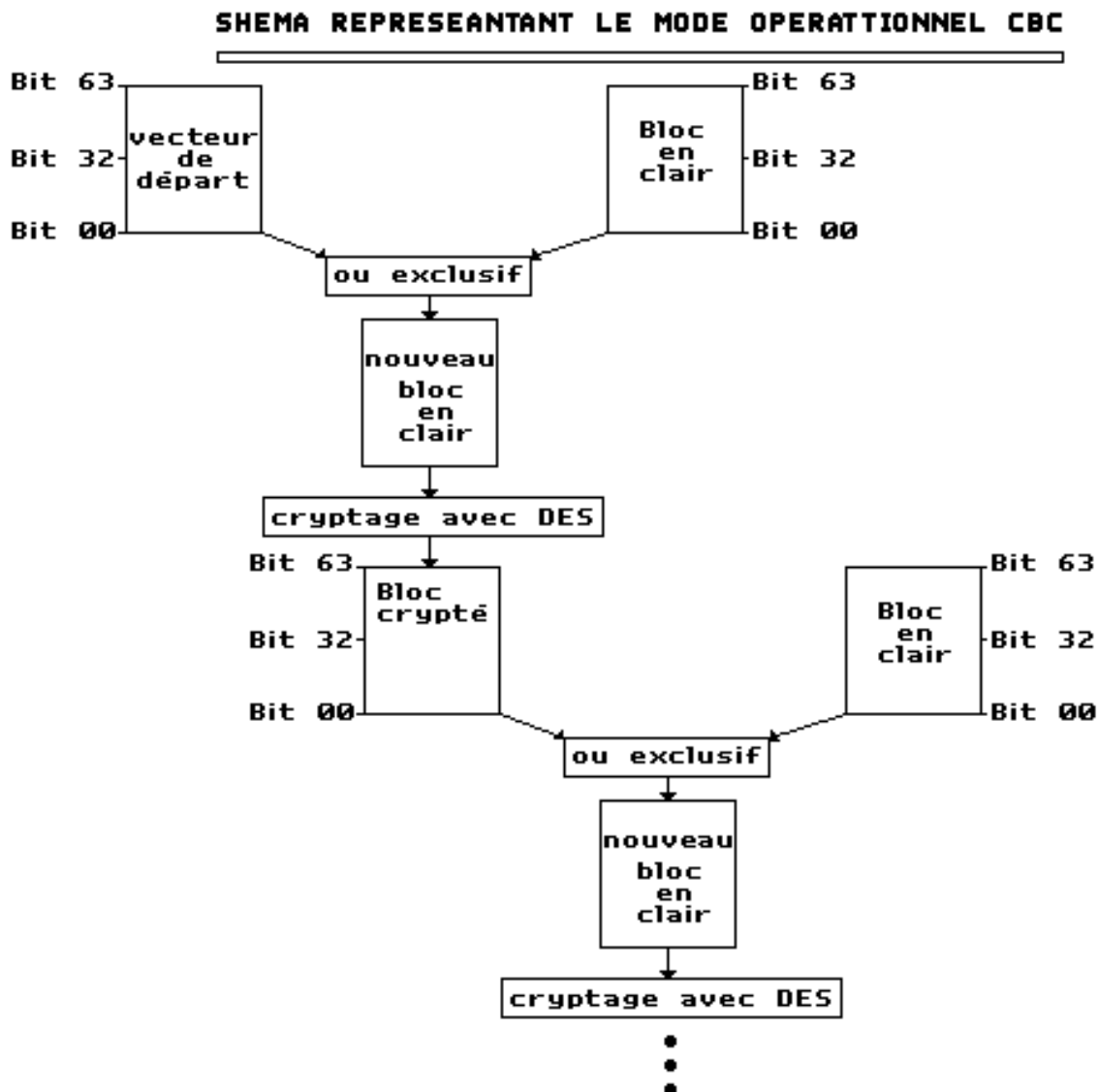
ECB signifie Electronic Code Book ("catalogue électronique de codes"). Dans ce mode, on découpe le document à crypter ou à décrypter en blocs de 64 bits qu'on crypte les uns indépendamment des autres. Puisque, à chaque bloc en clair correspond un bloc crypté, pour une clé donnée, cela peut faire penser à un "catalogue de codes".

### 3.2.3.2 Le mode opérationnel CBC

CBC signifie Chain Block Cipher ("Cryptogramme à blocs chaînés"). Comme nous l'avons vu précédemment, le mode opérationnel ECB ne protège pas contre la présence de blocs redondants, puisqu'ils sont cryptés indépendamment les uns des autres. La seconde faiblesse est qu'un bloc en clair, hors contexte, et codé toujours avec la même clé, produira toujours le même bloc crypté.

Le CBC lui, répond à ces deux problèmes. Pour ce faire, avant de crypter un bloc en clair, on va effectuer un "ou-exclusif" entre ce bloc en clair et le bloc précédemment crypté. Cela nous donnera un nouveau bloc en clair que l'on cryptera.

En plus de posséder une clé secrète en commun, les deux interlocuteurs doivent dorénavant se mettre d'accord sur un bloc de 64 bits de départ qu'on appellera "vecteur de départ", ou "vecteur initial".



## 4 L'algorithme RSA

## 4.1 Histoire de RSA

R.S.A. signifie Rivest-Shamir-Adleman, en l'honneur de ses inventeurs : Ron Rivest, Adi Shamir et Leonard Adleman qui l'ont inventé en 1977. Le brevet de cet algorithme appartient à la société américaine RSA Data Security, qui fait maintenant partie de Security Dynamics et aux Public Key Partners, (PKP à Sunnyvale, Californie, Etats-Unis) qui possèdent les droits en général sur les algorithmes à clé publique. RSA est un algorithme à clé publique qui sert aussi bien à la cryptographie de documents, qu'à l'authentification. Grâce au fait qu'il était à clé publique, et au fait qu'il était très sûr, l'algorithme RSA est devenu un standard de facto dans le monde.

## 4.2 Description de l'algorithme RSA

Tout le principe de RSA repose sur le fait (qui n'a toujours pas été prouvé !) qu'il est très difficile et très long de factoriser un très grand nombre en deux facteurs premiers.

### 4.2.1 La génération des clés publiques et privées

Pour commencer, il nous faut choisir deux nombres premiers  $p$  et  $q$  très grands (de l'ordre de 100 chiffres). Il y a des algorithmes de génération aléatoire de nombres premiers qui existent. Ensuite on trouve le nombre  $n$  facilement :  $n=p.q$ . Ensuite il nous faut trouver un entier  $e$  compris entre 2 et  $\varphi(n)$ .  $\varphi(n)$  est la fonction indicatrice d'Euler, c'est en fait le nombre d'entiers inférieurs à  $n$  qui sont premiers avec lui, on a  $\varphi(n)=(p-1)(q-1)$ .  $\varphi(n)$  se calcule très facilement ici, puisque l'on a  $p$  et  $q$ . Maintenant que l'on a  $n$  et  $e$ , nous sommes prêts à crypter. Les nombres  $n$  et  $e$  forment ici notre clé publique que l'on notera  $[n,e]$ . Il nous faut calculer le nombre  $d$  qui sera nécessaire au décryptage. Selon la théorie de RSA, nous devons avoir  $d$  tel que  $(e.d-1)$  soit divisible par  $\varphi(n)$ . Pour trouver  $d$  nous devons alors résoudre l'équation diophantienne  $d+k.\varphi(n)=1$  à l'aide de l'arithmétique. Comme  $e$  et  $\varphi(n)$  sont premiers entre eux, le théorème de Bezout prouve qu'il existe  $d$  et  $k$  dans  $\mathbf{Z}$  tel que  $e.d+k.\varphi(n)=1$

On pourra résoudre l'équation grâce à l'algorithme d'Euclide. Après résolution, on arrivera à une classe de solution de la forme  $d=r.\varphi(n)+d_0$  (où  $r$  appartient à  $\mathbf{Z}$ ) puisque  $e$  a été choisi premier avec  $\varphi(n)$ . L'ensemble des solutions  $d$  à l'équation diophantienne  $e.d+k.\varphi(n)=1$  est une classe de congruence modulo  $\varphi(n)$ , il y a donc une unique solution  $d$  comprise entre 2 et  $\varphi(n)$ , donc  $d=d_0$ . Nous voilà prêts à décrypter. Le nombre  $d$  est notre clé privée.

Nous pouvons à présent rendre publique notre clé publique  $[n,e]$  et garder secrète notre clé privée. Quant aux nombres  $p$ ,  $q$ , et  $\varphi(n)$ , on doit, soit les conserver secrets, soit les détruire car ils ne serviront plus.

### 4.2.2 Le cryptage avec l'algorithme RSA

Pour crypter un document que l'on aura auparavant transformé en un nombre  $m$  inférieur à  $n$  il nous faut effectuer l'opération  $c=m^e \bmod n$ .  $c$  est ici notre nombre  $n$  une fois crypté. La première opération peut être très longue à effectuer à la main, l'utilisation d'un ordinateur et d'un programme spécial est fortement conseillée.

### 4.2.3 Le décryptage avec l'algorithme RSA

Pour décrypter un document  $c$ , il nous faut effectuer l'opération  $m=c^d \bmod n$ .  $m$  sera bel et bien notre nombre décrypté, qu'il ne restera plus qu'à retransformer en texte ou en autre chose. La preuve de cette algorithme de chiffrement est faite avec le théorème de Fermat et le théorème chinois des restes connus depuis quelques siècles !

## 5 L'authentification de documents

L'authentification d'un document, c'est le fait d'être sûr de l'identité de l'auteur d'un document. Cette authentification peut s'avérer indispensable pour la justice lors d'un litige sur un contrat par exemple. L'authentification se fait toujours sur un contrat papier par une signature manuscrite, à priori infalsifiable. Le problème de l'authentification d'un document "informatique", est l'impossibilité physique d'y apposer une signature manuscrite à sa fin. On va donc y apposer une signature "digitale". Pour ne pas être falsifiable, on



va crypter cette signature par exemple avec l'algorithme RSA.

## 5.1 Les signatures digitales avec RSA

Pour bien prouver qu'un document a été composé par nous, il nous suffira de crypter par exemple notre Nom, Prénom et fonction ou n'importe quoi d'autre, avec notre clé privée (en théorie connue de nous seul). Ainsi, quiconque qui voudra vérifier l'auteur de ce document, n'aura qu'à utiliser notre clé publique pour le décryptage. Et si le décryptage fonctionne, cela veut bien dire que la signature a été "forgée" avec notre clé privée.

## 5.2 Tableau récapitulatif de la gestion des clés avec RSA

Pour ...	on utilise ...	de qui ?
Envoyer un document crypté à quelqu'un	la clé publique	du destinataire
Envoyer une signature cryptée à quelqu'un	la clé privée	de l'expéditeur
Décrypter un document	la clé privée	du destinataire
Décrypter une signature	la clé publique	de l'expéditeur

## 6 La cryptanalyse actuelle

La cryptanalyse est l'étude des procédés de décryptage. Ou, plus généralement la science qui étudie la sécurité des procédés cryptographiques. Le cryptographe est toujours cryptanalyste puisque qu'il doit en créant un algorithme de cryptographie s'assurer de sa sécurité, et pour ce faire, il a besoin de la cryptanalyse. La cryptanalyse tente de tester la résistance d'un algorithme de cryptographie en simulant différents type "d'attaques", qu'un ennemi pourrait effectuer si il interceptait le document crypté. Un ennemi, en cryptologie, est une personne qui tentera, une fois le document crypté intercepté d'opérer une attaque passive, ou une attaque active.

### 6.1 Les attaques passives

Faire une attaque passive est le fait de tenter de décrypter un document dans le but d'en prendre connaissance uniquement, sans l'altérer.

### 6.2 Les attaques actives

Faire une attaque active est le fait de tenter de décrypter un document dans le but de pouvoir en prendre connaissance d'une part, et d'autre part dans le but de le modifier, ou d'en modifier la signature pour le falsifier, en général dans son intérêt.

### 6.3 L'attaque d'un document crypté avec DES

La seule méthode connue à ce jour pour décrypter un message crypté avec DES, est la méthode dite "brute" qui consiste à tester la totalité des différentes clés de 56 bits possibles. Le problème majeur est qu'il y en a  $2^{56}$ , soit exactement 72 057 595 037 927 936 différentes ! Cela peut prendre un temps considérable. Cependant, les services secrets peuvent avoir les moyens matériels de briser de tels codes, il leur suffit d'avoir une ou des machines extrêmement puissantes, ce qui pourrait tout à fait être possible pour des nations importantes...

### 6.4 L'attaque d'un document crypté avec RSA

Comme on l'a vu précédemment, la résistance d'un document crypté avec l'algorithme RSA s'appuie sur le fait qu'il est extrêmement difficile de factoriser en deux facteurs premiers un très grand nombre. L'attaque va donc consister à utiliser des algorithmes de factorisation les plus rapides, et les plus puissants possibles, pour factoriser le nombre  $n$  extrêmement grand de la clé publique visée. L'attaque d'un tel document est encore beaucoup plus long (pour une taille du nombre  $n$  raisonnable) que l'attaque d'un document crypté avec DES. C'est pourquoi, de grandes recherches en mathématiques sur des algorithmes de factorisation de plus en plus

rapides sont effectuées partout dans le monde. La méthode RSA, réputée pour sa quasi-invulnérabilité (quand elle est utilisée avec une très grande clé) pourrait s'écrouler si quelqu'un parvenait un jour à écrire un tel algorithme. Car RSA repose sur un principe qui a l'air évident mais qui n'a jamais été prouvé ! Actuellement, il n'y a aucun algorithme/méthode connu, capable de factoriser dans un temps convenable une très grande clé. Avec les algorithmes de factorisation actuels, il faudrait au briseur de code une puissance beaucoup plus importante pour arriver à ses fins. Mais avec une puissance de calcul plus importante, l'utilisateur peut aussi agrandir la taille de la clé de un bit ou deux, par exemple. Or l'augmentation de la taille de la clé de un/deux bits signifie une multiplication par deux/quatre le nombre maximum que peut être la clé ! Par exemple *RSA Labs* a mis sur le marché il y a quelques mois un processeur dédié à la méthode RSA comportant des instructions dites "*de haut niveau*" directement implémentées sur le processeur, comme une instruction permettant de calculer le modulo d'un grand nombre avec un autre grand nombre rapidement, et une instruction permettant de factoriser un grand nombre. Ce processeur factorise en effet beaucoup plus vite qu'un ordinateur normal, puisque sur l'un, l'algorithme de factorisation est implémenté en *hardware* alors que sur l'autre, il est implémenté en *software*. On peut remarquer que ce processeur avantage plus ou moins également le crypteur que le briseur de code.

[F. MARIE](#)

[\(partie suivante ...\)](#)

## Le principe de PGP

PGP est de loin le logiciel de cryptographie le plus utilisé dans la communauté Internet par les particuliers. Et ce, parce qu'il est à la fois rapide, très sûr, pratique et gratuit. Philip R. Zimmerman a même eu des problèmes avec le gouvernement des Etats Unis qui a voulu interdire l'exportation de ce produit.

Ce logiciel utilise le principe de cryptographie à clé publique. Alors, avant d'utiliser ce logiciel, vous devrez créer vos clés privé et publique. Une fois ces deux choses (parfois délicates ...) faites, tout est prêt pour crypter et décrypter.

Pour crypter et décrypter, PGP utilise deux algorithmes distincts : IDEA (algorithme à clé privé) et RSA. L'opération de cryptage se fait donc en deux étapes principales :

- PGP crée une clé secrète IDEA de manière aléatoire, et crypte les données avec cette clé.
- PGP crypte la clé secrète IDEA précédemment créée au moyen de la clé RSA publique du destinataire.

De même, l'opération de décryptage se fait elle aussi en deux étapes :

- PGP décrypte la clé secrète IDEA au moyen de la clé RSA privée.
- PGP décrypte les données avec la clé secrète IDEA précédemment obtenue.

C'est la combinaison *algorithme symétrique (IDEA pour crypter les données) / algorithme asymétrique (RSA pour crypter la clé IDEA)* qui confère à PGP sa vitesse et sa grande sécurité.

[F. MARIE](#)

[\(conclusion ...\)](#)

## Conclusion

En matière de réglementation, la France a pendant longtemps fait preuve de sévérité, avec un régime strict de déclarations et d'autorisations préalables imposés par le Service central pour la sécurité des systèmes d'informations, qui dépend du premier ministre.

Mais aujourd'hui, l'usage de la cryptologie est libre en ce qui concerne les fonctions de signature et d'intégrité des messages. Pour la confidentialité, en revanche, elle ne peut être assurée que par des logiciels employant des clés de petite taille (comme 40 bits) que les services gouvernementaux peuvent "craquer" sans difficulté. Le passage aux 56 bits promis récemment par Lionel JOSPIN et par le secrétaire d'état à l'industrie, reste en suspens, pour des raisons techniques de décryptage. Pour crypter au delà de 40 bits, il faudra donc déposer ses clés secrètes chez un *tiers de confiance*. L'utilisateur bénéficiera d'une paire de clés. L'une, que l'on nomme publique, permettra à ses interlocuteurs de chiffrer les messages qu'ils souhaitent lui faire parvenir ; l'autre, que l'on appelle secrète, permettra de les déchiffrer. Un exemplaire de la clé secrète sera donc remise au *tiers de confiance* qui la conservera ou la remettra entre les mains de la justice, le cas échéant.

Mais ce nouveau système pose certaines polémiques. Par exemple, dans un contexte de guerre économique et de renseignement industriel, il est difficile d'imaginer comment des interlocuteurs étrangers accepteront de confier leurs clés secrètes à un *tiers de confiance* français. Ce système de *tiers de confiance* risque, finalement, et s'il parvient à se mettre en place, de rester strictement français .

[\(voir annexe pour l'illustration de ce nouveau système français\)](#)

La cryptologie a donc connu une rapide évolution à notre époque et c'est en partie dû à deux facteurs essentiels : l'irruption des mathématiques et de l'informatique et le développement des moyens de télécommunication, qui a eu pour effet de multiplier les activités où intervient la cryptologie.

Le rôle de la cryptologie a évolué au fil des siècles. Avant elle n'avait pour rôle que de protéger un texte écrit ; maintenant, la cryptologie s'étend dans différents domaines tels que la téléphonie, le télétraitement, le stockage des données, communication avec les satellites...

Depuis une vingtaine d'années, la cryptologie s'est enrichie de nouvelles techniques de cryptage électronique. Il est vraisemblable que la cryptologie ne disparaîtra pas du fait des nouvelles techniques. Si elle devait disparaître, ce ne pourrait être que par suite d'une nouvelle conception des rapports humains. Le chiffre, lui non plus, n'est pas prêt de disparaître puisqu'il a été et reste encore le moyen le plus sérieux d'assurer la sécurité des correspondances. Il tend de plus en plus vers une structure mathématique.

Il y a aujourd'hui une perpétuelle remise en cause de la cryptologie par la cryptanalyse. C'est une sorte de véritable combat. Les progrès de la cryptanalyse entraînent nécessairement des progrès en cryptologie et vice-versa. C'est une évolution sans fin. On peut se demander si la confidentialité des messages ne se

trouve pas alternée dans ces progressions. On peut citer, comme exemple, la nouvelle réglementation française qui illustre bien que le secret n'est plus préservé comme il l'était il y a quelques années. Les nouvelles techniques sont si puissantes à l'heure actuelle que les gouvernements imposent des lois qui réglementent peut-être trop sévèrement l'utilisation de la cryptologie.

Mickaëlle LEBEL  
Fanny GENETÉY  
[Grégory PAIRE](#)  
[Fabrice MARIE](#)

[Remerciements](#)

# REMERCIEMENTS

Nous tenons vivement à remercier M Didier TROTOUX pour son aide et les divers documents qu'il a pu nous fournir. Nous remercions aussi Mme Christelle POIRIER, et M Nicolas MALANDAIN ainsi que leurs collègues de la M.R.S.H. pour leur soutien ou leur aide.

# Glossaire

**stéganographie** : procédé visant à dissimuler l'existence même du texte.

**substitution mono-alphabétique** : procédé de remplacement d'une lettre en clair en une seule cryptée.

**substitution polyalphabétique** : procédé de remplacement d'une lettre en clair en plusieurs cryptées.

**transposition** : les lettres sont mélangées, leur ordre normal est bouleversé.

**cryptogramme** : texte chiffré

**cryptologie** : science pure énonçant les principes et les idées de la cryptographie.

**cryptographie** : science appliquée englobant à la fois les techniques du chiffre et de la cryptanalyse.

**cryptanalyse** : technique étudiant les moyens de chiffrement et recherchant les méthodes permettant de décrypter.