Cryptographie et sécurité cryptographique

1. Génèse de la cryptographie

La cryptographie est l'art d'écrire les messages. La manipulation et le contrôle des nombres appellent la numérologie et d'autres disciplines ésotériques. A défaut de savoir déchiffrer les mystères de la nature, l'Homme trouve sa joie à concevoir des systèmes de cryptage et met quiconque en défi de décrypter des informations codées émises par un autre.

Malheureusement beaucoup de systèmes cryptographiques se sont révélés vulnérables ou peu pratiques, et ont dû être abandonnés.

Si les messagers des rois et des princes ou des agents secrets ont pu les utiliser à une époque, parce qu'il leur était plus facile de communiquer par ce biais vu le nombre insignifiant de cryptanalistes, il n'en est plus de même aujourd'hui. La cryptographie s'est enrichie de méthodes très sures, s'est entourée d'experts, et a quitté le monde occulte de l'**espionnage** pour franchir les remparts de l'industrie, du commerce et autres.

La cryptographie informatique professionnelle, non ludique, est un phénomène récent, rendu indispensable du fait que les informations sont accessibles pratiquement à tous par des réseaux publics. La cryptographie moderne est orientée vers la manipulation de chiffres, et utilise avec abondance des résultats de l'arithmétique, établis souvent il y a longtemps, et dont l'utilité pratique n'avait pas été prouvée.

2. Description d'un système moderne

Pour envoyer une information secrète à un destinataire, on choisit un algorithme, une ou plusieurs clés de sécurité de son choix et un média de transmission. On peut créer des myriades d´algorithme de cryptage sans clé, d´une complexité inouïe, et d´une sûreté quasi-totale, tant que l´algorithme demeure inconnu.

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 rédigèrent délibérément leurs écritures de façon obscure sur les pierres funéraires pour soit disant attirer l'attention des lecteurs.

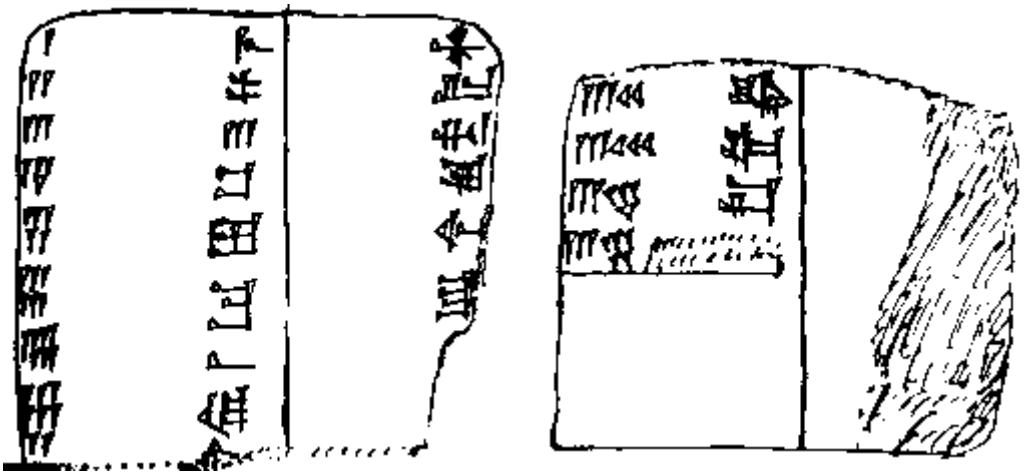
Cela ne fut pas le cas, car aucun dictionnaire n'était disponible. Ces inscriptions possédaient le deuxième élément essentiel de la cryptologie : le secret. Cependant cette méthode échoua complètement car au lieu de raviver les intérêts, elle éteignit jusqu'au moindre désir de lire l'introduction d'une 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 Ciceron en remplaçant chaque lettre claire par celle située 3 rangs plus loin dans l'alphabet.

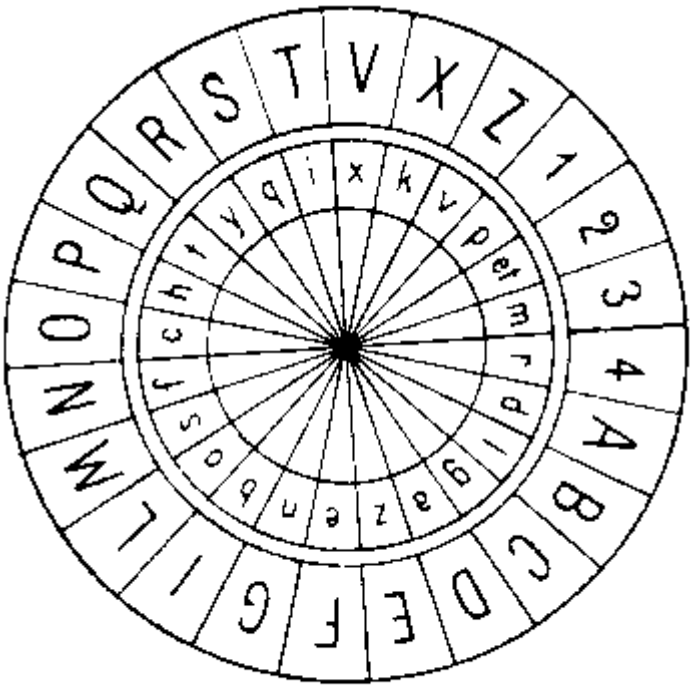
Durant le moyen-âge la cryptologie évolue faiblement car peu la pratique. Seul les moines en Europe utilisent cette science plus par jeu que par nécessité. Ils ont été probablement influencés par les Saintes écritures de "l'ancien testament" chapitre 25 verset 36 où la ville de Babylone (Babel) apparaît 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 naquît 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 débuter 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.

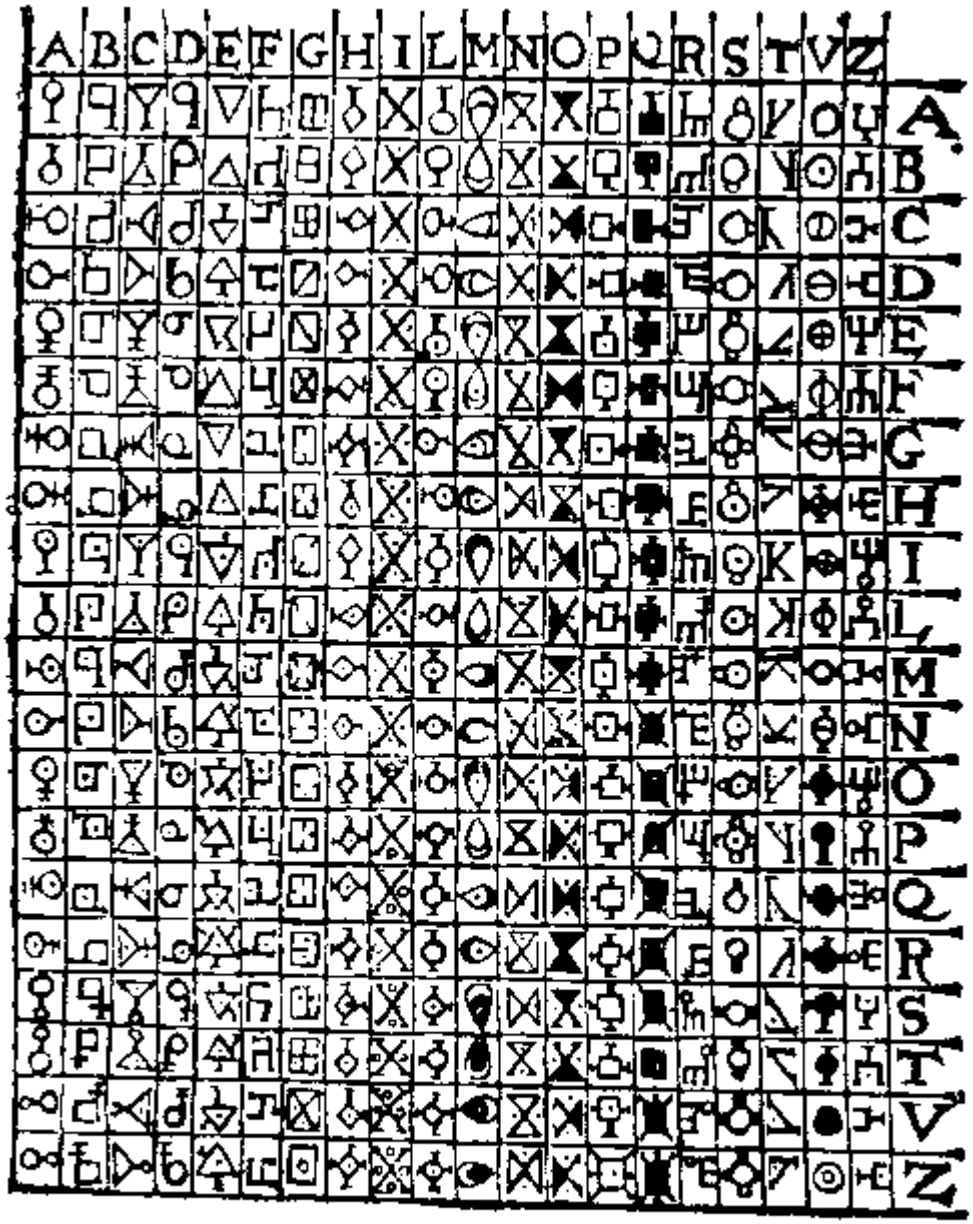
Un moine bénédictin en 1518 conçut aussi un système de substitution polyalphabétique, Jean Trithème. Il utilisait un tableau qu'il appela *"tabula recta"*.

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 crée 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 bigammatique de l'histoire de la cryptologie.



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

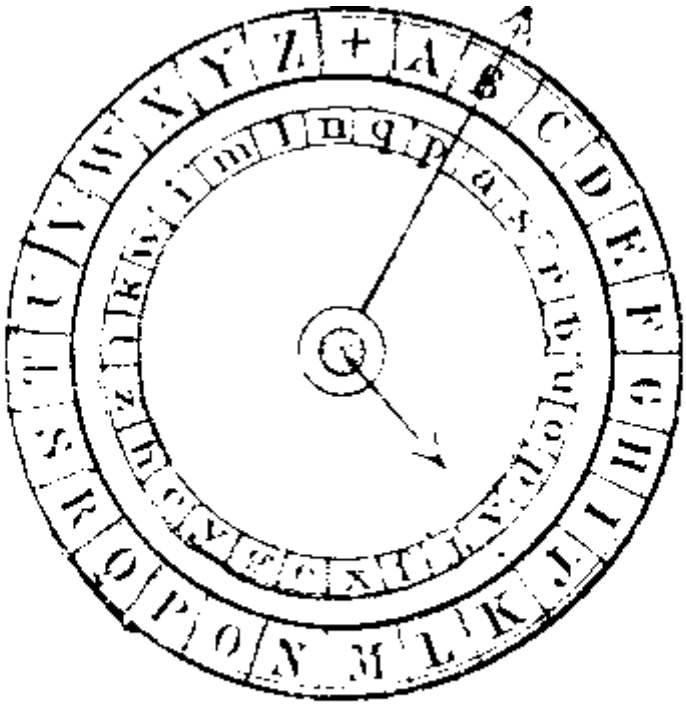
l'évolution de la bataille, mieux qu'il n'aurait pu le faire sur le terrain. Le temps des généraux à cheval, surveillant la bataille du sommet d'une colline comme Napoléon, était révolu.

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 naquît 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 dégageait, avec une extraordinaire lucidité, les principes fondamentaux qui, encore de nos jours, guident les travaux des cryptologues, un illustre savant anglais, Wheastone, 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.

La première guerre mondiale

1. Bureau 40

Le bureau 40 a été crée 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 étaient 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.

2. 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 accélérait 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'ÜBCHI*, 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.

La seconde guerre mondiale

1. 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.

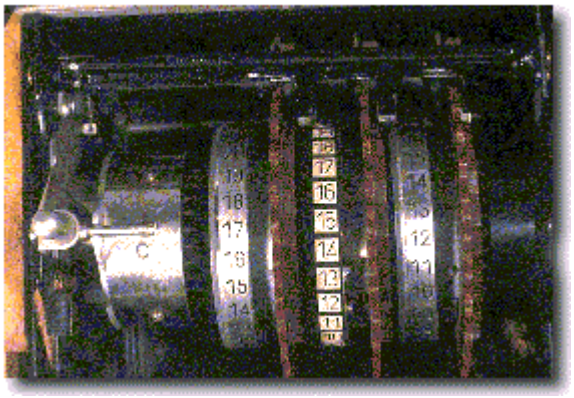
2. La cryptographie russe

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.

3. 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 Chieffrienmaschinen 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 connue 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 ENIGMASon 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

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 Hetlman 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 crée 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.

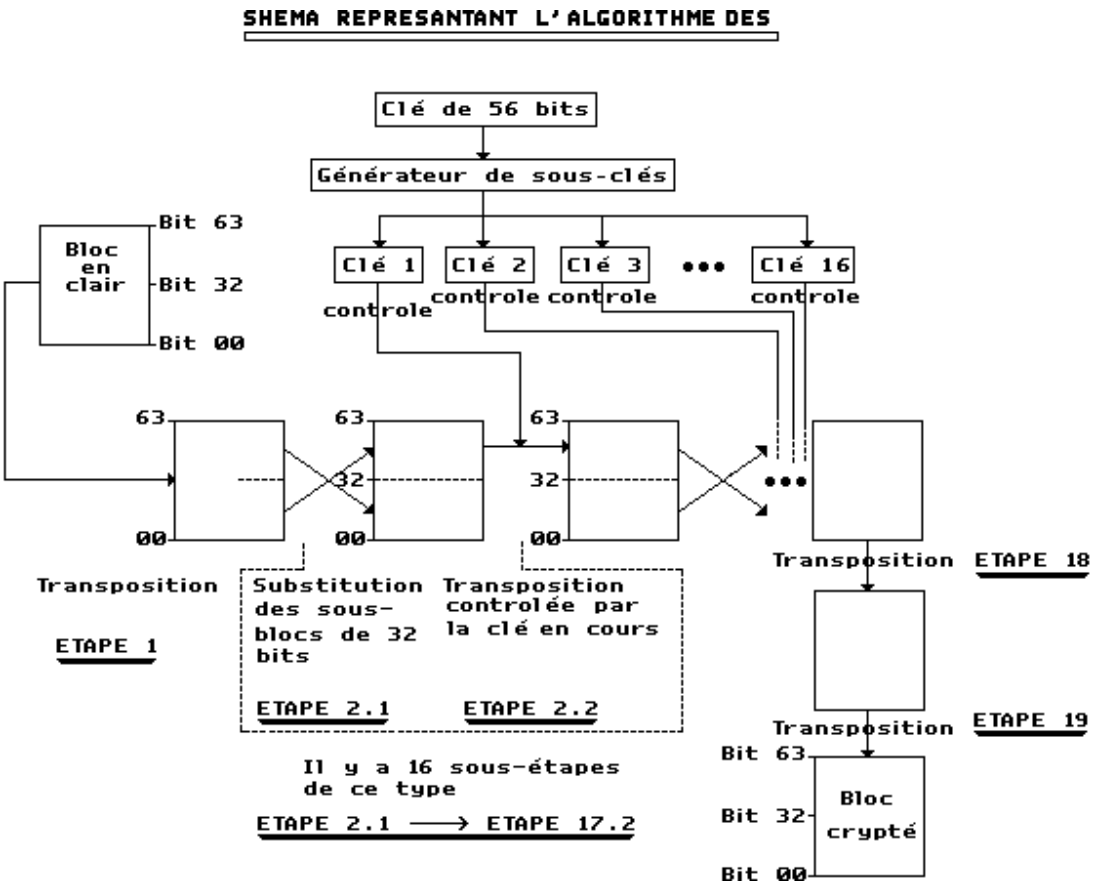
3.2 Description de l'algorithme DES

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.

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

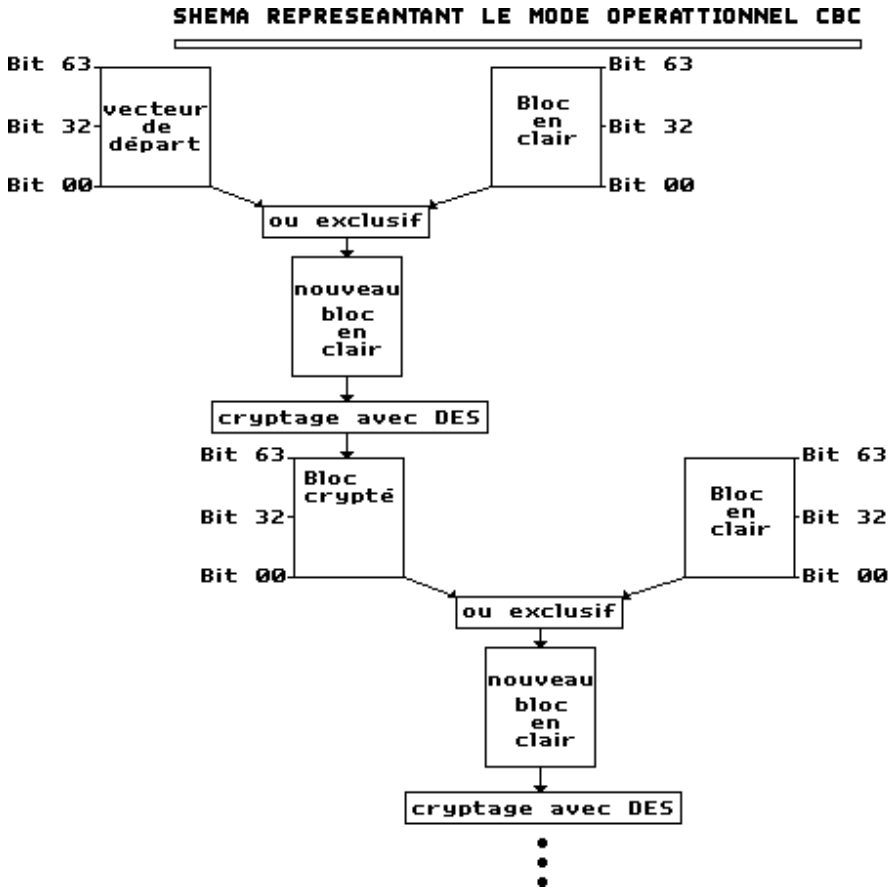
indépendamment des autres. Puisque, à chaque bloc en clair correspond un bloc crypté, pour une clé donnée, cela peut faire penser à un "catalogue de codes".

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 Parteners, (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 : $n=n.q$. 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 **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 **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 cryptologiste 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 et 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.

Les cryptosystèmes

1 Définition

Un cryptosystème a pour but de chiffrer un message clair en un message chiffré (Cryptogramme) suivant des techniques complexes , incompréhensible par toute personne curieuse (Cryptanaliste ou décrypteur) différente du destinataire légitime.

2 Cryptographie à clé symétrique ou secrète

Historiquement, les cryptosystèmes à clé secrète ont été les premiers à être mis au point pour assurer la protection des informations. Les algorithmes de codage (qui étaient **jadis** de longues suites d'opérations sur des caractères) étaient tenus secrets car on pensait que mettre la main dessus équivalait à ruiner la sécurité du système.

Ainsi a-t-on vu des générations d'esprits contribuer à la construction de systèmes de codage redoutables, lesquels bien que sécrètes, ne possédaient pas le label de robustesse cryptographique Aujourd´hui, la cryptographie à clés secrètes s'oriente vers les systèmes dont les algorithmes de codage et de décodage sont connus par tous comme le DES. Ce qui veut dire que seule une clé permet d'assurer la confidentialité.

2.1 Relation entre théorie de l'information et cryptographie

La théorie de l'information de Shanon vous permet de répondre à la question selon laquelle <Avec l'affluence de plusieurs échantillons de messages ou fichiers cryptés, à quel moment est-il théoriquement possible d´opérer une cryptanalyse sérieuse? >.

En fait la théorie introduit l'entropie E exprimée en bits de l'espace des clés utilisables et la redondance r (exprimées en bits) des textes clairs (Ex: En français la valeur de la redondance est approximativement de 3,6 bits par caractère).

Si L est la longueur du texte clair, le Cryptanaliste pourra opérer un déchiffrage qui lui semble correct avec un nombre de fausses clés égal à 2E-Lr. Ainsi donc la quantité minimale de texte crypté que doit posséder l'espion pour **croire** que c'est l'unique solution plausible s'obtient en écrivant que E-rL=0. On notera ceci d, distance d'unicité du système, égale au rapport de E par:

d = E/r=log2 (N)/r

Bien entendu cette distance ne donne en aucun cas de renseignements sur le temps nécessaire pour venir à bout du code.

Certains systèmes moins solides proposent le changement de clé dès que L dépasse d. Il faut donc en ce moment émettre une clé K tous les d caractères.

2.2 Les attaques

Selon le degré **de** sécurité requis, on utilise des algorithmes plus ou moins performants. Il existe quatre possibilités d'attaque d'un cryptosystème à clés secrètes:

- *L'attaque gloutonne*: consiste à tester toutes les clés, si l'algorithme est connu de l'espion.

- *L'attaque à textes chiffrés*: consistant à découvrir tout ou partie de la clé à partir de messages cryptés.

- *L'attaque à textes chiffrés et clairs*: par un moyen rusé, l'espion possède des textes chiffrés pour lesquels il connaît le texte clair correspondant.

- *L'attaque à texte clair choisi*: consiste à choisir les textes clairs pour obtenir en retour les textes cryptés correspondants. Souvent elle peut être camouflée afin de rendre le retournement difficile.

La sécurité vis-à-vis de la deuxième attaque repose sur la qualité de brouillage opéré par les algorithmes sur le temps de forçage pour tester toutes les solutions. Forcer un code consisterait à repérer des régularités au sein des données apparemment **obscures**. Il est donc évident que la complexité du brouillage va de pair avec la difficulté pour un cryptanaliste de forcer un code

Or les crytanalistes savent très bien que tout système de cryptage laisse en générale quelques traces de son utilisation dans un **fichier** crypté. Dés lors, tout l'art du cryptologue pour empêcher la deuxième attaque est de faire que ces traces soient le plus imperceptibles possibles. Le choix des clés aléatoires est en général vivement conseillé, car la redondance permet à un espion de prédire ou de deviner l'un des composants de la clé. Et dans ce cas, le nombre de clés à utiliser pour forcer un code est considérablement réduit. On parle alors de *fichiers cryptés par essaim de clés.*

Les procédés cryptographiques

1. Les substitutions

Une façon de forcer le code d'un message consiste à utiliser **une** substitution des caractères. Seulement ce type de codage n'est pas à conseiller en cryptanalyse car entre le message clair et le texte transformé par substitution, le contenu fréquentiel n'a pas changé. En effet il est souvent très facile de retrouver la substitution. En plus il suffit de très peu de texte pour y parvenir. En langue française par exemple, environ 28 caractères sont nécessaires pour y parvenir.

Ex: Soit P=ABCDEFGHIJKLMNOPQRSTUVWXYZ

C=VZXTRPNLJHBFDACEGIKMOUQSWY

Alors si le texte clair est M=VIVELUJF

le texte crypté sera M'=UJUROHP

2 Les codes poly-alphabétiques

Ce procédé a été très utilisé en cryptographie par le passé. Le principe est basé sur le codage d'un caractère de plusieurs façons différentes, selon les différentes positions dans une liste d'alphabet.

On choisit une clé d'entrée dans une grille poly-alphabétique comportant autant d'alphabets que de symboles codants. Pour coder un caractère du texte clair, il suffit de lire dans la grille son substitué dans l'alphabet déterminé par la clé.

Ex: Considérons un alphabet de 4 caractères (A,B,C,D) et la table poly-**alphabétique** suivante:
e **A B C D**
k**A** C B D A
B D C A B

C C A B D

D B D A C

Si la clé est DBCBAA

le texte clair ABCBAC

le texte crypté BCAADD

En utilisant des clés de même longueur que le texte clair, on complexifie le codage poly-alphabétique en rendant la reconstruction de la table et la recherche des clé quasi impossible, surtout quand la longueur des clés devient très élevée. Mais ce type de codage fut abandonné justement à cause de longueur de ces clés.

3. Les transpositions

C'est une permutation de caractères du texte clair suivant une fonction quelconque et période P.

4. L'utilisation de la suite syracusienne

4.1 Méthode directe

La suite syracusienne atteint toujours 8, puis 4, puis 2 et enfin 1, après un **série** d'oscillations quelque soit son premier terme.
Par exemple, en partant de U(0) = 7 on a successivement :

7à 11 à 17 à 26 à 13 à 20 à 10 à 5 à 8.

La suite binaire associée est donc: **11101001**. On émet ces 8 bits, précédé du codage du nombre 8.

Son principal défaut réside dans l'augmentation considérable de la taille d'un fichier. En contrepartie, le contenu fréquentiel du fichier crypté est assez uniforme lorsque la taille des nombres utilisés est élevée.

4.2 Méthode Inverse

Il s´agit de la réciproque de la méthode précédente. Le principe réside dans le fait qu'on se donne un algorithme de génération de nombres pseudo-aléatoires Pi et une clé K. On lit ensuite le fichier par bloc de Pi bits, et on cherche un nombre ni (non unique) dont le codage précédant commence par la suite binaire des Pi bits
Ex:

On prend P=7 , et le bloc de 7 bits: 1000100, et on cherche les entiers n **correspondants** :

n est impair (premier bit 1) : donc n=2k+1 et U(n)=3k+2;

U(n) est pair (second bit 0): donc U(n)=6k+2 et n=4k+1; U2(n)=3k+1;

U2(n) est pair (troisième bit 0); donc U2(n)=6k+4 et n=8k+5.

En continuant ainsi on obtient à la septième étape: n = 128k+69. On peut alors choisir librement n'importe lequel des entiers n:

On est sûr que les 7 premiers bits du codage seront 1000100, car:

64 à 104 à52 à 26 à 13 à 20 à 10 à 5

En prenant k=0, soit n=69, on remplace 7 bits par 7 autres bits: 69=1000101. Mais pour des valeurs de k plus élevées, la substitution est plus difficile à déceler. Il est conseillé d'utiliser ce codage avec des tailles de blocs pseudo-aléatoires élevées (8 octets au moins).

5. Utilisation de l'algorithme de calcul du PGCD

Un calcul simple du plus grand commun diviseur de deux entiers a et b peut être obtenu de manière récursive jusqu'à l'égalité des deux entiers a et b (qui ont alors égaux au PGCD).

Pgcd (a,b)=Pgcd (max (a,b) - min(a,b),min(a,b)).

Ex: Pgcd (20,8)=Pgcd(12,8)=Pgcd(4,8)=Pgcd(4,4)=4;

Pgcd (17,7)=Pgcd(3,7)=Pgcd(4,3)=Pgcd(1,3)=Pgcd(2,1)=Pgcd(1,1)=1.

On donne une clé K et on lit le fichier à crypter par bloc de taille fixe (sensiblement égale à la taille de K). Puis pour chaque bloc B, on déroule l'algorithme du Pgcd de B et de K.

A chaque itération, on émet un bit 0 ou 1 pour dire si le terme max(a,b) est à gauche (0) ou à droite (1). Ces bits permettent de reconstruire les blocs b à partir des blocs cryptés et des Pgcd.

Pour les exemples ci dessus, cela donne:

- Suite binaire = 001 et Pgcd =4;

- Suite binaire = 01010 et Pgcd = 1.

6 Algorithmes à clé symétrique connus

Il existe plusieurs algorithmes à clé symétrique communément utilisés, ce sont **par** exemple:

* *Le DES*: que nous étudierons plus tard.

* *Le Triple DES*: crée pour remplacer le DES.

* *Le RC2 et RC4*.

* *Le IDEA* (Internatinal Data Encrypton Algorithm) crée en 1991. Est conçu pour être efficace sous forme logicielle. Il a la réputation d'être très solide.

La cryptographie asymétrique ou à clé secrète

La grande percée s'est faite **dans** les années 1970 avec l'invention de la cryptographie à clé publique ou cryptographie asymétrique. Ici une clé est utilisée pour coder le message et une autre pour décoder le message crypté.

Dans un système à clé publique , chaque personne dispose de deux clés: une publique et une privée. Les messages chiffrées avec l'une des clés peuvent seulement être déchiffrés par l'autre clé de la paire. Ainsi tout message chiffré avec une clé privée peut seulement être déchiffré par une clé publique et vice versa. Quelques notions mathématiques nous permettrons de mieux cerner cette notion de cryptographie asymétrique.

1. Fonction à sens unique

La théorie de la calculabilité et de la complexité algorithmique introduit une classe de fonction dite à sens unique , dont l´existence est toujours une conjecture.

F est à sens unique <--> Quelque **soit** x , y = f(x) est calculable rapidement.

X = f-1(y) se calcule en un temps très long.

La notion de temps unique signifie que tout algorithme de calcul de l'inverse nécessite un temps de calcul extrêmement long (La complexité de l'algorithme est exponentielle).

Les fonctions ap mod n de la variable p, appelées exponentielles modulaires, sont probablement à sens unique, bien que ce ne soit toujours pas démontré. Leurs inverses, qui ne sont difficilement calculables, portent le nom de logarithmes discrets.

2. Fonctions <trappe> ou à brèche secrète

Une fonction est dite trappe ou à brèche secrète si elle est à sens unique sauf pour toute personne connaissant un secret ou une brèche, permettent de calculer un algorithme d'inversion rapide.

On appelle exponentiation modulaire de la variable a la fonction *ap mod n* (p fixe). Si l´existence d'un algorithme permettant de calculer des racines p-ièmes modulo n est démontré, on ne connaît néanmoins pas cet algorithme. Par contre, si on connaît la factorisation de n (la brèche), on peut très facilement inverser l'exponentiation modulaire.

Conclusion

1. Cryptosystèmes à échanges quantiques

Toute transmission de données sur une ligne peut être espionnée. Ce système propose un moyen de contrer l'espionnage en énonçant un principe simple: établir un canal de communication que nul ne peut espionner sans risquer de perturber la transmission de façon détectable.

Un tel système nécessite un dispositif de transmission différent, par exemple l'utilisation de photons polarisés. La lumière polarisée peut être obtenue en faisant passer un rayon de lumière ordinaire à travers un polariseur comme un filtre Polaroïd ou un cristal.

En effet, l´information est représentée par la polarité du photon (0°,45°,90°,135°.).

Ainsi, toute écoute du canal de transmission va changer la polarité des photons.

Ce système est pour l'instant expérimental mais si les recherches aboutissent, nous aurons alors un système avec une sécurité absolue.

2. Avantages et inconvénients des cryptosystèmes

Type de cryptosystème	Avantages	Inconvénients
Clé symétrique	* Rapide * Peut être facilement réalisée sur une puce	* Les deux clés sont identiques * Difficulté de distribuer les dés * Ne permet pas de signature électronique *

Clé publique	* Utilise deux clés différentes * Fournis des garanties d'intégrité et de non répudiation par signature électronique	Lent et demandant beaucoup de calculs

3. La signature numérique

Le fait d'avoir deux clés numériques présente un autre avantage: la signature numérique.

Imaginons un peu qu'au lieu de chiffrer le message avec la clé secrète , on utilise plutôt la clé publique (qui est connu de tous). Conséquence tout le monde peut lire le message car il n'est plus secret du tout. C'est totalement vrai, mais il est vrai aussi que seule et seulement seule la personne ayant à l'origine chiffré le message l'a bel et bien fait. Car elle est la seule personne capable d´écrire un message lisible par sa clé publique(En supposant bien évidemment que personne d'autre ne possède cette même clé secrète).

Le but de la signature numérique est de garantir l'intégrité et l'authenticité du message.

Prenons un exemple clair:

Pierre désire émettre un message à tous ses collègues leur disant qu'il ne peut pas assister à la réunion du lendemain. Il ne se soucie pas tellement de savoir qui va lire le message, mais il veut garantir à ses associés que le message est réellement de lui et pas de quelqu'un d'autre.

* Pierre écrit le message et le chiffre en utilisant sa clé privée.
* Pierre émet le message sur le réseau pour ses associés.
* Les associés reçoivent le message et le déchiffrent avec la clé publique de Pierre.

Maintenant que faire si Pierre veut envoyer à Caroline un message à la fois secret et signé?

* Pierre écrit le message et le chiffre en utilisant sa clé privée (Il signe le message).

Il chiffre ensuit le résultat avec la clé publique d'Caroline (Il le rend secret).

* Alain envoie le message doublement chiffré à Caroline.

* Caroline reçoit le message

* Elle déchiffre le message deux fois: tout d'abord avec sa clé privée et ensuite avec la clé publique de Pierre.

* Caroline peut donc lire le message et être certaine que c'est bel et bien Pierre qui l'a écrit. Elle est aussi certaine que le message n'a pas été modifié car pour le faire il faudrait avoir la clé privée de Pierre. (*Théoriquement seul Pierre l'a*).

4. Combinaison de la cryptographie à clé publique et symétrique

Un exemple clair nous permettra de mieux comprendre comment cela peut être possible.

Pierre veut émettre un message à Caroline en utilisant une combinaison de cryptographies à clé publique et symétrique.

Cela fonctionne comme suit:

* Pierre écrit le message et le chiffre en utilisant la cryptographie à clé symétrique avec une clé qu'il crée aléatoirement pour ce seul message. Cette clé est appelée clé de message ou de session

* Pierre chiffre cette clé avec la clé publique de Caroline.

* Caroline déchiffre la clé de session avec sa clé privée.

* Elle déchiffre alors le message en utilisant la clé de session reçue.

* Caroline peut alors lire le message.

Cette méthode a bien évidemment les points forts des deux types de crypto-systèmes: la vitesse de la cryptographie symétrique et les mécanismes simples de gestion des clés offerts par la cryptographie à clé publique.

Authentification dans le cadre d'Internet

L'authentification est un élément important de tout système de sécurité Internet. Les entités qui communiquent sur Internet doivent avoir certains moyens pour savoir exactement avec qui ils parlent. Plusieurs applications et méthodes permettent d'avoir des niveaux de confiance différents les uns des autres. Dans le cadre d'Internet, plus le niveau de confiance de l'identification d'un utilisateur est élevé, plus les méthodes à appliquer seront couteuses et difficiles.

Au lieu d'utiliser un mot de passe réutilisable, quatre techniques proposées dans les paragraphes suivant nous permettent l'authentification de l'identité d'une personne.

1. Techniques principales d'authentification

1.1 Ou vous êtes

On utilise couramment cette forme d'authentification basée sur l´emplacement. Elle est habituellement réalisée par le rappel ou des systèmes d'identification d'appel. Notons que cette méthode ne prouve rien malgré le fait qu'elle est bonne en elle même. Car on peut pénétrer un emplacement sûr ou même tromper la centrale téléphonique en lui faisant suivre le rappel quelque part ailleurs.

Beaucoup de réseau comptent sur un identifiant d'utilisateur et l'adresse réseau d'origine pour l'authentification. C'est à dire que l'authentifiant suppose que l'identité d'origine peut être déduite de l'adresse de réseau d'ou viennent les paquets.

L´authentification fondée sur l'adresse n'est pas soumise aux attaques par écoute et par découverte de mots de passe car toutes les données d'authentification sont connues. Mais elle est soumise à plusieurs autres menaces:

-> *Les systèmes sur pénétrés*. Un intrus peut pénétrer le système basé sur les adresse de réseau et imiter un utilisateur du système.

-> *L'imitation d'adresse*. Ici on configure un ordinateur pour imiter un système sûr.

Ex: Le trucage IP.

1.2 Ce que vous savez

Ce système fondé sur ce que quelqu'un connaît est peut être le plus vieux et le plus commun. Il combine généralement le nom et le mot de passe de l'utilisateur. Beaucoup de problèmes sont liés aux mots de passe et on peut les mettre en échec de plusieurs façons:

* *Découverte*: en entrant en possible de la base de donnée des mots de passe

* *Tromperie sur l'utilisateur*: consiste au partage de mot de passe par les utilisateurs.

* *Ecoute*: notons que les attaques par écoute sont assez courantes sur Internet. Avec ce type d'attaque, tous les mots de passe en clair, même bien choisis, sont vulnérables.

Le seul obstacle à ces attaques semble être les mots de passe à usage unique

(Ex: méthode ACTIVCARD).

1.3 Ce que vous êtes

Elle est moins utilisée et fondée sur ce qu'est l'entité à authentifier. Cette catégorie comprend les attributs physiques (tels que les empreintes digitales) des personnes ou ordinateurs.

Il est évident qu'une telle méthode, utilisée dans de bonnes conditions fonctionnerait correctement . Aujourd´hui un système à empreinte digital serait facile à utiliser. Mais ces systèmes dits biométriques sont très coûteux et encore en phase d'expérimentation.

Certains systèmes sur le marché utilisent l'authentification d'après les attributs physiques de l'ordinateur.

1.4 Ce que vous avez

Est fondé sur ce qu'une personne ou une entité possède. Par exemple le fait que quelqu'un utilise une carte spéciale pour son ordinateur pourrait être utilisé pour l'authentifier.

Plusieurs périphériques peuvent être utilisés pour ces fins comme les cartes mémoires ou tout simplement une carte électronique.

2. Avantages et inconvénients des systèmes d'authentification

Mécanisme	Avantage	Inconvénient
Identification biométrique	· Identifie les utilisateurs individuellement. · Difficile, voire impossible de truquer ou de contourner. · Quelques méthodes comme l´analyse graphologiques sont facile pour l'utilisateur.	· Coûteuse · Technologie encore à développer et pas complètement acceptée.
Rappel	· Réalisation rapide. · Peu coûteuse. · Peut résoudre des problèmes de facturation téléphonique en plus des aspects de sécurité. · Identifie l'emplacement de l'utilisateur, ce qui donne un élément dans un schéma d'authentification double.	· Peut être trompé par le transfert d'appel · Peut être trompé si le téléphone ne peut pas décrocher à temps. · Difficile à gérer avec de grandes listes d'appel en retour. · Ne fonctionne pas pour les utilisateurs en déplacement vers des lieux inconnus. · Ne fonctionne pas partout. · Authentifie uniquement le lieu et non l'utilisateur. · Repose sur la sécurité de la compagnie téléphonique
Identification de l'appelant	· Difficile à truquer · Peu coûteuse · Facile à réaliser · Identification de	· Impossible quand on utilise plusieurs zones de compagnies téléphoniques. · Ne fonctionne pas partout · Repose sur la sécurité des

	l'emplacement de l'utilisateur.	compagnies téléphoniques.
Identification du noeud	· Identifie seulement le PC · Ne gêne pas l'utilisateur car elle se déroule en tâche de fond · Pas de gestion de matériel ou logiciel	· Une solution propriétaire · Identifie les machines pas les utilisateurs.
Mot de passe à usage unique	· Peu coûteuse · Peut être réalisé sans matériel ni logiciel spéciaux · Techniquement difficile à tromper	· L'utilisateur d'une liste peut ne pas être acceptable par certains utilisateurs.
Carte PCMCIA	· Protège l'intégrité et la confidentialité des données stockées · Facile d'emploi · Relativement petite	• Nécessite un port PCMCIA · Relativement coûteuse pour des installation à grande échelle · Fragile
Carte à puce	· Facile d'emploi · Relativement petite · Protège l'intégrité et la confidentialité des données stockées	· Nécessite un lecteur de carte à puce · Coûteux pour une installation à grande échelle
Smartdisks	· Protège l'intégrité et la confidentialité de données stockés · Facile d'emploi · Petite · Fonctionne sur du matériel existant	· Technique propriétaire · Choix limité des mécanisme de sécurité · Demande que chaque utilisateur ait un Smartdisk · Coûteuse à grande échelle
Carte électronique	· Idem que le Smartdisk · Fonctionne avec des terminaux muets	· Ne peut pas être utilisé sans préavis de l'utilisateur · Affecte la disponibilité du système · Demande que chaque utilisateur ait une carte
Mot de passe	· Peu coûteux	· Facilement contournable

	· Facile d'emploi · Facile à gérer · Traité universellement	· Peut être observé et réutilisé · Peut être volé par une action d´ingénierie sociale

Le standard des algorithmes de cryptage: le DES d'IBM

C'est en 1977 que la société IBM met au point un système de cryptologie approuvé par le bureau fédéral des standards des Etats-Unis. Conçu à l'origine pour des documents classés ou secrets, ce système de cryptage est majoritairement utilisé dans l'industrie du génie logiciel et des cartes à puces.

C'est algorithme portera le nom élogieux de <DES> (Data Encrypton Standart). Ce qui signifie <Standard des algorithmes de cryptage>. L´aspect positif de sa philosophie repose principalement sur la rapidité de chiffrement et le déchiffrement. Il peut être développé en 200 lignes de code et s'exécute beaucoup **plus** vite sur des cartes électroniques dédiées(Cartes à puces, systèmes électroniques de communication). Sur Internet on trouve facilement des implémentations du DES pour certains systèmes comme le Dos, Unix et MacOs.

1 Genèse

Dans les années 60, un chercheur des laboratoires **IBM**, Feistal Horst, propose l'idée d'un algorithme de cryptage très fiable dont les composantes simples permettent le codage très facilement sur un circuit électronique. Le projet est retenu et sera développé sous le **nom** de code LUCIFER.

1972: A la recherche de l'algorithme le plus sûr possible, le NBS (National Bureau of Standard) lance un appel d'offre à travers un cahier de charge. Vu les traits de ressemblance avec le projet LUCIFER, IBM apporte quelques modifications afin de satisfaire la norme proposée.

1977: L'algorithme de cryptage conçu par IBM est retenu par le NBS sous le nom élogieux de DES (Data Encrypton Standard). D'après les créateurs, le DES ne peut être **utilisé** que dans le cas des documents non classés secret défense.

1978: L'ANSI (American National Standard Institute) valide à son tour cet algorithme sous le nom de DEA (Data Encrypton Algorithm), ce qui provoquera inéluctablement son succès auprès des entreprises.

2. Principe

Le DES n'est qu'un code-produit dont l'idée vient de Shanon: il combine simultanément diffusion et confusion qui sont des méthodes peu sûres quand on les utilise séparément. Néanmoins, leur combinaison permet d'atteindre **un** niveau de sécurité assez considérable. Nul ne pourrait démontrer l'inviolabilité d'un tel produit, mais l´aspect aléatoire du produit des bits chiffrés rendrait la tache très difficile à tout Cryptanaliste.

La diffusion utilise ici des permutations dont le but est d'éclater dans le fichier crypte la redondance présente dans le fichier clair.

La confusion qui a pour but de compliquer la liaison entre le fichier crypté et les clés secrètes, utilise ici des substitutions, non linéaires, de façon à produire un système cryptographique qui résiste à toute cryptanalise mathématique.

Notons que à l'origine, le DES est un code à blocs de 64 bits. Le fichier clair est donc découpé en plusieurs blocs de 64 bits. La transformation d'un bloc comporte 16 itérations d'un processus de codage, qui effectue respectivement une étape de confusion, puis une étape de diffusion.

*On se demande donc où se trouve le neud de **la** sécurité d'un tel système.*

En effet, la sécurité des données cryptées repose sur une clé secrète de 8 octets, **dont** les bits de parité sont éliminés définitivement et n'interviennent pas dans le codage des données.

3. Les six étapes de l´algorithme

3.1 Première étape

On fait subir à chaque bloc de 64 bits, une permutation Po, qui n'a lieu que lors de la première itération. Ensuite le résultat de l'opération qui est un bloc de 64 bits est scindés en deux. On obtient alors deux blocs de 32 suivant la matrice suivante:

58	50	42	34	26	18	10	2
60	**52**	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	**45**	37	29	21	13	5
63	55	47	39	31	23	15	7

Soit:

(b1,b2,.....,b64) --------> (b58,b50,b42,b34,.....,bk,bk-8,.....) ------> (Go , Do)

3.2 Deuxième étape

Les 32 bits de Do entre dans une table de sélection de bit E, où il sont mélangés et répété. Ceci afin d'obtenir 48 bits (*c'est à dire 16 de plus que le bloc initial*).

La table de sélection de bits se présente de la manière suivante:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1
12	13	14	15	16	17

donc:

Do -------> B'=(b32;b1,b2,b3,b4,b5;b4,b5,b6,b7,b8,b9;b8,b9,...)

3.3 Troisième étape

On calcule la clé K1 à partir de la clé d'origine K codé sur 64. Les 48 bits de B' sont transformés par OU-Exclusif avec K1: *B'*---->*B'*+ *K*.

Nous verrons plus tard comment sont générées les clés.

3.4 Quatrième étape

Le résultat de l'étape précédente est divisé en 8 blocs de Doj de 6 bits chacun. Chaque bloc prend alors cette forme: (d1,d2,d3,d4,d5,d6).

La décomposition permettra de déterminer une position dans une table de sélection S à blocs de 16 colonnes et 4 lignes.

Le nombre binaire (d1 d6) représente le numéro de ligne x,

le nombre binaire (d2 d3 d4 d5) le numéro de colonne y.

Une fois la position (x,y) trouvée, on substitue au bloc Doj le bloc de 4 bits déterminé par son adresse (x,y) dans la table. Ce qui nous donne un résultat de 32 bits.

Exemple*: Si le bloc de 6 bits a la forme suivante G=(0.1.1.0.0.1) le résultat sera 1001*

3.5 Cinquième étape : Permutation

Le résultat de l'étape précédente subit une nouvelle permutation P. Cette dernière s'effectue suivant le tableau suivant: soit:

(b1,b2,b3,.....,b32)---------->(b16,b7,b20,b21,b29,b12,b28,b17,.....b11,b4,b25).

3.6 Sixième étape

Nous arrivons à la dernière partie de notre cheminement.

Le résultat de l'étape 5 est soumis à un Xor avec Go (Partie gauche du résultat de la première étape) qu'on n'avait pas encore touché jusqu'alors.

Ainsi s'achève la première itération.

On répète 14 fois la procédure ci-dessus de l'étape 2 à l'étape 6, en prenant comme clé Ki . Par contre la seizième itération ne se termine pas comme les précédentes.

Elle consiste en la réunion des deux parties gauches et droites obtenues à la fin des 14 itérations, ensuite à une permutation finale PI-1.

Notons que: *G16=D15 et D16=G15 + F[Ki,D15]*

4 Génération des clés

La clé secrète K est une clé de 64 bits donc les 8 premier bits sont des bits de parité qui ne sont pas utilisés lors de la construction des clés Ki. Ainsi donc si les 7 premiers bits sont **0101101**, le huitième bit sera 0, pour qu'il y' ait un nombre pair de 1.

La permutation des clés Ki une permutation avec oubli, puisqu'en entrée on a 56 bits et en sortie on se retrouve avec 48 bits. Tout ceci dans le but de pouvoir réaliser le XOR avec le résultat de l'étapes des itérations citée ci dessus (Codées sur 48 bits).

Le principe générale de l'algorithme utilisé est le décalage vers la gauche de chacune des moitiés de la clé.

Notons que le nombre de décalage de bits varie en fonction de l'itération i de la manière suivante:

Nombre de bits de décalage = (1,1,2,2,2,2,2,2,1,2,2,2,2,2,2,1).

5. Décodage du DES

Le DES est un processus symétrique, ce qui signifie que les opérations de codage sont égales à leur propre inverse. Donc, pour décrypter, il suffit d'effectuer les mêmes opérations que pour le cryptage, en utilisant les mêmes clés Ki, mais en partant de K16, au lieu de K1.

Algorithme RSA

1. Le protocole d'encryption RSA

L'algorithme proposé par Rivest, Shamir et Adleman en 1977, est fondé sur l'utilisation de l'exponentiation modulaire, réputée être une *fonction brèche* basée sur l'envoi de messages confidentiels et l'authentification par toute personne du message envoyé par un individu.

La sécurité du RSA réside dans l'impossibilité pratique de factoriser un grand nombre de quelques centaines de chiffres en un temps raisonnable.

2. Calcul de base

Soit un nombre premier n. On recherche deux nombres entiers d **et** e tels que, pour tout entier a compris entre 0 et n-1, on ait: (ad)e**mod** n = aed **mod** n = a. D'après le théorème de Fermat on choisira d et e tel que ed**mod**(n-1)=1. Sachant bien sûr que pour n premier e et d sont compris entre 0 et n-1. Ce problème peut facilement être résolu par l'algorithme d'Euclide.

3 Envoi de messages confidentiels

La clé est un triplet (p,q,e).

(n,e) sont publiés: ce sont donc des clés publiques.

-> d est gardée secrète.

L'envoi d'un message M au propriétaire des paramètres (n,e) se déroule comme suit:

- Décomposition de M en plusieurs blocs mi de taille connue;
- * Calcul, pour tout i: mi'=mi**mod**n;

* Former M' en regroupant les blocs mi', et l'envoyer à son destinataire.

4. Décodage

C'est l'opération inverse. La sécurité du schéma précédent repose sur le fait que seul le propriétaire de (n,e) connaît l'exposant d et peut calculer le texte clair en recevant le texte crypté et en inversant le RSA.

M=(M')dmod n

Toute personne ignorant l'exposant secret <d> ne peut pas, à priori, inverser le processus de cryptage, à moins de calculer . Ce qui est bien sûr impossible dans un temps raisonnable.

5. Détermination des clés

Pour d'une part assurer le bon fonctionnement de l'algorithme RSA et d'autre part assurer une sécurité maximale, il est important de suivre rigoureusement la méthode suivante pour déterminer les deux clés de la méthode RSA.

Choix de n

n doit simplement être le produit de deux nombres premiers p et q.
n = p.q
Le calcul F(n) **s**'effectue de la façon suivante : F(n) = (p-1)(q-1)

Choix de e et d

Pour qu'une exponentielle modulaire de modulo n et d'exposant **e** ait une inverse de modulo n et d'exponentielle e, il faut que cette équation soit vérifiée.
e.d = K.F(n)+1

K est une constante quelconque à choisir de façon à éviter d'avoir **e** ou **d** sous forme de fraction.
Il faut aussi prendre en compte les considérations suivantes lors du choix de **e** :

-> e et n doivent êtres premiers entre eux.
-> e doit être choisi dans l'intervalle [2,F(n)-1].

Les trois paramètres **e**,**d** et **n** sont les seuls nécessaires au fonctionnement de RSA, toutes les autres données ayant permis de les déterminer sont à détruire.

6. La sécurité du système RSA

6.1 Choix de nombres premiers

Les concepteurs du système RSA ont proposé un certain nombre de règles à suivre lorsqu'il s'agit de choisir le quadruplet (p, q, d, e), car un mauvais choix de ces paramètres peut rendre le système relativement vulnérable.
Pour bien choisir p et q il faudrait:

* Choisir n = p*q de taille supérieure ou égale à 512 bits.
* Prendre p et q de taille sensiblement égale, tels que PGCD(p-1, q-1) soit petit par rapport à p et q.
* Choisir si possible des nombres premiers p et q <surs>, de la forme 2x+1, avec x premier, et tel que x-1 possède de grands facteurs premiers.

6.2 Attaques possibles de RSA

On ne sait pas calculer les racines e-ièmes modulo n du message chiffré: ce n'est donc pas de cette façon là que la méthode RSA sera attaquée. En examinant la méthode de détermination des clés on devine facilement comment forcer RSA. Le choix des clés s'effectue à partir de la formule :

$e.d = K.F(n)+1$

L'astuce consiste à déterminer la clé secrète (e ou d) à partir de la clé publique, en résolvant cette équation. Il suffit pour cela de connaître la valeur F(n). La seule façon d'obtenir F(n) à partir de n (rappelons que n est public), est de décomposer ce chiffre en ses facteurs premiers p et q.