Histoire du chiffrement et de ses méthodes

SYNTHÈSE CHRONOLOGIQUE DU CHIFFREMENT À TRAVERS LES ÂGES

Sommaire

1. Introduction

La généralisation rapide des communications par Internet engendre un besoin impérieux de sécurisation des informations et des technologies associées. D'où le rôle de plus en plus capital du chiffrement.

Pourtant, l'histoire du chiffrement ne date pas d'aujourd'hui puisqu'il faut remonter à la civilisation babylonienne, environ 3 000 ans avant notre ère, pour en trouver les premières traces. Quant à son application, elle s'est peu à peu étendue des seuls champs militaire et politique pour investir la sphère civile, notamment sous l'impulsion d'Internet et de l'explosion des volumes de données qui révolutionnent notre quotidien sous bien des aspects.

L'histoire du chiffrement retrace une épopée passionnante dans laquelle cryptographes (« crypteurs ») et cryptanalystes (« décrypteurs ») se livrent une bataille acharnée, éternel recommencement de développement d'un algorithme par les uns, de décodage par les autres, de développement d'un nouvel algorithme plus puissant, etc.

Ce document vous invite à un survol chronologique du chiffrement, de ses méthodes et des technologies qui ont révolutionné son histoire, avant d'énoncer un certain nombre de mesures à mettre en place dans le monde actuel du cryptage.

2. Période classique : l'Antiquité

Les plus anciens chiffrements connus se présentent sous la forme de hiéroglyphes retrouvés sur des monuments datant de près de 3 000 ans avant J.C. Longtemps, les hiéroglyphes furent considérés comme indéchiffrables, avant que la découverte de la célèbre pierre de Rosette et le travail de Jean-François Champollion ne permettent d'en percer les mystères.

Mais retournons vers l'Antiquité, au VIe siècle avant notre ère, dans la cité grecque de Sparte et sa fameuse scytale, un épais bâton autour duquel l'expéditeur enroulait une bande de parchemin pour y écrire son message. Seul le parchemin était ensuite envoyé au destinataire. Si cette personne possédait un bâton d'un même diamètre, elle pouvait alors enrouler la bande autour de celui-ci afin de décrypter le message.

Les méthodes de cryptage de ce type – qui consistent à changer l'ordre des lettres – entrent dans la catégorie du « chiffrement par transposition ».

Plus tard, au Ier siècle avant J.C., on assista à l'émergence du chiffre de César. Fréquemment utilisée par l'empereur lui-même (d'où son nom), cette méthode de cryptage figure parmi les plus célèbres de l'Histoire.

Son principe ? Substituer chaque lettre du message original par une autre située à distance fixe dans l'alphabet. Cette distance devait être connue de l'expéditeur comme du destinataire. Notre exemple montre ainsi un décalage de trois lettres :

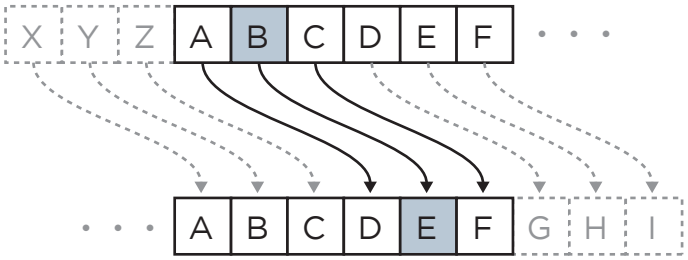

Figure 1

Les méthodes de ce type, qui consistent à décaler les lettres dans un ordre alphabétique, entrent dans la catégorie du « chiffrement par décalage ». Avec un maximum de 26 combinaisons possibles, la méthode du décalage fixe est aisément déchiffrable. D'où l'introduction d'une substitution aléatoire qui permet, quant à elle, d'augmenter considérablement le nombre de permutations possibles (soit 26 x 25 x 24 x …. = 403291461126605635584000000!). De quoi compliquer sérieusement la tâche des cryptanalystes.

Texte clair (non crypté)	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Texte crypté	SMKRATNGQJUDZLPVYOCWIBXFEH

Les méthodes de cryptage de ce type, pour lesquelles une règle fixe s'applique à la substitution des lettres du texte clair, sont connues sous le nom de « chiffrement par substitution ». Il s'agit là des systèmes cryptographiques les plus couramment utilisés à travers les âges. Pour preuve, la célèbre machine de chiffrement mécanique Enigma, sur laquelle nous reviendrons plus en détail, n'est autre qu'une application moderne du chiffrement par substitution.

Les méthodes de type chiffre de César, qui reposent sur une règle de substitution de lettres alphabétiques, font partie de la famille des chiffrements dits « par substitution simple ». Or, le fait que cette technique repose sur la correspondance d'une paire lettre cryptée / lettre claire la rend particulièrement vulnérable au décryptage par analyse de fréquences.

Le principe de cette cryptanalyse consiste à deviner les lettres d'un texte clair sur la base de leur fréquence d'apparition, selon des paramètres linguistiques tels que ceux énoncés ci-dessous pour le français :

- 'e' est la lettre la plus fréquemment utilisée (voir Figure 2).
- 'q' est presque toujours suivi d'un 'u'.
- Des mots tels que 'un', 'une', 'le', 'la', 'les' et 'des' apparaissent très souvent.

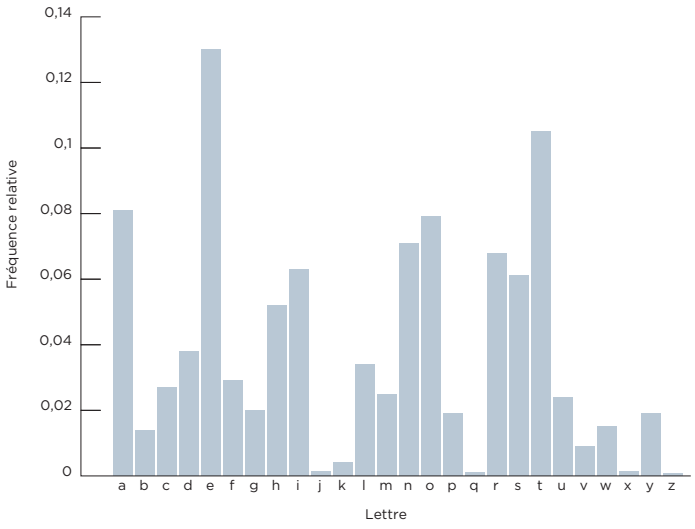

Figure 2

Tous les chiffrements étudiés jusqu'ici, y compris les techniques de substitution et transposition, se composent d'un algorithme cryptographique et d'une clé. Ici, l'algorithme correspond à la règle appliquée lors du cryptage et du décryptage du texte.

Par exemple, dans le cas d'un chiffrement par substitution, l'algorithme correspond au décalage des lettres de l'alphabet. Dans la technique par transposition, l'algorithme cryptographique n'est autre que l'écriture d'un texte sur une bande de parchemin enroulée autour d'une scytale. La clé d'un chiffrement par substitution correspond donc au nombre de lettres entre le texte d'origine et son équivalent crypté. Dans le cas d'un chiffrement par transposition, il s'agira de l'épaisseur de la scytale. Ainsi, une même méthode de chiffrement peut donner lieu à une multitude de clés différentes. Par exemple, avec le chiffre de César, le décalage des lettres pourra varier le long de l'alphabet.

3. Période classique : le Moyen Âge

Le Moyen Âge représente une période charnière pour le développement des technologies cryptographiques. Ce fut en effet l'époque où les chiffrements classiques furent décodés, engendrant par là même l'apparition de nouvelles méthodes. Dans le même temps, l'intensification des activités diplomatiques entraîna un accroissement du volume d'informations confidentielles échangées, et donc de l'usage de la cryptographie.

Chiffre de Marie Ière, reine d'Écosse

Comme nous l'avons évoqué, l'inconvénient des chiffrements par substitution simple, comme le chiffre de César, réside dans sa permutation monoalphabétique facilement déchiffrable. Marie Ière d'Écosse (XVIe siècle), plus connue en France sous le nom de Marie Stuart, l'apprit à ses dépens lorsque le décryptage de ses communications permit de dévoiler sa participation à un complot d'assassinat de la reine Elisabeth Ière d'Angleterre. Marie fut alors condamnée puis exécutée pour trahison.

La méthode de chiffrement utilisée par la reine d'Écosse et les autres conspirateurs s'apparentait en réalité à une nomenclature. Hormis le remplacement de chaque lettre de l'alphabet, cette nomenclature prévoyait également la substitution de certains mots et expressions par des symboles. Dans ce cas, un livre-code (la clé) devait être partagé par l'expéditeur et le destinataire, ce qui compliquait le décryptage de ce chiffre par rapport aux méthodes précédentes. Pas assez cependant pour sauver la tête de cette pauvre Marie !

Chiffre de Vigenère

Dans le cas des chiffrements du type de celui de Marie Ière d'Écosse, le décryptage des modèles monoalphabétiques se limite à une simple substitution. En outre, les nomenclatures présentent elles aussi des inconvénients liés à la rédaction d'un épais livre-code, sans compter le problème de sa distribution aux utilisateurs. Cette question de la diffusion de la clé de chiffrement a toujours représenté un casse-tête pour les utilisateurs, non seulement au Moyen Âge, mais aussi dans des temps plus récents marqués par des technologies cryptographiques avancées.

Au XVe siècle, Leon Battista Alberti développa un prototype de chiffrement par substitution polyalphabétique qui, comme son nom l'indique, faisait intervenir de multiples alphabets de substitution. Il ouvrit ainsi la voie à une succession d'innovations dans ce domaine, dont la plus marquante fut celle du Français Blaise de Vigenère, aussi connue sous le nom de « chiffre de Vigenère ».

Ce chiffre, particulièrement puissant pour l'époque, repose sur une grille, la table de Vigenère (voir Figure 3). Par exemple, pour chiffrer le texte clair « MEDAILLE DE BRONZE » à l'aide du mot « OLYMPIQUE », commencez par repérer les colonnes correspondant aux lettres de votre texte clair en haut de la table. Puis, localisez les lignes correspondant aux lettres de votre clé partant de l'extrémité gauche de la table. Les intersections entre ces lignes et colonnes vous fourniront les lettres à utiliser dans votre texte chiffré.

Texte clair	MEDAILLEDEBRONZE
Clé	OLYMPIQUEOLYMPIQ
Texte chiffré	APBMXTBYHSMPACHU

	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

Figure 3

En fonction de la clé, cette méthode de chiffrement produira des textes cryptés complètement différents. Résultat : même si la table de conversion tombe entre de mauvaises mains, le décryptage s'avérera extrêmement difficile sans la clé. Mieux encore, le nombre de lettres composant le mot clé (boucle) étant théoriquement illimité, le nombre de clés possibles est lui aussi infini.

Toutefois, le chiffre de Vigenère ne s'est pas fait en un seul jour – plus d'un siècle s'est écoulé entre sa conception et sa formulation. En outre, à l'époque, les méthodes de chiffrement par simple substitution restaient très utilisées du fait de leur relative simplicité de cryptage et de décryptage. Plus complexe, le chiffre de Vigenère mit donc un certain temps à s'imposer.

Le chiffre d'Uesugi

Une méthode de chiffrement similaire, reposant elle aussi sur une table de conversion, vit le jour dans le Japon du XVIe siècle. On attribue à Usami Sadayuki, conseiller militaire du seigneur de guerre Uesugi Kenshin, la création d'une table de cryptage à partir d'un carré de Polybe. L'alphabet japonais traditionnel (tiré du poème iroha-uta) comportant 48 lettres, la table se compose de sept lignes et sept colonnes, chacune désignée par un numéro. Dans le message crypté, chaque lettre sera alors représentée par un numéro à deux chiffres. (voir Figure 4).

7	6	5	4	3	2	1	
we	a	ya	ra	yo	chi	i	1
hi	sa	ma	mu	ta	ri	ro	2
mo	ki	ke	u	re	nu	ha	3
se	yu	fu	wi	so	ru	ni	4
su	me	ko	no	tsu	wo	ho	5
n	mi	e	o	ne	wa	he	6
	shi	te	ku	na	ka	to	7

Figure 4

4. Méthodes de chiffrement modernes – De la Première Guerre mondiale à l'avènement des machines de cryptage mécanique

La Première Guerre mondiale fut un véritable catalyseur des communications cryptographiées, et donc de la cryptanalyse.

Quand les Britanniques rompent le câble de communication allemand

En 1914, au moment même où la Grande Bretagne déclarait la guerre à l'Allemagne, Londres ordonnait le sectionnement du câble de communication sous-marin de l'ennemi. Les Britanniques portaient ainsi un sérieux coup à l'armée allemande, contrainte d'utiliser les lignes internationales, via la Grande Bretagne, ou les transmissions radio pour ses communications avec l'étranger. Les forces allemandes durent alors crypter tous leurs messages dans l'espoir d'éviter leur interception par des puissances hostiles. C'était peine perdue. La Grande Bretagne dirigea toutes les communications interceptées vers le « Bureau 40 », une unité de l'amirauté britannique spécialisée dans la cryptanalyse, qui parvint à casser le code allemand – dont le fameux télégramme Zimmermann.

Le télégramme Zimmermann

L'entrée en guerre des États-Unis en avril 1917 changea le cours du conflit et précipita la défaite allemande. Trois mois plus tôt, le ministre des affaires étrangères de l'Empire allemand, Arthur Zimmermann, tentait de décourager les velléités guerrières des Américains en incitant le Mexique et le Japon à attaquer les États-Unis. Pour mettre son plan à exécution, Zimmermann envoya un télégramme contenant ses instructions à l'ambassadeur allemand au Mexique. Malgré son décryptage par le Bureau 40, la Grande Bretagne décida de ne pas rendre le message public, de crainte d'éveiller les soupçons des Allemands et d'entraîner le développement d'un nouveau chiffrement plus puissant. Au final, la Grande Bretagne obtint une version en clair du télégramme envoyé au Mexique depuis l'ambassade allemande à Washington, grâce à un espion posté au bureau des télégraphes de Mexico. Sa publication entraîna la déclaration de guerre des États-Unis à l'Allemagne, et le ralliement de l'Oncle Sam à l'Entente.

L'autre point important de cette anecdote réside dans le fait que les cryptanalystes se gardent généralement de rendre leurs découvertes publiques. Et pour cause : le décryptage avéré d'un code engendre le développement systématique d'un nouveau chiffrement plus puissant. Les cryptographes ont donc tout intérêt à décrypter les messages dans l'ombre, à l'insu de l'expéditeur. Ce cycle interminable de développement et de décryptage des chiffrements se prolonge encore de nos jours.

Chiffre ADFGVX

En 1918, les Allemands passèrent au chiffre ADFGX, conçu par le colonel Fritz Nebel. Basée sur un carré de Polybe, cette méthode utilisait les cinq lettres ADFGX comme en-tête des lignes et colonnes. Chaque lettre claire de la table correspondait à deux lettres cryptées. Jusqu'ici, le chiffre ADFGX ressemble à s'y méprendre au chiffre d'Uesugi. Sauf que les Allemands appliquaient ensuite une méthode de chiffrement par transposition sur les séries de lettres obtenues. Le chiffre ADFGX fit rapidement place à ADFGVX, un algorithme plus puissant puisque composé d'une ligne et d'une colonne supplémentaires (voir Figure 5). Pourquoi ces lettres plutôt que d'autres en en-têtes des lignes et colonnes ? Tout simplement parce qu'elles sont plus faciles à différencier en cas d'envoi d'un message en Morse.

	A	D	F	G	V	X
A	d	h	x	m	u	4
D	p	3	j	6	a	o
F	i	b	z	v	9	w
G	1	n	7	0	q	k
V	f	s	l	y	c	8
X	t	r	5	e	2	g

Figure 5 : chiffre ADFGVX

Dès lors qu'une clé à usage unique est utilisée à chaque envoi, il devient quasiment impossible de décrypter les messages chiffrés à l'aide de cette table. Toutefois, en pratique, le problème du transport d'un grand nombre de clés rendait quasiment impossible leur partage avec la ligne de front en situation de combat.

Naissance d'Enigma

Formulé manuellement jusqu'à la fin du XIXe siècle, le décryptage des chiffrements se compliqua davantage avec l'avènement des machines de chiffrement mécanique au début du XXe siècle.

La plus célèbre d'entre elles fut sans aucun doute Enigma, une machine portable et puissante mise au point par l'ingénieur allemand Arthur Scherbius en 1918. Au moment du lancement d'Enigma, l'armée allemande ignorait encore que son chiffre avait été cassé. Ne voyant donc aucune raison de procéder à une mise à niveau coûteuse de son dispositif existant, elle décida de faire l'impasse sur la nouvelle machine.

Mais une fois l'Allemagne vaincue – une issue dans laquelle le décryptage du chiffre allemand par les Britanniques fut pour beaucoup –, l'état-major outre-Rhin prit conscience du rôle capital de la cryptographie dans les conflits à venir, et se résolut donc à adopter la technologie Enigma.

Enigma intégrait une méthode de chiffrement par substitution polyalphabétique. La machine se composait de multiples rotors comportant les 26 lettres de l'alphabet, un dispositif appelé « brouilleur », ainsi que d'un pupitre de connexions qui effectuait les conversions monoalphabétiques. C'est cette combinaison qui formait la clé du chiffrement. Une fois le brouilleur configuré, le texte clair était saisi par l'intermédiaire d'un clavier, puis passé à travers le brouilleur pour enfin apparaître crypté sur un tableau lumineux. Pour chaque lettre saisie sur le clavier, le brouilleur tournait d'un cran, changeant ainsi la clé de cryptage à chaque nouvelle frappe.

Autre caractéristique : Enigma utilisait les mêmes clés au chiffrement et au déchiffrement, ce qui facilitait les deux processus.

Suite au déploiement du modèle initial dans l'armée allemande, Enigma connut plusieurs évolutions : ajout de deux rotors supplémentaires pour arriver à cinq en tout, brouilleur capable de choisir trois rotors entre les cinq installés, etc.

L'Allemagne nazie développa une foi inébranlable en Enigma. C'était sans compter sur la Pologne qui, menacée d'invasion par son voisin, s'attela au décryptage du code allemand et toucha de près au but grâce à l'invention d'une « bombe » cryptologique évoluée. Toutefois, face aux améliorations d'Enigma et à l'introduction d'un nombre croissant de schémas de cryptage, la Pologne dut se résoudre à abandonner ses travaux par manque de moyens. Durant l'été 1939, elle transmit les résultats de ses recherches et travaux à la Grande Bretagne, mieux dotée en ressources financières et humaines. Deux semaines plus tard, l'invasion de la Pologne marquait le déclenchement de la Seconde Guerre mondiale.

Une fois en possession de ces précieux algorithmes cryptographiques, la Grande Bretagne poursuivit ses efforts de décryptage d'Enigma. Elle profita notamment des travaux polonais effectués sur les clés des messages, qui consistaient en un schéma de trois lettres, répétées deux fois au début du texte crypté, servant à configurer le brouilleur. Le décryptage de ce schéma représenta une avancée majeure : le code d'Enigma était enfin cassé.

Les informations obtenues grâce au décryptage d'Enigma furent baptisées « Ultra ». Cette source fut d'une importance capitale pour les Alliés jusqu'à la fin de la guerre. Toutefois, le cassage du code allemand resta confidentiel jusqu'à la capitulation du Troisième Reich. Convaincu de l'invincibilité de sa machine, la pouvoir nazi continua de l'utiliser en toute confiance jusqu'à sa chute. Le décryptage d'Enigma ne fut rendu public qu'en 1974, soit plus de 30 ans après les faits.

5. Méthodes de chiffrement actuelles – Le cryptage à l'ère de l'informatique et d'Internet

Depuis la Seconde Guerre mondiale, le cryptage et le décryptage sont eux aussi passés du mécanique au numérique. Outre les applications militaires traditionnelles, le raz-de-marée informatique dans le secteur privé engendra un besoin croissant de cryptage de transactions commerciales et autres usages civils.

Algorithme DES

Comme pour Enigma par le passé, les activités de décryptage restèrent longtemps classées secret défense dans tous les pays de la planète. Mais 1973 vint changer la donne. Cette année-là, le National Bureau of Standards américain (NBS, aujourd'hui rebaptisé National Institute of Standards and Technology, NIST) lança un appel d'offre pour la création d'un système cryptographique standard.

Pour commencer, le NBS rendit public l'algorithme de chiffrement qui, avec la clé, constitue l'un des deux éléments essentiels de la cryptographie. Cette démarche représenta un véritable tournant dans l'histoire de la cryptographie. En 1976, le NBS approuva l'algorithme DES (Data Encryption Standard), qui devint donc la méthode de chiffrement standard dans le monde entier.

L'utilisation de la cryptographie à des fins civiles appelait en effet à une standardisation, compte tenu du coût ruineux pour les entreprises de systèmes de cryptographie configurés individuellement pour chaque utilisation. Ainsi, dans les années 70, pour transmettre certains messages à leurs grands comptes, les banques faisaient parvenir une clé de cryptage aux clients en mains propres. Mais voilà, le nombre de clés à livrer augmenta avec l'expansion des entreprises, jusqu'à devenir un véritable casse-tête pour les banques. La cryptographie publique standard leur offrait donc une véritable bouffée d'air, en même temps qu'une solution plus pérenne.

Si la divulgation des algorithmes au public s'avéra une étape décisive dans l'évolution de la cryptographie, le principe fondamental du DES s'apparentait encore au chiffre de César, en ce sens que la même clé servait au cryptage et au décryptage (chiffrement à clé symétrique). Or, avec ce type de cryptographie, le plus grand problème reste encore la distribution de la clé.

Cryptographie à clé publique

L'avènement de la cryptographie à clé publique offrit enfin une solution au problème ancestral de la distribution des clés. Visionnaires de l'informatique en réseaux, Bailey Whitfield Diffie, Martin Hellman et Ralph Merkle se penchèrent sur la question jusqu'alors insoluble des clés communes. En 1976, lors d'une conférence informatique aux États-Unis, ils révélèrent les résultats de leurs travaux sur la cryptographie à clé publique, qui permit de crypter des communications sans distribution préalable des clés. Basée sur une clé asymétrique (clé publique/clé privée), cette méthode fournit une clé publique accessible à tous pour le cryptage, ainsi qu'une clé privée connue du seul destinataire, pour le décryptage du message.

Le concept d'échange de clés Diffie-Hellman-Merkle utilise l'arithmétique modulaire $Y=A^X \pmod B$, une arithmétique dite « à sens unique » du fait de la difficulté pratique à inverser l'exponentiation modulaire. Un calcul à l'aide de la méthode suivante, qui utilise la fonction selon laquelle A^x divisé par B donne Y, a la particularité étonnante d'offrir le même résultat. C'est selon ce principe que la cryptographie à clés communes a pu évoluer.

- **L'expéditeur et le destinataire partagent déjà A et B (par exemple, A=7 et B=11).**
- **X correspond à une valeur que les deux parties connaissent mais ne partagent pas (par exemple, X=3 et x=6).**
- **Les valeurs respectives de Y sont déterminées à partir de celles de A et B, partagées, et des valeurs respectives de X (ainsi Y=2 et y=4).**

- **L'expéditeur et le destinataire partagent alors leurs valeurs respectives de Y.**
- **Ils recalculent enfin la solution par arithmétique modulaire, à l'aide de leurs propres X respectifs et du Y de leur interlocuteur. Résultat : $(Y^x \pmod{11}) = 2^6 \pmod{11} = 9$, $y^X \pmod{11} = 4^3 \pmod{11} = 9$**

Selon cette méthode, il est possible de mener une conversation confidentielle sur une place publique. Cette invention révolutionnaire transforma radicalement l'un des principes directeurs de la cryptographie qui voulait que l'échange de clés s'opère en secret.

Toutefois, ce n'est qu'avec l'apparition de l'algorithme RSA que l'on put passer de la théorie à la pratique.

Algorithme RSA

La méthode mathématique servant à mettre en pratique le concept de clé publique de Diffie-Hellman fut développée par trois chercheurs du MIT (Massachusetts Institute of Technology) : Ronald L. Rivest, Adi Shamir et Leonard M. Adleman. L'appellation RSA correspond aux initiales des noms de famille des trois chercheurs. Côté méthodologie, l'algorithme repose sur la factorisation d'un nombre donné en produit de nombres premiers (nombres divisibles uniquement par eux-mêmes et par 1), comme le montre l'exemple ci-dessous.

$95 = 5 \times 19$
$851 = 23 \times 37$
$176653 = 241 \times 733$
$9831779 = 2011 \times 4889$

Dans le cadre de la cryptographie à clé publique, le nombre situé à gauche de l'équation sert de clé publique et fait partie de la clé privée. Si le nombre premier est un très grand nombre entier, il devient très difficile de décrypter le nombre premier à droite de l'équation dans un délai raisonnable par factorisation première. L'explication mathématique va bien au-delà du champ d'étude de ce document. Disons simplement que les caractéristiques de la factorisation première rendent difficile en pratique la lecture de la clé privée à partir de la clé publique.

Enfin, notons qu'un cryptographe britannique avait développé un algorithme très similaire environ trois ans avant Rivest, Shamir et Adleman. Or, les nouvelles méthodes de chiffrement étant encore classées secret défense à cette époque, ce n'est qu'en 1997 que ses travaux furent rendus publics.

L'un des grands avantages de la cryptographie à clé publique est qu'elle facilite l'échange de clés par Internet et leur décryptage par les seuls destinataires licites. En d'autres termes, cette méthode offre la solution tant attendue au problème ancien de la distribution des clés. Avec RSA, même si la clé publique est accessible sur Internet par un nombre incalculable d'individus connectés, la clé privée, elle, reste quasiment incassable dans un délai raisonnable.

Nous vous proposons ici un exemple SSL simple, illustrant parfaitement comment des informations transmises sur Internet peuvent être cryptées à l'aide d'une combinaison de cryptographies à clé symétrique et à clé publique (RSA). SSL (Secure Sockets Layer) est un protocole de communication sécurisée entre un serveur Web et un client, introduit par Netscape Communications et intégré à son navigateur Netscape Navigator.

Le protocole SSL se caractérise par l'émission d'un certificat électronique qui vérifie l'identité du serveur (serveur Web ou de messagerie), dès lors qu'une communication SSL est engagée, pour attester de manière explicite que les échanges sont bien menés avec le bon serveur. Ensuite, le cryptage des messages prévient toute interception, fuite ou autre violation des données.

La cryptographie à clé publique transmet en toute sécurité la clé symétrique (ou plus précisément les nombres aléatoires sous-jacents de la clé symétrique). Ainsi, il est possible d'établir des communications de données cryptées, sans le sempiternel problème de distribution des clés.

Contrairement à la cryptographie à clé symétrique, cette méthode permet à la clé d'être publique. Par ailleurs, puisque le traitement du cryptage prend un certain temps, une méthode combinée est déployée afin de crypter le texte clair à l'aide d'une clé symétrique, transmise de façon sécurisée par la cryptographie à clé publique.

Décryptage des algorithmes DES

Revenons quelques instants sur l'algorithme DES et sur son décryptage.

La clé DES est composée de 56 bits. Il existe donc 256, soit environ 7 quadrillions (7 x 1016) de combinaisons possibles, ce qui la rend quasiment impossible à décrypter. Toutefois, le code DES fut finalement cassé en 1994. De fait, les chiffrements d'aujourd'hui deviendront progressivement plus simples à décrypter, à mesure que les ordinateurs gagneront en puissance de calcul.

Renforcement du cryptage SSL

Pour répondre à cette évolution, la longueur des clés publiques SSL est passée de 1 024 bits à 2 048 bits, avec en parallèle de nouvelles mesures en faveur d'une signature numérique SSL SHA2 pour les clés publiques. Ces évolutions sont la résultante d'une coopération entre éditeurs de navigateurs et autorités de certification pour définir des calendriers et politiques basés sur les recommandations du NIST, l'organisme américain de normalisation cryptographique. Récemment, SHA2 a suscité un intérêt de plus en plus vif au sein de grandes entreprises soucieuses de se conformer aux directives PCI DSS, dont les recommandations du NIST sont partie intégrante.

Pour en savoir plus sur le passage aux clés de 2 048 bits, rendez-vous sur http://www.thawte.com/resources/2048-bit-compliance/index.html

De leur côté, les utilisateurs de communications SSL cryptées sont invités à actualiser régulièrement leurs navigateurs Web, PC, mobiles, smartphones et autres terminaux clients afin de bénéficier de nouvelles fonctions de hachage et de clés plus longues.

6. Cryptage : les perspectives d'avenir

Comme cette chronologie nous le rappelle, l'histoire de la cryptographie est un éternel recommencement d'inventions d'algorithmes, de cassage de ces codes, puis d'apparition de nouveaux algorithmes renforcés, etc. La cryptographie quantique constitue en ce sens une étape importante de cette évolution.

Un quantum représente la plus petite mesure indivisible. Dans notre cas, il s'agit d'un photon de lumière. En mouvement, les photons polarisés oscillent selon un angle précis. L'information cryptée pourra donc être reçue en mesurant l'angle de cette oscillation. Toute fuite sera immédiatement détectée, du fait du changement de l'angle en cas d'interception du flux de données.

Chaque époque a apporté son lot de méthodes de chiffrement réputées indéchiffrables, du moins dans un délai raisonnable. Le chiffrement quantique change la donne dans la mesure où il est considéré comme impossible à déchiffrer, du fait de la détection immédiate des interceptions.

7. De l’efficacité du cryptage SSL

En théorie, l’algorithme cryptographique utilisé dans la technologie SSL n’est pas impossible à décrypter. En pratique, l’exercice est cependant trop long et trop coûteux. Les ressources consacrées au cryptage doivent refléter le type et l’importance des données à crypter, sous peine d’être déchiffrées par les cryptanalystes.

L’Histoire a connu de nombreuses périodes de latence pendant lesquelles aucun chiffrement réellement efficace n’était utilisé, le dernier en date ayant été décrypté et toujours pas remplacé. Cela peut paraître étonnant dans le monde actuel où les méthodes de cryptage n’ont jamais été aussi nombreuses. De fait, en l’absence d’un système cryptographique efficace, Internet n’aurait jamais connu l’essor qui est le sien.

Les méthodes de cryptographie intégrées à la technologie SSL ne pourront maintenir leur efficacité que si les navigateurs, les serveurs et les certificats serveurs SSL évoluent de pair avec la puissance cryptographique, elle-même un passage obligé dans la prévention des décryptages.

En matière de chiffrement, l’attentisme conduit tôt ou tard à un décryptage du code. Tant les utilisateurs que les fournisseurs doivent en prendre conscience et adopter les mesures qui s’imposent pour la mise en place de moyens de protection adaptés.

Références

Simon Singh, Histoire des codes secrets, Le Livre de Poche, 2001