Comprendre le chiffrement

Évolution des algorithmes de chiffrement et de déchiffrement à travers les âges

digicert®

Sommaire

Introduction

Le chiffrement n'a rien de nouveau puisqu'on l'utilisait déjà il y a plus de 3 000 ans. Mais avec l'explosion d'Internet et des volumes de données échangés quotidiennement, il revêt aujourd'hui une importance capitale pour la sécurité de l'information en ligne.

L'histoire du chiffrement retrace une épopée passionnante dans laquelle les cryptographes (chiffrement) et les cryptanalystes (déchiffrement) se livrent une lutte sans merci. Concrètement, chaque nouveau chiffre développé par les uns finit par être percé par les autres, ce qui donne lieu au développement d'un nouveau code qui est cassé à son tour, et ainsi de suite.

Ce document retrace le parcours 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.

Les origines

Les plus anciens chiffrements connus se présentent sous la forme de hiéroglyphes retrouvés sur des monuments datant de près de 3 000 ans avant notre ère. Considérés comme indéchiffrables jusqu'au XIX^{e} siècle, les hiéroglyphes étaient à leur époque si peu enseignés et maîtrisés que l'on peut les considérer comme une forme de chiffrement.

Un peu plus proche de nous, au VI^{e} siècle avant notre ère, la cité grecque de Sparte utilisait la scytale, un épais bâton autour duquel l'expéditeur enroulait une bande de parchemin pour y écrire son message (voir Figure 1). La bande ne pouvait alors être lue que par une personne possédant un bâton de longueur identique.

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

Figure 1

Considéré comme l'une des méthodes les plus emblématiques de l'histoire, le chiffre de César est apparu au premier siècle avant notre ère et doit son nom au célèbre Empereur romain qui en a fait largement usage. Son principe : substituer chaque lettre du message original par une autre située à une distance fixe dans l'alphabet, ce décalage étant connu uniquement de l'expéditeur et du destinataire.

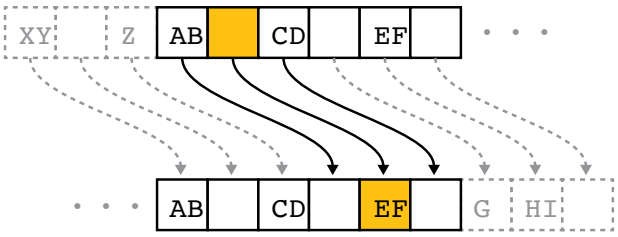

Figure 2

Les méthodes de ce type – qui consistent à décaler les lettres dans un ordre alphabétique – entrent dans la catégorie des « chiffrements 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 …. = 400000000000000000000000000!). De quoi compliquer sérieusement la tâche des cryptanalystes.

Texte clair (non chiffré)	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Texte chiffré	SMKRATNGQJUDZLPVYOCWIBXFEH

Une méthode qui consiste à réorganiser la séquence des caractères selon une règle fixe, comme celle illustrée ci-dessus, est appelée « chiffrement par substitution ». Il s'agit là du système cryptographique le plus utilisé à travers les âges, dont la machine Enigma représente l'une des applications les plus célèbres. Mais n'allons pas trop vite.

Le problème avec les chiffres de substitution, y compris le chiffre de César, c'est qu'ils peuvent tous être percés à l'aide d'une analyse de fréquence, méthode qui utilise des paramètres linguistiques pour deviner les lettres selon leur fréquence d'apparition. Dans la langue française par exemple :

- Le 'e' est la lettre la plus fréquemment utilisée (voir Figure 3).
- Le 'q' est presque toujours suivi d'un 'u'.
- Des mots tels que 'un', 'une', 'le', 'la', 'les' et 'des' apparaissent très souvent.

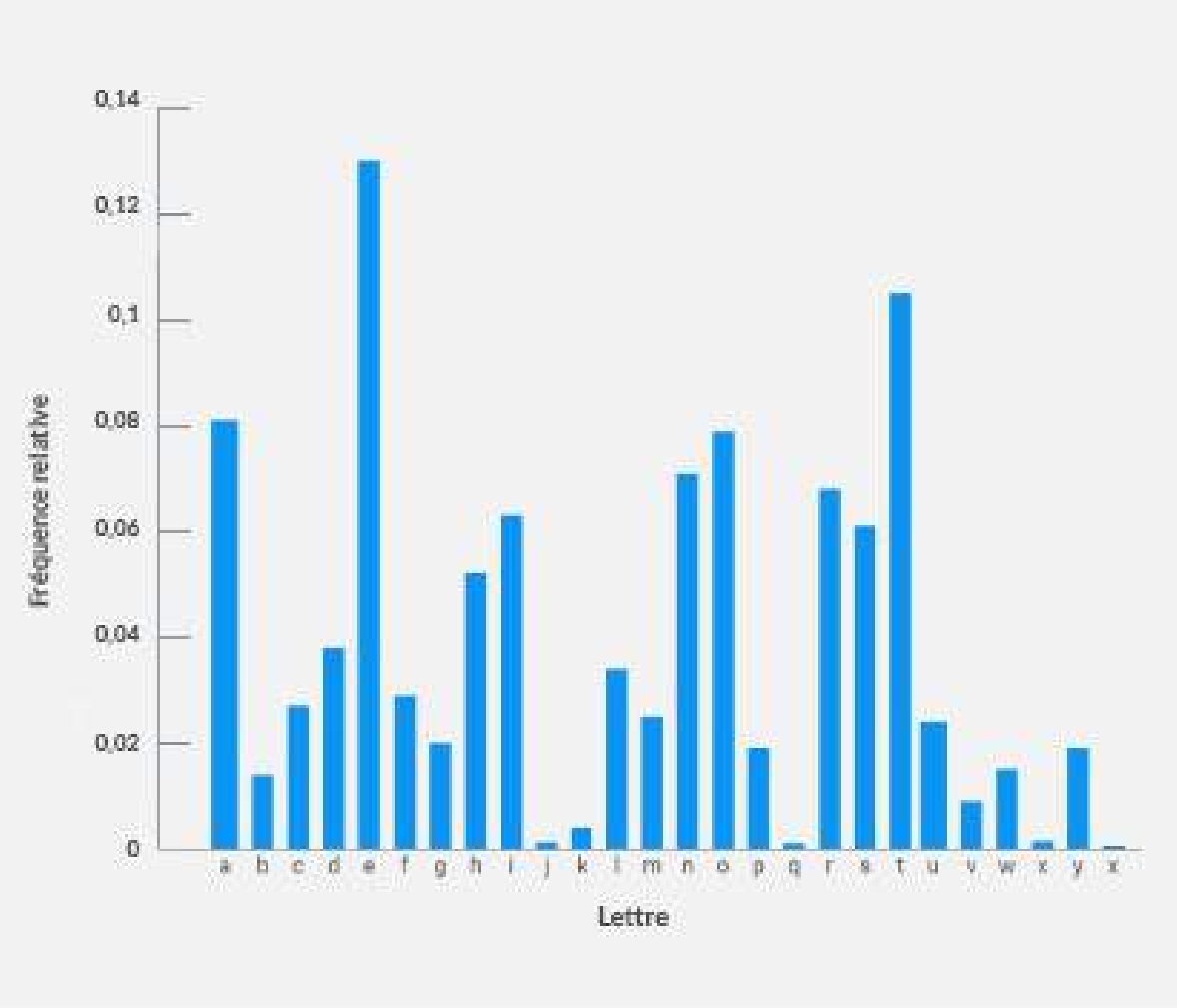

Figure 3

La renaissance de la cryptologie

Au Moyen-Âge, l'intensification des relations diplomatiques engendre des avancées majeures dans le développement des technologies cryptographiques. Les chiffrements classiques ayant été décodés, de nouvelles méthodes sont alors inventées pour protéger un volume toujours plus important d'informations confidentielles.

Chiffre de Marie, reine d'Écosse

Au XVIe siècle, la méthode de chiffrement utilisée par la reine d'Écosse et ses partisans s'apparentait 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 suivant un livre-code. Mais le point faible de cette méthode, à savoir la permutation monoalphabétique, finit par être exploité pour déchiffrer les messages de Marie. Accusée de participer à un complot d'assassinat de la reine Elisabeth Ire d'Angleterre, elle fut condamnée pour trahison puis exécutée au château de Fotheringay.

Texte clair	MEDAILLEDEBRONZE
Clé	OLYMPIQUEOLYMPIQ
Message chiffré	APBMXTBYHSMPACHU

Chiffre de Vigenère

Au XVe siècle, pour palier les failles inhérentes au chiffrement par substitution et éviter le recours à un livre-code volumineux, 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 repose sur une grille, la table de Vigenère (voir Figure 4), servant à chiffrer un texte clair. Par exemple, le texte « MEDAILLE DE BRONZE » chiffré à l'aide de la clé « OLYMPIQUE ». Résultat : même si la table de conversion tombe entre de mauvaises mains, le déchiffrement s'avérera extrêmement difficile sans la clé.

	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ
A	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ
B	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA
C	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB
D	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC
E	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD
F	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE
G	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF
H	HI	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG
I	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH
J	JK	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI
K	KL	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ
L	LM	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK
M	MN	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL
N	NO	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM
O	OP	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN
P	PQ	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO
Q	QR	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP
R	RS	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ
S	ST	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR
T	TU	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS
U	UV	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST
V	VW	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU
W	WX	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV
X	XY	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW
Y	YZ	AB	CD	EF	GH	IJ	KL	MN	OP	QR	ST	UV	WX
Z	ZA	BC	DE	FG	HI	JK	LM	NO	PQ	RS	TU	VW	XY

Figure 4

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 chiffrement 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 chiffré, chaque lettre est alors représentée par un numéro à deux chiffres (voir Figure 5).

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 5

Le chiffrement comme arme de guerre

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

Rupture des communications allemandes

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. L'armée allemande fut alors contrainte d'utiliser les lignes internationales, via la Grande-Bretagne, ou les transmissions radio pour ses communications avec l'étranger. Toutes les communications interceptées furent alors dirigées vers le « Bureau 40 », une unité de l'amirauté britannique spécialisée dans la cryptanalyse.

Le télégramme Zimmermann

En 1917, le ministre des affaires étrangères de l'Empire allemand, Arthur Zimmermann, tenta d'empêcher le ralliement des Américains aux Forces de l'Entente 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 déchiffrement par le Bureau 40, la Grande-Bretagne décida de ne pas rendre le message public, de crainte que les Allemands ne développent un nouveau chiffre plus puissant. Les Britanniques ne le publièrent qu'après avoir obtenu une version en clair du télégramme, ce qui entraîna la déclaration de guerre des États-Unis à l'Allemagne.

Chiffre ADFGVX

En 1918, les Allemands passèrent au chiffre ADFGX, conçu par le colonel Fritz Nebel. À l'image du chiffre d'Uesugi, cette méthode se basait sur un carré de

Polybe, utilisant les cinq lettres ADFGX comme en-tête des lignes et colonnes. Chaque lettre claire de la table correspondait à deux lettres chiffrées. 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 6).

	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 6

Dès lors qu'une clé à usage unique est utilisée à chaque envoi, il devient quasiment impossible de déchiffrer les messages codés à l'aide de cette table. Cette force était aussi sa faiblesse car il exigeait de partager un grand nombre de clés, ce qui le rendrait inutilisable dans une situation de combat en ligne de front.

La machine de chiffrement Enigma

Au début du XX^{e} siècle, le déchiffrement des codes les plus complexes fut grandement facilité par l'avènement des machines électromécaniques.

La plus célèbre d'entre elles fut sans aucun doute Enigma, un appareil portable et puissant mis au point par l'ingénieur allemand Arthur Scherbius en 1918. À cette époque, 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. Ce n'est qu'après avoir réalisé que sa défaite était en grande partie due au déchiffrement de son code par les Britanniques que l'Allemagne se résolut 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. Pour chaque lettre saisie sur le clavier, le brouilleur tournait d'un cran, changeant ainsi la clé de chiffrement à chaque nouvelle frappe.

Alors sous la menace d'une invasion allemande, la Pologne inventa quant à elle une machine de chiffrement baptisée « Bombe ». Cependant, face aux améliorations incessantes d'Enigma et à sa capacité à créer de plus en plus de combinaisons de chiffrement, Varsovie dut renoncer à ce projet, faute de moyens. En 1939, deux semaines avant le début des hostilités, les autorités polonaises aux abois décidèrent de transmettre les résultats de leurs travaux à la Grande-Bretagne. Munis de ces informations et de machines saisies à l'ennemi, Alan Turing et ses équipes ont alors pu élucider les mystères du code Enigma.

Les informations obtenues grâce au déchiffrement 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, le pouvoir nazi continua de l'utiliser en toute confiance jusqu'à sa chute. Il fallut même attendre 1974 pour que la nouvelle du déchiffrement d'Enigma soit rendue publique.

La cryptographie à l'ère de l'informatique

Depuis la Seconde Guerre mondiale, le chiffrement et le déchiffrement 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 chiffrement pour les transactions commerciales et autres usages civils.

Algorithme DES

En 1973, le National Bureau of Standards américain (NBS), plus tard rebaptisé National Institute of Standards and Technology (NIST), lançait un appel d'offre pour la création d'un système cryptographique standard, rendant de fait l'algorithme accessible au public. Trois ans plus tard, le NBS approuvait l'algorithme DES (Data Encryption Standard) qui devint ainsi la méthode de chiffrement standard dans le monde entier.

Cette démarche représenta un véritable tournant dans l'histoire de la cryptographie, notamment dans ses applications à des fins civiles. En effet, les entreprises disposaient désormais d'un moyen pratique et économique de chiffrer et déchiffrer des informations sensibles via une méthode de cryptographie à clé symétrique – un peu comme avec le chiffre de César.

Cryptographie à clé publique

L'avènement de la cryptographie à clé publique offrit enfin une solution au problème ancestral de la distribution des clés. Créée en 1976 par Bailey Whitfield Diffie, Martin Hellman et Ralph Merkle, cette méthode permet de chiffrer les communications, sans exiger une distribution préalable des clés, à l'aide d'une clé publique accessible à tous pour le chiffrement et d'une clé privée connue du seul destinataire, pour le déchiffrement du message.

Le concept d'échange de clés Diffie-Hellman-Merkle utilise une fonction unidirectionnelle, appelée arithmétique modulaire, qui permet 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.

Restait encore à développer une fonction unidirectionnelle permettant un chiffrement asymétrique à l'aide de différentes clés de chiffrement et déchiffrement. Ce fut chose faite avec l'apparition de l'algorithme RSA, qui permit de 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, dont les initiales respectives ont donné son nom au RSA.

Notons toutefois qu'un cryptographe britannique avait développé un algorithme très similaire environ trois ans avant Rivest, Shamir et Adleman. Mais, 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.

Côté méthodologie, l'algorithme RSA repose sur la factorisation d'un nombre donné en produit de nombres premiers, servant de clé publique et en partie de clé privée, comme le montre l'exemple ci-dessous.

$95 = 5 \times 19$

$851 = 23 \times 37$

$176653 = 241 \times 733$

$9831779 = 2011 \times 4889$

Même si la clé publique est facilement accessible, en pratique, les caractéristiques d'une telle factorisation première rendent difficile la lecture de la clé privée à partir de la clé publique dans un délai raisonnable. L'échange de clés sur Internet et leur déchiffrement n'est donc possible que par les parties concernées.

Prenons le cas du TLS/SSL (Transport Layer Security/ Secure Sockets Layer). Introduit par Netscape Communications et intégré au navigateur Netscape Navigator, ce protocole a pour mission de sécuriser les communications entre un serveur web et un client. Le protocole TLS/SSL se caractérise par l'émission d'un certificat électronique qui vérifie l'identité du serveur (serveur web ou de messagerie) de manière explicite. Une fois la vérification faite, les messages sont chiffrés à l'aide d'une clé symétrique, transmise de façon sécurisée par la cryptographie à clé publique, ce qui empêche toute interception, fuite ou autre forme de compromission des informations transmises sur Internet.

Alternatives à l'algorithme RSA

1. **Algorithme DSA (Digital Signature Algorithm)**
   Certifié et approuvé par le gouvernement des États-Unis, l'algorithme DSA (Digital Signature Algorithm) a été développé par la NSA en 1991 comme alternative à l'algorithme RSA standard. Il offre le même niveau de sécurité et de performance que le RSA, mais utilise une formule mathématique différente et moins répandue pour la signature et le chiffrement. La paire de clés DSA est de longueur identique à son équivalente RSA. Toutefois, avec DSA, la génération des clés et les signatures numériques sont plus rapides. À l'inverse, la vérification des clés est légèrement plus lente.

2. **Cryptographie par courbes elliptiques (ECC)**
   La cryptographie par courbes elliptiques (ECC) repose sur une structure algébrique de courbes elliptiques sur des corps finis. Tandis que les clés RSA s'appuient sur la complexité mathématique liée à la factorisation d'un nombre entier de deux facteurs premiers ou plus, l'ECC part du principe selon lequel il est impossible de trouver le logarithme discret de l'élément d'une courbe elliptique aléatoire par rapport à un point de base publiquement connu. Dans le contexte actuel, une courbe elliptique représente une courbe plane formée d'un point à l'infini (∞) et d'une série de points dont les coordonnées répondent à l'équation « $y^2=x^3+ax+n$ ». Les coordonnées doivent être sélectionnées à partir d'un corps fini fixe dont la caractéristique est différente de 2 et 3, au risque de complexifier davantage l'équation de la courbe. Associé à l'opération de groupe relative au théorème de groupe des courbes elliptiques, cet ensemble forme ce que l'on appelle un groupe abélien, le point à l'infini étant défini comme élément d'identité. La structure du groupe est issue du groupe de diviseurs de la variété algébrique sous-jacente.

   Lors de la RSA Conference de 2005, la NSA lançait la Suite B, une série d'algorithmes ECC destinée exclusivement aux signatures numériques et aux échanges de clés. Cette suite a pour vocation de protéger les systèmes et informations de sécurité nationale classés et non classés secrets.

3. **Tailles de clés recommandées par la NIST**
   Organisme fédéral américain, le NIST (National Institute of Standards and Technology) est une « agence publique œuvrant avec les acteurs du secteur au développement et au déploiement de technologies, mesures et standards. » Les recommandations formulées par le NIST font partie de l'écosystème de standards respectés par les navigateurs web et les Autorités de certification.

Minimum size (bits) of Public Keys				Key Size Ratio
Security (bits)	DSA	RSA	ECC	RSA/DSA to ECC
112	2048	2048	N/A	1:09
128	3072	3072	256-383	1:12
192	7680	7680	384-511	1:20

comporte trois avantages : hausse des performances serveur, augmentation des connexions simultanées possibles, baisse de la consommation processeur.

Un défi permanent

Une clé DES est composée de 56 bits. Il existe donc 2 puissance 56, soit environ 7 quadrillions (7×10^{16}) de combinaisons possibles, ce qui la rend quasiment impossible à décrypter. Mais avec l'arrivée de nouveaux ordinateurs surpuissants, le code DES finit par être cassé en 1994.

L'algorithme de cryptographie utilisé dans la technologie TLS/SSL n'est pas infaillible non plus. L'exercice est tout simplement trop long et trop coûteux à réaliser avec les ordinateurs actuels. Ainsi, pour ne pas subir le même sort que les clés DES, les clés publiques TLS/SSL ont vu leur longueur passer de 1024 à 2048 bits. Plus proche de nous, un mouvement en faveur d'une signature numérique des clés publiques TLS/SSL avec l'algorithme SHA-2 a également pris de l'importance face au désir des entreprises de s'aligner sur le standard PCI DSS (Payment Card Industry Data Security Standard).

De leur côté, les navigateurs web, PC, portables, smartphones et autres terminaux client sont régulièrement actualisés pour être compatibles avec de nouvelles fonctions de hachage et des clés plus longues. Le maintien d'un chiffrement fort reste cependant une priorité.

Conscient des limites des certificats RSA 1024 bits utilisés avec la technologie TLS/SSL, le NIST fixa à janvier 2014 la date limite de migration vers des certificats 2048 bits. Cette migration a permis de résoudre de nombreuses problématiques de sécurité, les clés plus courtes n'étant plus suffisamment sûres face à de nouvelles techniques d'attaque et des ordinateurs plus puissants. Mais l'augmentation de la taille des clés RSA peut également avoir un impact négatif sur les performances des serveurs et le nombre de connexions simultanées possibles. Une alternative consiste à utiliser une cryptographie par courbes elliptiques dont le principe repose sur la création de paires de clés publique/privée en se basant sur les points d'une courbe. Ce type de chiffrement est extrêmement difficile à percer par force brute. Il offre ainsi une solution plus rapide et moins impactante que le chiffrement RSA.

Comme tous les autres types de chiffrement, les méthodes de cryptographie utilisées avec la technologie TLS/SSL ne pourront maintenir leur efficacité que si les navigateurs, les serveurs et les certificats serveurs TLS/SSL évoluent de pair avec la puissance cryptographique. Tant les utilisateurs que les fournisseurs doivent adopter les mesures qui s'imposent pour la mise en place de moyens de protection adaptés. À défaut, ces codes finiront par être cassés, avec les graves conséquences que l'on imagine pour Internet et son avenir.

Un avenir malgré tout radieux

Comme cette chronologie nous le rappelle, l'histoire de la cryptographie ressemble à un cycle sans fin où les nouveaux algorithmes finissent tôt ou tard par être déchiffrés. On peut donc d'ores et déjà affirmer que l'avenir appartiendra à la cryptographie quantique, une nouvelle technologie de chiffrement basée sur les propriétés quantiques des photons polarisés.

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.

Références

Simon Singh, Histoire des codes secrets, Le Livre de Poche, Shinchosha Publishing Co. Ltd, 2001

http://freemasonry.bcy.ca/texts/templars_cipher.html
http://www.nsa.gov/ia/programs/suiteb_cryptography/
http://www.nsa.gov/public_info/_files/cryptologic_spectrum/early_history_nsa.pdf

Pour plus d'informations, écrivez à nos experts en sécurité à contactus@digicert.com.

Amériques

Lehi, États-Unis
2801 North Thanksgiving Way, Lehi, Utah 84043, États-Unis

Mountain View, États-Unis
485 Clyde Ave., Mountain View, Californie 94043, États-Unis

Asie-Pacifique

Bangalore, Inde
RMZ Eco World, 10th Floor, 8BCampus
Marathalli Outer Ring Road, Bangalore - 560103, Inde

Melbourne, Australie
437 St Kilda Road, Melbourne, 3004, Australie

Tokyo, Japon
Ginza Six 8F, 6-10-1 Ginza Chuo-Ku, Tokyo
104-0061, Japon

Europe, Moyen-Orient et Afrique

Nieuwegein, Pays-Bas
Nevelgaarde 56 Noord, 3436 ZZ Nieuwegein
Pays-Bas

Le Cap, Afrique du Sud
Gateway Building, Century Blvd & Century Way 1
Century City, 7441, Le Cap, Afrique du Sud

Dublin, Irlande
Block 21 Beckett Way, Park West Business Park
Dublin 12, D12 C9YE, Irlande

Saint-Gall, Suisse
Poststrasse 17, Saint-Gall, Suisse, 9000

Londres, Angleterre
7th Floor, Exchange Tower,
2 Harbour Exchange Square, E14 9GE, Londres

Malines, Belgique
Schaliënhoevedreef 20T, 2800 Malines, Belgique

Munich, Allemagne
Ismaninger Strasse 52, 81675 Munich, Allemagne

digicert®