AFNUM

Alliance Française des Industries du Numérique

Chiffrement

Pierre angulaire de notre sécurité collective

ADHÉRENTS

ADALTRA
Adobe
AIRBUS
amazon
ART-Fi
AUMOVIO
aws
brother at your side
Canon
cisco
CROSSCALL
DELL Technologies
DIGITACCESS
DOCUP
Dolby
DXOMARK
Enchanted Tools
EPSON
ERARD
ERICSSON
FRACARRO
FUJIFILM
Google
hp
Hewlett Packard Enterprise
IBM
Kodak alaris
Leica
Lenovo
Lexmark
LG
Microsoft
MobiWire Group
Nikon
NOKIA
NVIDIA
OM SYSTEM
OPTEX
Panasonic
PHILIPS
quadient
Qualcomm
QUANDELA
RICOH imagine. change.
SAMSUNG
SEQUANS
SERVIMAT
SIGMA
SKYNOPY
SONY
TAMRON Focus on the Future
TCL
Televes
TETENAL
THALES
Western Digital
WISI
xiaomi

Introduction

La cryptographie, ensemble de disciplines permettant de chiffrer et de déchiffrer des informations ou des communications, est utilisée depuis l'Antiquité pour sécuriser les échanges et les données sensibles. Initialement réservées aux armées et aux institutions publiques, les techniques cryptographiques ont été généralisées dès la seconde moitié du XXe siècle pour constituer le socle de la sécurisation de nos sociétés numériques. Au quotidien, le chiffrement est indispensable à la continuité du système bancaire, à la protection des actifs des entreprises, à la sécurité des communications d'État et à la protection des droits et libertés des citoyens.

Véritable pierre angulaire de notre sécurité collective, le chiffrement fait aujourd'hui l'objet d'un débat politique nourri. Plusieurs initiatives législatives ont visé à affaiblir ces technologies, sans tenir compte des réalités techniques ni des impératifs constitutionnels de protection des libertés fondamentales : liberté d'entreprendre, liberté de communication et protection de la vie privée.

Dans un contexte de guerre hybride dans le cyberespace, la tendance à réduire le chiffrement aux seules contraintes qu'il poserait, notamment pour les forces de police, sans regard pour son rôle fondamental dans l'économie et la société, est particulièrement préoccupante. **En tant que représentante des industriels du numérique, dont les protocoles de chiffrement protègent au quotidien les États, l'économie française et les citoyens, l'Alliance Française des Industries du Numérique (AFNUM) souhaite apporter à ce débat des éclairages techniques et juridiques importants.**

Afin d'appréhender la complexité de ces enjeux, ce document présente l'état de l'art des techniques cryptographiques et en analyse les enjeux juridiques et sociétaux.

Le sommaire

P.3 INTRODUCTION

P.6 1 - LE CHIFFREMENT : COMMENT PROTÉGER NOS COMMUNICATIONS À L'ÈRE NUMÉRIQUE

a. Chiffrer, c'est quoi ?
b. Combien de clés utiliser ?
c. Comment gérer les clés ?
d. Le chiffrement de bout en bout
e. Peut-on chiffrer « à moitié » ? Le mythe de la solution intermédiaire

P.18 2 - LA CRYPTOGRAPHIE : PILIER DE LA CONFIANCE À L'ÈRE DU NUMÉRIQUE

a. Un outil central à la protection des intérêts des États
b. Le chiffrement, outil indispensable à la protection de notre économie
c. La confidentialité des correspondances privées, un droit fondamental

- Une liberté déjà encadrée, soumise à un équilibre avec la sécurité publique
- Une coopération des prestataires encadrée avec les autorités

P.28 CONCLUSION

1

Le chiffrement : comment protéger nos communications à l'ère numérique

Le chiffrement est au cœur de nos échanges numériques quotidiens, qu'il s'agisse d'envoyer un message, de réaliser un virement bancaire ou de consulter un site web. Pourtant, les débats parlementaires récents ont révélé une absence de détail technique sur son fonctionnement réel et sur ce qu'il est réellement possible, ou non, de faire pour y accéder. Cette synthèse vise à poser les bases nécessaires à une compréhension éclairée de ces enjeux.

a. **Chiffrer,** c'est quoi ?

Le chiffrement consiste à transformer un message lisible en un message illisible pour quiconque ne possède pas la bonne clé. Ce principe existe depuis l'Antiquité : Jules César décalait déjà les lettres de l'alphabet pour coder ses ordres militaires. Les objectifs n'ont pas changé depuis lors :

1

Garantir la **confidentialité** de l'échange, c'est-à-dire empêcher toute interception par un tiers non autorisé

2

Garantir **l'authenticité** des interlocuteurs, en s'assurant que les parties qui communiquent sont bien celles qu'elles prétendent être

3

Garantir **l'intégrité** des messages, en s'assurant qu'ils n'ont pas été altérés ou manipulés en transit

Pour atteindre ces objectifs, toutes les méthodes de chiffrement, qu'elles soient anciennes ou modernes, reposent sur un outil commun : **une clé**, c'est-à-dire un secret partagé ou calculé, permettant de transformer (crypter) les données et de les restituer (décrypter) dans leur forme originale. La robustesse d'un système de chiffrement dépend ensuite en grande partie de la manière dont cette clé est générée, protégée et transmise.

© Photo de Sasun Bughdaryan sur Unsplash

La clé, cœur de la sécurité depuis l'Antiquité

Avant toute chose, il convient de distinguer les différents concepts qui seront abordés dans ces pages. La cryptologie est la science du secret, et regroupe deux disciplines principales : la **cryptographie**, qui est l'art de concevoir des systèmes pour protéger les informations, et la **cryptanalyse**, qui est l'art de casser, ou de contourner ces systèmes.

En pratique, la cryptographie recoupe donc un certain nombre de méthodes visant à protéger des informations ou des communications contre des accès non autorisés. Ces méthodes comprennent le **chiffrement**, une opération mathématique visant à rendre des données inaccessibles sans utiliser la bonne clé, ou encore le **hachage**, une opération à sens unique permettant de transformer des données en une suite alphanumérique afin de pouvoir en assurer l'intégrité.

Le chiffrement de César

L'une des premières méthodes connues de chiffrement est le « chiffrement de César », utilisé sous l'empire romain. Cette technique consistait à décaler chaque lettre de l'alphabet d'un nombre prédéfini, connu uniquement des deux interlocuteurs.

Par exemple, si le décalage convenu est de trois positions vers la droite, la lettre A devient D, B devenant E, etc. Une fois le décalage appliqué à l'ensemble du message, celui-ci est considéré comme chiffré, et **le nombre de décalage devient la clé de déchiffrement**.

Aussi simple à mettre en œuvre qu'à comprendre, la méthode du chiffrement de César présente une vulnérabilité intrinsèque : sa clé est tout aussi facile à casser et donc le message facilement déchiffrable.

En effet, même sans connaitre ce nombre, il était possible de reconstituer le message chiffré par analyse de fréquence, en s'appuyant sur les lettres les plus courantes dans la langue ciblée.

En français, par exemple, la lettre E est la plus fréquente. Il suffit alors de repérer la lettre la plus récurrente dans le message chiffré (disons K) et de mesurer l'écart avec E pour en déduire le décalage appliqué, puis de reporter cet écart à l'ensemble du message pour reconstituer le message d'origine.

Le chiffrement de César est ainsi qualifié de chiffrement « faible », car :

- Il repose sur une logique unique et répétitive (le décalage est toujours le même pour chaque lettre)
- La même clé (le décalage choisit) sert à la fois à chiffrer et à déchiffrer

Ces faiblesses ont conduit à l'élaboration de nouvelles méthodes plus robustes pour renforcer la confidentialité des échanges.

Della Porta et Vigenère : les systèmes poly-alphabétiques

Au XVIème siècle, l'écrivain, Giambattista Della Porta, proposa une méthode plus élaborée fondée sur un système poly-alphabétique : il a mis au point un jeu de 13 alphabets de substitution, regroupés par paires de lettres (AB, CD, EF, etc.), que l'on peut mobiliser pour coder un message.

Le principe est inspiré du chiffrement de César : chaque alphabet permet de substituer une lettre par une autre selon un décalage prédéfini, comme illustré ci-dessous.

	Clé	Lettres du message												
1	AB	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
2	CD	A	B	C	D	E	F	G	H	I	J	K	L	M
		Z	N	O	P	Q	R	S	T	U	V	W	X	Y
3	EF	A	B	C	D	E	F	G	H	I	J	K	L	M
		Y	Z	N	O	P	Q	R	S	T	U	V	W	X
4	GH	A	B	C	D	E	F	G	H	I	J	K	L	M
		X	Y	Z	N	O	P	Q	R	S	T	U	V	W
5	IJ	A	B	C	D	E	F	G	H	I	J	K	L	M
		W	X	Y	Z	N	O	P	Q	R	S	T	U	V
6	KL	A	B	C	D	E	F	G	H	I	J	K	L	M
		V	W	X	Y	Z	N	O	P	Q	R	S	T	U
7	MN	A	B	C	D	E	F	G	H	I	J	K	L	M
		U	V	W	X	Y	Z	N	O	P	Q	R	S	T
8	OP	A	B	C	D	E	F	G	H	I	J	K	L	M
		T	U	V	W	X	Y	Z	N	O	P	Q	R	S
9	QR	A	B	C	D	E	F	G	H	I	J	K	L	M
		S	T	U	V	W	X	Y	Z	N	O	P	Q	R
10	ST	A	B	C	D	E	F	G	H	I	J	K	L	M
		R	S	T	U	V	W	X	Y	Z	N	O	P	Q
11	UV	A	B	C	D	E	F	G	H	I	J	K	L	M
		Q	R	S	T	U	V	W	X	Y	Z	N	O	P
12	WX	A	B	C	D	E	F	G	H	I	J	K	L	M
		P	Q	R	S	T	U	V	W	X	Y	Z	N	O
13	YZ	A	B	C	D	E	F	G	H	I	J	K	L	M
		O	P	Q	R	S	T	U	V	W	X	Y	Z	N

Figure 1 : Illustration des alphabets de Della Porta

Par exemple, en choisissant l'alphabet « KL », toutes les lettres A seront remplacées par V, les B par W, les C par X, et ainsi de suite. L'originalité et la force de cette méthode résident dans la possibilité de changer d'alphabet à chaque lettre selon un mot-clé, ce qui ajoute une part de hasard bien plus importante.

Pour permettre au destinataire de décoder le message, **les correspondants s'accordaient à l'avance sur un mot-clé, dont les lettres indiquaient la séquence des alphabets à utiliser**. Concrètement, pour chiffrer le mot « BIENTOT » en utilisant cette méthode, il conviendrait de choisir un autre mot pour servir de clé, par exemple « JUSTE », puis de superposer les deux :

Message clair : BIENTOT
Clé : JUSTE

Il faut désormais appliquer à chaque lettre du message en clair la lettre de l'alphabet correspondant : la lettre **B** dans l'alphabet **J** devient un **X**, le **I** dans l'alphabet **U** devient un **Y** etc.

Message clair : BIENTOT
Message codé : XYVJIFD

Le chiffrement de Della Porta marqua une avancée considérable et resta utilisé par les armées et les diplomates pendant de nombreuses années. Cependant, il souffrait de limites structurelles, notamment du fait du nombre restreint d'alphabets disponibles.

Pour pallier ces faiblesses, Blaise de Vigenère propose à la fin du XVIème siècle un perfectionnement majeur dans son «Traité des chiffres». Il élabora un tableau complet, aujourd'hui appelé carré de Vigenère, composé de 26 alphabets, chacun correspondant à un décalage distinct.

	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 2 : Illustration du carré de Vigenère

Le mécanisme de chiffrage est quant à lui identique au chiffrement de Della Porta : un mot clé est superposé au message en clair, et chaque lettre est convertie en se référant à la ligne correspondante dans le tableau.

Cette approche marque un tournant historique dans la cryptographie : **la multiplication des alphabets et leur enchaînement rendent l'analyse de fréquence beaucoup moins efficace**.

Néanmoins, malgré leur sophistication relative, les systèmes de Della Porta et de Vigenère restent vulnérables sur un point central : la clé.Celle-ci est utilisée à la fois pour chiffrer et pour déchiffrer le message. Son interception ou sa compromission met donc en péril l'ensemble de l'échange. C'est la limite structurelle du chiffrement symétrique.

Des algorithmes éprouvés, standardisés au niveau international

Le masque jetable de Vernam

Dès le début du XXème siècle, avec l'explosion des techniques et des capacités de calcul, les méthodes de chiffrement se transforment en profondeur. Les techniques historiques, bien qu'ingénieuses à leur époque, elles ne résistent plus aux attaques automatisées et aux méthodes de cryptanalyse fondées sur les mathématiques modernes.

Une étape majeure dans cette transition est l'invention en 1917 par Gilbert Vernam du chiffrement dit par « masque jetable », aussi appelé chiffrement de Vernam. Inspiré des méthodes de Della Porta et Vigenère, il repose sur le même principe de substitution lettre à lettre, mais **introduit trois exigences majeures qui en font un système de sécurité théoriquement parfait** :

- La clé doit être aussi longue que le message à chiffrer (pas de répétition de la clé comme chez Della Porta)
- Les caractères de la clé doivent être réellement aléatoires (pas de mot clé du dictionnaire envisageable)
- La clé doit être à usage unique

Ces contraintes garantissent en théorie une sécurité absolue : aucune analyse statistique ne permet de retrouver le message initial sans connaissance de la clé.

Toutefois, l'usage pratique du chiffrement de Vernam est limité. En effet, la génération et la distribution sécurisée de clés aléatoires et uniques pour chaque message sont des opérations difficilement envisageables à grande échelle. En outre, la question du stockage et de la synchronisation des clés devient rapidement un obstacle technique.

Pour répondre aux exigences de performance et de faisabilité, les industriels ont développé des méthodes plus souples, certes moins parfaites sur le plan théorique, mais largement éprouvées dans la pratique.

b. **Combien de clés** utiliser ?

On distingue deux catégories de chiffrement en fonction du nombre de clés utilisées.

Le **chiffrement symétrique** est la forme la plus ancienne et la plus intuitive : la même clé sert à la fois à chiffrer et à déchiffrer le message. Les deux interlocuteurs doivent donc préalablement se mettre d'accord sur ce secret commun. Efficace et rapide, cette méthode souffre d'une limite fondamentale : si la clé est interceptée lors de son échange, toute la sécurité du système s'effondre. Si les algorithmes modernes de chiffrement symétrique comme l'AES (Advanced Encryption Standard), standard mondial depuis 2001, ont considérablement renforcé la robustesse mathématique des échanges, ils n'ont pas permis de résoudre ce problème de distribution sécurisée de la clé.

Le **chiffrement asymétrique** a été développé dans les années 1970 pour surmonter cette limite. Son principe repose sur l'utilisation de deux clés distinctes et mathématiquement liées :

Une **clé publique**, librement accessible, que n'importe qui peut utiliser pour chiffrer un message

Une **clé privée**, strictement confidentielle, que seul le destinataire possède et qui permet de déchiffrer ce message

Une analogie utile consiste à voir la clé publique comme une boîte aux lettres : visible de tous, elle permet à n'importe qui d'y déposer un message[1]. La clé privée est la clé physique qui permet d'ouvrir cette boîte et que seul son propriétaire détient. Ce mécanisme élimine le besoin d'échanger un secret préalable et donc le risque d'interception, au cœur de la faiblesse du chiffrement symétrique.

En pratique toutefois, le chiffrement asymétrique est plus lent et plus coûteux en calcul que le symétrique. C'est pourquoi les systèmes modernes adoptent une **approche hybride** : le chiffrement asymétrique est utilisé pour échanger de manière sécurisée une clé de session temporaire, puis le chiffrement symétrique prend le relais pour chiffrer rapidement l'ensemble des données échangées. Cette combinaison est au cœur de protocoles utilisés quotidiennement, comme HTTPS pour la navigation web sécurisée, ou les signatures électroniques.

[1] ANSSI, *Guide des mécanismes cryptographiques*, 1er janvier 2020

Le chiffrement par blocs

Le chiffrement symétrique moderne repose principalement sur le chiffrement par blocs[2].

Dans ce modèle, le message est découpé en blocs de taille standard, généralement 64 ou 128 bits. Une clé de chiffrement vient ensuite chiffrer chaque bloc individuellement. Une fois réunis, ils constituent le message global chiffré. L'Advanced Encryption Standard (AES), standard du NIST (institut américain de normalisation), est aujourd'hui l'un des algorithmes de chiffrement les plus utilisés : on le retrouve dans les messageries électroniques, les sites web sécurisés ou encore les fichiers compressés protégés par mot de passe.

Authentifier la clé publique

Cependant, ce système pose une nouvelle exigence : il faut pouvoir garantir que la clé publique utilisée pour chiffrer les données appartient bien à la bonne personne. Autrement dit, l'authenticité de la clé publique devient un enjeu central.

Pour répondre à cette problématique, des mécanismes de certification ont été développés reposant sur des autorités de confiance capables de garantir l'identité du détenteur d'une clé publique.

[2] « Qu'est-ce que le chiffrement symétrique ? », Annie Badman, Matthew Kosinski, IBM, 5 août 2024, https://www.ibm.com/fr-fr/think/topics/symmetric-encryption

Le chiffrement hybride, étape par étape

Outre la navigation web sécurisée et les signatures électroniques, le chiffrement asymétrique est utilisé par les services de communication sécurisée et par la blockchain. Combiné au chiffrement symétrique, il fonctionne de la manière suivante :

1. L'expéditeur génère une clé symétrique temporaire
2. Il la chiffre à l'aide de la clé publique du destinataire
3. Le destinataire déchiffre cette clé symétrique avec sa clé privée
4. Les deux parties utilisent ensuite cette clé partagée pour échanger les données via un chiffrement symétrique rapide et efficace

c. Comment **gérer les clés ?**

© Photo de Kaitlyn Baker sur Unsplash

Au-delà des algorithmes eux-mêmes, la manière dont les clés sont générées, stockées et distribuées détermine en grande partie la robustesse réelle d'une solution de chiffrement. Deux grandes approches s'opposent ici : l'architecture centralisée et l'architecture décentralisée.

L'**architecture centralisée** confie l'ensemble du cycle de vie des clés (génération, distribution, stockage, révocation) à un tiers de confiance unique. Cette approche présente des avantages opérationnels importants : elle est plus simple à déployer, à administrer et à auditer, notamment dans des environnements réglementés. Elle permet également une réponse plus rapide en cas d'incident. Sa contrepartie est structurelle : elle crée un point de défaillance unique. Si le serveur central est compromis, c'est potentiellement l'ensemble des communications qui est exposé.

L'**architecture décentralisée** répond à cette limite en répartissant la gestion des clés sur un réseau d'acteurs interconnectés, où chaque utilisateur stocke ses propres clés localement sur son appareil. En supprimant le serveur central, elle élimine ce point de vulnérabilité unique. Cette robustesse accrue a pour contrepartie une complexité plus importante : synchronisation entre appareils, gestion des mises à jour, fiabilité dans des environnements hétérogènes. Ce type d'architecture est notamment utilisé dans des contextes à haut niveau d'exigence de sécurité, comme certaines communications sensibles ou dans des zones à risque.

Entre faisabilité technique, efficacité opérationnelle et exigence de confidentialité, le choix d'architecture est le résultat d'un compromis structurant, dont les implications dépassent la seule dimension technique pour toucher à la gouvernance, à la souveraineté et à la question de l'accès aux données.

d. Le chiffrement **de bout en bout**

L'ensemble de ces enjeux — algorithme, gestion des clés, architecture — convergent dans la technique aujourd'hui considérée comme la plus aboutie en matière de protection des communications : le chiffrement de bout en bout (ou « end-to-end encryption », E2EE).

Son principe fondateur répond à la question suivante : comment garantir que les entités permettant aux utilisateurs finaux d'échanger des informations n'aient pas elles-mêmes accès à ces informations ? Dans les systèmes classiques, même chiffrés, l'opérateur qui achemine les messages opère le chiffrement au sein de ses propres infrastructures : les données lui parviennent en clair avant d'être chiffrées, ce qui lui donne techniquement la possibilité d'y accéder.

Le chiffrement de bout en bout supprime cette possibilité en déplaçant l'opération de chiffrement directement sur l'appareil de l'émetteur. **Le message est chiffré avant même de quitter le téléphone ou l'ordinateur de l'expéditeur, et ne peut être déchiffré que sur l'appareil du destinataire.** Entre les deux, le message transite sous forme chiffrée y compris auprès des serveurs de l'opérateur. La clé de déchiffrement ne quitte jamais l'appareil du destinataire et n'est donc accessible à personne d'autre.

Techniquement, ce système repose sur une architecture hybride comme évoqué précédemment : le chiffrement asymétrique est utilisé pour l'échange sécurisé des clés de session, tandis que le chiffrement symétrique assure le chiffrement rapide des messages eux-mêmes. Les clés privées sont stockées localement, selon un modèle décentralisé.

C'est cette architecture qui explique concrètement pourquoi des messageries comme Signal, Olvid ou des services de visioconférence comme Tixeo affirment ne pas pouvoir fournir le contenu des communications à des tiers, y compris à des autorités judiciaires ou de renseignement. Il s'agit d'une impossibilité technique. L'opérateur ne dispose tout simplement pas des clés de déchiffrement.

C'est précisément cette réalité qui est au cœur des débats actuels sur l'accès des autorités aux communications chiffrées, et qui rend indispensable une compréhension technique solide des enjeux avant d'envisager toute mesure législative.

e. Peut-on chiffrer « à moitié » ? **Le mythe de la solution intermédiaire**

Dans le contexte actuel de lutte contre la criminalité organisée et le terrorisme, les autorités publiques sont parfois tentées d'affaiblir les mécanismes de chiffrement pour faciliter les enquêtes. Ainsi, si aucun acteur ne remet frontalement en cause le principe même du chiffrement, des approximations techniques conduisent à des propositions dites de « compromis » ou de « solutions intermédiaires », censées permettre à la fois la confidentialité des échanges et l'accès ciblé aux communications suspectes.

Cette idée est séduisante, mais techniquement inexacte. En effet, ce type d'approche repose sur l'hypothèse d'un chiffrement qui fonctionnerait pour les utilisateurs de bonne foi, tout en restant accessible aux autorités de manière ciblée et sans vulnérabilité généralisée. Or, une telle solution n'existe pas aujourd'hui. Le chiffrement est une technique assurant que seules les personnes possédant la clé de déchiffrement pourront voir le message.

Parmi ces solutions dites « intermédiaires », l'une des plus fréquemment évoquées est la « proposition du fantôme ». Elle consiste à ajouter silencieusement un tiers à une conversation chiffrée, souvent une autorité, sans que les communicants n'en soient informés, et ce par le biais d'une faille de sécurité créée spécialement pour l'occasion, et qui ne serait donc utilisée que par le tiers en question.

Cette approche soulève deux problèmes majeurs. Elle nécessite une refonte complète des architectures techniques des plateformes pour permettre une infiltration invisible et, surtout, **elle ouvre la porte aux cybercriminels et aux États autoritaires qui pourraient exploiter ces failles de sécurité pour s'introduire dans des conversations privées sans alerter les utilisateurs**[3].

[3] « *La proposition du fantôme : De quoi s'agit-il, quels sont ses impacts, et peut-elle atteindre ses objectifs ?* », Internet Society, 24 mars 2020, https://www.internetsociety.org/fr/resources/doc/2020/la-proposition-du-fantome/

2

La cryptographie : pilier de la confiance à l'ère du numérique

Les bases techniques posées précédemment permettent de mesurer pleinement les enjeux que soulève toute tentative de restriction du chiffrement. Dans une société où la quasi-totalité des informations circulent sous forme numérique (communications privées, données professionnelles, échanges financiers, opérations administratives, ...) le chiffrement s'impose comme un axe stratégique majeur tant pour les entreprises que pour les États.

L'augmentation de la puissance de calcul et la massification des échanges numériques ont rendu son renforcement constant indispensable. Ces outils, devenus instruments du quotidien pour des milliards de citoyens et des millions d'institutions et d'entreprises, font du chiffrement un enjeu désormais universel.

Dans ce contexte, le chiffrement ne peut plus être perçu comme un simple outil technique réservé à quelques spécialistes. Il constitue un socle fondamental assurant la protection des intérêts stratégiques des États, la compétitivité de notre économie et l'effectivité de nos droits fondamentaux.

a. Un outil central à la **protection des intérêts des États**

Si la question du chiffrement est souvent abordée sous le seul angle des communications privées, ses mécanismes jouent un rôle crucial pour l'État lui-même dans la préservation de ses intérêts stratégiques. Trop souvent perçu comme un frein à l'action des forces de l'ordre, le chiffrement est en réalité un levier indispensable à la conduite des missions régaliennes, depuis la protection des infrastructures à la confidentialité des communications gouvernementales.

Au-delà de la protection des messageries personnelles qui sont souvent citées en exemple pour illustrer les enjeux du chiffrement, celui-ci est en réalité omniprésent dans l'ensemble des services numériques sur lesquels repose le bon fonctionnement de l'État et de ses administrations :

- Informatique en nuage (cloud computing)
- Échanges de courriels et documents internes
- Stockage sécurisé des données sensibles
- Systèmes de contrôle industriel et d'exploitation des services publics

C'est dans ce contexte que l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a intégré des exigences cryptographiques précises dans son référentiel SecNumCloud[4] destiné aux prestataires de services d'informatique en nuage souhaitant être qualifiés pour traiter des données sensibles de l'administration.

Parmi les exigences figurent notamment :

- La mise en œuvre d'un mécanisme de chiffrement robuste
- La protection contre la récupération des données en cas de récupération du support physique
- Le respect des recommandations techniques en matière de gestion des clés et de protection des métadonnées

La nécessité d'assurer la confidentialité des communications des autorités publiques a également conduit à l'adoption de solutions chiffrées pour les échanges entre membres du gouvernement. Ainsi, par une circulaire du 22 novembre 2023, Elisabeth Borne, alors Première Ministre, avait imposé à l'ensemble des membres du gouvernement d'utiliser la messagerie chiffrée Olvid. Cette décision venait formaliser une pratique déjà largement répandue, tout en reconnaissant la nécessité de protéger les échanges de l'exécutif contre toute forme d'ingérence ou de compromission.

[4] Version 3.2 du 8 mars 2022, Section 10, https://cyber.gouv.fr/sites/default/files/document/secnumcloud-referentiel-exigences-v3.2.pdf

Les failles de sécurité imposées par les autorités peuvent se retourner contre l'État lui-même. Ainsi, la campagne de cyberespionnage d'origine chinoise SaltTyphoon visait principalement l'exploitation de failles de sécurité mises en place par les opérateurs télécoms sur injonction des autorités publiques américaines[5]. L'attaque aurait ainsi touché les communications du Président et Vice-Président des Etats-Unis d'Amérique, ou encore Jean-Noël Barrot, ministre des Affaires étrangères de la République française.

Le chiffrement est ainsi d'une importance capitale pour l'administration au même titre que la sécurité physique des installations, les plans de continuité d'activité ou la gestion des accès aux systèmes d'information.

[5] « Salt Typhoon : voilà le risque que les cyber pirates chinois font peser pour la France », Atlantico.fr, https://atlantico.fr/article/decryptage/salt-typhoon-voila-le-risque-que-les-cyber-pirates-chinois-font-peser-pour-la-france-cybermenace-chine-pekin-piratage-fabrice-epelboin

Post-quantique : la souveraineté se joue maintenant

Depuis plusieurs décennies, les systèmes de chiffrement constituent la colonne vertébrale de la sécurité numérique mondiale. Qu'il s'agisse de protéger des transactions financières, de sécuriser des communications diplomatiques ou encore de garantir l'intégrité de bases de données médicales, ces solutions reposent sur des algorithmes conçus pour résister aux attaques des ordinateurs classiques.

Toutefois, l'émergence progressive de l'informatique quantique remet en question l'équilibre actuel. L'avènement d'un **« *Q-Day* », c'est-à-dire le jour où un ordinateur quantique suffisamment puissant sera capable de casser certains algorithmes de chiffrement courants,** ne peut être daté avec certitude. Les autorités de cybersécurité, notamment l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France, dans le cadre de la feuille de route européenne, et le National Institute of Standards and Technology (NIST) aux États-Unis, fixent toutefois la migration vers des algorithmes résistants au quantique **à l'horizon 2030-2035**.

Cette échéance pose dès aujourd'hui des enjeux stratégiques de souveraineté et de résilience numérique. En effet, des attaques du type « *store now, decrypt later* » (stocker maintenant, déchiffrer plus tard) se multiplient, visant à enregistrer un maximum de données actuellement chiffrées, en attendant de pouvoir les déchiffrer plus tard grâce aux technologies quantiques. Ces attaques menacent donc potentiellement des secrets gouvernementaux, technologies sensibles et secrets d'affaires, ainsi que la vie privée des citoyens.

Sur le plan technique, deux solutions sont actuellement envisagées afin de contrer cette menace :

La cryptographie quantique, théoriquement inviolable mais extrêmement coûteuse sur le plan technique et financier

La cryptographie post-quantique, visant à développer et à déployer de nouveaux algorithmes de chiffrement capables de résister au déchiffrement quantique, tout en restant fondés sur des infrastructures classiques

Cette seconde approche est privilégiée aujourd'hui par les régulateurs, tant français qu'américains, qui travaillent à sa standardisation. Afin de préparer cette transition, l'ANSSI recommande par ailleurs depuis 2022 une anticipation du « *Q-Day* » en mettant en place des stratégies d'hybridation cryptographiques. Il s'agit de combiner algorithmes classiques et algorithmes post-quantiques afin de garantir un double niveau de sécurité, tout en permettant de rester sur des infrastructures existantes.

La transition vers l'ère post-quantique ne peut être perçue comme une simple mise à jour technique mineure. Elle impose une mutation profonde de la gouvernance des données, ce que l'on appelle la **crypto-agilité**. Cette capacité des systèmes à substituer rapidement un algorithme par un autre, sans refonte totale de l'infrastructure, deviendra demain le socle du maintien de la confiance numérique.

Le défi du « *Q-Day* » n'est donc pas seulement une course contre la montre technologique, mais une opportunité de repenser la sécurité dès la conception « *security by design* », garantissant que l'innovation de demain ne sacrifie pas la confidentialité d'aujourd'hui. Au-delà, la maîtrise de la cryptographie post quantique sera demain un levier stratégique majeur pour les Etats, équivalent à la maîtrise des semi-conducteurs ou des technologies spatiales aujourd'hui.

© Wikimedia Commons

b. Le chiffrement, outil indispensable à la **protection de notre économie**

Le chiffrement ne protège pas seulement les intérêts régaliens : il est également au cœur de la souveraineté économique. Dans un contexte économique mondialisé où la donnée est devenue l'un des actifs les plus précieux, la sécurisation de l'information constitue une condition essentielle de compétitivité.

Les entreprises ne manipulent plus seulement des volumes croissants de données personnelles ou financières, elles produisent également de l'innovation, des recherches et des secrets industriels dont la valeur stratégique est considérable. Le chiffrement vient garantir que seules les personnes autorisées puissent accéder à l'information sensible, et ce, même en cas d'interception ou de vol de données.

Au-delà de la protection stricto sensu des données internes, le chiffrement est également un outil de confiance commerciale. Clients, partenaires et investisseurs attendent des garanties solides quant à la protection de leurs informations. La mise en œuvre de solutions de chiffrement robustes renforce cette confiance et contribue directement à la réputation et à la compétitivité de l'entreprise sur son marché.

© Photo de Markus Spiske sur Unsplash

Cette importance se double désormais d'une dimension juridique incontournable. Les réglementations autour de la protection des données, telles que le Règlement général sur la protection des données (RGPD), ou encore la directive européenne dite « NIS2 », imposent des niveaux de sécurité élevés et des mécanismes avancés de sauvegarde de la confidentialité. Dans ce contexte, le chiffrement est explicitement reconnu comme une mesure technique appropriée pour protéger les données à caractère personnel.

Le chiffrement ne constitue donc plus seulement une option technologique avancée : c'est une exigence de conformité qui engage directement la responsabilité juridique et financière des organisations. Cette dimension est d'autant plus importante que les autorités de contrôle disposent de pouvoirs de sanction conséquents, pouvant atteindre plusieurs millions d'euros ou un pourcentage significatif du chiffre d'affaires annuel.

Le chiffrement doit ainsi être compris comme un volet intégral de toute stratégie globale de cybersécurité. Il ne s'agit pas d'un dispositif isolé, mais d'un maillon qui complète d'autres mesures, comme la gestion des accès, la détection d'intrusion, ou encore la sauvegarde sécurisée. Contrairement à d'autres défenses qui peuvent céder devant une attaque sophistiquée, le chiffrement constitue une protection intrinsèque de la donnée elle-même, en en faisant une garantie de défense durable dans un environnement numérique soumis à des pressions croissantes.

Dans un monde interconnecté où les menaces cyber et les ingérences étrangères se multiplient, le chiffrement est à la fois un levier de compétitivité et un instrument de protection de la souveraineté économique des États.

c. **La confidentialité des correspondances privées**, un droit fondamental

La notion de correspondance privée doit être entendue, au sens juridique, de manière extensive. Elle recouvre l'ensemble des procédés de communication privée et à distance : lettres, fax, courriers électroniques, messageries instantanées, communications téléphoniques.

Une circulaire de 1988 précise cette notion en indiquant qu'il y a « correspondance privée lorsque le message est exclusivement destiné à une (ou plusieurs) personne, physique ou morale, déterminée et individualisée »[6].

Ce droit est solidement ancré dans le droit français et européen :

Il est protégé par le Code civil[7] et le Code pénal[8]

Il est reconnu comme une liberté fondamentale de rang constitutionnel

Il est garanti par l'article 8 de la Convention européenne des droits de l'homme[9] (CEDH) ainsi que par l'article 11 de la Déclaration des droits de l'Homme et du Citoyen[10]

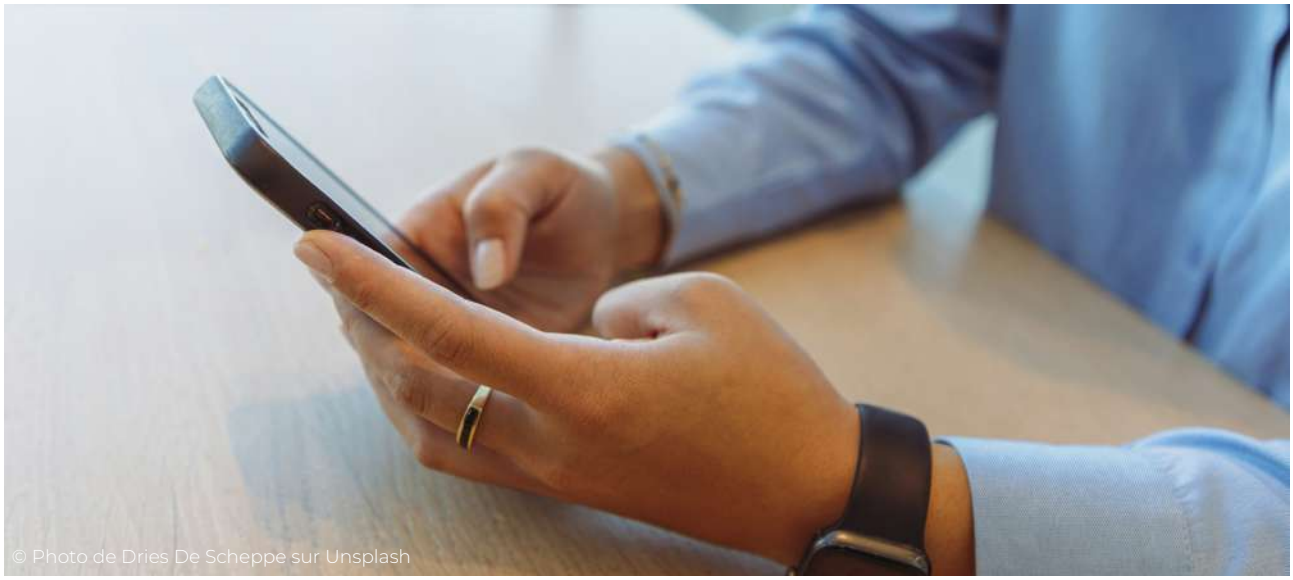
Si les dispositions de ces différents articles s'appliquent indistinctement de la nature pratique des correspondances, des dispositions spécifiques ont été adoptées en matière de communications électroniques :

La loi du 10 juillet 1991 précise que « le secret des correspondances émises par la voie des télécommunications est garanti par la loi »

L'article 1 de la loi pour la confiance dans l'économie numérique (LCEN) a élargi cette garantie aux courriels et messages électroniques

Dans ce cadre juridique, le chiffrement n'est pas seulement un outil technique : il est la modalité concrète par laquelle le droit au secret des correspondances trouve son effectivité dans l'environnement numérique. **En rendant les données inaccessibles à toute personne non autorisée, il constitue la traduction technique d'une garantie fondamentale.**

[6] Circulaire du 17 février 1988 Prise en application de l'art.43 de la loi 86-1067 du 30-09-1986 relative à la liberté de communication, concernant le régime déclaratif applicable à certains services de communication audiovisuelle
[7] Article 9
[8] Article 432-9 et 226-15 du Code pénal réprimant l'ouverture ou le détournement du courrier par les agents publics et les simples particuliers.
[9] « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* », CEDH
[10] « *La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi.* », DDHC, 1789


© Photo de Dries De Scheppe sur Unsplash

1 Une liberté déjà encadrée, soumise à un équilibre avec la sécurité publique

Ce droit, aussi fondamental soit-il, n'est pas absolu. La jurisprudence constante de la CEDH rappelle que ce droit peut être limité à condition que les restrictions soient nécessaires, proportionnées et encadrées par des garanties suffisantes.

Ainsi, dans son célèbre arrêt Big Brother Watch (2021), la CEDH valide le principe de l'interception en masse sous réserve de garanties procédurales « de bout-en-bout ». Cette position illustre la tension structurelle avec le chiffrement, dont l'intégrité technique devient la condition matérielle du respect effectif de la vie privée face à la surveillance d'État[11].

Par cet arrêt, la Cour rappelle la nécessité de maintenir un équilibre entre libertés fondamentales et impératifs de sécurité publique.

Cet équilibre impose de concilier le respect de la vie privée ainsi que les exigences constitutionnelles d'adéquation et de proportionnalité des mesures, avec les impératifs de sécurité et de justice. Il doit être apprécié en tenant compte des réalités techniques du chiffrement moderne : **dans les systèmes de bout en bout, les prestataires techniques ne disposent pas des clés de déchiffrement, ce qui rend certaines injonctions techniquement inexécutables.**

[11] Dans son arrêt du 21 mai 2021 Big Brother Watch et autres contre Royaume-Uni (2021) la Cour rappelle que « compte tenu des multiples menaces auxquelles les Etats doivent faire face dans les sociétés modernes, le recours à un régime d'interception en masse n'est pas en soi contraire à la Convention. Toutefois, elle a jugé que pareil régime doit être encadré par des « garanties de bout-en-bout », c'est-à-dire qu'au niveau de la nation la nécessité et la proportionnalité des mesures prises devraient être appréciées à chaque étape du processus, que les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ ».

© Photo de Compagnons sur Unsplash

2 Une coopération des prestataires encadrée avec les autorités

Les entreprises fournissant des services de cryptographie ne s'opposent pas aux autorités judiciaires : elles coopèrent activement avec elles, dans les pays où leurs services sont disponibles. Ces entreprises publient régulièrement des rapports de transparence détaillant leurs modalités de coopération, notamment la nature des demandes reçues, les informations transmises et les capacités techniques dont elles disposent pour y répondre. Ces capacités dépendent de l'architecture de chaque service : lorsqu'un service est chiffré de bout en bout, le prestataire ne peut transmettre que les données qu'il détient (données d'identification, certaines métadonnées), à l'exclusion du contenu des communications.

Chaque entreprise applique ses propres politiques internes, dans le respect du cadre légal applicable. Ces coopérations reposent sur une vérification préalable de la légalité de la demande au regard de la juridiction émettrice, de la nature des informations sollicitées et de la forme employée. La distinction est notamment opérée entre données de contenu et métadonnées (données de connexion, identifiants, etc.). Si la demande satisfait aux exigences légales, l'entreprise transmet les informations strictement nécessaires. Dans la grande majorité des cas (plus de 95 % sur certaines plateformes[12]), les informations transmises aux autorités portent sur des éléments d'identification et non sur le contenu des communications. Cet encadrement est par ailleurs nécessaire sur le plan procédural afin d'assurer l'admissibilité des preuves devant les juridictions compétentes.

[12] Voir les rapports de transparence publiés par les principaux fournisseurs de services numériques. Les demandes portant sur des données de contenu y sont minoritaires et concernent des services qui ne sont pas chiffrés de bout en bout.

Les entreprises du numérique coopèrent ainsi quotidiennement avec les autorités publiques, dans le strict respect des exigences légales applicables, lesquelles organisent un équilibre entre la nécessité d'accès aux données et le principe de minimisation des informations transmises.

Loin d'être un obstacle à la mission des pouvoirs publics, le chiffrement constitue en réalité un outil central de leur exercice. Ce constat est d'autant plus important que certains discours politiques tendent à banaliser l'idée de l'existance de solutions intermédiaires ou de portes dérobées.

Il convient en outre de souligner que toute atteinte à l'intégrité du chiffrement mènerait de manière automatique à des méthodes de contournement de la part des criminels. Ainsi, le cas de la mise en œuvre de réseaux de chiffrement parallèles basés sur de téléphones spécialement conçus pour la criminalité organisée et distribués dans des circuits parallèles défraie régulièrement la chronique, comme dans le cas du téléphone Phantom Secure[13], une version modifiée d'un modèle BlackBerry utilisée exclusivement dans le cadre d'opérations massives de trafic de drogues.

Imposer une « solution intermédiaire comportant des portes dérobées » reviendrait à affaiblir un équilibre technique et juridique fragile, sans gain sécuritaire réel. **Les acteurs malveillants se replient systématiquement vers des outils clandestins dès que les solutions grand public sont compromises.**

Le chiffrement doit donc rester robuste, intégral et universel pour continuer à jouer son rôle de socle protecteur tant pour les libertés individuelles que pour la sécurité des intérêts stratégiques des États et pour notre sécurité collective. La question est donc moins de savoir s'il faut l'affaiblir, mais comment renforcer les capacités d'enquête dans le respect de ce cadre technique et juridique.

[13] UNODC, *True Crime Stories – Phantom Secure*, https://www.unodc.org/unodc/en/untoc20/truecrimestories/phantom-secure.html

© Photo de Markus Spiske sur Unsplash

Conclusion

Le chiffrement, longtemps perçu comme une discipline réservée aux mathématiciens et aux militaires s'est imposé comme un pilier central de notre société.

Il est aujourd'hui omniprésent : dans les échanges économiques, les communications privées, les systèmes administratifs, les services cloud, les infrastructures critiques, et jusque dans les plus hautes sphères de l'État.

À travers l'étude des différentes techniques de chiffrement, symétriques, asymétriques, hybrides, de bout en bout, et des architectures associées, ce document a mis en évidence une réalité souvent ignorée : le chiffrement est à la fois une condition de la liberté individuelle, un levier de souveraineté et un rempart contre les ingérences.

Les tentations de compromis techniques, de solutions dites « intermédiaires » ou d'aménagements politiques, reposent souvent sur une incompréhension des fondements mêmes de la cryptographie. Or, **il n'existe pas aujourd'hui de demi-chiffrement fiable, pas plus qu'il n'existe de porte dérobée qui ne fragilise pas l'ensemble du système**.

Dans un monde où les menaces sont nombreuses – espionnage, censure, cybercriminalité, désinformation… – le chiffrement n'est pas l'ennemi. Il est, au contraire, l'un des derniers garde-fous technologiques au service de la souveraineté de notre économie, des libertés citoyennes et de l'Etat de droit.

L'AFNUM EN QUELQUES CHIFFRES

8
commissions

59
adhérents

8 000
emplois en R&D

35 Mds
d'euros de chiffre d'affaires cumulés

80 000
emplois directs

contacts

Stella MORABITO
Déléguée Générale
smorabito@afnum.fr

Philippe de CUETOS
Directeur des Affaires Techniques et Réglementaires
pdecuetos@afnum.fr

Paul COLLIGNON
Chargé de mission Environnement et Affaires publiques
pcollignon@afnum.fr

© Rédaction : Afnum - 2026 | Graphisme et illustration : Afnum

AFNUM
Alliance Française des Industries du Numérique

CHIFFREMENT – PIERRE ANGULAIRE DE NOTRE SÉCURITÉ COLLECTIVE

AFNUM | 17 rue de l'Amiral Hamelin - 75016 Paris | contact@afnum.fr
01 45 05 72 25 | afnum.fr | **in** @afnum