# [Fiche 11] Le chiffrement des données

Une très large part de nos vies est "numérisée". Nos écrits, nos communications et échanges sont transformés en "bits" (0 ou 1), afin de pouvoir être interprétés et exploités par les ordinateurs, mais aussi stockés sur des mémoires informatiques et transmis *via* les réseaux.

Ces techniques offrent d'énormes capacités de stockage et de communication, mais elles ont leur revers. Elles facilitent l'intrusion par quelqu'un · de mal intentionné ·e. S'il importe de limiter ses traces et de protéger ses informations confidentielles, cela reste insuffisant.

Heureusement, il existe des méthodes, issues notamment des mathématiques, qui, bien employées, permettent de protéger ses données et ses communications en les rendant incompréhensibles, sauf de soi et de ses correspondants.

## La cryptographie : protéger ses données par le chiffrement

L'idée générale est de "brouiller" le contenu des données par des méthodes mathématiques. On parle alors de "cryptographie" ou le secret des écrits, dont les applications permettent le **chiffrement** des données et des communications. Un exemple très connu : la méthode dite du "chiffre de César", qui est une forme de chiffrement simple : chaque lettre du message est remplacée par une autre selon un nombre de décalages choisi (qui servira de code). Avec un décalage de 5 le A devient F, le B devient G, etc. BONJOUR devient GTSOTZW.

L'objectif des outils présentés ci-après est analogue : rendre des données incompréhensibles si l'on ne connait pas le code. Évidemment, le "chiffre de César" est une technique très rudimentaire et facile à décrypter (à déchiffrer sans connaitre le code). Les outils présentés dans cette fiche mettent eux en jeu des techniques bien plus complexes où la méthode de chiffrement est publique, donc analysable par une personne compétente pour s'assurer qu'il n'y a pas de faille, mais où, sans connaissance du code utilisé, il est quasiment impossible pour un attaquant de décrypter les données. Attention, le simple échange de données chiffrées est en soi une information.

Sans trop entrer dans les détails, le CECIL propose deux fiches sur le chiffrement pour éviter les mauvaises pratiques. L'objectif principal y est de présenter des outils majoritairement considérés comme fiables.

Cette fiche présente les outils permettant de chiffrer **ses données stockées**. La suivante explique comment protéger **ses communications** par chiffrement.

## Chiffrer ses données stockées

Pour améliorer la sécurité et la confidentialité de ses données et documents, les chiffrer est une bonne pratique. Sans protection, ces données peuvent être consultées par quiconque peut y accéder, par exemple par l'insertion d'une clé USB, le vol d'un ordiphone, la récupération du disque dur ; les simples protections d'accès à la machine (mot de passe de session, schéma de déblocage...) sont insuffisantes. De même, si ces données sont conservées ou sauvées sur un serveur extérieur (dans le "nuage"), elles sont aussi accessibles à ceux qui y ont accès (notamment l'entreprise qui gère ce service).

### Chiffrer tout ou partie d'un disque dur ou d'un périphérique de stockage

### Gnu-Linux

Pour l'utilisat·rice d'un système d'exploitation Gnu-Linux récent (Ubuntu, Linux Mint, Tails, Kali...), c'est très simple : à l'installation un choix est proposé de chiffrer intégralement le disque dur ou le dossier personnel (*via* le logiciel dm-crypt avec LUKS). Pour un usage personnel classique, le CECIL conseille vivement de chiffrer son disque dur ou, si l'ordinateur est partagé, au moins le dossier personnel avec un code fiable (telle une phrase de passe). Ce code protégera l'accès à la session (un minimum vital) et le déchiffrement des données.

### Windows et Mac OS X

Pour Windows ou Mac OS X, il faudra télécharger un logiciel. En effet, ceux préinstallés (BitLocker pour Windows, Filevault pour Mac) sont "propriétaires", ils ne peuvent donc être audités et sont donc susceptibles de comporter des failles ou portes dérobées.

Le CECIL recommande donc un logiciel libre : **Veracrypt**

> Une fois téléchargé, puis installé et lancé en suivant les instructions, cliquer sur "*Create Volume*", puis sur "**Encrypt the system partition or entire system drive**" et continuer à suivre les instructions selon les spécificités.
> La procédure n'est pas complexe, mais il est important de ne pas se tromper et il est préférable d'avoir une sauvegarde de ses données. Des tutoriels très bien décrits sont disponibles sur le site Nextinpact - VeraCrypt : comment chiffrer et cacher un OS complet.
> * Pour Mac OS X, il n'est pour le moment pas possible de chiffrer tout le système avec Veracrypt, il faudra pour cela utiliser le logiciel AESCrypt

Dans le cas où Filevault serait malgré tout utilisé, il faut faire attention à l'utiliser correctement, voir pour cela les explications sur le site securitemac.com.

## Chiffrer certains fichiers ou dossiers

Dans la partie précédente, l'objectif était de chiffrer tout ou partie d'un disque dur ou un périphérique de stockage, selon la situation (ordinateur partagé, etc.), cela peut être inadapté ou contraignant. Il existe des logiciels permettant de ne chiffrer que certains fichiers particuliers et sensibles. Le CECIL recommande le logiciel libre 7zip, adapté aux trois systèmes d'exploitation, qui permet de réaliser rapidement des archives compressées et chiffrées de documents *via* la méthode AES256 considérée comme fiable.

- Pour les distributions Gnu-Linux, il est généralement installé par défaut sous le nom de p7zip :

  Pour l'utiliser, il suffit de sélectionner les fichiers ou dossiers à protéger, de réaliser un clic droit et de cliquer sur "Compresser".
  Il faut ensuite choisir l'emplacement de destination de l'archive et une phrase de passe. L'archive produite sera ainsi chiffrée.
  Il faudra par contre penser à supprimer complètement les fichiers originels qui sinon resteraient accessibles. Si le besoin en sécurité est important, il faut aussi s'assurer qu'ils ne seront pas récupérables en utilisant un logiciel de nettoyage tel que Bleachbit.

- Pour Windows, pour utiliser 7zip :

Après avoir téléchargé le logiciel, l'installer en conservant les options par défaut qui l'intégreront au menu contextuel (accessible par clic droit sur un fichier ou un dossier).
Sélectionner ensuite les fichiers à chiffrer, un clic droit -> "7-zip" -> "Ajouter à l'archive"
Dans la fenêtre qui s'affiche choisir le code de chiffrement, le chiffrement AES 256 et cocher "Chiffre les noms de fichiers" si cela a une importance et "Effacer les fichiers après compression".

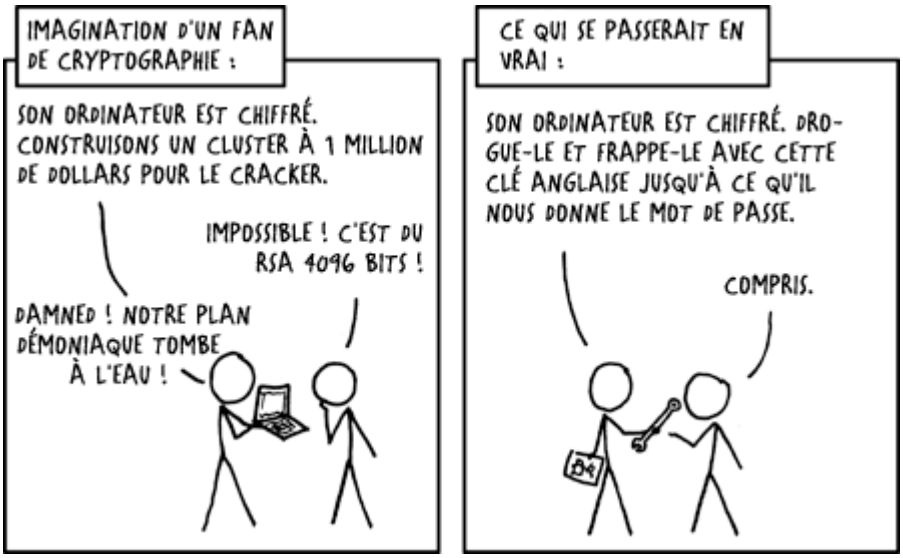
- Pour Mac OS X, il s'agit du logiciel 7zx.

# Limites au chiffrement des données

Attention même si actuellement ces méthodes sont considérées comme fiables, pour autant elles ne sont pas infaillibles :

- failles encore non détectées, portes dérobées,
- dépendance dans le système d'exploitation propriétaire qui aura accès aux données,
- présence d'un virus, d'un enregistreur de frappes espion, d'une surveillance directe de l'ordinateur,
- augmentation constante de la puissance de calcul,
- etc.

Elles ne protègent surtout pas d'une erreur ou d'une faiblesse humaine, comme l'exprime parfaitement ce strip de XKCD sur la sécurité.




Ces limites valent aussi pour le chiffrement des communications.

# Pour aller plus loin :

### Sur la cryptologie et le chiffrement en général

Plus généralement, le chiffrement des données et des communications ouvre un débat public. En effet, cette protection sérieuse, nécessaire pour sécuriser sa vie privée, ses données et ses communications, peut rendre plus complexe le travail des différentes autorités. Le débat est vif, on peut s'en convaincre avec les articles suivants :

- la page Wikipedia sur le Chiffrement sur le chiffrement avec des rappels historiques,
- P. Aigrain, Blog Mediapart, 5 fév. 2015, *Le droit à l'anonymat et au chiffrement*,
- G. Champeau, Numerama, 8 sept. 2015, *Les eurodéputés demandent le chiffrement systématisé de bout en bout*,
- A. Guiton, Liberation, 13 sept. 2015, *Cryptographie : la justice cherche la clé*,
- S. Bortzmeyer, sur son blog, 1 sept. 2013, *La cryptographie nous protège t-elle vraiment de l'espionnage par la NSA ou la DGSE ?*,
- S. Bortmeyer, sur son blog, 7 nov. 2013, *L'IETF et l'espionnage, et maintenant ?*,
- H. Corrigan-Gibbs, nov.2014, The Intercept (en anglais), *Keeping Secrets*, qui retrace l'historique du conflit politique "chercheurs contre NSA" autour du chiffrement,
- Zythom, expert judiciaire en informatique, zythom.blogspot.fr, *Face à Truecrupt*, qui évoque la protection que permet Truecrypt ainsi que les aspects juridiques et pénaux du chiffrement,
- attention au vocabulaire : le champ disciplinaire s'appelle la "cryptologie". Le chiffrement utilise un code pour rendre un message incompréhensible, le déchiffrement pour le rendre compréhensible à l'aide de la bonne clé. Alors que décrypter signifie "casser le code du message" sans connaitre la clé.
- sur Nonblocking.info, *Cryptographie de comptoir*, quelques éléments présentant le chiffrement et des explications sémantiques sur les termes inadaptés (cryptage, etc.).

**Sur le chiffrement de ses données**

- La distribution Gnu-Linux Tails - The Anonymous Incognito Live System, compile les principaux outils de protection des données et des communications et peut être utilisée en Live-USB pour garantir au mieux la protection de données sensibles.
- Moserware.com, A Stick Figure Guide to the Advanced Encryption Standard (AES), une BD pédagogique en anglais sur le chiffrement et l'algorithme AES. Elle commence par les notions très simples et elle se termine par des aspects très techniques,
- un article très complet de M. Lee sur *The Intercept* (en anglais), *Encrypting Your Laptop Like You Mean It*, explique ce que permet ou non le chiffrement et les attaques possibles. Toutefois, l'article propose d'utiliser (et décrit comment le faire) BitLocker pour Windows et Filevault pour OS X, deux logiciels que le CECIL déconseille,
- Gfi.com (en anglais), *The top 24 free tools for data encryption*, un résumé des différents outils de chiffrement existants,
- un tutoriel de l'*EFF*, *Instructions de chiffrement de votre dispositif Windows*. Attention, rien ne garantit qu'il n'y ait pas de porte dérobée sur Windows ou OS X donnant un accès insoupçonné aux données déchiffrées,
- À noter que Veracrypt est un *fork* du logiciel libre *TrueCrypt* qui autrefois faisait référence, mais a été victime d'un épisode étrange en 2014. Il s'appuie toutefois sur une ancienne version de TrueCrypt qui a été auditée et ne semble pas contenir de failles de sécurité,
- le logiciel BleachBit (équivalent libre de CCleaner) permet de supprimer définitivement les données en réinscrivant des 0 et des 1 aléatoirement à la place des anciens fichiers en de multiples passages. Il permet aussi de supprimer d'autres traces (fichiers temporaires, historiques de navigation, précédentes recherches...). Un tutoriel d'utilisation présentant aussi ses limites (notamment sur les clefs USB et les disques SSD) est disponible sur le site https://ssd.eff.org/fr/. Sur ce point voir également les préconisations du Guide d'autodéfense numérique : Guide.boum.org, **Effacer des données "pour de vrai"**.

**Fiche 11 [publiée le 6 novembre 2015, dernière mise à jour avril 2018]**


IMAGINATION D'UN FAN DE CRYPTOGRAPHIE :
SON ORDINATEUR EST CHIFFRÉ. CONSTRUISONS UN CLUSTER À 1 MILLION DE DOLLARS POUR LE CRACKER.
IMPOSSIBLE ! C'EST DU RSA 4096 BITS !
DAMNED ! NOTRE PLAN DÉMONIAQUE TOMBE À L'EAU !
CE QUI SE PASSERAIT EN VRAI :
SON ORDINATEUR EST CHIFFRÉ. DROGUE-LE ET FRAPPE-LE AVEC CETTE CLÉ ANGLAISE JUSQU'À CE QU'IL NOUS DONNE LE MOT DE PASSE.
COMPRIS.