

# Journalisme et Chiffrement



Genma

Paris - 27 février 2016



This work is licensed under the *Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License*.



## A propos de moi

### Où me trouver sur Internet?

- Le Blog de Genma :  
<http://genma.free.fr>
- Twitter :  
<http://twitter.com/genma>

**Le Blog de Genma**

**Rencontre avec Genma IRL**

publié le 3 août 2013 par Genma

Si tu es un lecteur régulier de ce blog, que tu souhaites me voir autour d'un verre, pour manger dans un resto où/ou tout simplement discuter, contacte moi que l'on se fixe un rendez-vous. En effet, je serai disponible du dimanche 11 août au mardi 20 août, en fin de journée ou le soir, à l'endroit que tu souhaites, sur Paris, France. Si tu es partant, fais signe... A la suite de cette rencontre, je pourrais faire (ou non), si tu es d'accord, un petit compte-rendu sur mon blog, ainsi que quelques (...)

**POUR LIRE LA SUITE...**

[f](#) [t](#) [i](#) [u](#) [s](#) [s](#) [s](#)

**Lifehacking - L'importance du matériel**

publié le 3 août 2013 par Genma

Un bon artisan doit avoir de bons outils pour faire du bon travail. Le meilleur musicien ne sera pas aussi bon si son instrument de musique n'est pas de qualité. Il en est de même pour l'informatique. Ce n'est pas la taille qui compte.

En fait si. Pendant deux ans, sur ma mission précédente, j'avais pour travailler du bi-écran. Un écran écran 23" et un écran 15" (celui du portable), l'un au-dessus de l'autre. Avec ma nouvelle mission, je suis passé sur un unique écran de 19", avec un PC plus lent (je (...))

**POUR LIRE LA SUITE...** TAGS : Lifehacking

[f](#) [t](#) [i](#) [u](#) [s](#) [s](#) [s](#)

# Programme

Pourquoi ne dit-on pas crypter ? Un peu de théorie

- Le principe du chiffrement
- Le chiffrement symétrique (Cesar)
- Le chiffrement asymétrique (les enveloppes) (Mails et GPG)

Cacher des documents sur son ordi, le coffre-fort numérique

- Le coffre-fort numérique avec TrueCrypt/Veracrypt

Pause Naviguer sur le web sans être vu, Tor

- Comment l'installer, comment ça marche...

Pourquoi ne dit-on pas crypter ?  
Un peu de théorie

# Le principe du chiffrement

## Le chiffrement

Le chiffrement consiste à chiffrer un document/un fichier à l'aide d'une clef de chiffrement. L'opération inverse étant le déchiffrement.

## Le cryptage

Le terme *cryptage* est un anglicisme, tiré de l'anglais encryption. Le décryptage existe : il s'agit de "casser" un document chiffré lorsqu'on n'en a pas la clef.

## La cryptographie

La science quant-à elle s'appelle la "cryptographie".

# Le chiffrement symétrique (Cesar)

## Le chiffrement symétrique

Cela consiste à chiffrer un message avec la même clef que celle qui sera utilisé pour le déchiffrement. Exemple : le code de César avec un décalage de lettres. A-C, B-D etc.

Nous venons en paix - Pqwu xgpqpu gp rckz

On applique le processus inverse pour avoir le message.

## Une clef de chiffrement c'est quoi?

Une clef s'appelle une clef car elle ouvre/ferme le cadenas qu'est l'algorithme de chiffrement utilisé.

- Ici, l'algorithme est dans la notion de décalage.
- La clef est le nombre de lettre décallées (ici deux lettres).

# Le chiffrement asymétrique 1/2

## Clef publique - clef privée

Le chiffrement asymétrique repose sur le couple clef publique - clef privée.

⇒ Ce qu'il faut comprendre/retenir :

- Ma clef privée est secrète.
- Ma clef publique est distribuée à tous.

## L'algorithme de chiffrement

L'algorithme de chiffrement est bien plus complexe que le fait de décaler des lettres ; il repose sur des notions mathématiques (nombre premiers...)

# Le chiffrement asymétrique 2/2

## Le chiffrement

Avec la clef publique de mon correspondant, je chiffre un fichier.  
⇒ Le fichier ne peut plus être déchiffré que par la personne qui possède la clef privée correspondant à la clef publique que j'ai utilisée (donc mon correspondant).

## Le déchiffrement

Avec sa clef privée, mon correspondant déchiffre le fichier.  
⇒ Il peut alors lire le message.

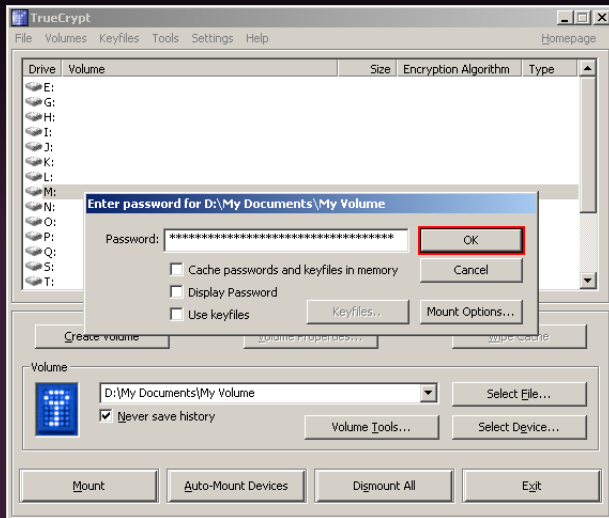
## Cas concret

Le chiffrement de ses mails avec PGP.

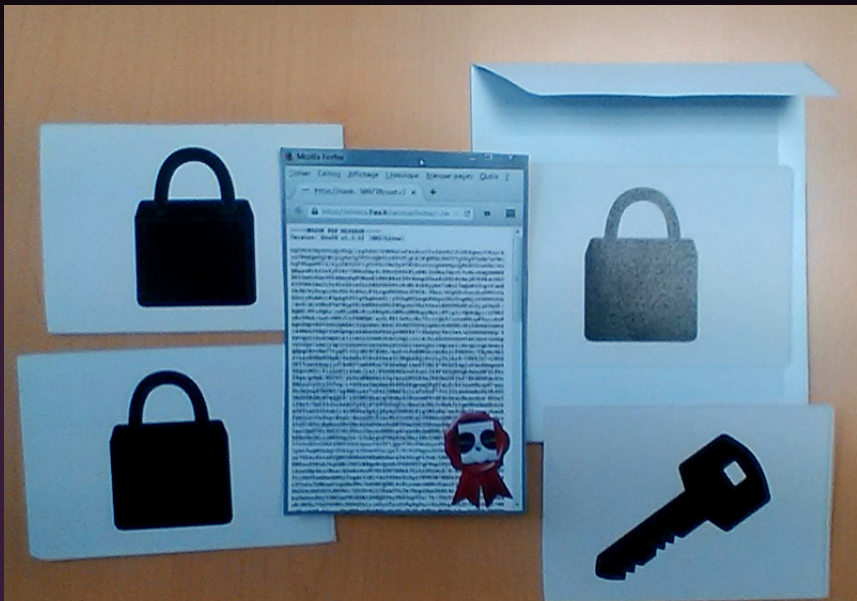


# Le chiffrement en pratique

# Le coffre-fort numérique avec TrueCrypt/Veracrypt



# Les enveloppes



# Les boîtes 1/2

## SIDE 1: METADATA

- GPG ENCRYPTION DOESN'T COME WITH ANONYMITY.
- ONLY THE **CONTENT** OF YOUR MESSAGE IS ENCRYPTED. IMPORTANT INFORMATION REMAINS UNENCRYPTED AND CAN BE READ BY THIRD PARTIES: TIME AND LOCATION, IDENTITY OF THE SENDER AND RECEIVER, ETC.
- BE CAREFUL. THE EMAIL SUBJECT LINE IS NEVER ENCRYPTED. DO NOT SEND ANY IMPORTANT INFORMATION IN THIS LINE.

## SIDE 2: CREATION DATE AND EXPIRATION DATE

- GENERATE KEYPAIRS WITH AN **EXPIRATION DATE**. YOUR PRIVATE KEY CAN BE COMPROMISED. AN EXPIRATION DATE OF A FEW YEARS LIMITS THE VALUE OF STEALING YOUR KEYS.



## SIDE 3: FINGERPRINT AND KEY ID

- EACH KEYPAIR HAS A **UNIQUE** FINGERPRINT AND KEY ID.
- THE **KEY ID** CONSISTS OF THE LAST CHARACTERS OF THE FINGERPRINT. IT IS THE NAME OF THE KEY. IT CAN BE USED TO FIND SOMEONE'S PUBLIC KEY ON A KEYSERVER.
- THE **FINGERPRINT** IS A STRING OF 40 CHARACTERS. IT IS USED TO **VERIFY** A PUBLIC KEY BELONGS TO A PARTICULAR PERSON. TO ULTIMATELY CHECK A FINGERPRINT, MEET ITS OWNER IN PERSON.

## SIDE 4: SIGNATURE

- SIGN YOUR EMAILS WITH YOUR PRIVATE KEY. A **SIGNATURE** PROVES THAT YOU ARE THE AUTHOR OF THE MESSAGE AND THAT IT HAS NOT BEEN MODIFIED.



## SIDE 5: ENCRYPTED MESSAGE

- AN **ENCRYPTED MESSAGE** LOOKS LIKE A RANDOM STRING OF NUMBERS, LETTERS AND SPECIAL CHARACTERS.

## LOOKS & KEYS

- WHEN YOU SEND AN EMAIL, YOU **ENCRYPT** IT WITH THE OTHER PERSON'S PUBLIC KEY. YOU **SIGN** IT WITH YOUR PRIVATE KEY.
- WHEN YOU RECEIVE AN EMAIL, YOU **DECRYPT** IT WITH YOUR PRIVATE KEY. YOU **VERIFY** ITS SIGNATURE WITH THE OTHER PERSON'S PUBLIC KEY.



# BUILD YOUR OWN GPG BOX! HOW TO TEACH EMAIL ENCRYPTION

## YOU NEED:

- TWO SHEETS OF CARDBOARD DIFFERENTLY COLORED
- TWO SMALL LOCKS WITH THEIR KEYS
- A PAPER HOLEPUNCHER
- STRING
- GLUE
- A PEN

## HOW TO BUILD:

(FOR MORE DETAILS, SEE PICTURES ON PAGE 2)

- PRINT OR DRAW THE TEMPLATE ON THE CARDBOARD
- CUT AND FOLD THE CUBES
- GLUE THE TABS
- PUNCH HOLES IN EACH BOX WITH THE HOLEPUNCHER AND ATTACH THE LOCKS
- WITH CARDBOARD AND STRING, LABEL THE LOCKS "PUBLIC KEY" AND THE KEYS "PRIVATE KEY".
- TO KNOW WHAT TO WRITE ON EACH SIDE OF THE GPG BOX, SEE PAGE 2

## WHAT IS A GPG BOX?

BUILD A GPG BOX TO TEACH GPG EMAIL ENCRYPTION IN THE EASIEST POSSIBLE WAY.

GPG BOXES VISUALIZE ASYMMETRIC ENCRYPTION SIMPLY.

EVERY SIDE OF THE GPG BOX HELPS EXPLAIN THE BASIC CONCEPTS OF GPG KEYPAIRS.

## Les boîtes 2/2



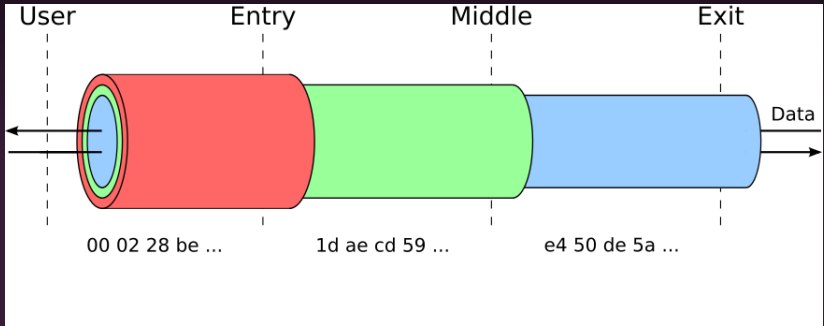
Aller plus loin? Tor et le  
TorBrowser

# Quelques mots sur Tor ?



Attention : la présentation *complète*  
dure une bonne heure et demie...

# Comment fonctionne Tor ?





# Tor et les enveloppes



# A quoi sert TOR?

## Ce que l'usage de Tor permet de faire

- d'échapper au fichage publicitaire,
- de publier des informations sous un pseudonyme,
- d'accéder à des informations en laissant moins de traces,
- de déjouer des dispositifs de filtrage (sur le réseau de son entreprise, de son Université, en Chine ou en France...),
- de communiquer en déjouant des dispositifs de surveillance,
- de tester son pare-feu,
- ... et sûrement encore d'autres choses.

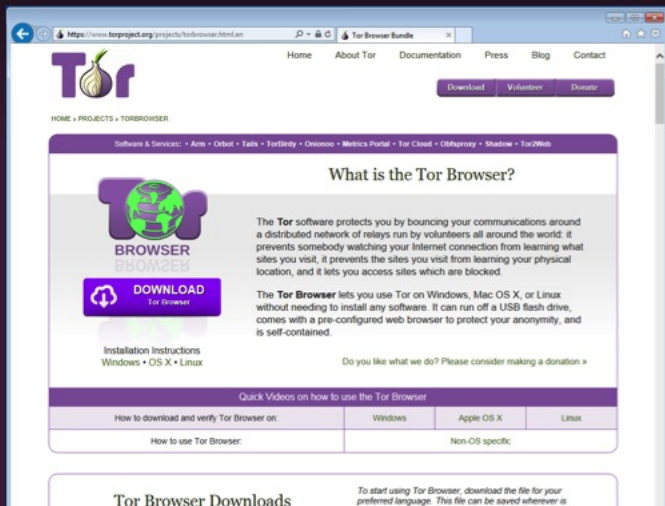
⇒ Tor dispose également d'un système de "services cachés" qui permet de fournir un service en cachant l'emplacement du serveur.

# Télécharger le Tor Browser

Toutes les versions (dans différentes langues, différents OS) sont disponibles sur le site du projet :

<https://www.torproject.org/>

Rq : Il existe la possibilité de le recevoir par mail...



The screenshot shows the Tor Project website's page for downloading the Tor Browser. The browser's address bar displays the URL <https://www.torproject.org/projects/torbrowser.html.en>. The page features the Tor logo (a purple onion) and navigation links: Home, About Tor, Documentation, Press, Blog, and Contact. A purple bar contains buttons for Download, Volunteer, and Donate. Below this, a breadcrumb trail reads HOME > PROJECTS > TORBROWSER. A secondary navigation bar lists various software and services: Software & Services: • Arm • Orbit • Tails • TorBirdy • Onionoo • Metrics Portal • Tor Cloud • Obfsproxy • Shadow • Tor2Web. The main content area is titled "What is the Tor Browser?" and includes a large graphic of the Tor logo with a globe. To the left of the text is a prominent purple "DOWNLOAD Tor Browser" button with a download icon. Below the button are links for "Installation Instructions" and "Windows • OS X • Linux". The text explains that the Tor software protects users by bouncing communications around a distributed network of relays run by volunteers, preventing surveillance and blocking access to certain sites. It also states that the Tor Browser allows using Tor on Windows, Mac OS X, or Linux without additional software, as it can run from a USB flash drive. A link to "Do you like what we do? Please consider making a donation" is provided. A section titled "Quick Videos on how to use the Tor Browser" contains a table with links to videos for downloading and using the browser on Windows, Apple OS X, Linux, and Non-OS specific systems. At the bottom, the "Tor Browser Downloads" section begins, with a note to download the file for the preferred language.

HOME > PROJECTS > TORBROWSER

Software & Services: • Arm • Orbit • Tails • TorBirdy • Onionoo • Metrics Portal • Tor Cloud • Obfsproxy • Shadow • Tor2Web

## What is the Tor Browser?

The **Tor** software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

The **Tor Browser** lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained.

Do you like what we do? Please consider making a donation »

### Quick Videos on how to use the Tor Browser

How to download and verify Tor Browser on:	Windows	Apple OS X	Linux
How to use Tor Browser:	Non-OS specific		

## Tor Browser Downloads

To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is

# Lancer le Tor Browser

A propos de Tor - Navigateur Tor

A propos de Tor

Saisir un terme à rechercher ou une adresse

Google

Le menu de l'oignon vert a maintenant un curseur de sécurité qui vous laisse ajuster votre niveau de sécurité. Découvrez le !

Ouvrir préférences de sécurité

Navigateur Tor 4.5



## Félicitations !

Ce navigateur est configuré pour utiliser Tor.

*Vous pouvez maintenant naviguer sur Internet de manière anonyme.*

[Tester les paramètres du réseau Tor](#)



### Que faire ensuite ?

Tor n'est PAS tout ce dont vous avez besoin pour assurer votre anonymat ! Vous devrez peut-être changer certaines de vos habitudes de navigation pour garder votre identité en sécurité.

[Conseils pour rester anonyme »](#)

### Vous pouvez aider !

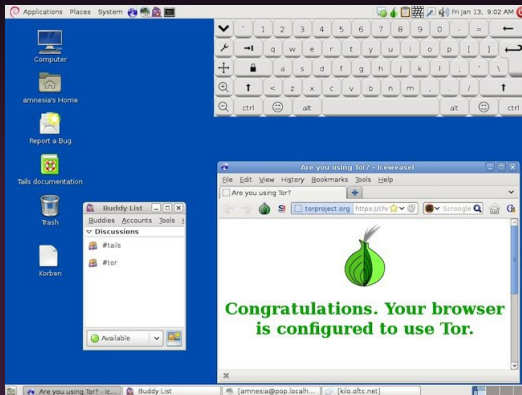
Vous pouvez aider à rendre le réseau Tor plus rapide et plus puissant de plusieurs manières :

- [Faire fonctionner un relai Tor »](#)
- [Devenir bénévole »](#)
- [Faire un don »](#)

Le projet Tor est une organisation à but non lucratif (US 501(c)(3)) dédiée à la recherche, le développement et l'éducation sur l'anonymat et la vie privée en ligne. [En savoir plus sur le projet Tor »](#)

# Utiliser Tor - Tails

Tails (The Amnesic Incognito Live System) est un système d'exploitation complet basé sur Linux et Debian, en live.



<https://tails.boom.org>



Café *vie privée*

Merci de votre attention.  
Place aux questions.



Me contacter?

Le Blog de Genma  
<http://genma.free.fr>

Twitter : @genma



# ANNEXES