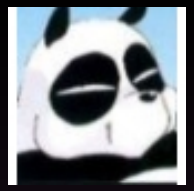
Ubuntu Party
Le chiffrement - introduction

Genma

15 novembre 2013



A propos de moi

Où me trouver sur Internet ?

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

Mes centres d'intérêts ?

Plein de choses dont :

- La veille technologique
- Le chiffrement

Ubuntu ? Depuis la version 4.10...

But de cette présentation

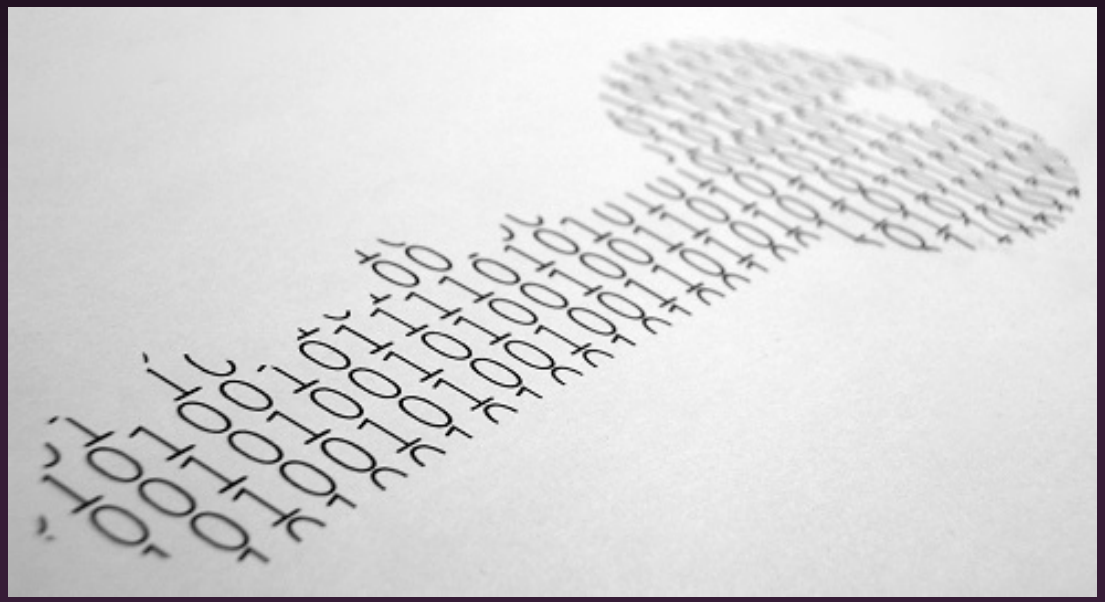
Ce que cette présentation est

Cette présentation est une introduction au chiffrement, à son rôle...
$\Rightarrow$ Son but est de lancer un débat sur le sujet.

Ce que cette présentation n'est pas

Un tutoriel sur le chiffrement de ses e-mails, de son disque dur, des ses communications.
$\Rightarrow$ Il y aura des ateliers pour ça.

Le chiffrement, c'est quoi ?



Définitions - cryptage, crypter, 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, comment ça se passe ?

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.

$\Rightarrow$ 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.

PGP, GPG ?

PGP

Pretty Good Privacy - PGP est un logiciel de chiffrement et de déchiffrement cryptographique, créé par l'américain Phil Zimmermann en 1991.

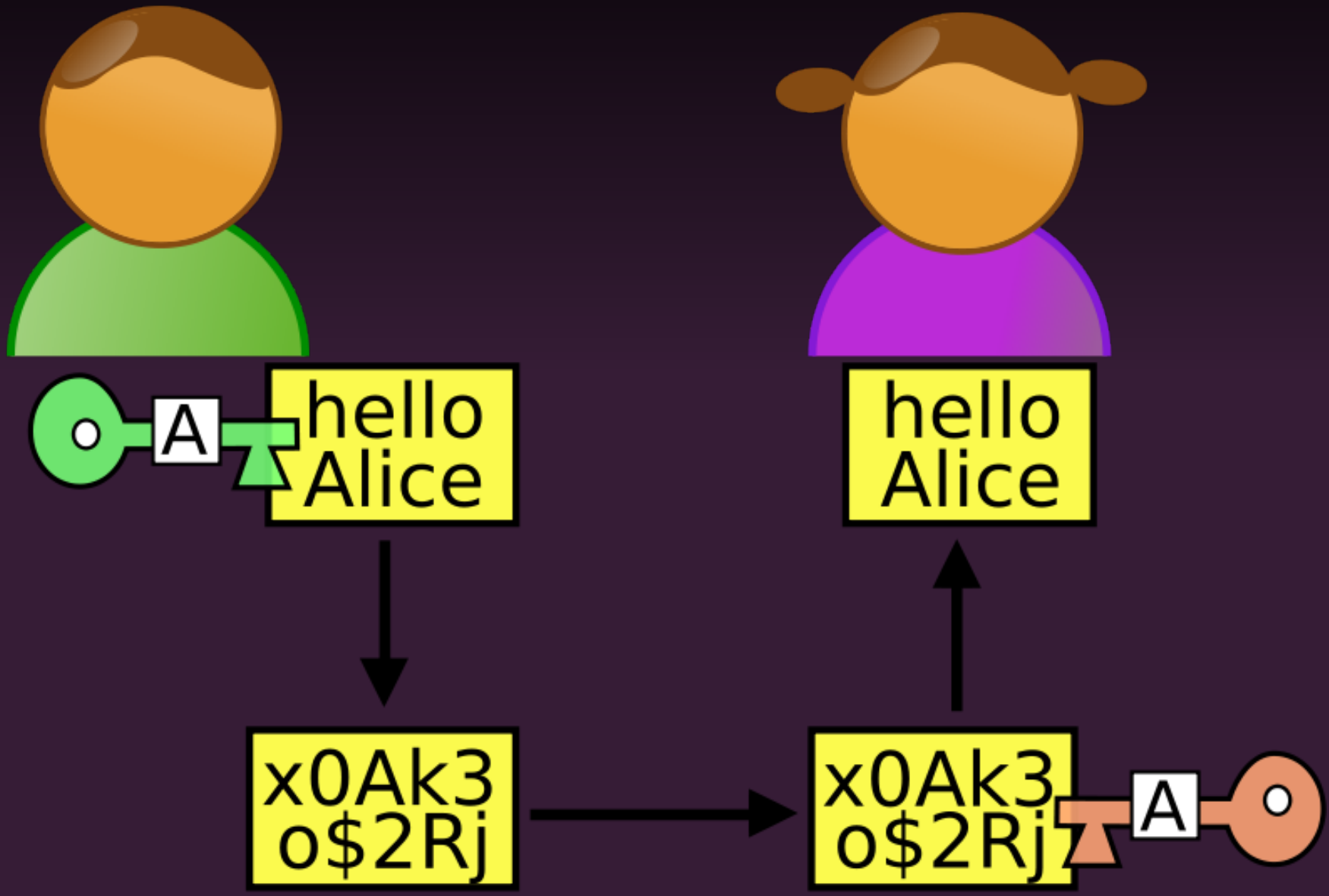
OpenPGP

Ce standard décrit le format des messages, signatures ou certificats que peuvent s'envoyer des logiciels comme GNU Privacy Guard. Ce n'est donc pas un logiciel, mais un format pour l'échange sécurisé de données, qui doit son nom au programme historique Pretty Good Privacy (PGP).

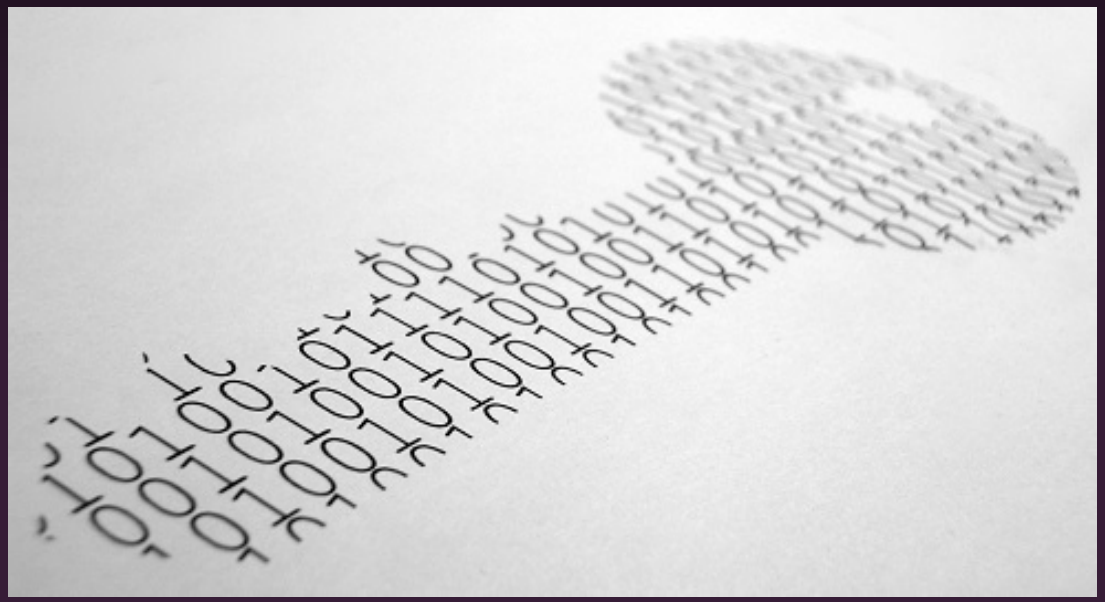
GnuPG

GnuPG (ou GPG, de l'anglais GNU Privacy Guard) est l'implémentation GNU du standard OpenPGP.

Bob envoit un message à Alice



Pourquoi chiffrer ?



Chiffrer - Les arguments contre

Personne ne le fait...

FAUX. Sans le savoir, vous le faîtes tous les jours.
Exemple 1 : "le cadenas" quand on se connecte
Exemple 2 : La clef du Wifi.

Je n'ai rien à cacher...

FAUX. Qui accepterait que le facteur lise son courrier médical ?

Le chiffrement, c'est pour les pédonazis de l'Internet...

FAUX. Cas des journalistes/blogueurs dissidents qui dénoncent des dictatures...

Chiffrer - Les arguments pour

Le chiffrement, ce n'est pas si compliqué

Ce n'est pas plus compliqué que d'utiliser un "logiciel" ; i faut comprendre le principe et c'est du clickodrome.

Protection et sécurité

Mes données personnelles, sensibles sont protégées. Cf. PRISM, NSA...

Confidentialité

Seule la personne à qui est destiné le "message" est en mesure de le lire.

Limites du chiffrement

Ce qui est chiffré aujourd'hui pourra être déchiffré demain

Les ordinateurs de demain pourront permettre de décrypter les données chiffrées aujourd'hui.

Si on perd la clef

On n'a plus accès aux données.

Métadonnées, graphe social

PGP ne protège pas contre l'analyse des métadonnée (serveurs de transit, adresses, headers, sujet). Ne pas oublier de nettoyer les métas-données des fichiers (tag EXIF des photos, documents de bureautiques avec le suivi des modifications). DNS, cas du tracking Internet...

Le chiffrement et la loi

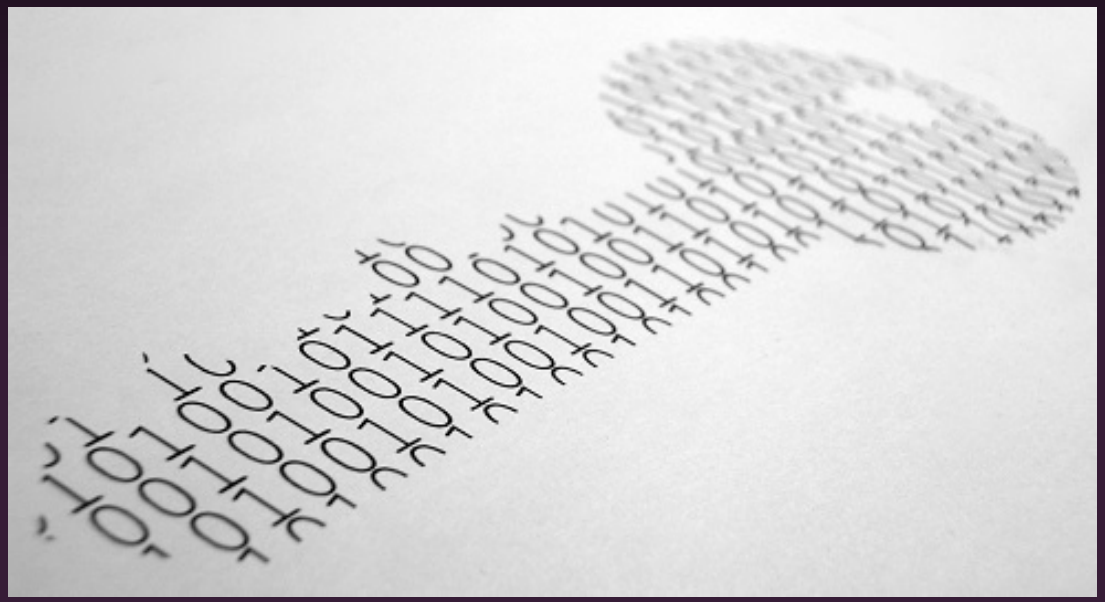
En France, la loi considère donc que l'utilisation de moyens de cryptologie est libre (LCEN article 30-1) et il n'y a donc, actuellement pas de limite à la taille de la clef de chiffrement que l'on peut utiliser.

En cas de perquisition,le refus de remise de la clef de chiffrement peut entraîner 3 ans d'emprisonnement ainsi que 45000€ d'amende.

Cette peine est aggravée dans le cas où le chiffrement a été utilisé pour commettre un délit.

Il est donc recommandé de donner la clef de déchiffrement, sauf dans le cas où les données déchiffrées entrainerait une procédure judiciaire dont la peine finale serait supérieure à celle de l'entrave à l'enquête judiciaire.

Quoi et comment chiffrer ?



Quoi et comment chiffrer ?

En local - ses données

- Son disque dur
- Sa clef USB
- Son smartphone

En réseau - ses communications

- Https : utilisation de l'extension HTTPSEveryWhere pour Firefox
- Ses e-mails : utilisation de GPG via Enigmail pour Thunderbird
- Sa connexion : utiliser un VPN, SSH, la clef "WIFI".

$\Rightarrow$ À chaque "usage", il y a une solution de chiffrement possible.

Mise en pratique aujourd'hui et demain

Clefs PGP et chiffrement des mails

- Création et gestion de ses clefs avec Seahorse
- Utilisation d'Enigmail et Thunderbird
- Signature des clefs

TrueCrypt, chiffrement des disques durs et clefs USB

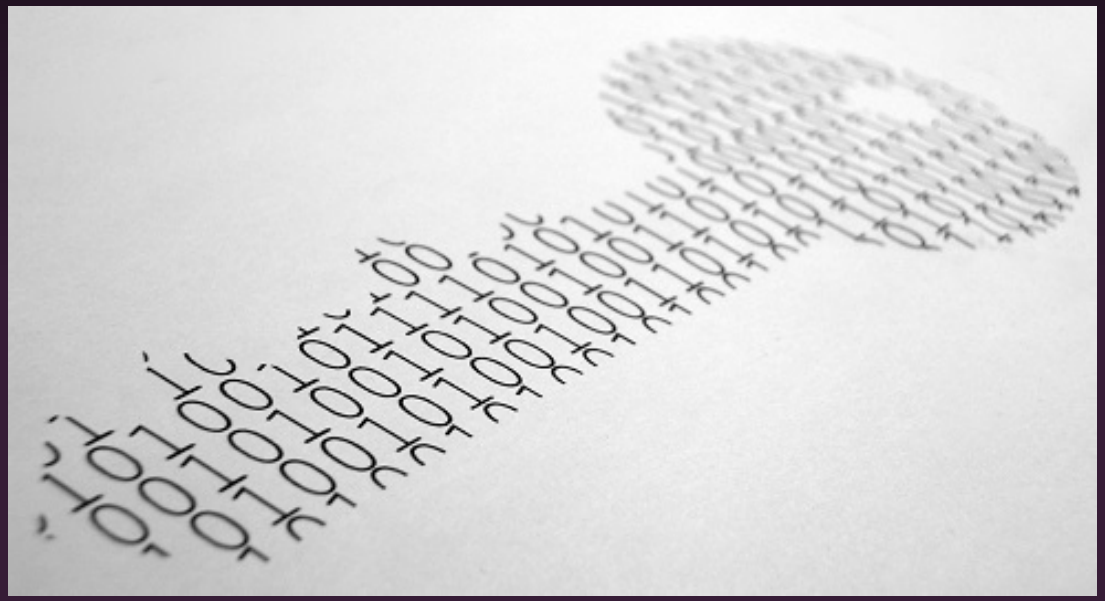
- Installation de TrueCrypt
- Création de volume TrueCrypt

Tor

- TorBrowser Bundle
- TAILS : Live cd-debian avec Tor

Vous êtes attendus - les bienvenus pour discuter, tester, essayer...

Conclusion



Conclusion

Chiffrer est légal et n'est pas réservé aux paranoïaques.

Chiffrer devient une nécessite dans un monde où les communications sont surveillées.

Chiffrer permet de protéger ses données et de se protéger.

Edward Snowden

Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.

Le chiffrement fonctionne. Correctement mis en œuvre, les systèmes cryptographiques forts sont l'une des rares choses sur lesquelles vous pouvez compter.

Merci de votre attention.
Place aux questions. Débattons...

Et toi tu chiffres ?

Genma Kun - Le blog de Genma

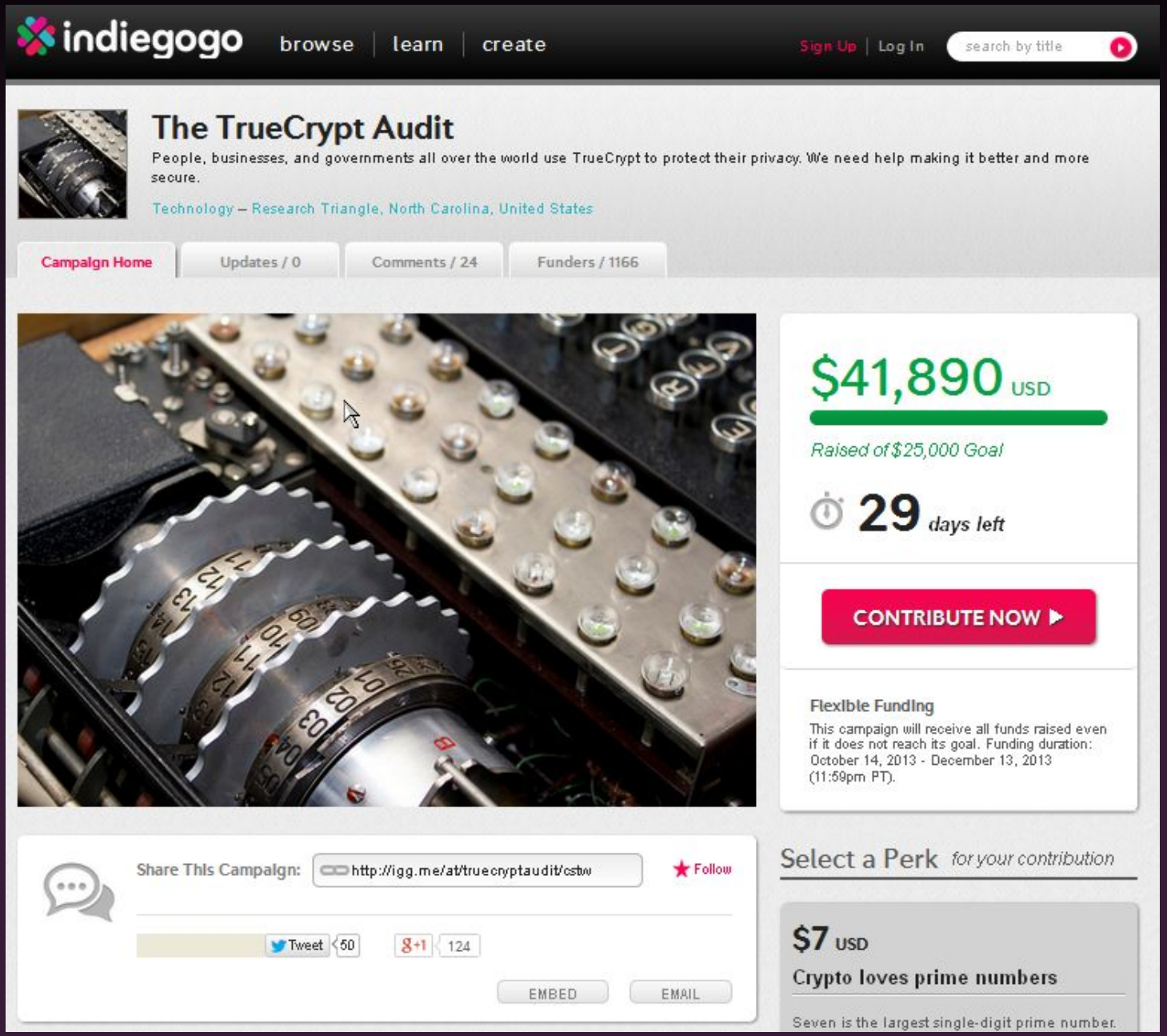
http://genma.free.fr

genma@riseup.net ; genma@free.fr

4096 bits RSA; Key-ID: 5AA Created: 2013-08-09

F520 6815 EEB3 E0E2 66E9

L'audit de TrueCrypt



Le crypto-anarchisme

Tout le monde chiffre et ce qui est vraiment important est chiffré et noyé dans la masse.

On crée du bruit ce qui empêche la surveillance de masse (Affaire PRISM...)

Attention, à l'heure actuel, le chiffrement étant peu répandu, toute personne qui chiffre ses e-mails pourra être considérée comme suspecte.

Chiffrer son disque dur

Logiciels intégrés aux systèmes d'exploitations

- Windows 7/8 : Bitlocker
- MacOS : FileVault
- GNU/Linux : Encfs

Indépendament du système d'exploitation

$\Rightarrow$ Le logiciel TrueCrypt. Pour une clef USB/un disque dur externe.

Annexes

La fonction de hashage

- Un hash est une fonction à sens unique permettant le calcul d'une empreinte.
- C'est une somme de contrôle qui permet de vérifier l'intégrité d'un fichier.
- C'est une façon de cacher quelque chose.

La phrase « Nous venons en paix »devient
9d6bd655e000f83685d64affde380a3d94a62d47d42d80a0be11a4bb4c6ee324