

La sécurité numérique et vous ?

Pascal Lafourcade

*Chaire industrielle,
Confiance numérique*



10 Novembre 2015



La sécurité numérique est déjà là



Mais prendre de bonnes habitudes ça prends du temps ...



même quand c'est important

Devenir acteur de sa sécurité numérique

Devenir acteur de sa sécurité numérique
car la sécurité c'est pas automatique.

Devenir acteur de sa sécurité numérique
car la sécurité c'est pas automatique.

Passwords

Emails

Octobre 2014



L'importance de la vie privée

Why privacy matters?

Par Glenn Greenwald

<http://jenairienacacher.fr>



Sécurité de mes mots de passe



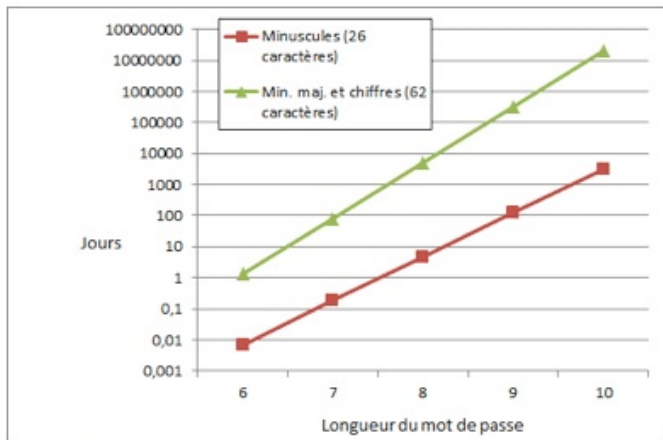
Sécurité de mes mots de passe



Top 25 en 2014

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 123456789
7. 1234
8. baseball
9. dragon
10. football
11. 1234567
12. monkey
13. letmein
14. abc123
15. 111111
16. mustang
17. access
18. shadow
19. master
20. michael
21. superman
22. 696969
23. 123123
24. batman
25. trustno1

Passwords: Brute force



Quelques conseils

Un mot de passe

1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il est jamais assez sophistiqué
7. la taille compte.

Quelques conseils

Un mot de passe

1. ne se prête pas
2. ne se laisse pas traîner
3. ne s'utilise qu'une fois
4. s'il est cassé, il faut en changer
5. il faut en changer régulièrement
6. il est jamais assez sophistiqué
7. la taille compte.



La sécurité des emails par défaut



La sécurité des emails par défaut



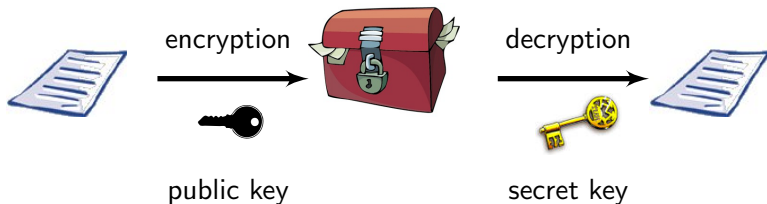
Première demande d'E. Snowden ...



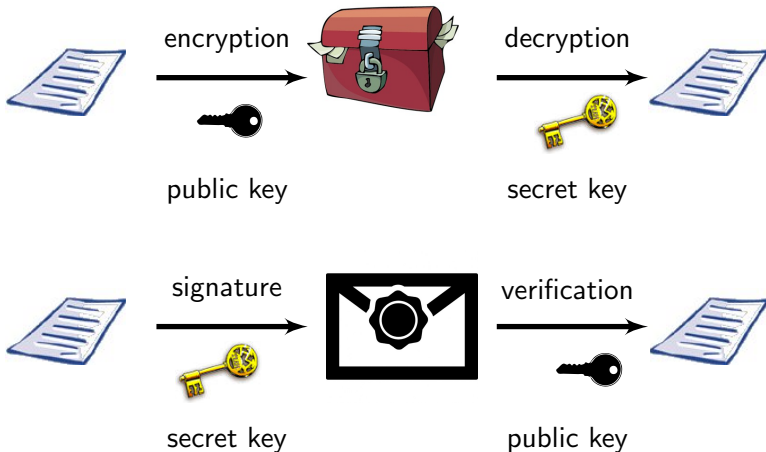
```
manesia@manesia: ~$ gpg -d
-----BEGIN PGP MESSAGE-----
h0IPABxdLvrAJngTAg/+LbH9jS2GCFp/TIcTPlRpS/Mwx5/HI ru/NKBnB14RHe/A
K50aPS0IKESlABE 1u0h4r4dmtz591 pmHhWvYVh31p0EGTPVc-WehWt 2X0Ul 5
KP20eQvLWZx rP02c4P2HvJ30aRq/MQF 15XhT r0u1u0pJj 9J2F rKMuUCMj) sNoEp
Y7Ak2S3nblHVr0BGI2lFAF8lj 1v125j flt/rPe/B1o0V0epumx0Lw1L1cd2ME90
5yJlRv mWfOSUFLh9HRCAu9wLsgj yqVq1 1yq2NnU50G0MBQAF0P1K2 Hb1F29X
vXMeV0V44ATZj 7E190RAD0ozII08LQ0oI AAvgT23Me1B7VaZPUnUI0x5R0J90BR
H3oIBTf6h6nLRI Tzn1kJANvE 1M/dX0g0FgJNE500Gx2o30rvrEKL5-hnE Ixyn0G8x9
F0vABTDun JnTzYGRlnlBEVksSVRxsDouT7B2e0LE1WUdh1c1UpoTJxvcZlZUw/fLc
SFYhN+TcHhDUA+n60TxD02ZnqPVB56x4WUyVdfac 5pGubtk0D-wbcHr TC7B25
ecsvByPPmjC/CE4168p0e 1w0AL1To2j+nepYwf1 30epKdmf0p5t5A00tcj WpPLeg
hhpChgFXP2NI J04CD4BLCoE#9OUJ2+VAl50j 5Pp0ELkP-wTN0L2lHh+fg00975-
ggFDn/M+LFC0duKp0kAGwEHL4FBWj 7BD0Axs5/bxpHZKE vnaV1 QwUG9HVTvnc
```

... utiliser PGP

Chiffrement à clef publique et signature



Chiffrement à clef publique et signature



Logiciel de chiffrement, déchiffrement, signature de courriers électroniques, inventé par Phil Zimmermann en 1991 (RFC 4880)

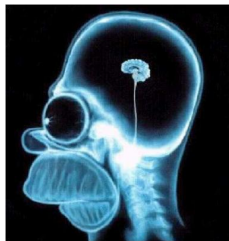


*Si la vie privée est mise hors la loi,
seuls les hors-la-loi auront une vie privée.*

If privacy is outlawed, only outlaws will have privacy

Est-ce si difficile ?

1. Télécharger l'outil GPG et l'installer.
2. Générer une paire de clefs ≥ 4096 bits
3. Importer votre clefs
4. Télécharger les clefs de vos amis
5. Envoyer des emails chiffrés.



Pour résumer

1. CHOISIR des mots de passes SÛRS.
2. AVOIR une clef PGP
3. SIGNER ses emails et CHIFFRER ses emails
4. AVOIR la LIBERTÉ de communiquer de manière sécurisée

Pour résumer

1. CHOISIR des mots de passes SÛRS.
2. AVOIR une clef PGP
3. SIGNER ses emails et CHIFFRER ses emails
4. AVOIR la LIBERTÉ de communiquer de manière sécurisée

Devenez acteur de la sécurité de votre vie numérique

Merci pour votre attention
Questions ?

Master • Ecoles d'ingénieurs

Architectures PKI et communications sécurisées

