La cryptographie de l'Antiquité à nos jours

Pascal Lafourcade

Chaire industrielle,
Confiance numérique

LIMOS

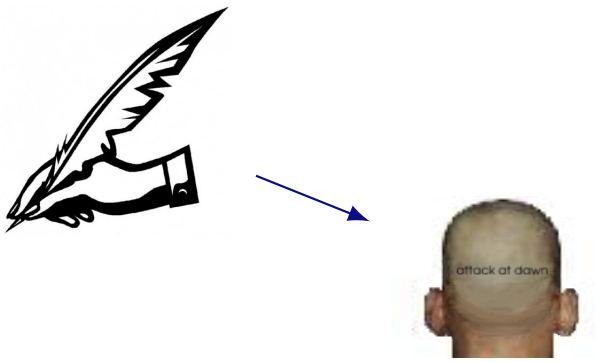
UdA

UNIVERSITÉ
Clermont Auvergne
& associés

1 Mars 2016

L'art de cacher un secret écrit

L'art de cacher un secret écrit



Stéganographie

L'art de cacher un secret écrit

Cryptographie

Stéganographie

L'art de cacher un secret écrit

Cryptographie

Transposition

Stéganographie

L'art de cacher un secret écrit

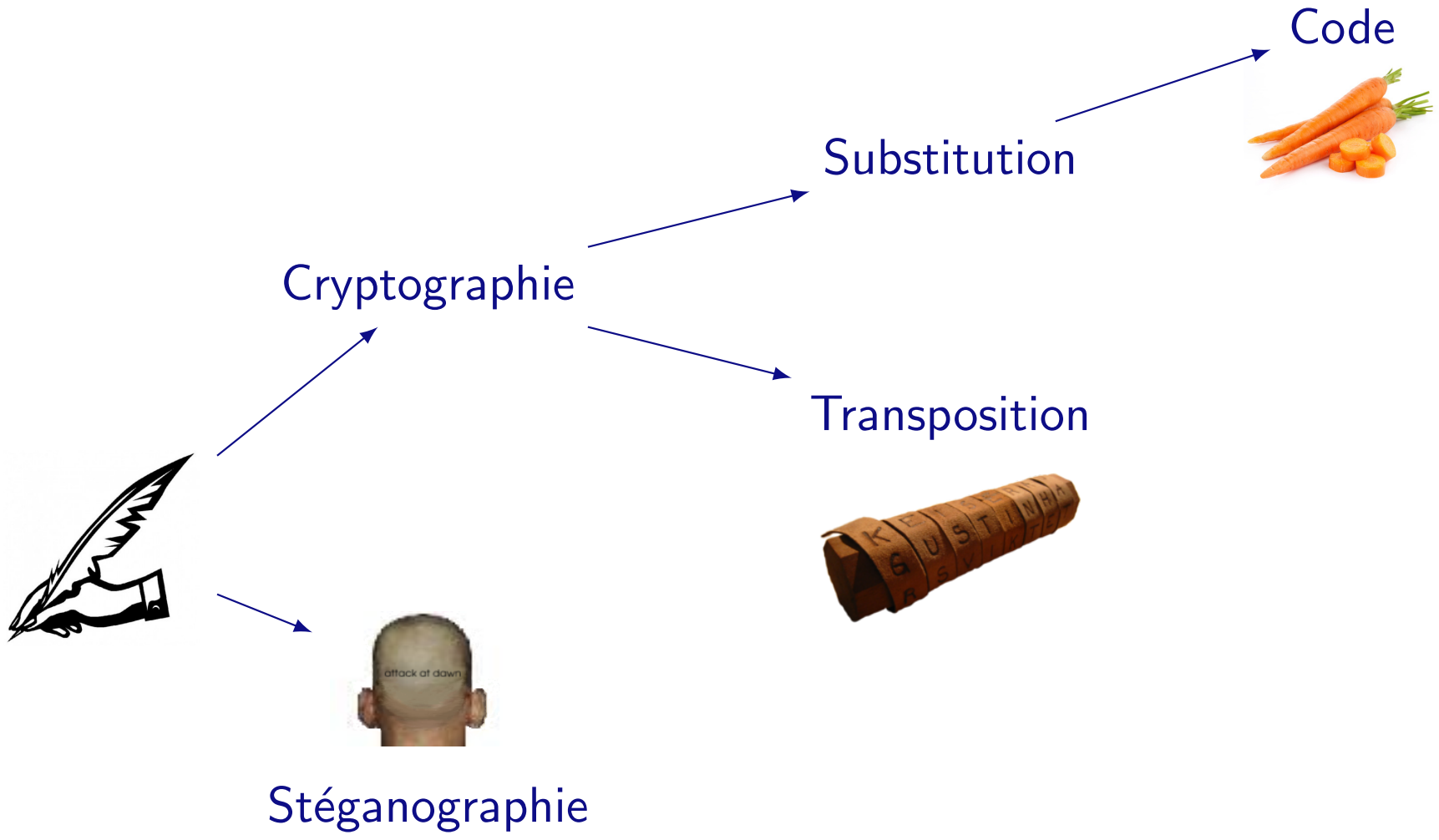
Substitution

Cryptographie

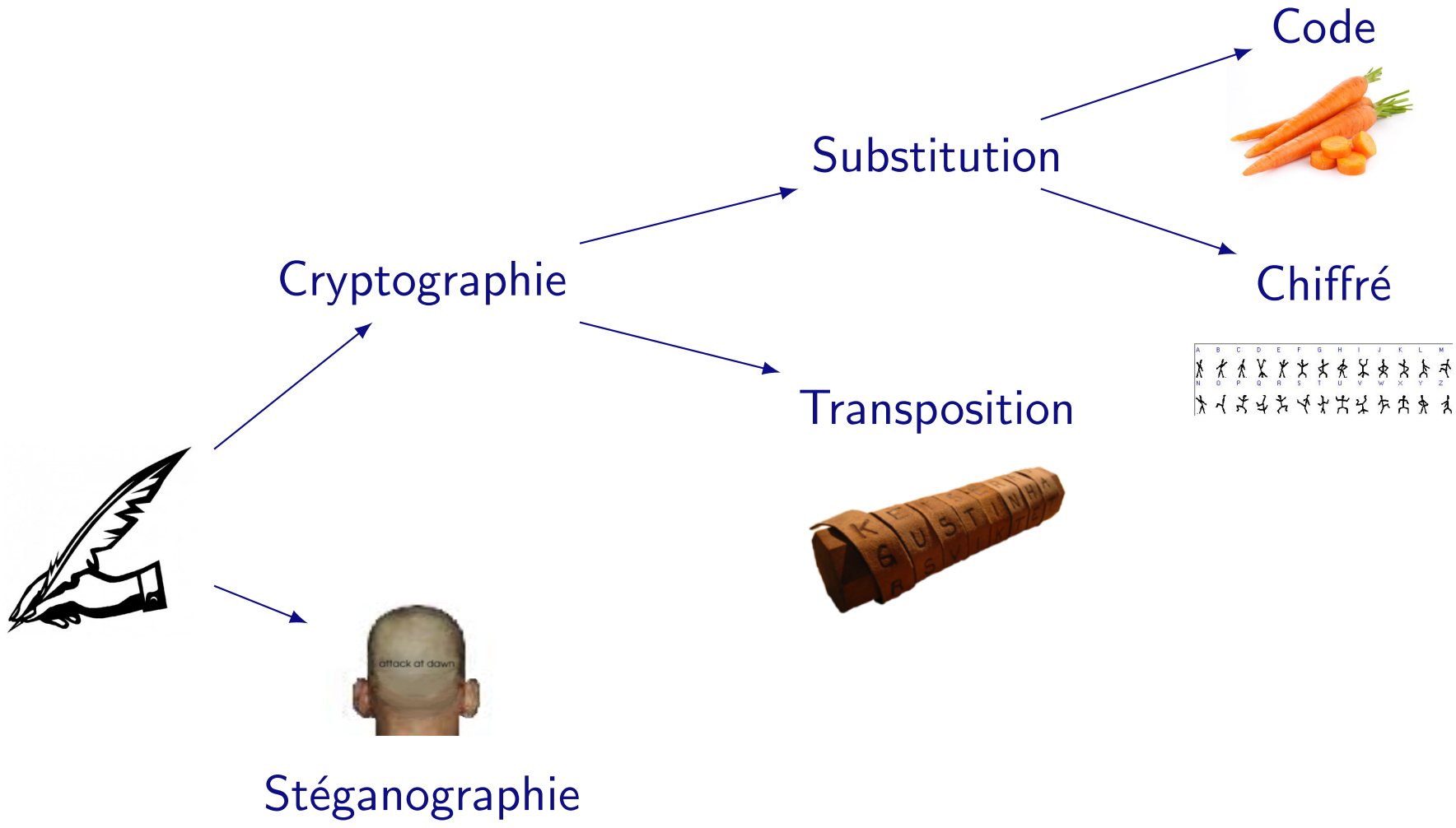
Transposition

Stéganographie

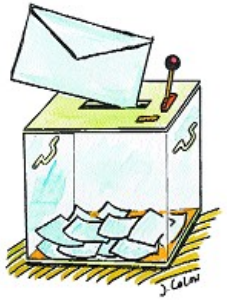
L'art de cacher un secret écrit



L'art de cacher un secret écrit



Applications



Plan

Plan

Plan

Plan

Plan

Plan

Il y a très longtemps

Les grecs

Les grecs

Transposition

Les Romains

Chiffrement de César
Substitution +3

Les Romains

Chiffrement de César
Substitution +3

Dyh Fhvdu

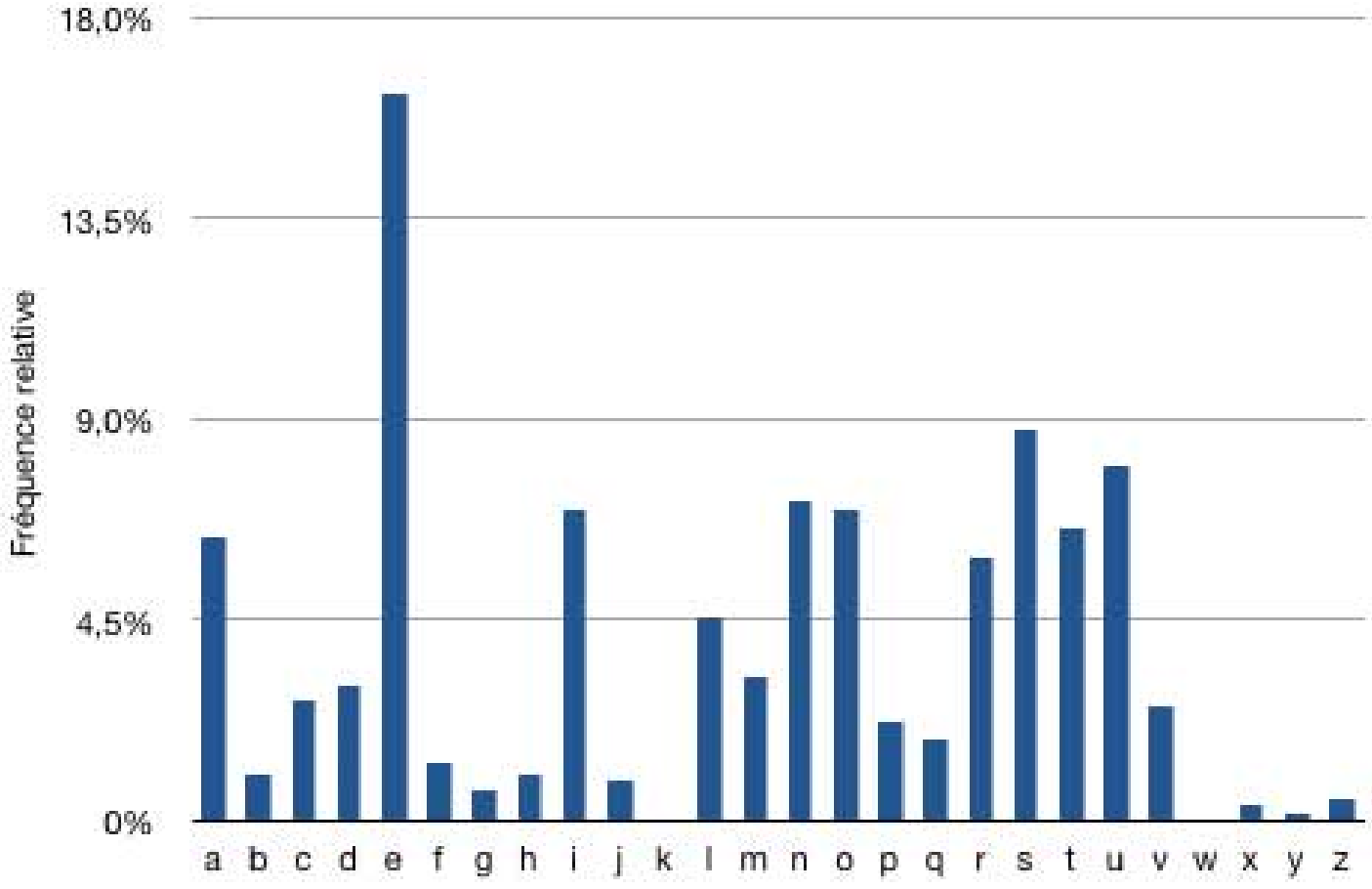
Les Romains

Chiffrement de César
Substitution +3

Dyh Fhvdu
Ave Cesar

Est-ce sûr?

Est-ce sûr?



Analyse de fréquences

Substitution polyalphabetique (Alberti, Vigenère 1553)

Exemple avec la clef k = 3,7,10

m = CON NAI TRE

Substitution polyalphabetique (Alberti, Vigenère 1553)

Exemple avec la clef k = 3,7,10

$$m = \text{CON NAI TRE}$$

$$E_k(m) = \text{FVX QHS WYO}$$

Chiffrement : Enigma (Seconde guerre mondiale)


+

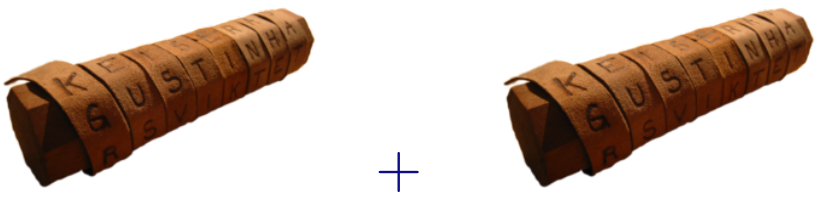
=

Chiffrement : Enigma (Seconde guerre mondiale)


+

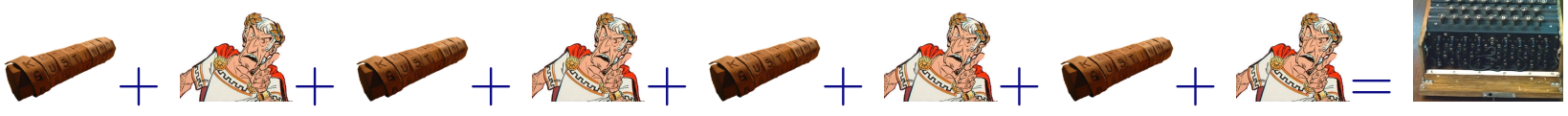
=


Chiffrement : Enigma (Seconde guerre mondiale)



Chiffrement : Enigma (Seconde guerre mondiale)

Chiffrement : Enigma (Seconde guerre mondiale)



One-Time Pad (Chiffrement de Vernam 1917)

Exemple:

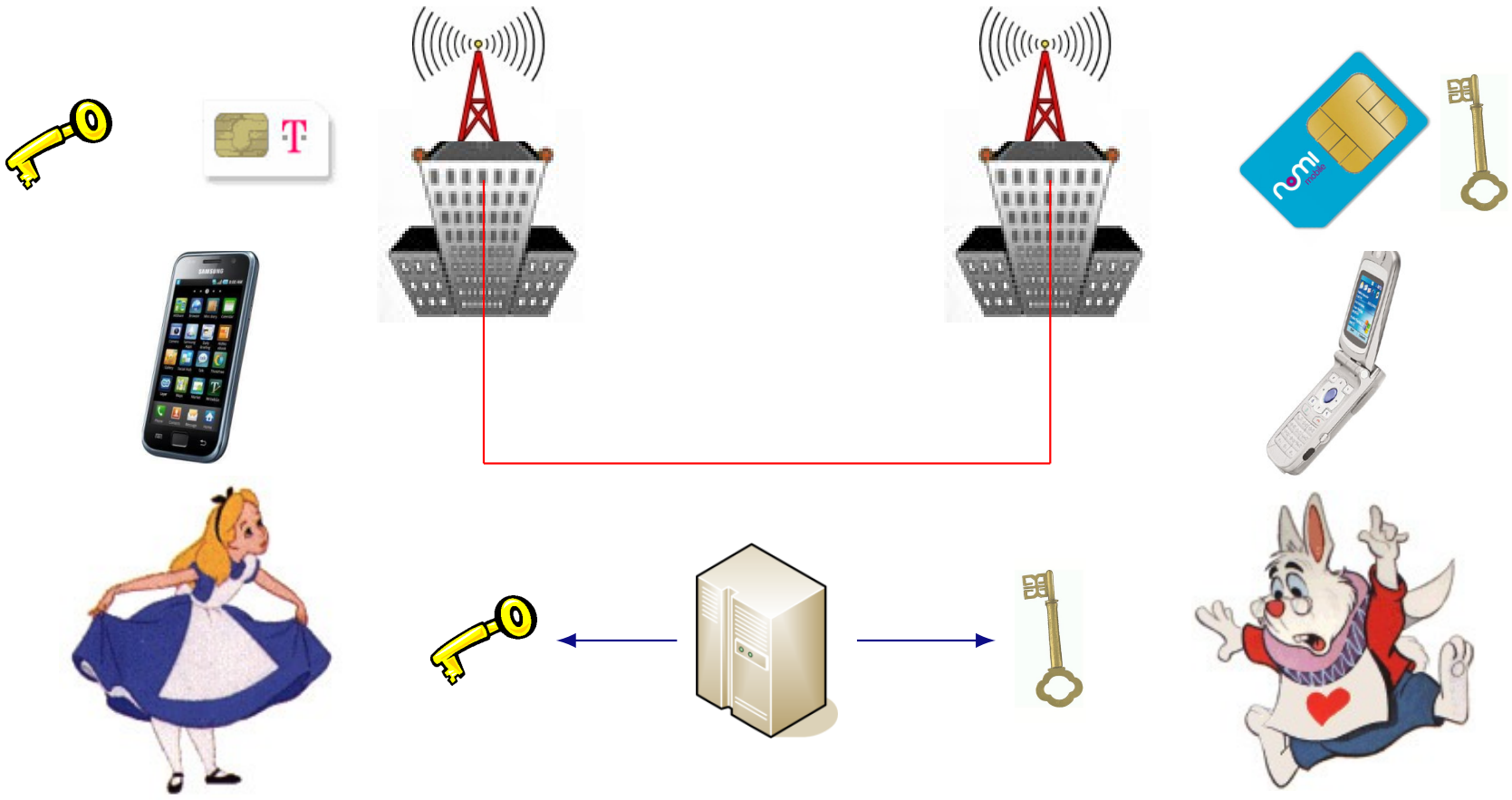
$$\begin{array}{rcl} m & = & 010111 \\ k & = & 110010 \\ \hline c & = & 100101 \end{array}$$

Clef symétrique

Exemples

- DES
- AES

Communications téléphoniques

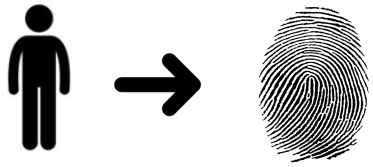


Chiffrement à clef publique

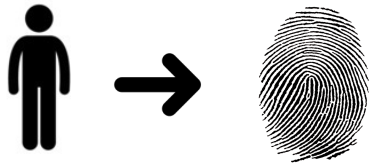
Exemples

- RSA : $c = m^e \mod n$
- ElGamal : $c \equiv (g^r, h^r \cdot m)$

Fonction de Hachage (SHA-1, SHA-3)

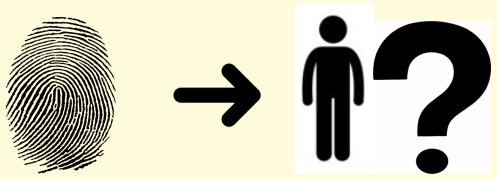


Fonction de Hachage (SHA-1, SHA-3)

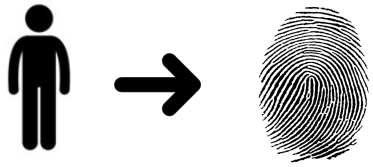


Propriétés de résitance

- Pré-image

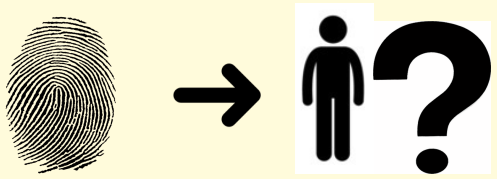


Fonction de Hachage (SHA-1, SHA-3)

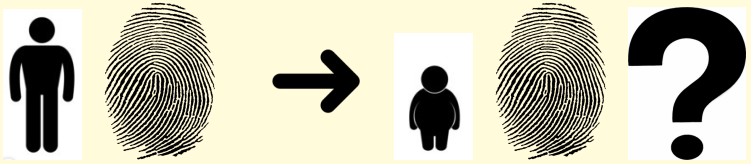


Propriétés de résitance

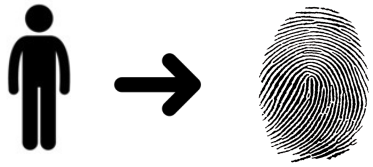
- Pré-image



- Seconde Pré-image

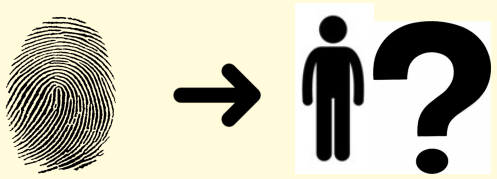


Fonction de Hachage (SHA-1, SHA-3)

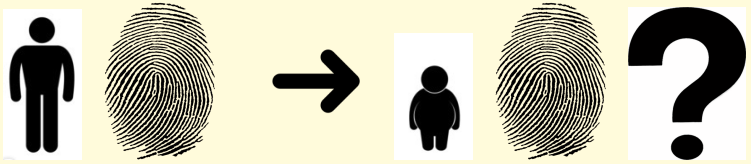


Propriétés de résitance

- Pré-image

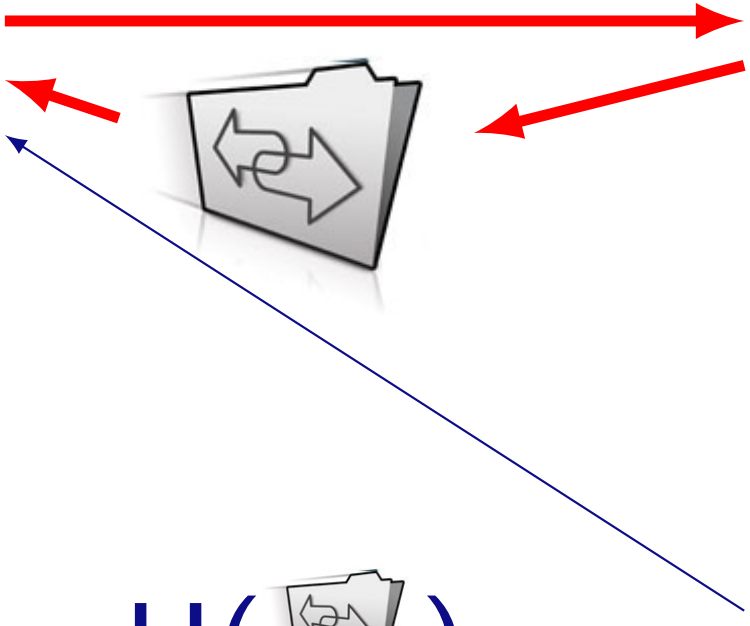


- Seconde Pré-image



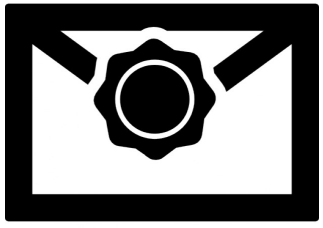
- Collision

Installation de logiciel

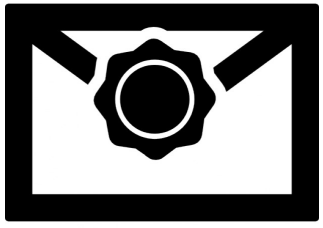


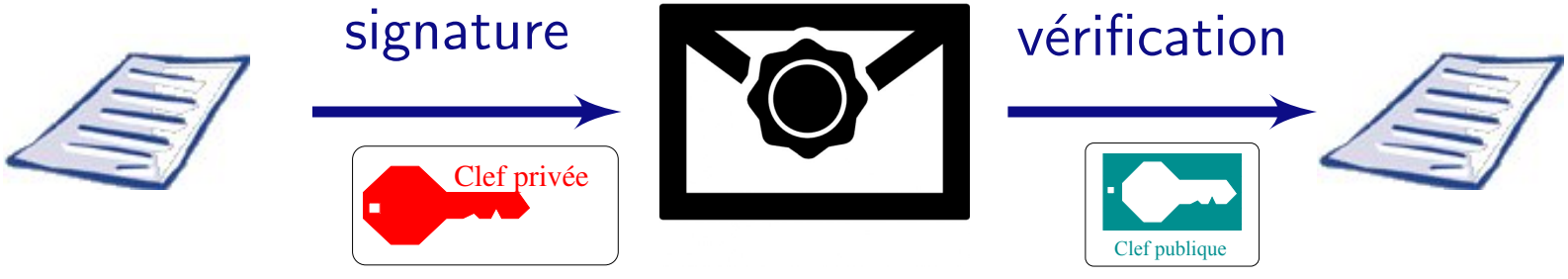
H()

Signature



Signature





RSA: $m^d \mod n$

Application : éviter la "*fraude au président*"

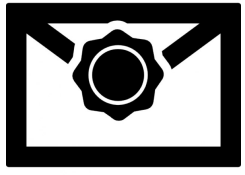
- En 2010 $>$ 485 millions d'euros
- En 5 ans 2.300 plaintes ont été déposées,

Application : éviter la "*fraude au président*"

- En 2010 $>$ 485 millions d'euros
- En 5 ans 2.300 plaintes ont été déposées,

Application : éviter la "*fraude au président*"

- En 2010 $>$ 485 millions d'euros
- En 5 ans 2.300 plaintes ont été déposées,

Solution : 

Plan

Secret ou Confidentialité

Secret ou Confidentialité

Secret ou Confidentialité

Authentication

"On the Internet, nobody knows you're a dog."

Mécanismes d'authentification

1. 

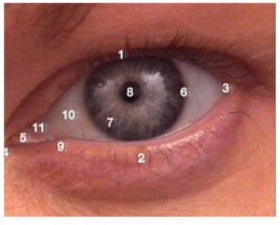
Mécanismes d'authentification

1. 

2. 

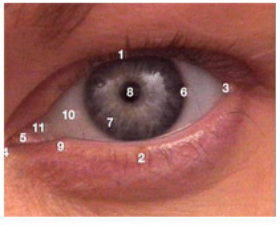
Mécanismes d'authentification

1. 

2. 
3. 

Mécanismes d'authentification

1. 

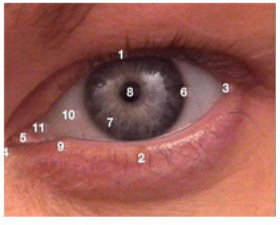
2. 
3. 


4. 

Mécanismes d'authentification

1. 

2. 

3. 


4. 

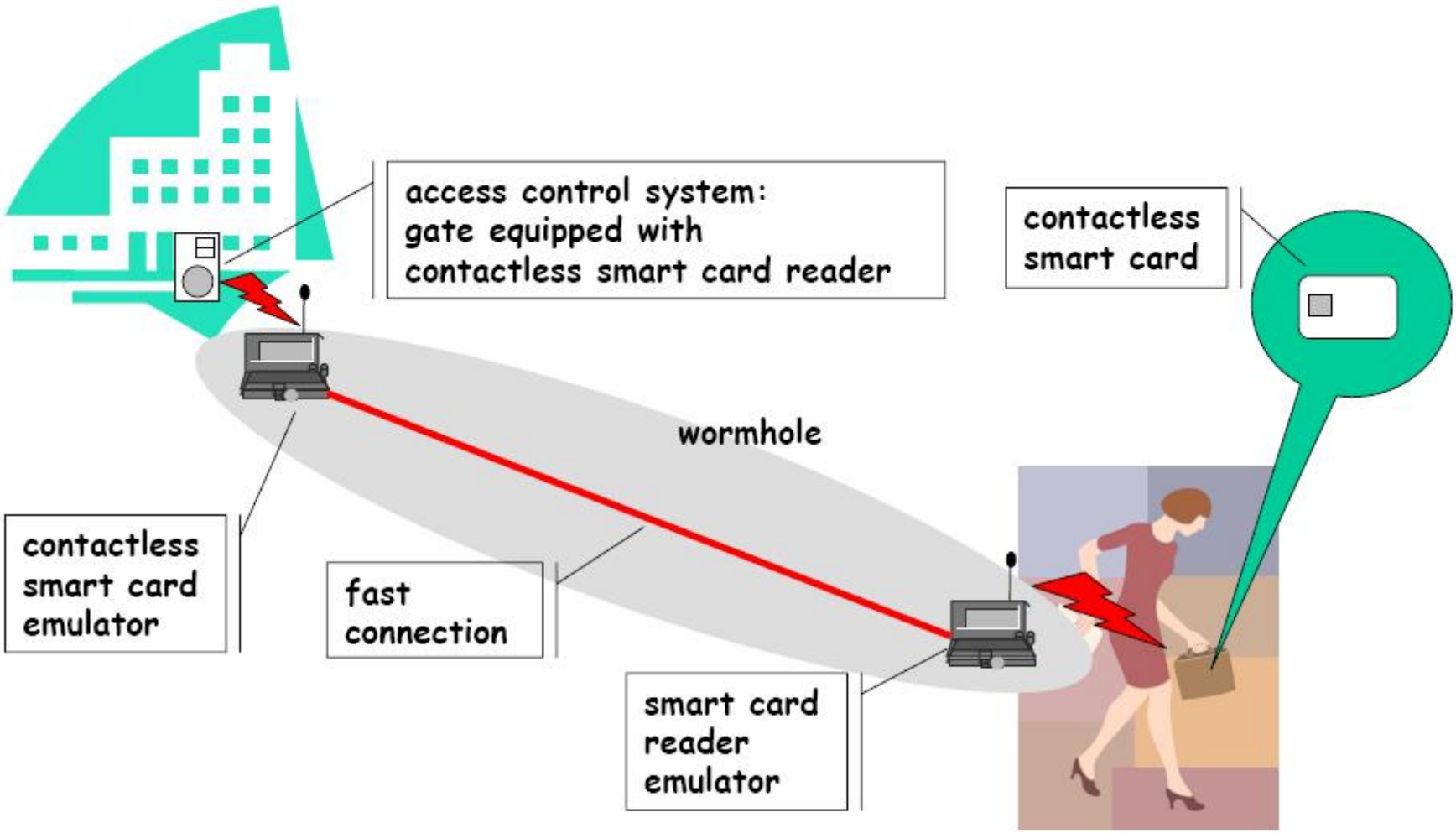
Authentification forte

Autre propriétés

- Integrité
- Disponibilité
- Non-repudiation
- Privacy
- Équité ...

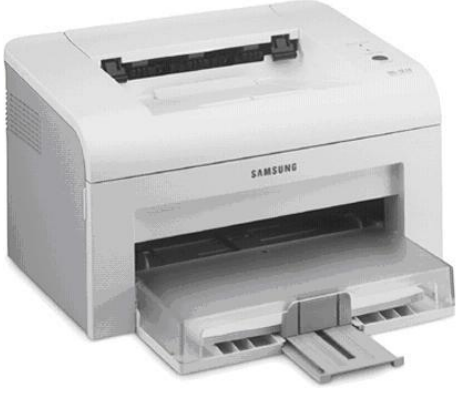
Plan

Wormhole Attack



Attaques sur des objects connectés IoT



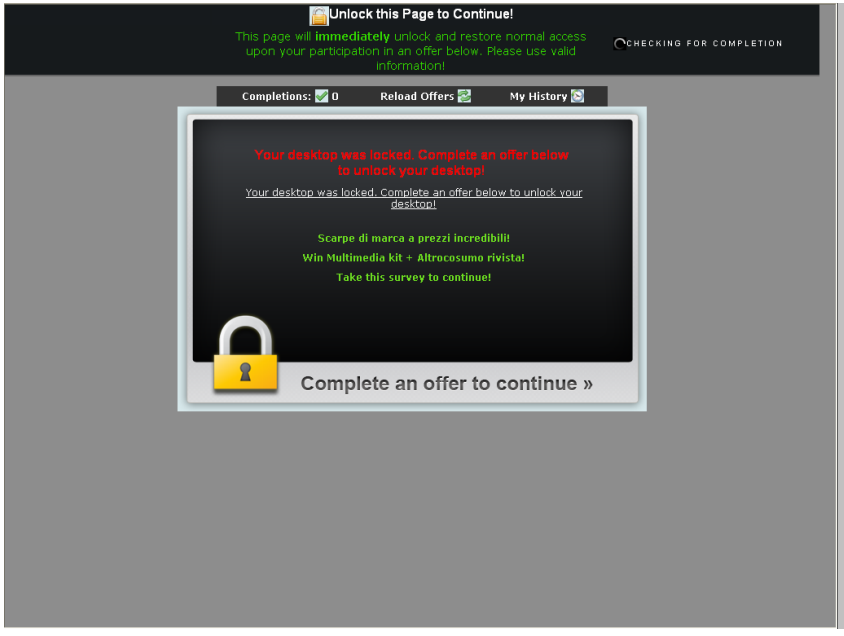



Séminaire Confiance numérique : 7 avril 14h00 Amphi B IUT

5 Familles de cyber criminalité

- Ransomwares
- Phishing
- Botnets et zombies
- Espionnage
- Sabotage

Ransomwares



http://stopransomware.fr/

Hameçonnage (Phising)

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

http://www.societegenerale.fr/espaceclient:
id=56452575711&res=lorem-ipsum-dolor&quux=2&lang=
frsessid=
jP3ie3qjSebbZRsC0c9dpcLVe2cAh0sCza3jcX7mSuRzwY4N0v1DBB71DMk
88.132.11.17

Botnets et Zombies

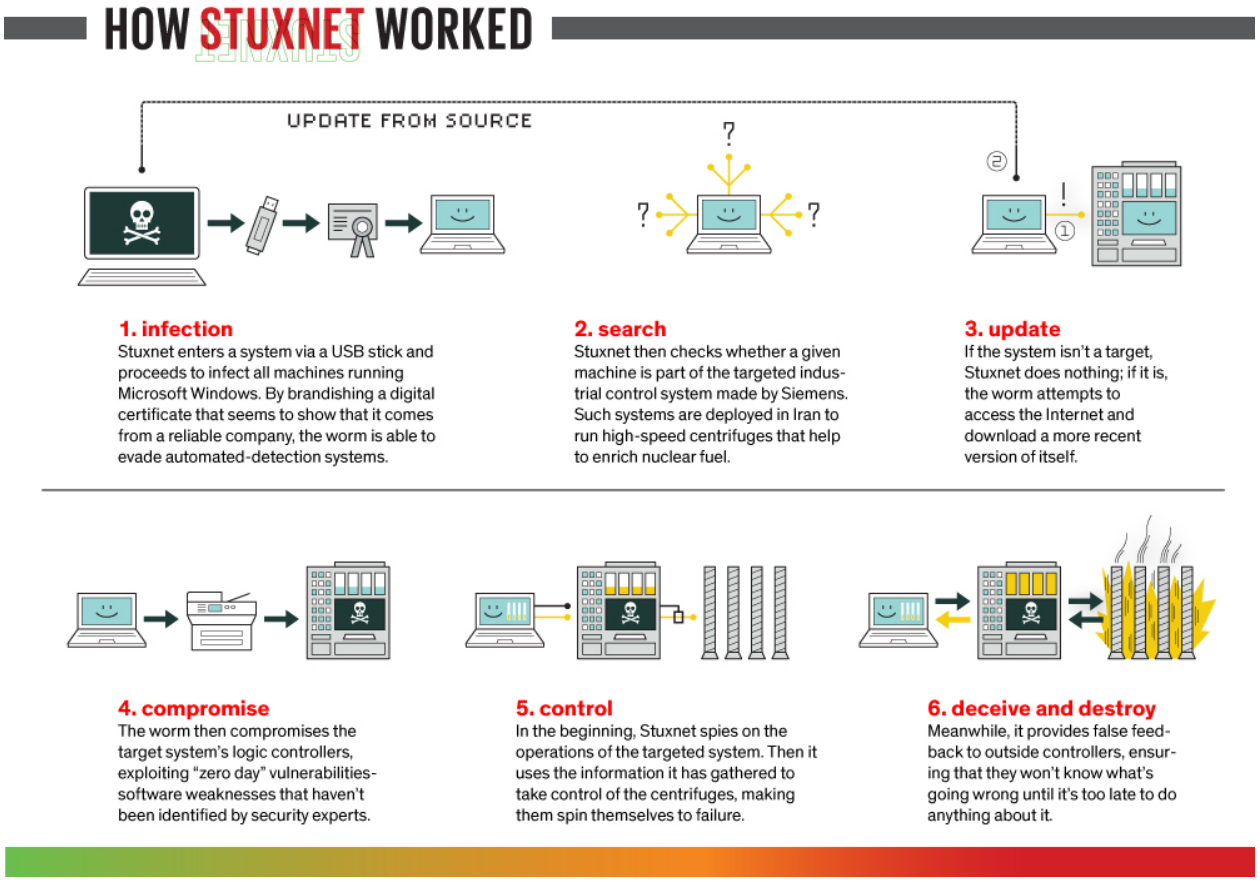
Espionnage

- Big Brother (Gouvernement)
- Medium Brother (Entreprise)
- Little Brother (Individu)

Edward Joseph Snowden, 6th june 2013

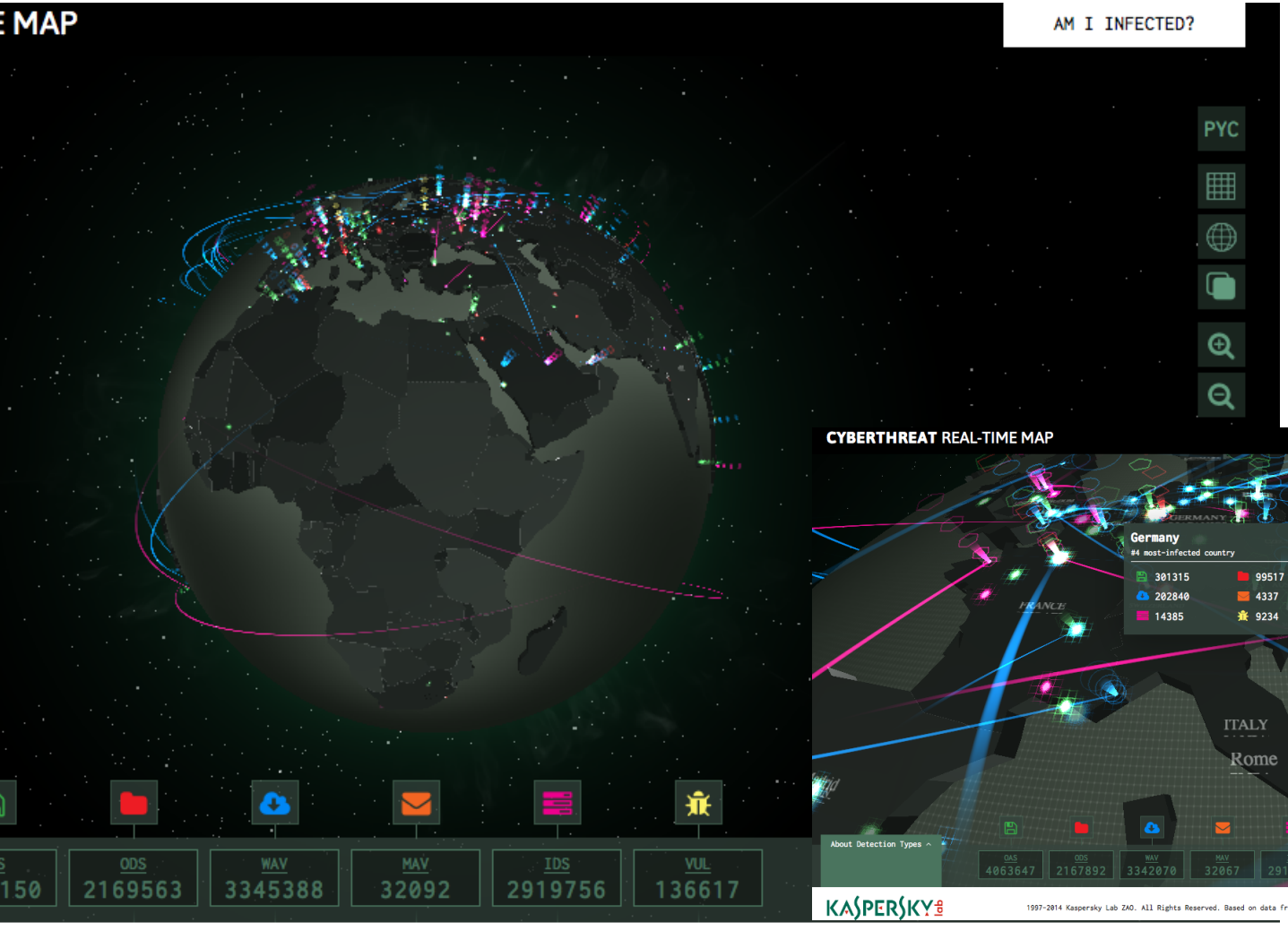
Sabotage

Stuxnet, 2010



Saudi Aramco 30 000 PC effacés.

http://cybermap.kaspersky.com/



Pourquoi y-a-t-il de plus en plus d'attaques?

- Faisable à la maison
- Peu cher, self-service
- Rapide, large échelle, semi-automatique
- Fausse impression d'être anonyme

Pourquoi y-a-t-il de plus en plus d'attaques?

- Faisable à la maison
- Peu cher, self-service
- Rapide, large échelle, semi-automatique
- Fausse impression d'être anonyme

HyperText Transfer Protocol

Pourquoi y-a-t-il de plus en plus d'attaques?

- Faisable à la maison
- Peu cher, self-service
- Rapide, large échelle, semi-automatique
- Fausse impression d'être anonyme

HyperText Transfer Protocol

Internet a été conçu pour fonctionner

Pourquoi y-a-t-il de plus en plus d'attaques?

- Faisable à la maison
- Peu cher, self-service
- Rapide, large échelle, semi-automatique
- Fausse impression d'être anonyme

HyperText Transfer Protocol

Internet a été conçu pour fonctionner

Pas pour être sûr !

Plan

La sécurité numérique est déjà là

Mais prendre de bonnes habitudes ça prend 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.

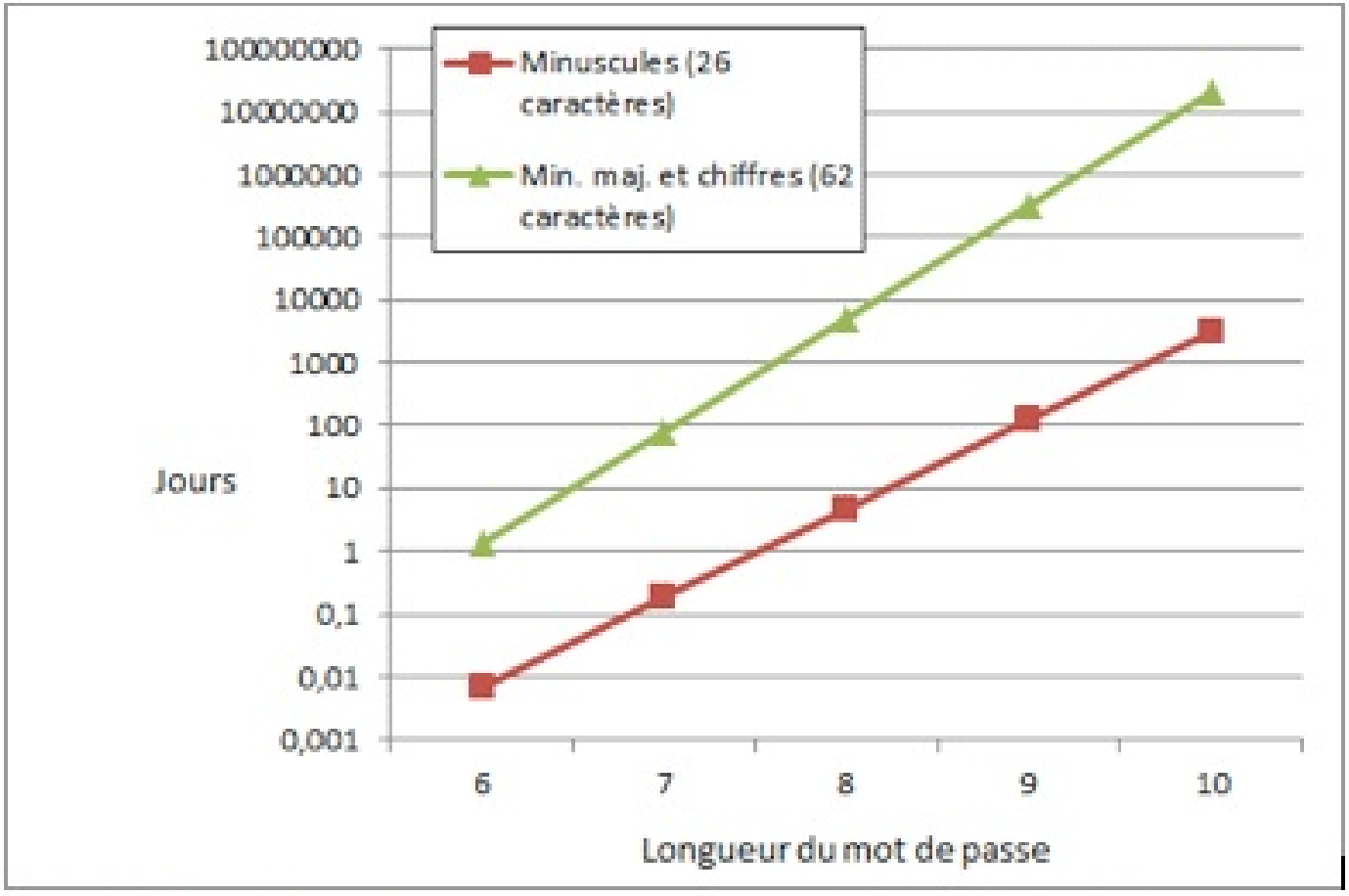
Sécurité de mes mots de passe

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.

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.

Exposé de Vincent Mazenod

Se protéger avec de bons mots de passe

`http://confiance-numerique.clermont-universite.fr/`

Plan

Octobre 2014

TED
Ideas worth spreading

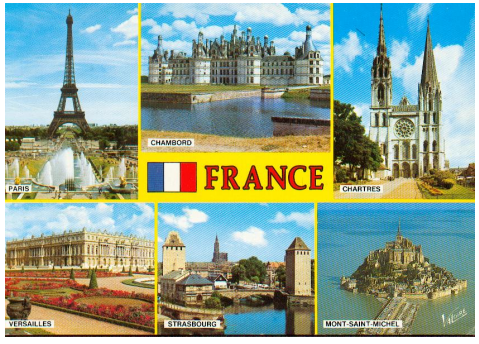
L'importance de la vie privée
Why privacy matters?

Par Glenn Greenwald

Les gens pensent ne rien avoir à cacher ...

`http://jenairienacacher.fr/`

La sécurité des emails par défaut



Première demande d'E. Snowden ...

```
amnesia@amnesia:~$ gpg -d

-----BEGIN PGP MESSAGE-----

hQIMA8xdLvrAJNGTAQ/+LbHB9i52GCPFjTICIP1RPs/WWx5/MIruNKBmB14RHe/A
KsDa/SO1KE5la8ETuDh4r4nQmtZ59TjnmIXHKyRvMo3ipQEGTPvEwNIwdI2X9Uls
KPa2oqQcWLzxrP0Zc4PzNvjXgarq/NQFlSXHtrRhiUdPij93ZFrKMxUCMOjsNOEp
Y7Ak2SY3nbiHVr0BgIZ1FaF8ljiviZSjflt/pE/81qOvQepumXOlwA1Ltcd2ME9o
5yJ1RVrnWf0SUFLh9HRCAu9wVLsgjyqVqi1yqZNnUSOGDWBKqAFDPIKz+uBiF29X
vXMeV0V44ATZj7ET9DRAOAozII08LQoQIAAvgTZ3MzIB7VaZPUnU1DxcSROJ90bR
H3oIBfH6nLRITZnlkJaNvE1M/dXDgOFGjNE500GXZo3OrvrEKL5+hnEIXyn0GBx9
fOvAbTDunJnTzY6R1nl8EvRs5VRxsdouT7B2eOLEiWUDhiciUpotJxvClZLUn/fL
SFVkhxTcHtbUsaI6OTxQOA2ZhqFV8S6aX4WUbVdFic5pGubtKoOwAbeChrTc7BcS
ecwv8vPPmjC/C64iG8pdETwQ5LVTo2J+epnVKfl3oeMCdWFOFp6tSaOozcjwPleg
hhpCHgFXP2NIJ04CD4BVLeoEm9EOUj2+VaL5Qj5PdOELKp+WTNOl2IHh+fGOQ97S
6gFDn/M+LGFcOdUKp0kAGWEHfL4F8Wi7Bb0Axs/bxpHZKEvnvAWIQWuG9HVTvtNc
```

... utiliser PGP

Pretty Good Privacy

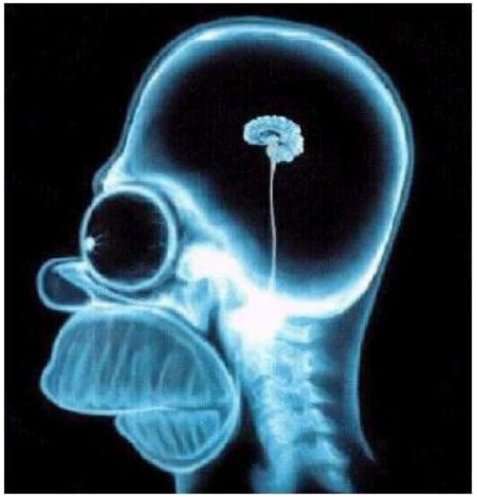
Logiciel de chiffrement, déchiffrement, signature de courriers électroniques, inventé par Phil Zimmermann en 1991.

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 $\geq$ 4096 bits
3. Importer votre clefs
4. Télécharger les clefs de vos amis
5. Envoyer des emails chiffrés.



Plan

Rappels

Choses à retenir

- La sécurité est omi-présente
- La sécurité c'est pas automatique
- Devenez acteur de votre sécurité
- Bien choisir ses mots de passe
- Chiffrer et signer vos emails

Merci pour votre attention.

Questions ?