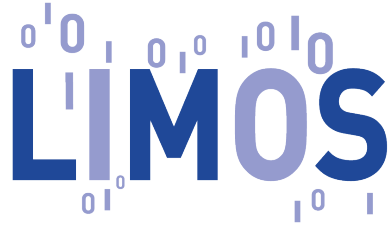
3A Security
Introduction
Cours 1

Pascal Lafourcade



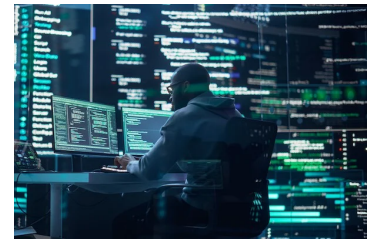
2024-2025

6 statistiques en cybersécrurité en 2019

1. 92% malwares sont propagés par email
2. 1.76 milliard données volées en Janvier 2019
3. Ransomwares coûteront $11.5 milliards en 2019
4. Phishing par email est responsable de 91% de cyberattaques
5. Coût global du cybercrime 2 millions de milliards $ en 2019
6. 7 entreprises sur 10 ne sont pas prêtes face aux cyber attaques

Source : `https://thebestvpn.com/cyber-security-statistics-2019`

En 2023

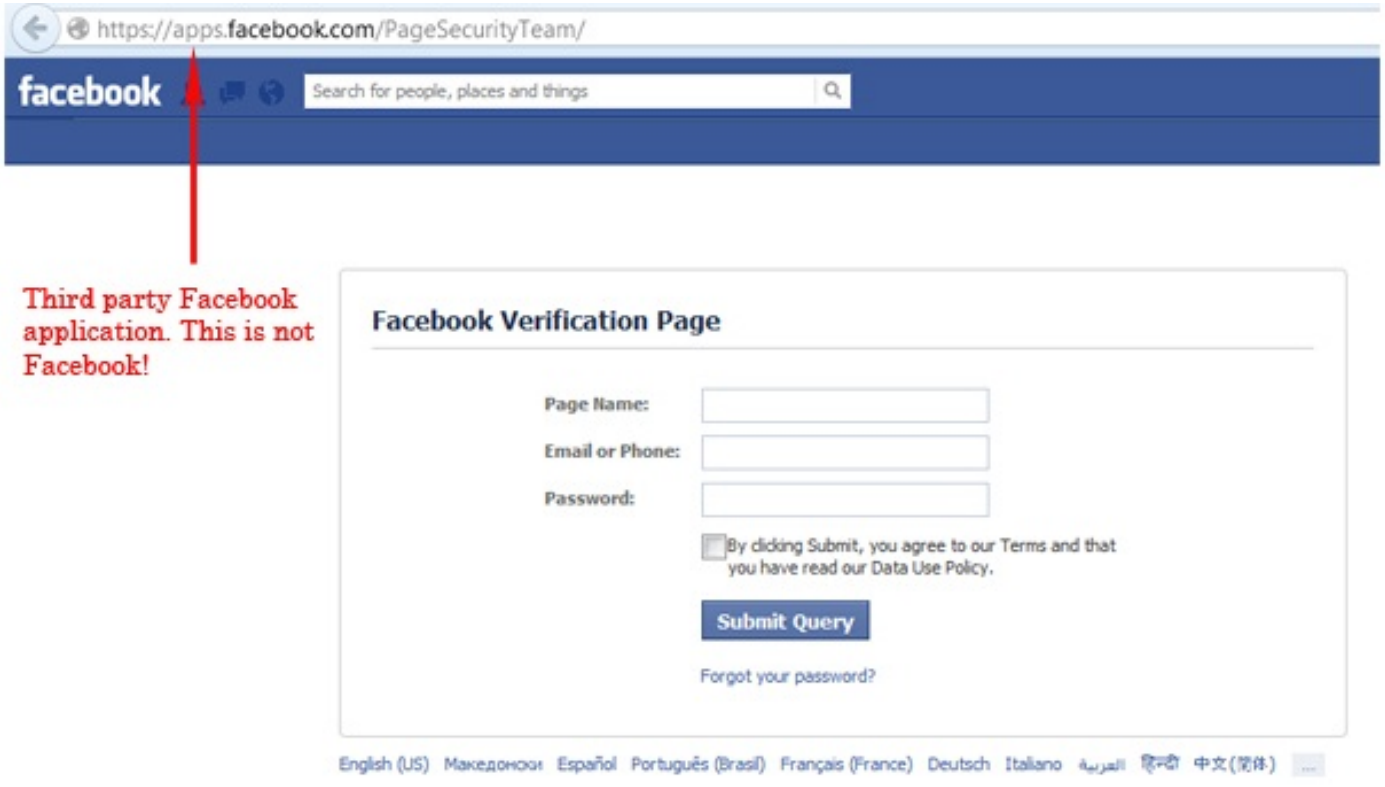


- 6 mois pour détecter une violation de données.
- 43 % des cyberattaques visent les petites entreprises.
- 91 % des attaques sont lancées par un courriel de phishing.
- Une entreprise est victime d'une attaque par ransomware toutes les 14 secondes.
- 38 % des pièces jointes malveillantes sont masquées sous la forme d'un fichier de type Microsoft Office ou autre.
- Les entreprises ont été confrontées à une moyenne de 22 violations de sécurité en 2020.
- Le coût mondial de la criminalité en ligne atteindra 10,5 billions de dollars par an d'ici 2025.
- Les estimations montrent que le marché de la cybersécurité atteindra 300 milliards de dollars d'ici 2024.
- Une hausse de 400 % des cyberattaques France depuis 2020.

5 Familles de Cybercriminalité

- Escroquerie
- Sabotage
- Ransomwares
- Espionnage
- Destabilisation

Escroquerie : Phishing



Voyant + Papillon

En 2019

CLASSEMENT VADESECURE DES MARQUES LES PLUS EXPLOITÉES PAR DES « PHISHERS » - *Quatrième trimestre 2019*

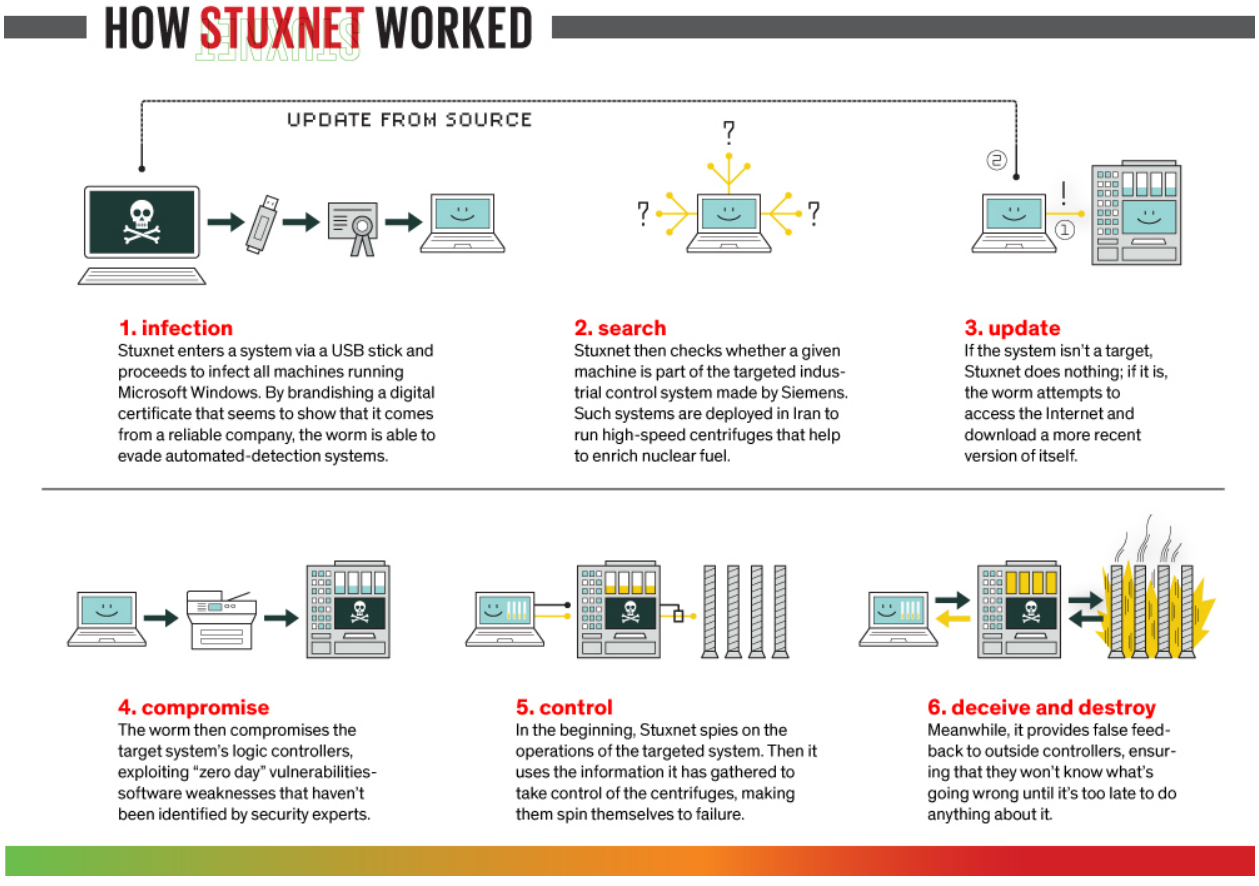
	Marque	Progression au classement sur le Q4	Nombre d'URLs Uniques	Croissance Q3 – Q4 2019
1	Paypal	=	11392	-31,2%
2	Facebook	+2	9795	-18,7%
3	Microsoft	-1	8565	-38,2%
4	Netflix	-1	6758	-50,2%
5	WhatsApp	+63	5020	+13467,6%
6	Bank of America	-1	4375	-21,5%
7	CIBC	+1	2414	-11,2%
8	Desjardins	+4	2243	-54,4%
9	Apple	-3	2126	-57,9%
10	Amazon	-1	2110	+0,6%
11	Chase	-4	2012	-14,6%
12	BNP Paribas	+3	1512	+23,1%
13	Instagram	+16	1401	+187,1%
14	Square	+19	1315	+246,1%
15	Dropbox	+1	1233	+0,7%

Escroquerie : Fraude au président

VIDEO

Sabotage

Stuxnet, 2010



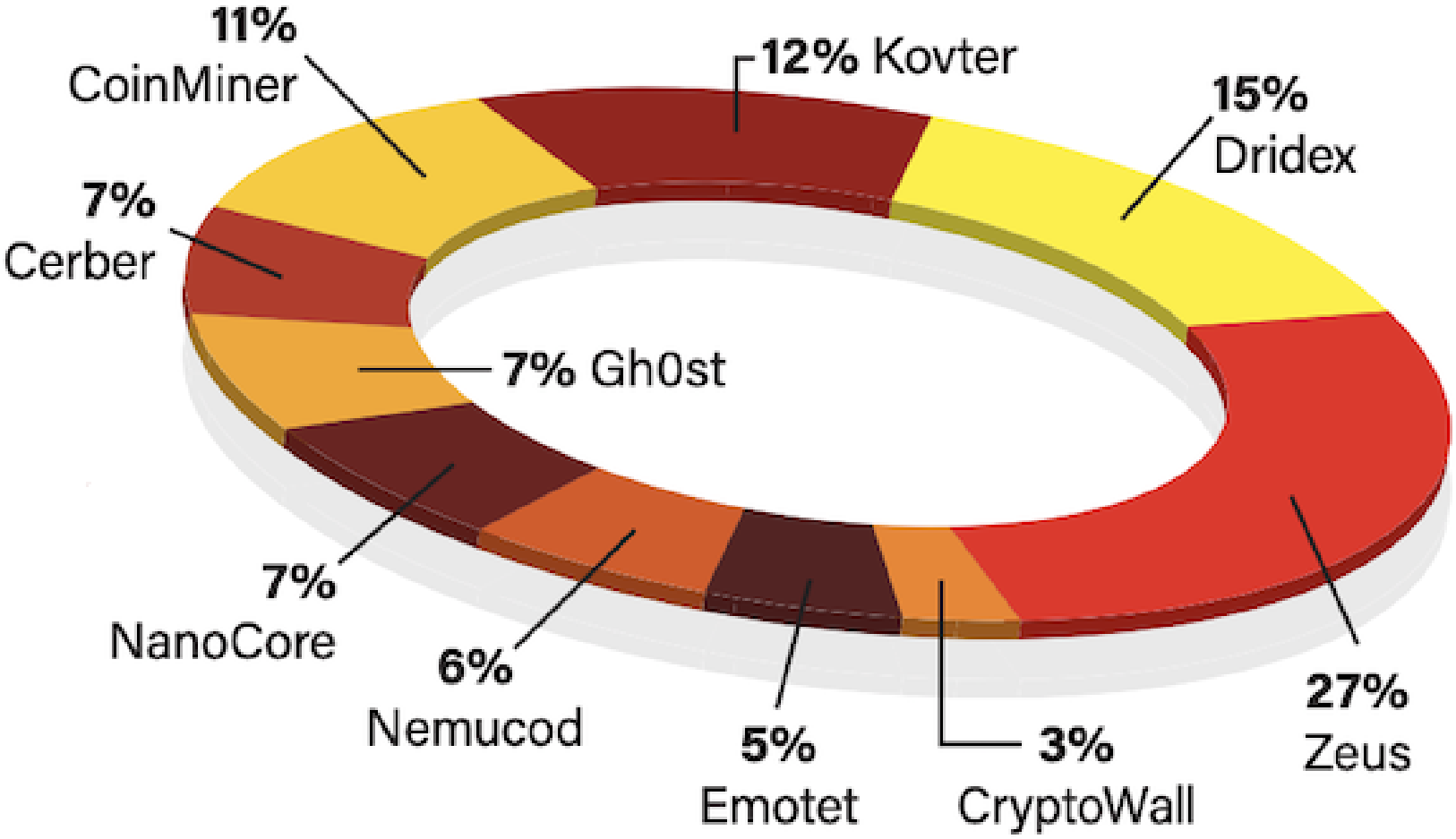
Saudi Aramco 35 000 PC deleted in 2012.

Ransomwares: Wannacry et al. 12 may 2017

http://stopransomware.fr/

Malwares stars de début 2020

Rapport CIS Janvier 2020



Espionnage

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

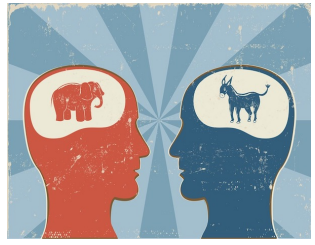
Edward Joseph Snowden, 6th june 2013

Citizen Four

Une technique d'espionnage : MICE

Monnaie

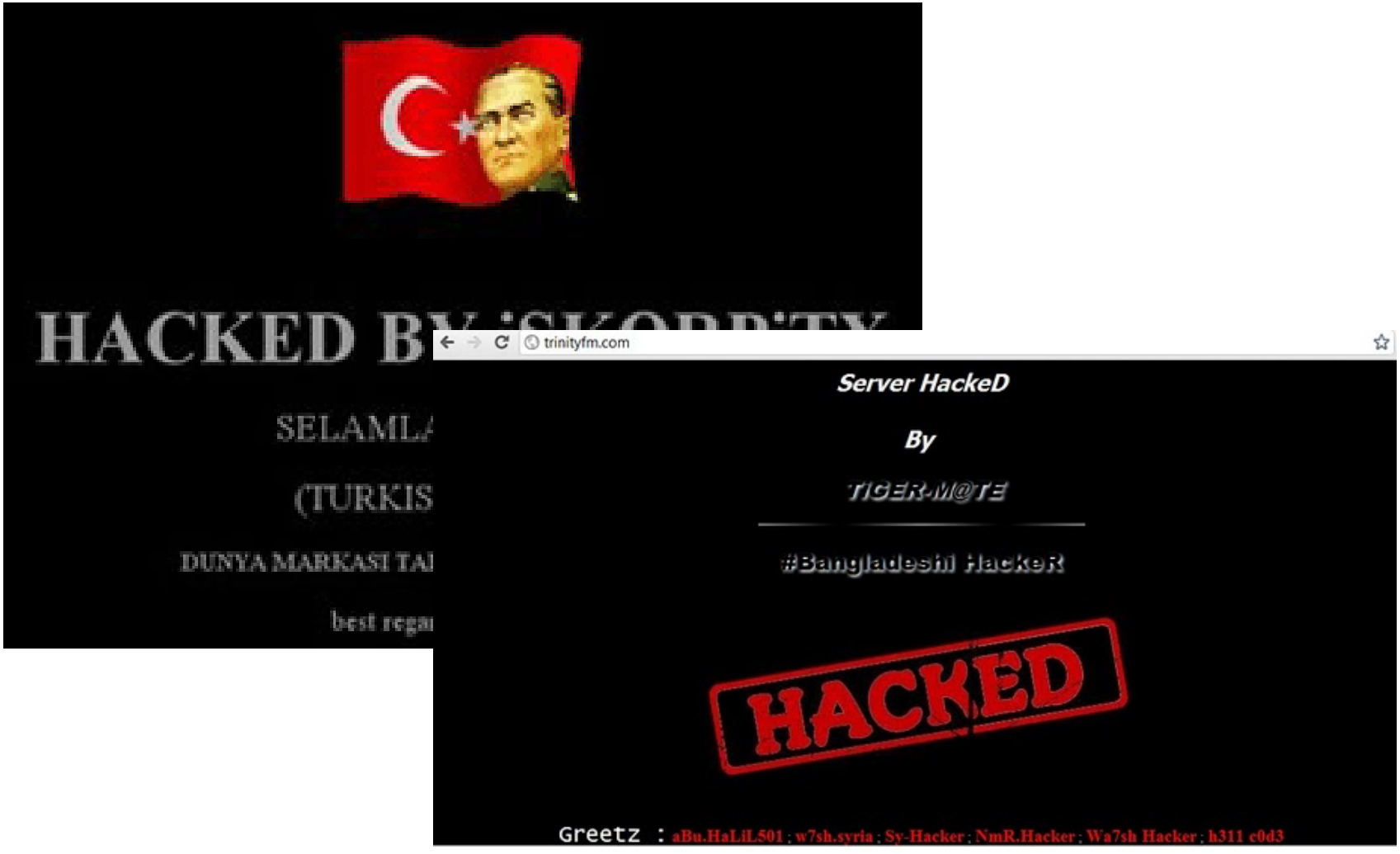
Idéologie



Compromission

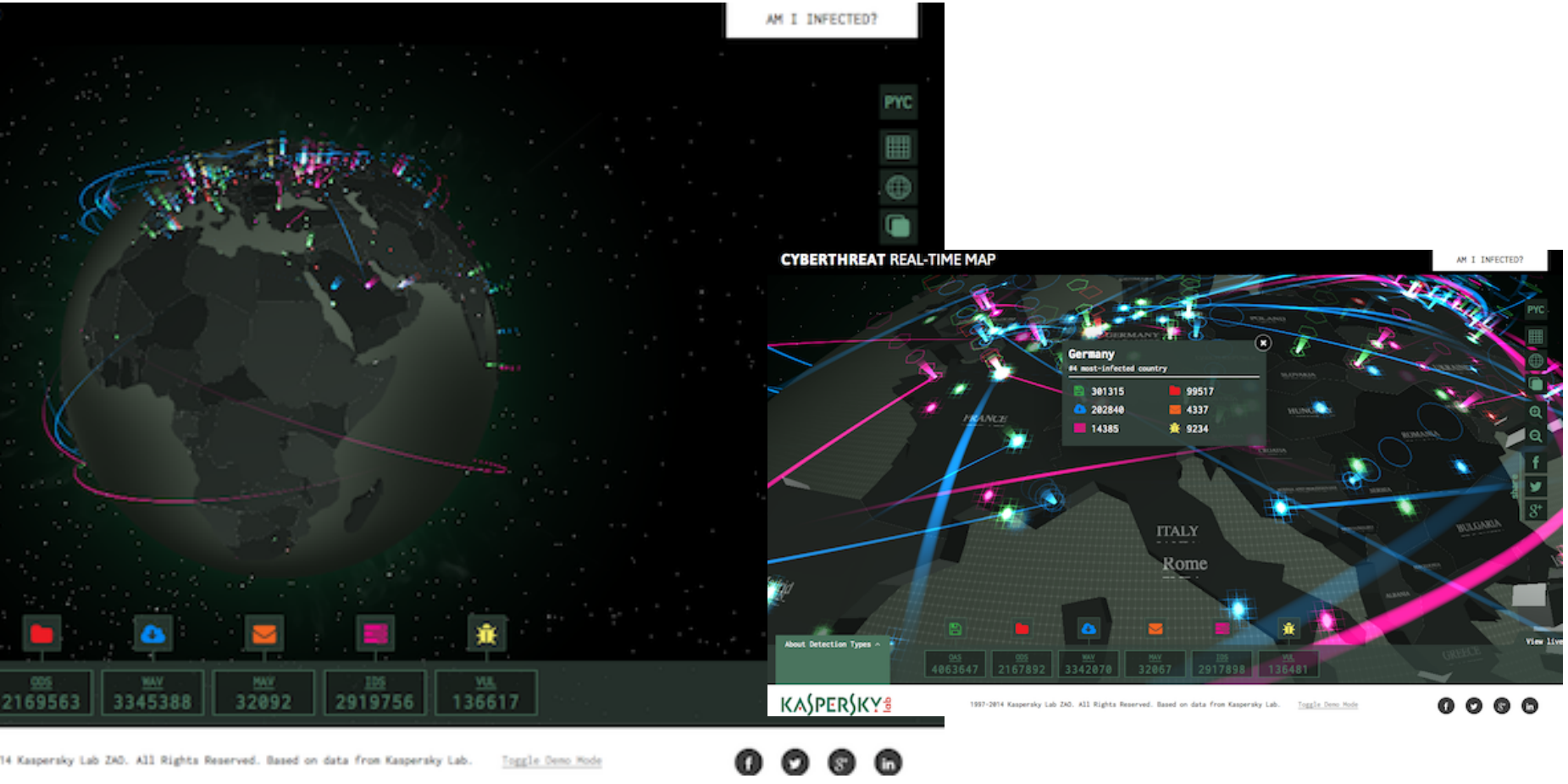
Ego

Destabilisation : Defacement



Destabilisation: Trojan, Botnets and Zombies

http://cybermap.kaspersky.com/



https://threatmap.fortiguard.com/

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

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

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

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

Rapide, large échelle, semi-automatique ...

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

Rapide, large échelle, semi-automatique ...

mais faussement anonyme !

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

Rapide, large échelle, semi-automatique ...

mais faussement anonyme !

Internet a été conçu pour fonctionner pas pour être sûr !

Agences pour la sécurité informatique

- 1919 

- 1952, 

- 1995, 
- 2002, 
- 7 Juillet 2009, 

ANSSI

Backdoors

- NSA's backdoor into `Dual_EC_DRBG` Dual Elliptic Curve Deterministic Random Bit Generator.
- Backdoor identified by academic researchers (Crypto 2007) and revealed by Snowden 2013.
- A kilobit hidden SNFS discrete logarithm computation, by Joshua Fried, Pierrick Gaudry, Nadia Heninger, Emmanuel Thomé. `https://eprint.iacr.org/2016/961.pdf`

Outline

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

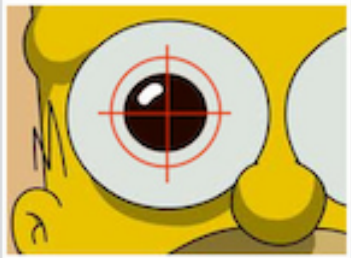
Devenir acteur de sa sécurité numérique

car la sécurité c'est pas automatique.

L'authentification

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

Plusieurs moyens

KNOW	HAVE	ARE	DO
			
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger	Behavior Location Reputation

Sécurité de mes mots de passe

Sécurité de mes mots de passe

Le plus simple et le plus utilisé moyen

- d'authentification
- d'attaque

Sécurité de mes mots de passe

Le plus simple et le plus utilisé moyen

- d'authentification
- d'attaque

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

Top 25 en 2015

1. 123456 (Unchanged)
2. password (Unchanged)
3. 12345678 (Up 1)
4. qwerty (Up 1)
5. 12345 (Down 2)
6. 123456789 (Unchanged)
7. football (Up 3)
8. 1234 (Down 1)
9. 1234567 (Up 2)
10. baseball (Down 2)
11. **welcome**
12. **1234567890**
13. abc123 (Up 1)
14. 111111 (Up 1)
15. **1qaz2wsx**
16. dragon (Down 7)
17. master (Up 2)
18. monkey (Down 6)
19. letmein (Down 6)
20. **login**
21. **princess**
22. **qwertyuiop**
23. **solo**
24. **passw0rd**
25. **starwars**

Top 25 en 2016

1. 123456 (Unchanged)
2. 123456789 (Up 5)
3. qwerty (Up 1)
4. 12345678 (Down 1)
5. 111111 (Up 9)
6. **1234567890**
7. 1234567 (Up 1)
8. password (Down 6)
9. **123123**
10. **987654321**
11. **qwertyuiop**
12. **mynoob**
13. **123321**
14. **666666**
15. **18atcskd2w**
16. **7777777**
17. **1q2w3e4r**
18. **654321**
19. **555555**
20. **3rjs1la7qe**
21. **google**
22. **1q2w3e4r5t**
23. **123qwe**
24. **zxcvbnm**
25. **1q2w3e**

Top 25 en 2017

1. 123456 (Unchanged)
2. Password (Unchanged)
3. 12345678 (Up 1)
4. qwerty (Up 2)
5. 12345 (Down 2)
6. **123456789**
7. **letmein**
8. 1234567 (Unchanged)
9. football (Down 4)
10. **iloveyou**
11. admin (Up 4)
12. welcome (Unchanged)
13. **monkey**
14. login (Down 3)
15. abc123 (Down 1)
16. **starwars**
17. **123123**
18. dragon (Up 1)
19. passw0rd (Down 1)
20. master (Up 1)
21. **hello**
22. **freedom**
23. **whatever**
24. **qazwsx**
25. **trustno1**

Top 25 en 2018

1. 123456 (Unchanged)
2. password (Unchanged)
3. 123456789 (Up 3)
4. 12345678 (Down 1)
5. 12345 (Unchanged)
6. **111111**
7. 1234567 (Up 1)
8. **sunshine**
9. qwerty (Down 5)
10. iloveyou (Unchanged)
11. **princess**
12. admin (Down 1)
13. welcome (Down 1)
14. **666666**
15. abc123 (Unchanged)
16. football (Down 7)
17. 123123 (Unchanged)
18. monkey (Down 5)
19. **654321**
20. **!@#$%^&***
21. **charlie**
22. **aa123456**
23. **donald**
24. **password1**
25. **qwerty123**

Top 25 en 2019

1. 123456 (Unchanged)
2. 123456789 (up 1)
3. qwerty (Up 6)
4. password (Down 2)
5. 1234567 (Up 2)
6. 12345678 (Down 2)
7. 12345 (Down 2)
8. iloveyou (Up 2)
9. 111111 (Down 3)
10. 123123 (Up 7)
11. abc123 (Up 4)
12. qwerty123 (Up 13)
13. **1q2w3e4r**
14. admin (Down 2)
15. **qwertyuiop**
16. 654321 (Up 3)
17. **555555**
18. **lovely**
19. **7777777**
20. welcome (Down 7)
21. **888888**
22. princess (Down 11)
23. **dragon**
24. password1 (Unchanged)
25. **123qwe**

Top 25 en 2020

1. 123456 (Unchanged)
2. 123456789 (Unchanged)
3. **picture1**
4. password (Unchanged)
5. 12345678 (Up 1)
6. 111111 (Up 3)
7. 123123 (Up 3)
8. 12345 (Down 1)
9. **1234567890**
10. **senha**
11. 1234567 (Down 6)
12. qwerty (Down 9)
13. abc123 (Down 2)
14. **Million2**
15. **000000**
16. **1234**
17. iloveyou (Down 9)
18. **aaron431**
19. password1 (Up 5)
20. **qqww1122**
21. **123**
22. **omgpop**
23. **123321**
24. 654321 (Down 8)
25. **qwer123456**

Top 25 en 2021

1. 123456 (Unchanged)
2. 123456789 (Unchanged)
3. qwerty (Up 11)
4. 12345678 (Up 1)
5. 111111 (Up 1)
6. 1234567890 (Up 3)
7. 1234567 (Up 4)
8. password (Down 4)
9. 123123 (Down 3)
10. **987654321**
11. **qwertyuiop**
12. **mynoob**
13. 123321 (Up 10)
14. **666666**
15. **18atcskd2w**
16. **7777777**
17. **1q2w3e4r**
18. 654321 (Up 6)
19. **555555**
20. **3rjs1la7qe**
21. **google**
22. **1q2w3e4r5t**
23. **123qwe**
24. **zxcvbnm**
25. **1q2w3e**

Top 25 en 2022

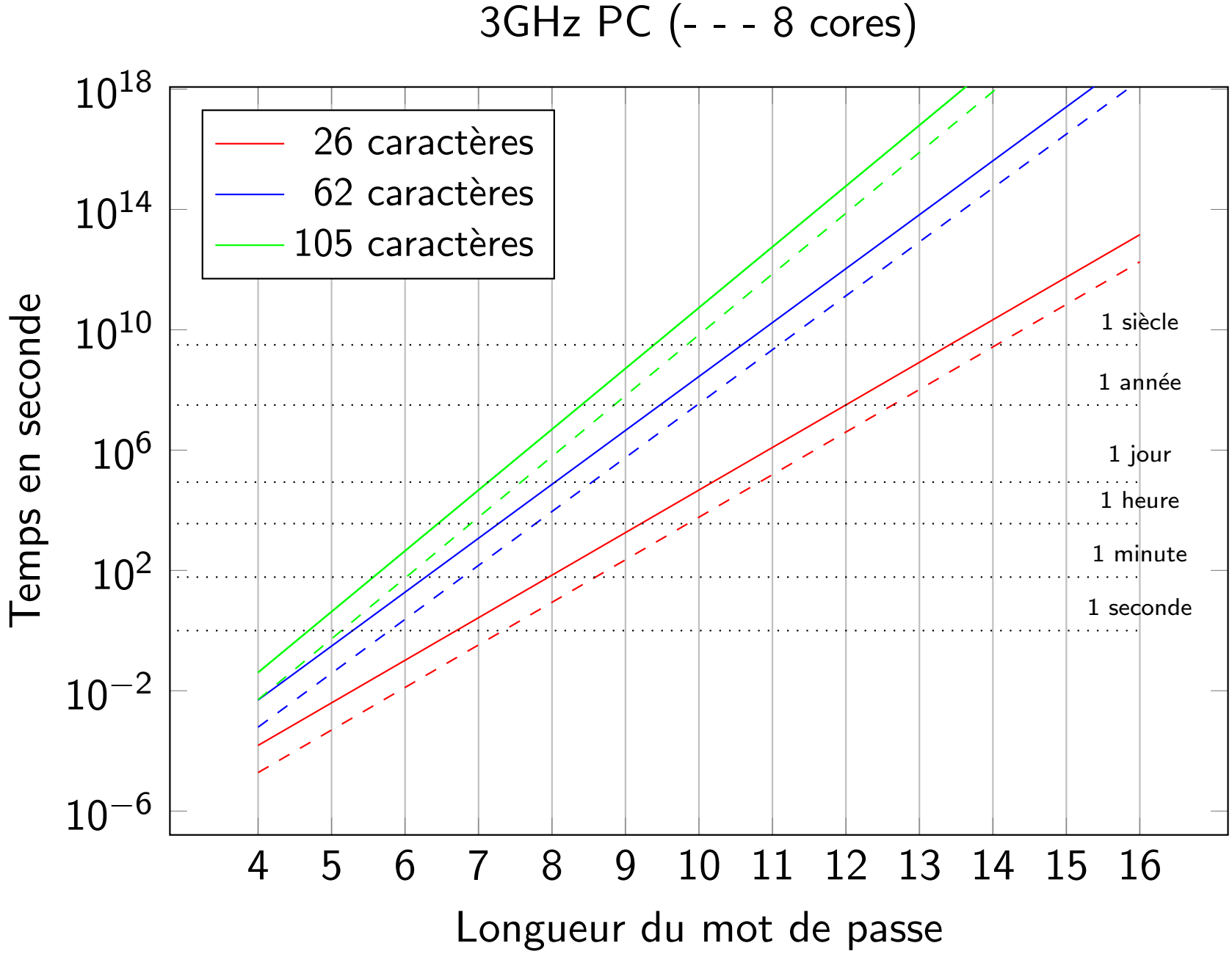
1. password (Up 8)
2. 123456 (Down 1)
3. 123456789 (Down 1)
4. **guest**
5. qwerty (Down 2)
6. 12345678 (Down 2)
7. 111111 (Down 2)
8. **12345**
9. **col123456**
10. 123123 (Down 1)
11. 1234567 (Down 4)
12. **1234**
13. **1234567890**
14. **000000**
15. 555555 (Up 4)
16. 666666 (Down 2)
17. 123321 (Down 4)
18. 654321 (Unchanged)
19. 7777777 (Down 5)
20. **123**
21. **D1lakiss**
22. **777777**
23. **110110jp**
24. **1111**
25. 987654321 (Down 15)

Passwords Brute Force

- N : nombre de caractères
- k : nombre de coeurs
- L : longueur du mot de passe
- V : vitesse du processeur en GHz
- T : temps pour énumérer tous les mots de passe en secondes

$$T = \frac{N^L}{k \times V \times 10^9}$$

Passwords Brute Force



Recommandation de l'ANSSI

Type de mot de passe	Taille de clé équivalente	Force	Commentaire
Mot de passe de 8 caractères dans un alphabet de 70 symboles	49	Très faible	Taille usuelle
Mot de passe de 10 caractères dans un alphabet de 90 symboles	65	Faible	
Mot de passe de 12 caractères dans un alphabet de 90 symboles	78	Faible	Taille minimale recommandée par l'ANSSI pour de passe ergonomiques ou utilisés de façon locale.
Mot de passe de 16 caractères dans un alphabet de 36 symboles	82	Moyen	Taille recommandée par l'ANSSI pour des mots d plus sûrs.
Mot de passe de 16 caractères dans un alphabet de 90 symboles	104	Fort	
Mot de passe de 20 caractères dans un alphabet de 90 symboles	130	Fort	Force équivalente à la plus petite taille de clé de l' de chiffrement standard AES (128 bits).

Suite aux fuites ...

Suite aux fuites ...

... j'ai changé mes mots de passe !

En réalité

En réalité


©Crown Copyright, 2012
www.dukeandduchessofcambridge.org


MilFlip Logon
Details
RMS
ATTENTION ALL
RMS STUDENTS

Root Me

root-me.org/fr/breve/Vol-de-donnees-password-reuse

verimag-local | sancy-local | CS253 - Web Sec... | Deus Ex Machina | Conférence PANO... | PGP | math.co.ro | MACsec Impleme...

Root Me

Rechercher

- Capture The Flag
- Challenges
- Communauté
- Documentation
- Informations
- Outils

330 visiteurs en ce moment

derniers inscrits :
ximbi emrxs nonoScOoP usap23 Desmoonde P00Y JazzyWork

Chatbox

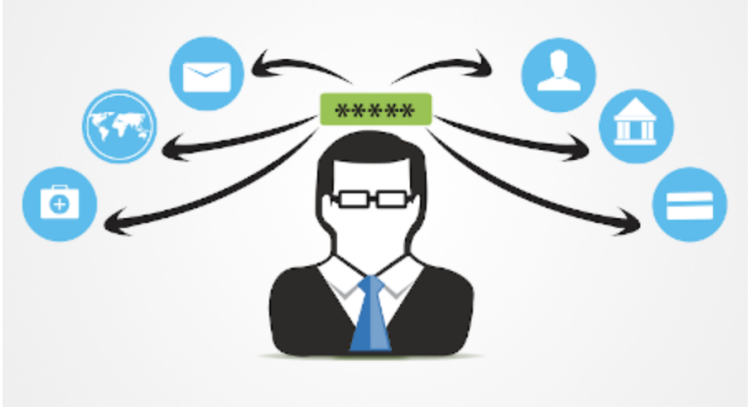
m31z0nyx

ACCUEIL

Vol de données - password reuse

samedi 30 mai 2020

Que s'est-il passé ?



Historiquement l'association Root-Me a toujours fait confiance à tous ses contributeurs et à ce titre les membres les plus actifs jouissent généralement de droits forts.
Un administrateur de la plateforme qui a beaucoup contribué à son époque puis s'est éclipsé pour poursuivre sa vie professionnelle et familiale a été victime d'une attaque par réutilisation de mot de passe : son mot de passe est apparu dans un leak quelconque et malheureusement c'était le même que sur la plateforme Root-Me. Ce compte compromis a permis un accès illégitime au backend depuis lequel nous gérons Root-Me.

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.

Remarques:

- Il est difficile de mémoriser 12 caractères aléatoires.
- Passphrase.
- `https://keepassxc.org/`

Comment stocker les mots de passe ?

Stockage

- En clair
- Haché (pwd) $\Rightarrow$ Rainbowtables !
- Haché (pwd + Salt)
- Haché (pwd + Salt-user)
- bcrypt(pwd + Salt-user)
  bcrypt = hachage plus lent ou PBKDF2
- AES(bcrypt(pwd + Salt-user), SecretKey)

John the Ripper / Hashcat

`www.openwall.com/john/`

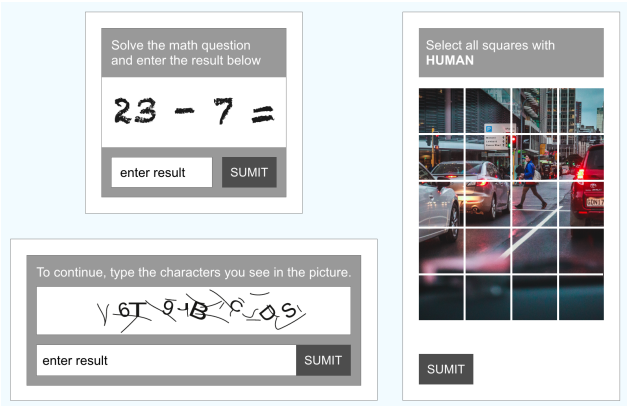
`https://hashcat.net/hashcat/`

Wireshark

https://www.wireshark.org/

Contre-mesures

- Challenge / Response:
  - C to S : hello
  - S to C : r
  - C to S : $H(r||pwd)$



- Limiter le nombre de tentatives: bloquer par exemple le système pour une certaine durée après un nombre d'essais.
- S'assurer que chaque essai est bien mené par un humain (et non pas un ordinateur) en utilisant des techniques de type CAPTCHA "*Completely Automated Public Turing test to tell Computers and Humans Apart*"
- OTP avec SMS en plus pour confirmer

Outline

Octobre 2014

TED
Ideas worth spreading

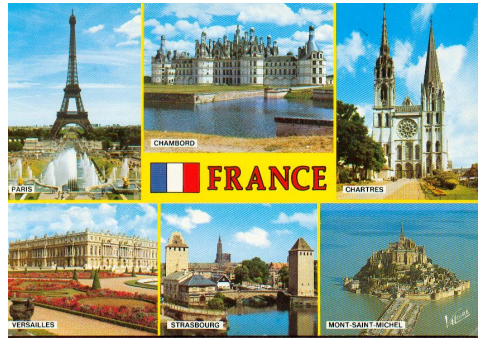
L'importance de la vie privée
Why privacy matters?

Par Glenn Greenwald

Les gens pensent ne rien avoir à cacher ...

`http://jenairienacacher.fr/`
`http://nothing2hide.org`

La sécurité des emails par défaut

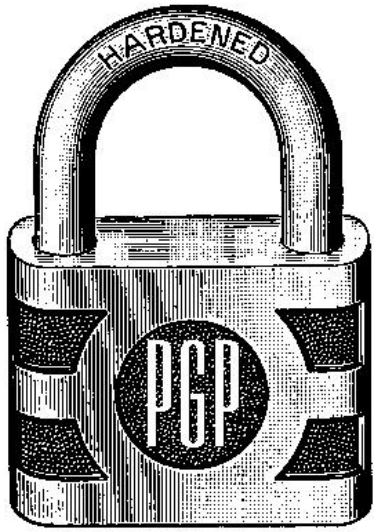


Première demande d'E. Snowden ...

... utiliser PGP

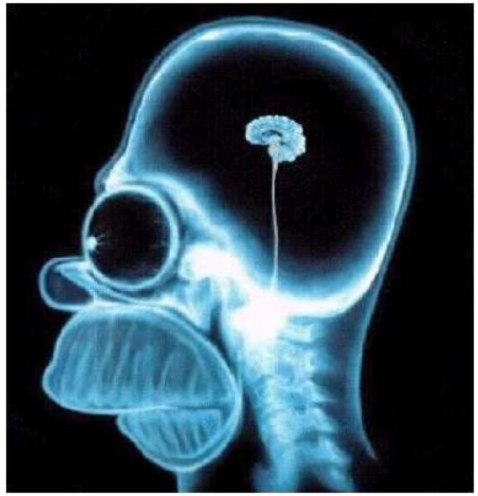
Pretty Good Privacy

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

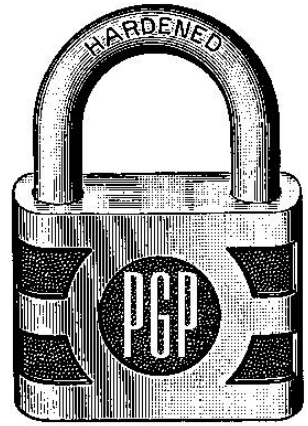


Est-ce si difficile ?

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.



Pretty Good Privacy (PGP) by Phil Zimmermann, 1991



Generate keys for you, and help you manage them

A "PGP key" has several parts:

- the name of its owner
- the numerical value(s) comprising the key
- what the key is to be used for
- the algorithm the key is to be used with
- (possibly) an expiration date

Software: OpenPGP, or GnuPG

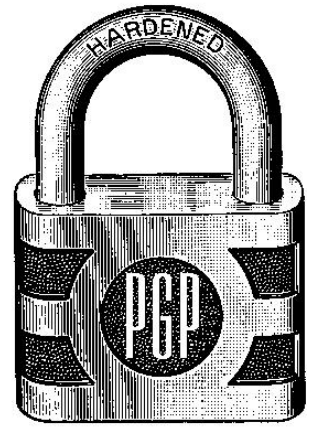
PGP

PGP stores lots of different keys for

- signing keys or emails or ...
- encrypting
- your own secret key (this will be stored encrypted with a passphrase)
- your own public key and the public keys of your friends and associates (stored in the clear)

The PGP software puts them in a file, called your keyring.

PGP



- Your private keys are in a file only you can read; for extra security, they are stored encrypted with a pass phrase.
- The public keys don't have to be protected.
- The keyring also stores certificates, i.e. copies of other people's public keys which are signed by you. These ones are known with certainty by you to belong to the people they claim to belong to.

PGP: How to send a message to someone

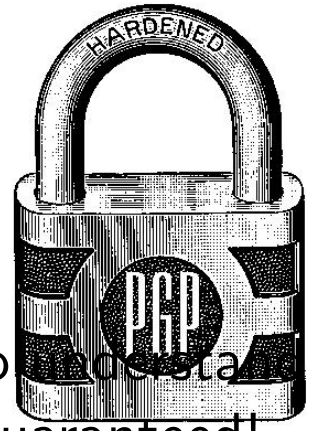
A "signed message"

PGP signs a hash of the message.

A message encrypted with their public key

- PGP encrypts it with a newly-generated symmetric key
- You send that encrypted version appended to the symmetric key encrypted with the public key.

Why does no-one use PGP?



- It's not considered necessary.
- It's quite complicated. You need to spend a day to understand it properly. And even then, understanding is not guaranteed!
- It's a hassle. You need to maintain your keys, your web of trust, you need to configure your mail client.

"Why Johnny can't encrypt ?" is an article explaining why people can't/don't want to use PGP.

Plan

CNIL créé en 1978

Commission nationale de l'informatique et des libertés

BUT

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

ANSSI créée le 7 juillet 2009.

STAD

Système de Traitement Automatisé de Données

"Tout ensemble composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité".

Aucune définition précise dans la loi

Dans les faits c'est presque tout :

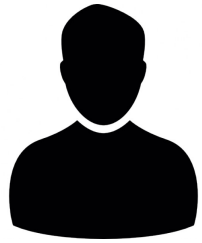
3 acteurs

Utilisateur

Responsable

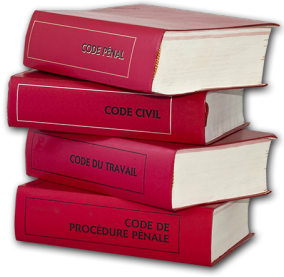
Pirate

L'utilisateur



Droits

- D'accès : demander directement au responsable d'un fichier s'il détient l'intégralité de ces données
- De rectification
- D'opposition dêtre dans un fichier
- Déréférencement sur le web par rapport au nom et prénom



Le responsable

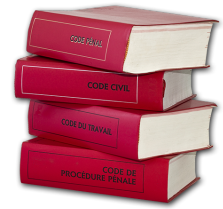
Et le sous-traitant via le contrat.

Devoirs

- Déclarer les traitements de données personnelles
  5 ans & 300 000
- Prendre toutes précautions pour la sécurité des données selon
  - la nature des données
  - les risques présentés par le traitement

  5 ans & 300 000

Lois informatique et libertés : Article 22 et Article 34.
Guide de la CNIL : La sécurité des données personnelles



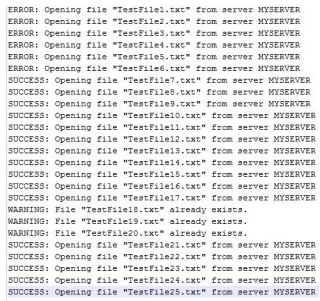
Conservation des logs

LCEN 2004

• 1 an pour les logs (jurisprudence de la BNP Paribas)

• Décret 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne:

- ip, url, protocole, date heure, nature de l'opération
- éventuellement les données utilisateurs
- éventuellement données bancaires
- accédées dans le cadre d'une réquisition
- conservées un an
- données utilisateurs pendant un an après la clôture



Article 226-20 : les logs ont une date de péremption

Le pirate

Risques (STAD (Article 323-1))

- accès frauduleux ou maintien frauduleux de l'accès **2 ans & 60 000**
- suppression ou modification des données **3 ans & 100 000**
- si données à caractère personnel **5 ans & 150 000**
- altération du fonctionnement **5 ans et de 75 000**
- si données à caractère personnel **7 ans & 100 000**

Risques encourus

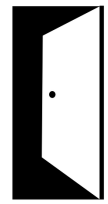
En pratique

- Atteintes aux intérêts fondamentaux de la nation (Sécurité nationale) Article 410-1 à 411-6
- Secret des communication pour l'autorité publique et FAI **3 ans et 45 000** Article 432-9
- Usurpation d'identité **5 ans et de 75 000** Article 434-23
- Importer, détenir, offrir ou mettre à disposition un moyen de commettre une infraction est puni

Sauf si

Pas de condamnation si

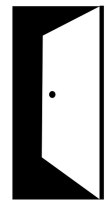
- aucune protection
- aucune mention de confidentialité
- accessible via les outils de navigation grand public
- même en cas de données nominatives



Sauf si

Pas de condamnation si

- aucune protection
- aucune mention de confidentialité
- accessible via les outils de navigation grand public
- même en cas de données nominatives



Il est donc important de protéger ces données

Plan

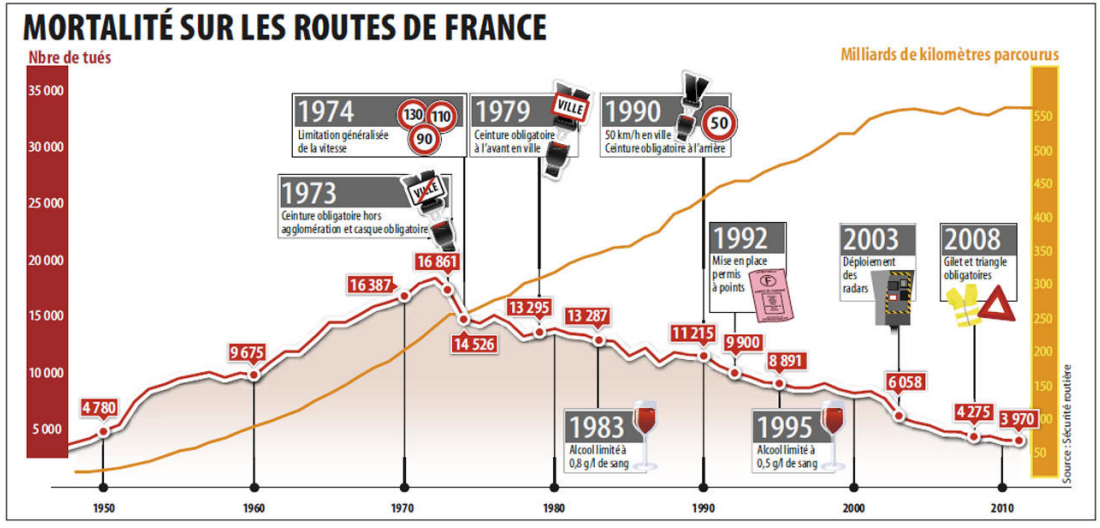

RIP


RIP


NON PORT DE LA CEINTURE DE SÉCURITÉ
-4 points
sur le permis de conduire
135 €
Amende forfaitaire
POINTS.12


RIP

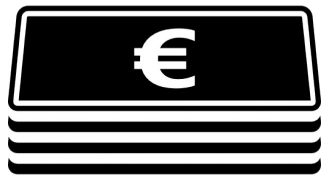

NON PORT DE LA CEINTURE DE SÉCURITÉ
-4 points
sur le permis de conduire
135 €
Amende forfaitaire
POINTS 12


MORTALITÉ SUR LES ROUTES DE FRANCE
Nbre de tués
Milliards de kilomètres parcourus
35 000
30 000
25 000
20 000
15 000
10 000
5 000
550
500
450
400
350
300
250
200
150
100
50
1974
Limitation généralisée de la vitesse
130
110
90
1979
Ceinture obligatoire à l'avant en ville
VILLE
1990
50 km/h en ville
Ceinture obligatoire à l'arrière
50
1973
Ceinture obligatoire hors agglomération et casque obligatoire
VILLE
1992
Mise en place permis à points
2003
Déploiement des radars
2008
Gilet et triangle obligatoires
1983
Alcool limité à 0,8 g/l de sang
1995
Alcool limité à 0,5 g/l de sang
4 780
9 675
16 387
16 861
14 526
13 295
13 287
11 215
9 900
8 891
6 058
4 275
3 970
1950
1960
1970
1980
1990
2000
2010
Source : Sécurité routière

L'argus

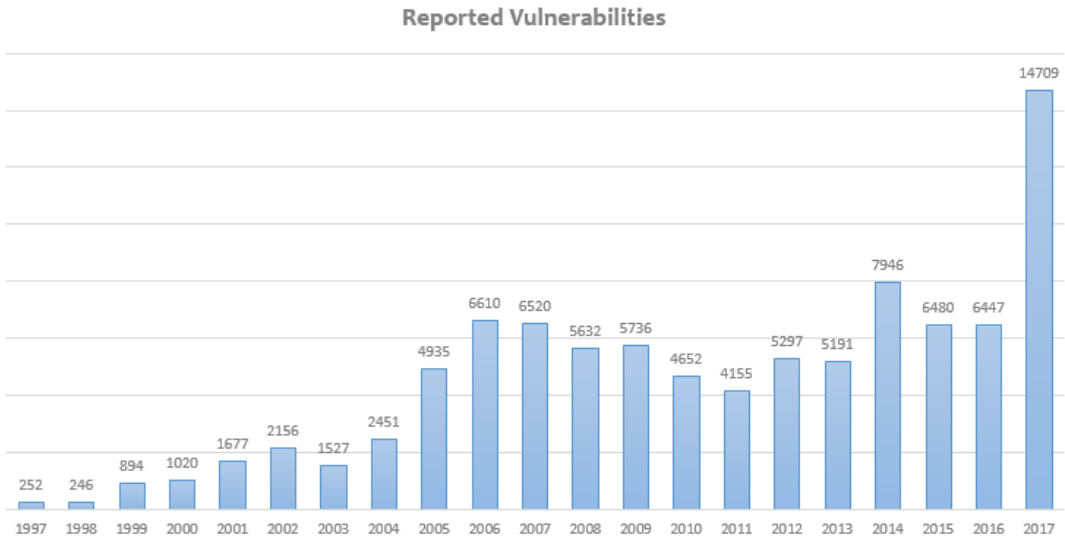
Sanctions

20 millions



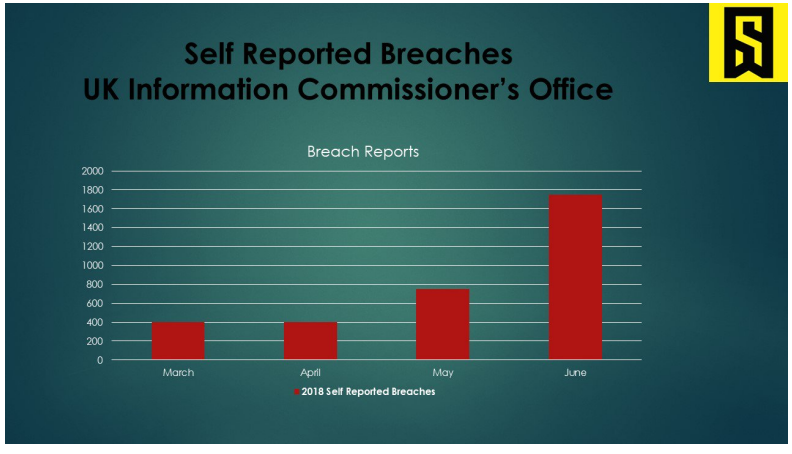
ou 4 %

En France la CNIL devient autorité de contrôle



Règlement Général sur la Protection des Données

GDPR : General Data Protection Regulation



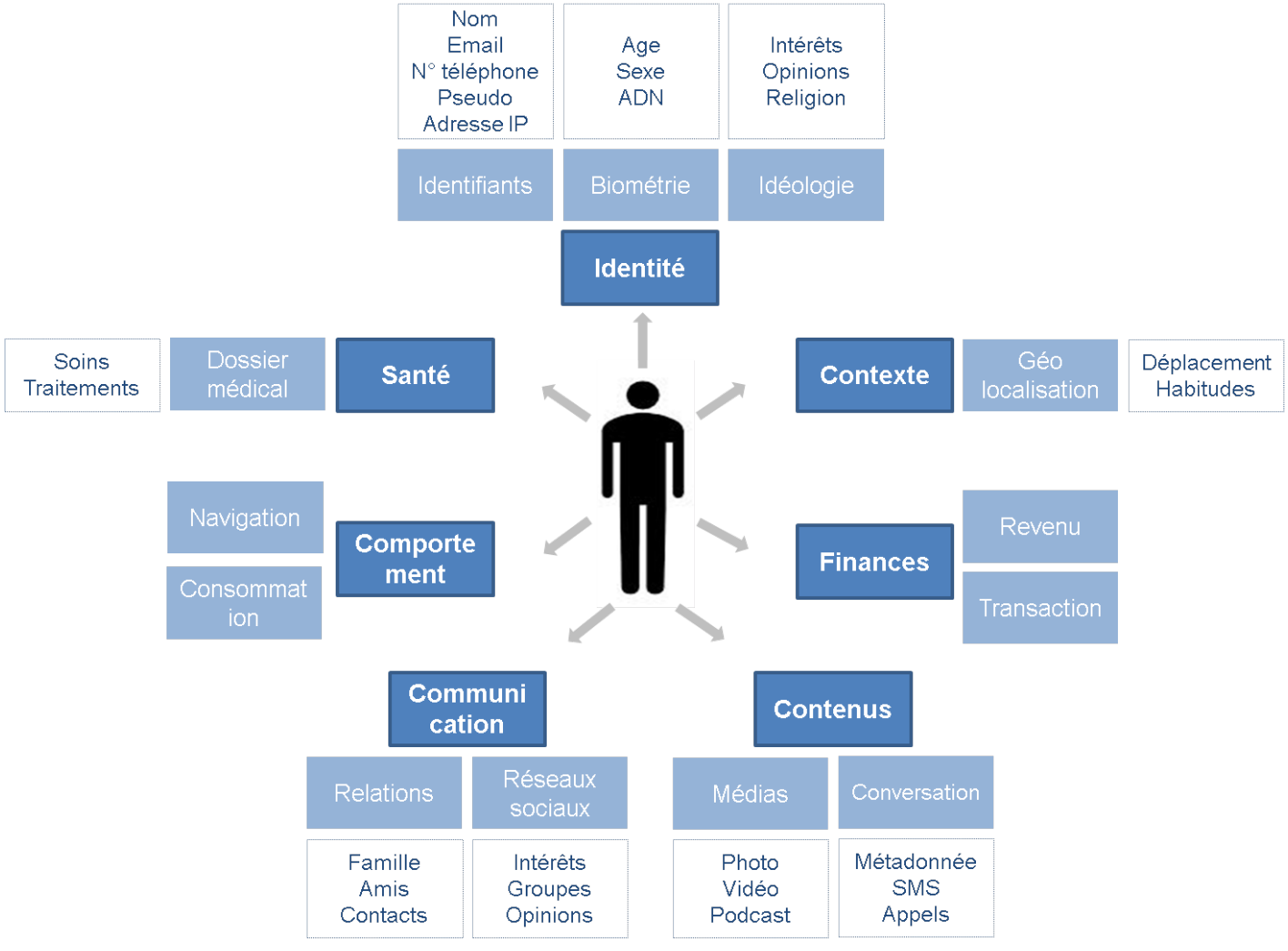
Qui est touché ?

TOUT LE MONDE !

5 types de données

1. neutres
2. personnelles
3. sensibles
4. pseudonymisées
5. anonymisées

Qu'est-ce qu'une donnée personnelle ?



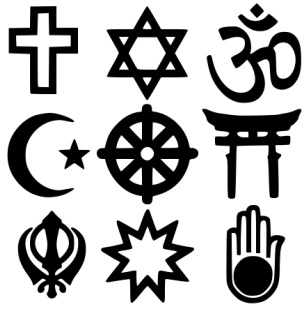
Toutes informations relatives à une personne physique qui peuvent être utilisées pour re-indentifier la personne.

Qu'est-ce qu'une donnée personnelle ?

Information qui permet d'identifier une personne physique, directement ou indirectement.

- un nom,
- une photographie,
- une adresse IP,
- un numéro de téléphone,
- un identifiant de connexion informatique,
- une adresse postale,
- une empreinte,
- un enregistrement vocal,
- un numéro de sécurité sociale,
- un mail, etc.

Qu'est-ce qu'une donnée personnelle **sensible**?



Collecte sans consentement préalable écrit, clair et explicite

Safe Harbor: 07 octobre 2015

- Invalidation par la Cour de Justice de l'Union européenne
- Une décision clé pour la protection des données,
- Quel niveau de protection des données personnelles transférées aux Etats-Unis ?

Safe Harbor: 07 octobre 2015

- Invalidation par la Cour de Justice de l'Union européenne
- Une décision clé pour la protection des données,
- Quel niveau de protection des données personnelles transférées aux Etats-Unis ?

Règlement Général sur la Protection des Données (RGPD)
Règlement no 2016/679 adopté le **27 avril 2016**.
Mise en application le **25 mai 2018**.

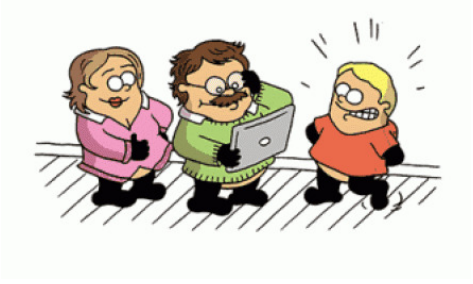
Plus de droits pour vos données !

Sanction

Plus de transparence

Droit à l'oubli

Guichet unique



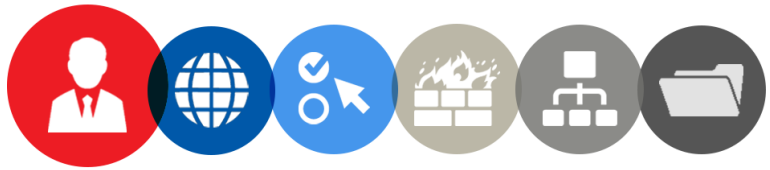
Protection des mineurs

Portabilité

RPGD : en 6 étapes @CNIL

1. Désigner un pilote
2. Cartographier
3. Prioriser
4. Gérer les risques
5. Organiser
6. Documenter

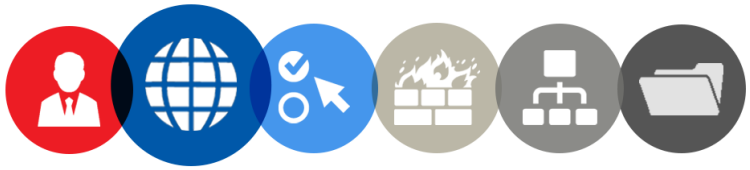
Étape 1 : Désigner un pilote



Délégué à la protection des données

Mission d'information, de conseil et de contrôle en interne.
Conformité au RGPD.

Étape 2 : Cartographier

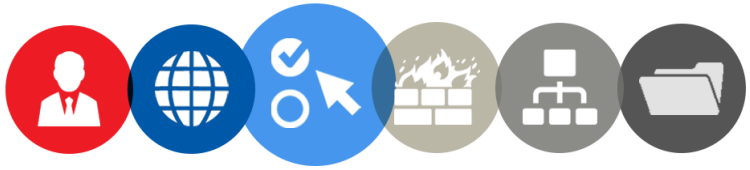


Tenir une documentation interne complète sur leurs traitements de données personnelles

- Catégories les données traitées
- Recenser précisement vos traitements de données personnelles (**Registre des traitements**)
- Lister les objectifs
- Identifier les acteurs
- Identifier les flux des données

But : Assurer que ces traitements respectent bien le règlement.

Étape 3 : Prioriser



1. Collecter et traiter **que les données nécessaires**.
2. **Base juridique du traitement** : consentement de la personne, contrat, obligation légale ...
3. Révisez vos **mentions d'information** : articles 12, 13 et 14: droits de la personne concernée : Transparence, Information et Transitivité
4. Vérifier vos **sous-traitants** et clause des contrats
5. Prévoyez les **modalités d'exercice des droits** des personnes concernées : droit d'accès, de rectification, droit à la portabilité, retrait du consentement...
6. Vérifiez les **mesures de sécurité** mises en place.

Étape 3 : VIGILANCE, des **types** de données

- origine prétendument **raciale ou ethnique**, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale,
- la **santé** ou l'orientation sexuelle,
- génétiques ou **biométriques**,
- infraction ou de condamnation **pénale**,
- sur les **mineurs**.

Étape 3 : VIGILANCE, votre traitement

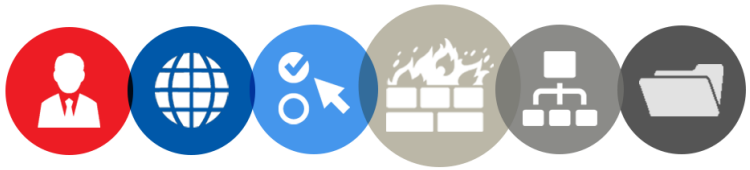
- la surveillance **systématique** à grande échelle d'une zone accessible au public
- l'évaluation **systématique** et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

Étape 3 : VIGILANCE **transfert** des données hors UE

- Vérifiez que le pays vers lequel vous transférez les données est reconnu comme adéquat par la Commission européenne ;
- Dans le cas contraire, encadrez vos transferts.

Privacy Impact Assessment (PIA)

Data protection impact assessment



- Principes et droits fondamentaux, **non négociables**, de la loi
- Gestion des **risques sur la vie privée** des personnes concernées, pour déterminer les mesures techniques et d'organisation pour protéger les données personnelles.

Un PIA contient :

- Une **description** du traitement étudié et de ses **finalités**.
- Une **évaluation de la nécessité et de la proportionnalité** des opérations de traitement au regard des finalités
- Une **évaluation des risques** pour les droits et libertés des personnes, les mesures envisagées pour faire face aux risques.

Étape 4 : Qui participe au PIA?

- **Le responsable de traitement** : valide et applique le PIA.
- **Le délégué à la protection des données** : élabore le plan d'action et se charge de vérifier son exécution ;
- **Le(s) sous-traitant(s)** : fournit les informations nécessaires à l'élaboration du PIA ;
- **Les métiers (RSSI, maîtrise d'ouvrage, maîtrise d'œuvre)** : aident à la réalisation du PIA en fournissant les éléments adéquats ;
- **Les personnes concernées** : donnent leurs avis sur le traitement.

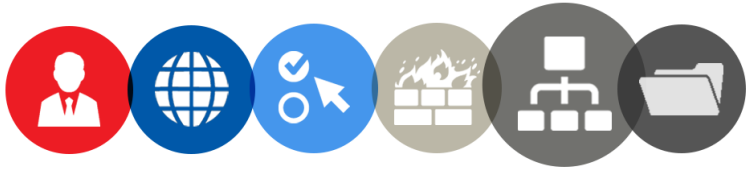
Étape 4 : **PIA obligatoire** Art. 35

Pour tout traitement susceptible d'engendrer des **risques élevés** pour les droits et libertés des personnes concernées.

1. Evaluation ou notation;
2. Décision automatisée avec effet juridique significatif;
3. Surveillance systématique ;
4. Données sensibles ou données à caractère hautement
5. Données personnelles traitées à grande échelle ;
6. Croisement d'ensembles de données ;
7. Données concernant des personnes vulnérables ;
8. Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ;
9. Exclusion du bénéfice d'un droit, d'un service ou contrat.

Si **au moins 2 de ces critères**, alors faire un PIA.

Étape 5 : Organiser



- Protection des données personnelles **dès la conception**
- **Sensibiliser et d'organiser la remontée d'information**
- Traiter les **réclamations et les demandes** des personnes concernées quand à l'exercice de leurs droits
- **Anticiper les violations de données**, dans les 72 heures aux autorités et personnes concernées

Étape 6 : Documenter

Prouver la conformité = Avoir la documentation nécessaire

- Traitements
- Information des personnes
- Contrat pour les acteurs

Étape 6 : Documenter les traitements

- Le **registre des traitements** (pour les responsables de traitements) ou des **catégories d'activités de traitements** (pour les sous-traitants)
- **PIA** pour les traitements à risque
- L'**encadrement des transferts** de données hors de l'Union européenne.

Étape 6 : Documenter l'information

- Les **mentions d'information**
- Les modèles de **recueil du consentement** des personnes concernées,
- Les procédures **mises en place** pour l'exercice des droits

Étape 6 : Documenter les contrats

- Les **contrats avec les sous-traitants**
- Les **procédures internes** en cas de violations de données
- Les **preuves** que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.

RGPD

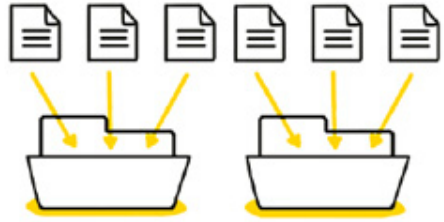
PASSER À L'ACTION

en 4 étapes

1

Constituez un registre de vos traitements de données

2



Faites le tri dans vos données

3

Respectez les droits des personnes

4

Sécurisez vos données

Plan

Loi sur la cyberrésilience

- Adopté par le Parlement européen le 12 mars 2019
- Adopté par le Conseil de l'Union européenne le 17 avril 2019
- Règlement européen Cybersecurity Act (UE 2019/881) a été publié le 7 juin 2019

ENISA : European Union Agency for Cybersecurity (2004)
En France, l'ANSSI est l'Autorité Nationale de Certification de Cybersécurité (ANCC / NCCA en anglais)

Loi sur la cyberrésilience : Objectifs

- Développement de produits sûrs et sécurité by design
- Fabricants peuvent choisir le niveau de cybersécurité visé
- Certification potentiellement obligatoire à terme pour le marquage CE

1. Améliorent de la sécurité des produits par les fabriquants
2. Garantir un cadre cohérent en matière de cybersécurité
3. Améliorer la transparence des propriétés de sécurité des produits
4. Permettre aux entreprises et aux consommateurs d'utiliser des produits sécurisés

3 Niveaux de Certification

Niveau élémentaire

- Cibles : objets grand public (ex : Internet des objets – IOT) ;
- Auto-évaluation des produits par leur fabricant (émission d'une attestation de conformité) ;

Niveau substantiel

- Cible : risque médian
- Évaluation de la conformité par un Organisme d'Evaluation de la Conformité (OEC / CAB en anglais) via un certificat

Niveau élevé

- Cible les solutions avec un risque d'attaques impliquant des compétences « significatives »
- Obligation de faire effectuer, par un tiers de confiance compétent, des tests de pénétration
- Certification est délivrée par une ANCC

Plan

Démarche

Publiée en octobre 2005 et révisée en 2013.

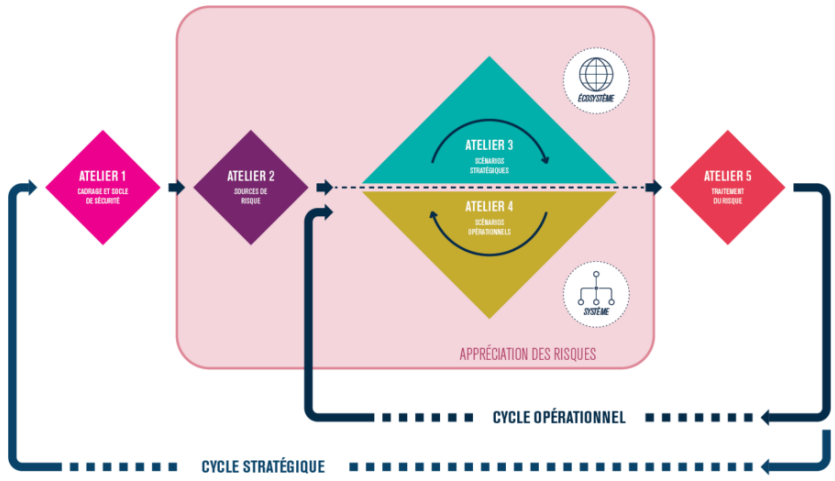
1. Phase d'établissement
2. Phase d'implémentation
3. Phase de maintien
4. Phase d'amélioration

SMSI : Système de management de la sécurité de l'information

Phase d'établissement (PLAN)

1. Définir la politique et le périmètre du SMSI
2. Identifier et évaluer les risques liés à la sécurité et élaborer la politique de sécurité (EBIOS)
3. Traiter le risque et identifier le risque résiduel par un plan de gestion (Évitement, réduction, transfert, acceptation)
4. Choisir les mesures de sécurité à mettre en place

EBIOS-RM



5 ateliers :

1. Périmètre : Identifier les actifs ;
2. Source de risque : Identifier les menaces ;
3. Scénarios stratégiques : Identifier les vulnérabilités ;
4. Scénarios opérationels : Identifier comment les exploiter ;
5. Traitement du risque : Trouver des solution.

`https://cyber.gouv.fr/la-methode-ebios-risk-manager`

Common criteria levels

The higher the level is, the more verification was done

- EAL1: Functionally Tested
- EAL2: Structurally Tested
- EAL3: Methodically Tested and Checked
- EAL4: Methodically Designed, Tested and Reviewed
- EAL5: Semi-Formally Designed and Tested
- EAL6: Semi-Formally Verified Design and Tested
- EAL7: Formally Verified Design and Tested

Plan

Competitive Intelligence

Control and protection of strategic information useful for any economic actor

3 piliers

- Information mastery, knowledge management
- Protection of information assets
- Influence strategy and lobbying

Information mastery

- Identify sources
- Collect information (monitoring, social networks ...)
- Exploitation: analysis and decision support
- Diffusion :

Protection of information

"**Only paranoiac survive**"

Andy GROVE, Co-fondator of Intel in 1968

Protection of information

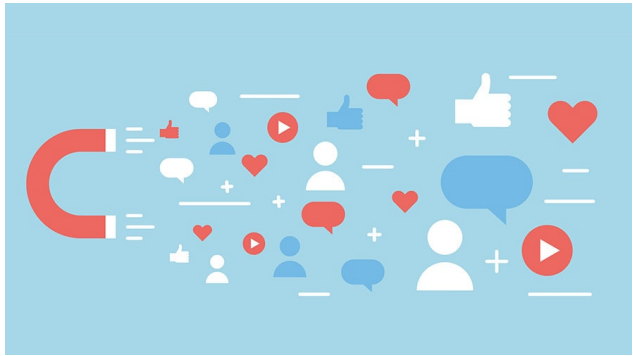
"**Only paranoiac survive**"

Andy GROVE, Co-fondator of Intel in 1968

1. Classification of information
2. Diagnosis
3. Access Protection
4. Awareness
5. Monitoring, detection

Strategies of Influence

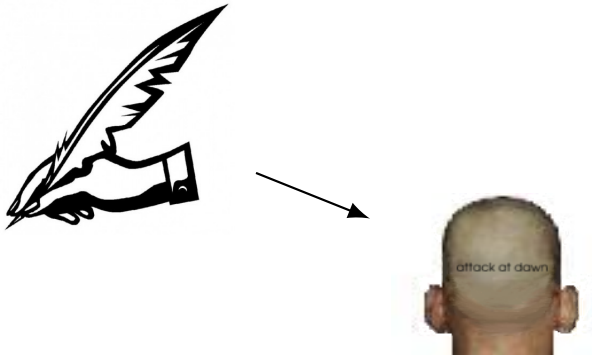
- Press, media
- Blog, social networks
- Crisis communication : information / disinformation



Plan

L'art de cacher un secret écrit

L'art de cacher un secret écrit



Stéganographie

L'art de cacher un secret écrit

Cryptographie

Stéganographie

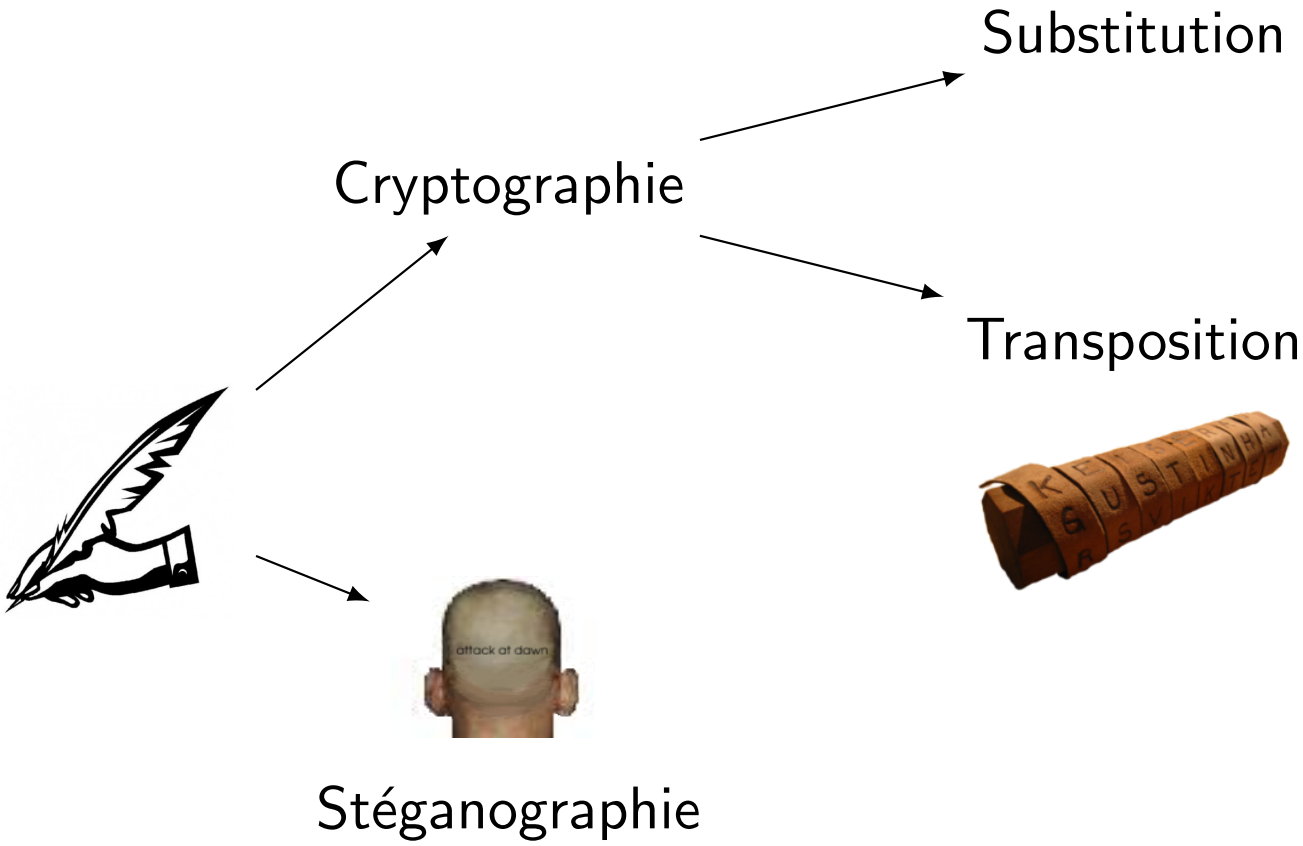
L'art de cacher un secret écrit

Cryptographie

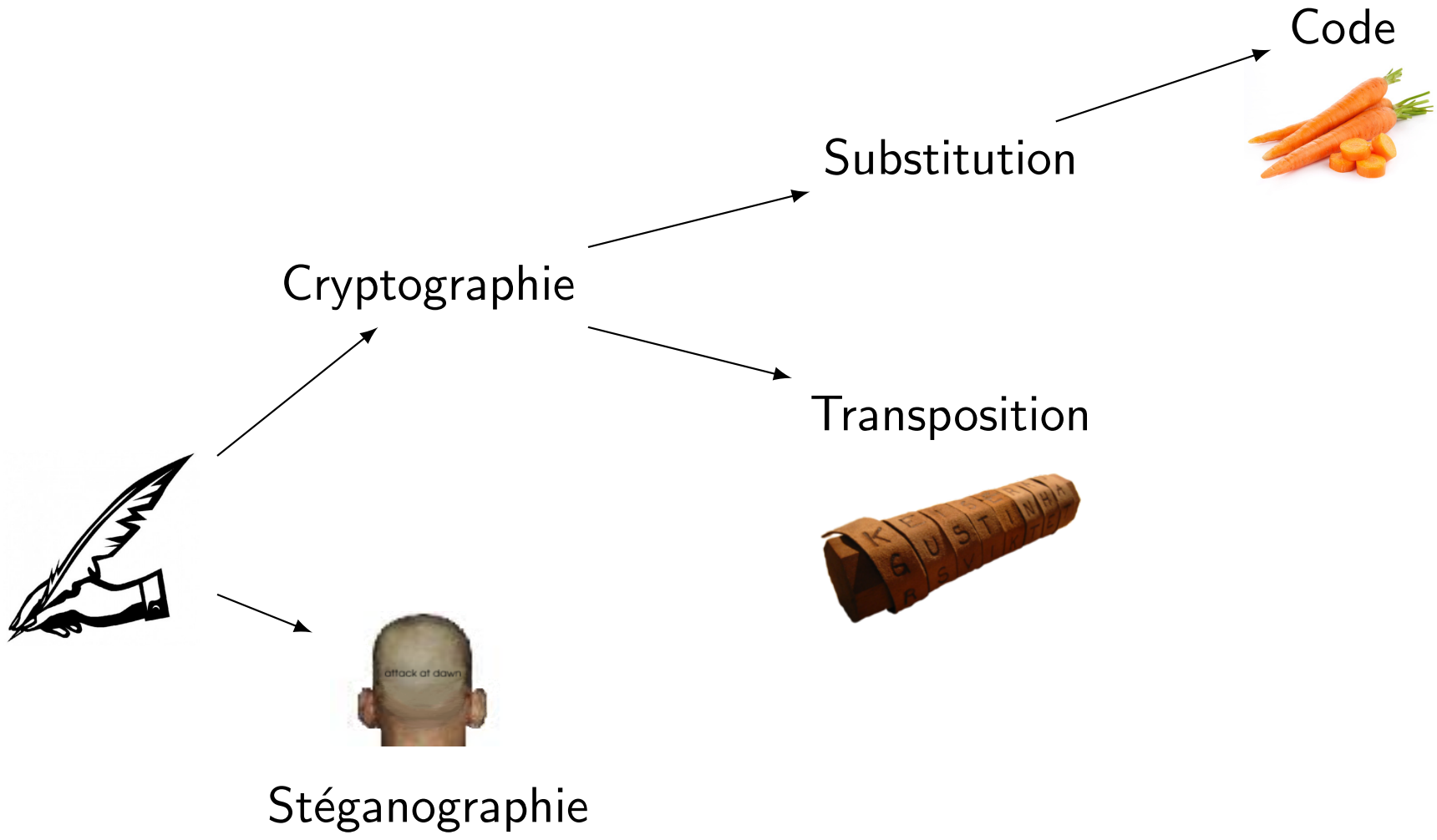
Stéganographie

Transposition

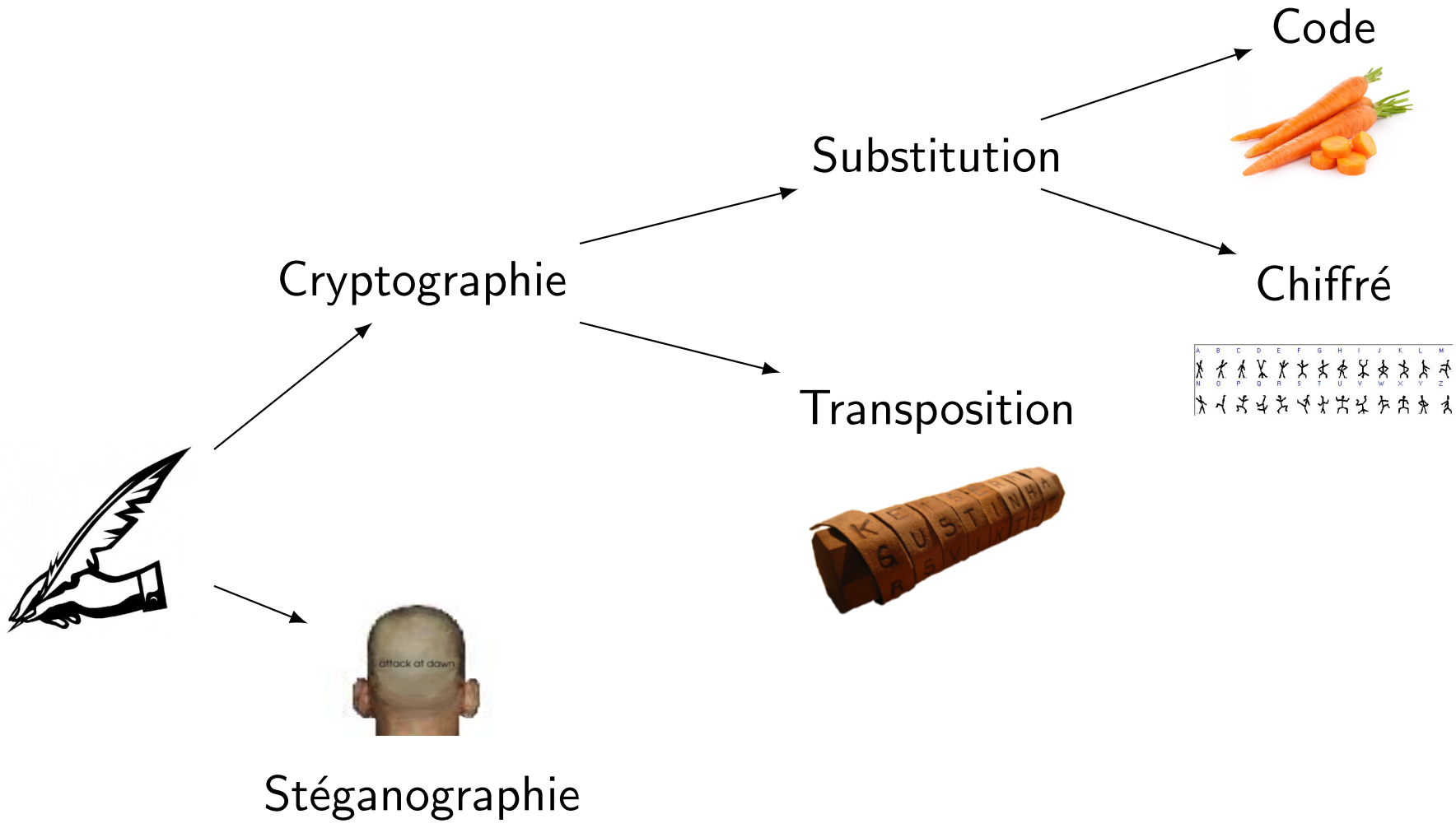
L'art de cacher un secret écrit



L'art de cacher un secret écrit



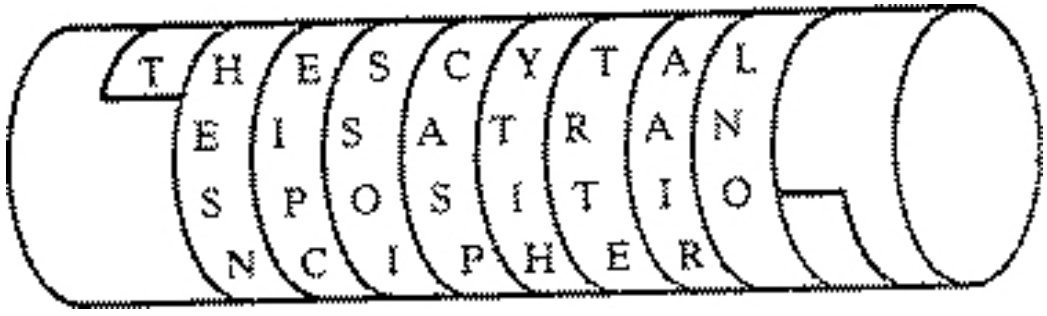
L'art de cacher un secret écrit



Applications

Les grecs inventent la Scythale

Les grecs inventent la Scythale



Transposition

Les Romains

Chiffrement de César
Substitution +3

Les Romains

Chiffrement de César
Substitution +3

Dyh Fhvdu

Les Romains

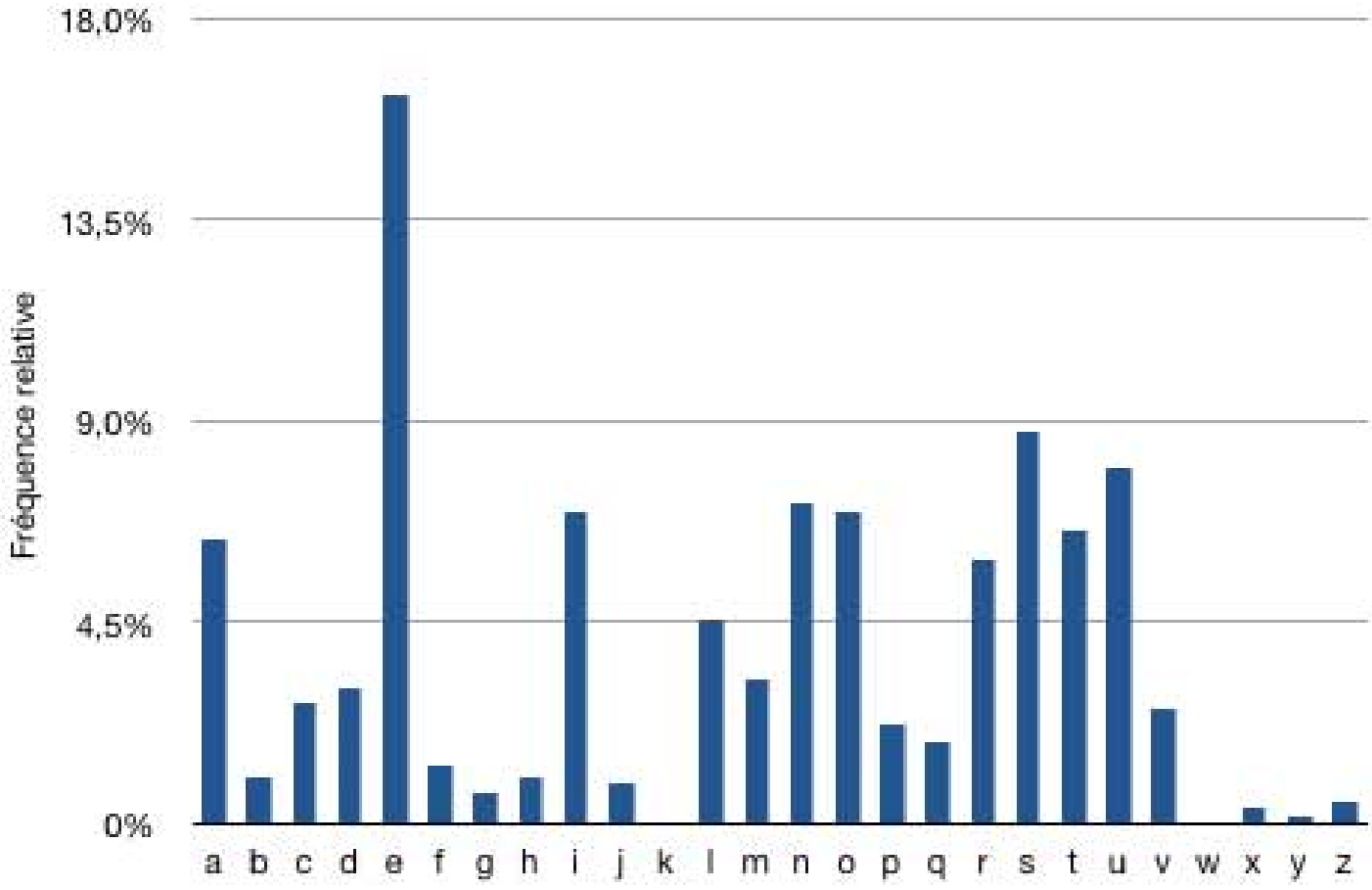
Chiffrement de César
Substitution +3

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

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

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

Kerchoff's Principle

In 1883, a Dutch linguist Auguste Kerchoff von Nieuwenhof stated in his book "La Cryptographie Militaire" that:

"the security of a crypto-system must be totally dependent on the secrecy of the key, not the secrecy of the algorithm."

Author's name sometimes spelled Kerckhoff

Chiffrement : Enigma (Seconde guerre mondiale)


+

=

Chiffrement : Enigma (Seconde guerre mondiale)


+

=


Chiffrement : Enigma (Seconde guerre mondiale)


+

=



+

=

Chiffrement : Enigma (Seconde guerre mondiale)


+

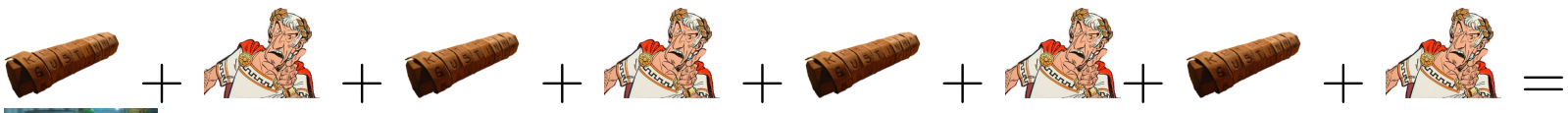
=



+

=


Chiffrement : Enigma (Seconde guerre mondiale)



One-Time Pad (Chiffrement de Vernam 1917)

Exemple:

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

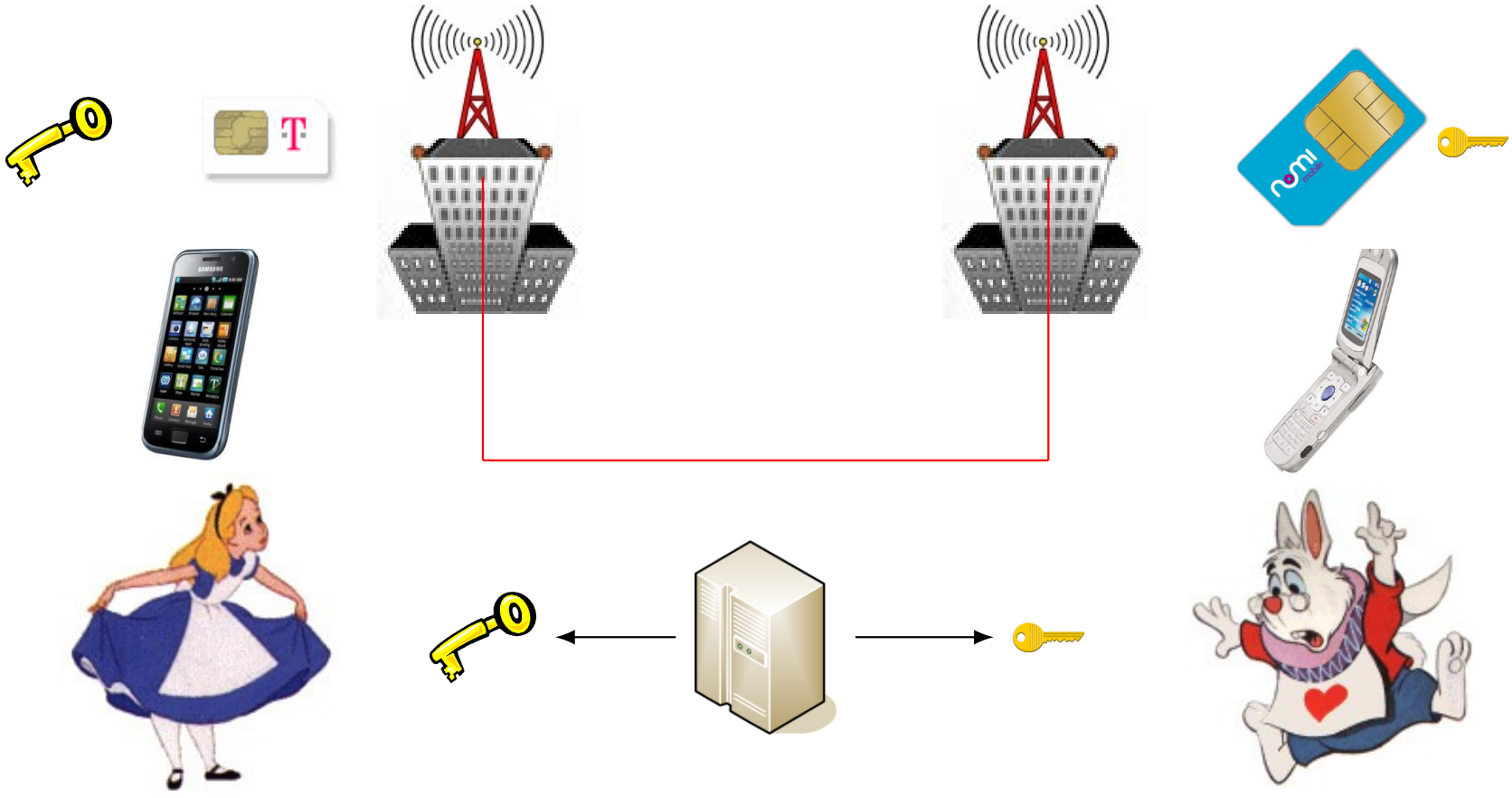
Plan

Clef symétrique

Exemples

- DES
- AES

Communications téléphoniques



Chiffrement à clef publique

Exemples

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

Comparison

- Size of the key
- Complexity of computation (time, hardware, cost ...)
- Number of different keys ?
- Key distribution
- Signature only possible with asymmetric scheme

Computational cost of encryption

2 hours of video (assumes 3Ghz CPU)

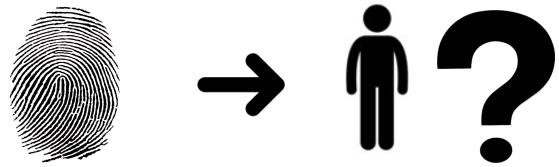
	DVD 4,7 G.B		Blu-Ray 25 GB	
Schemes	encrypt	decrypt	encrypt	decrypt
RSA 2048(1)	22 min	24 h	115 min	130 h
RSA 1024(1)	21 min	10 h	111 min	53 h
AES CTR(2)	20 sec	20 sec	105 sec	105 sec

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

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

Propriétés de résitance

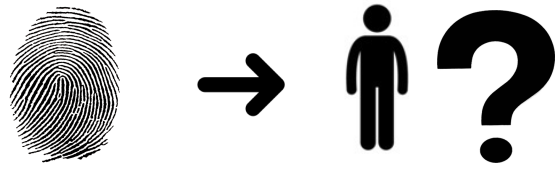
- Pré-image



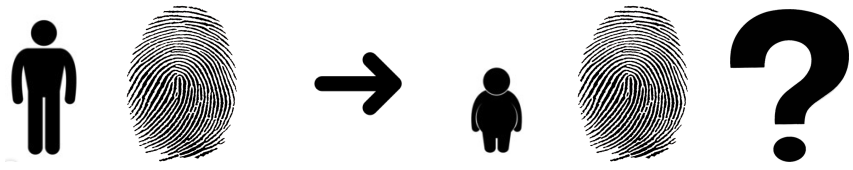
Fonction de Hachage (SHA-1, SHA-3)

Propriétés de résitance

- Pré-image



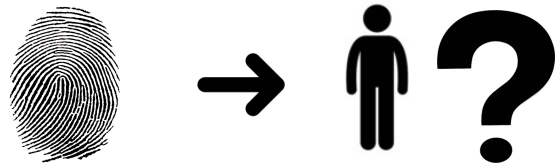
- Seconde Pré-image



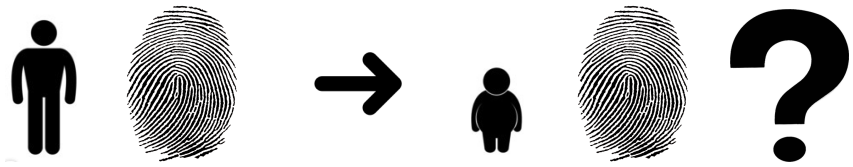
Fonction de Hachage (SHA-1, SHA-3)

Propriétés de résitance

- Pré-image

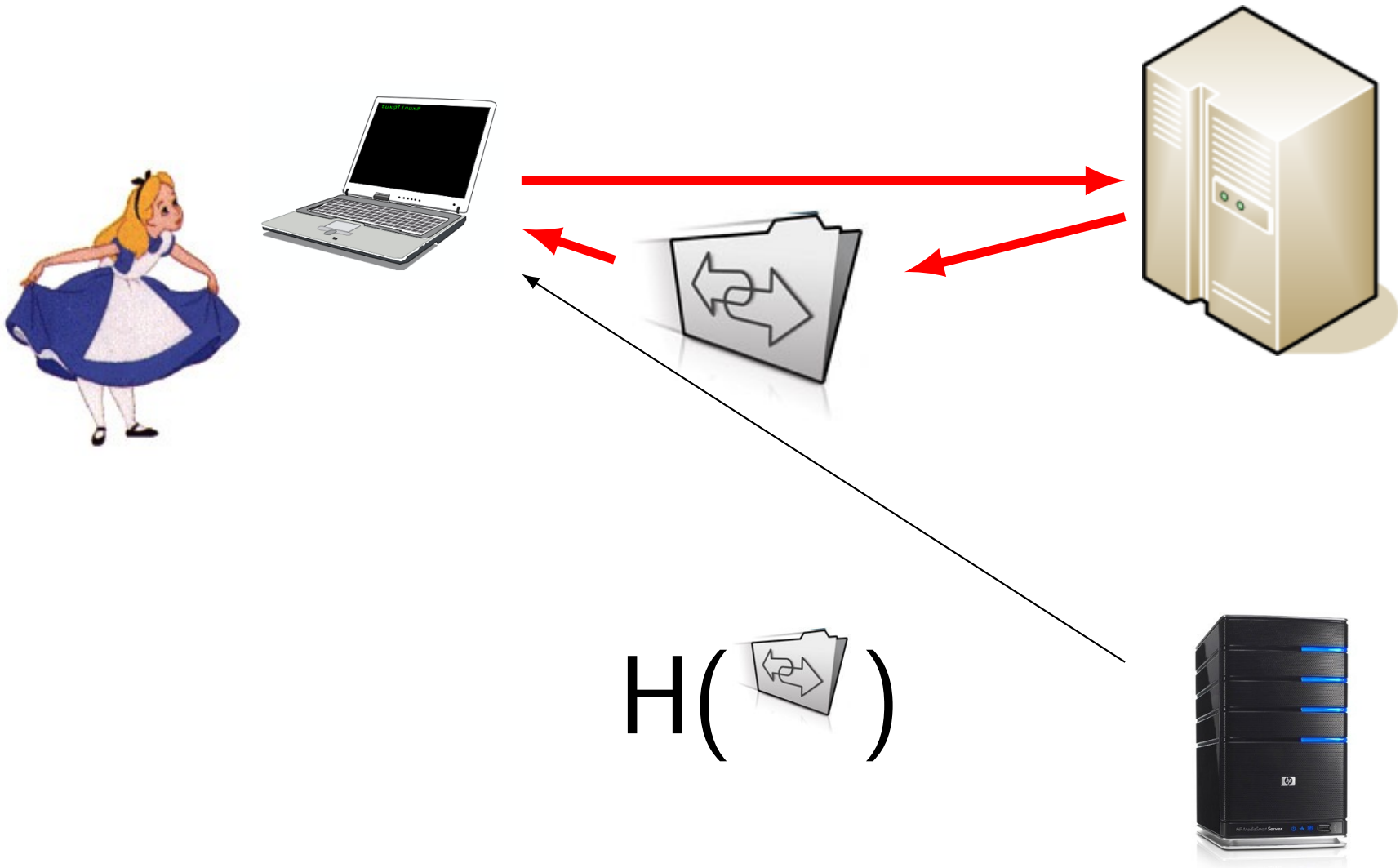


- Seconde Pré-image

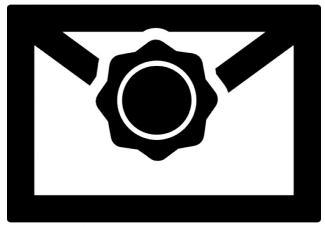


- Collision

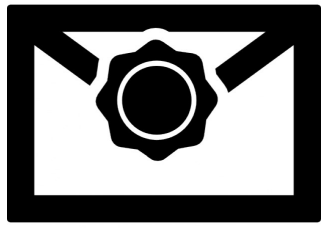
Installation de logiciel

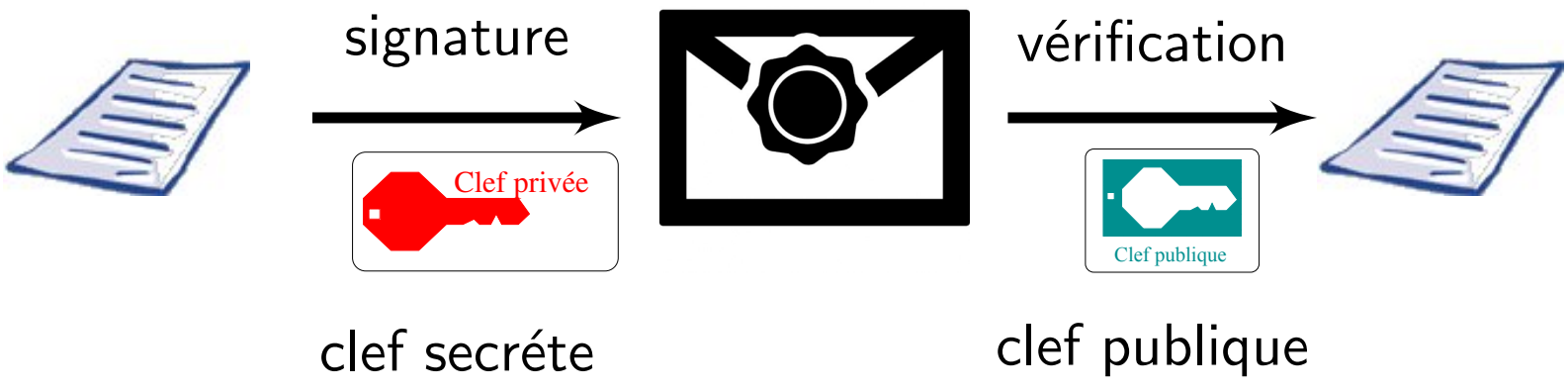


Signature



Signature





RSA: $m^d \mod n$

Application : éviter la "*fraude au président*"

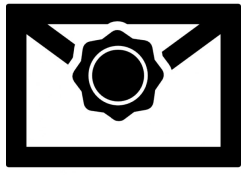
- En 2010 $>$ 485 millions d'euros
- En 5 ans 2.300 plaintes ont été déposées,

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

Today

1. Introduction
2. GDPR
3. Historic of Cryprography
4. Cryptographic primitives

Ron Rivest

“Once you have something on the Internet, you are telling the world, please come hack me.”