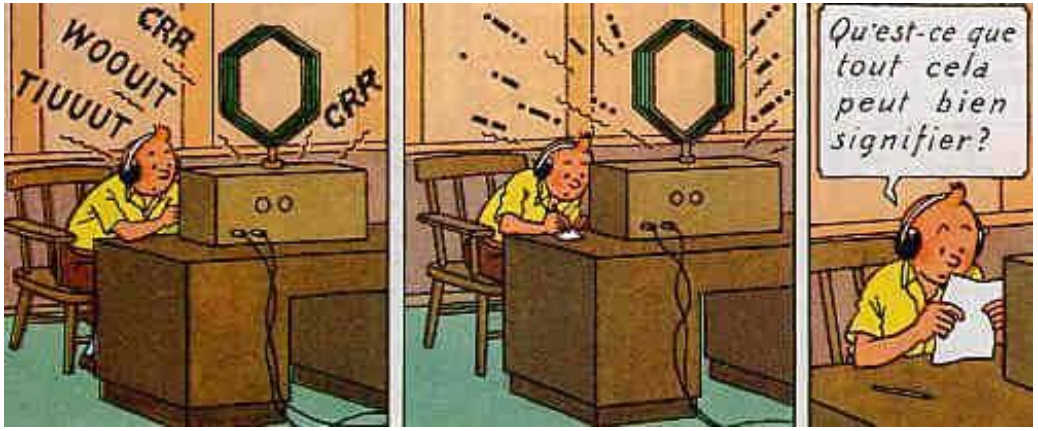
Présentation générale de la Cryptographie

Jacques Patarin

Qu’est-ce que la Cryptographie ?



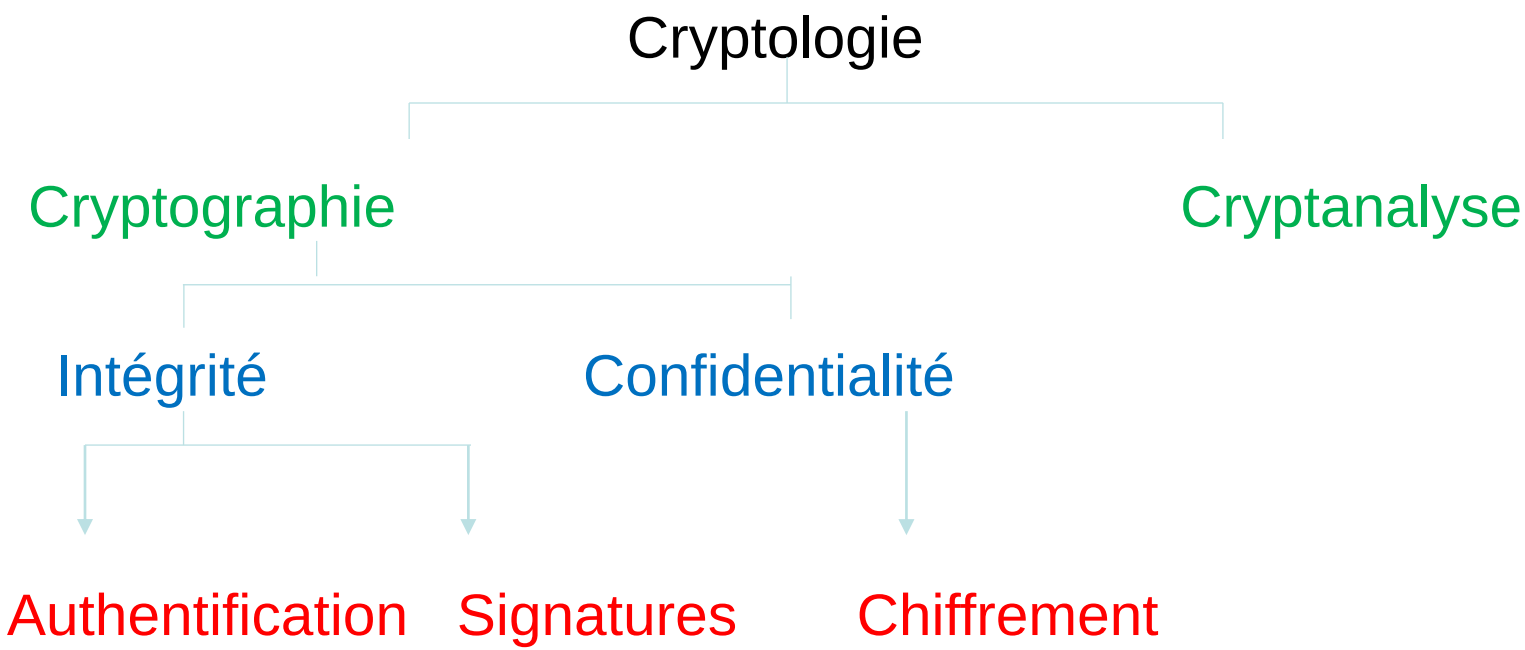
Une définition actuelle

- La Cryptologie est la science des communications sécurisée. (C'est ce que le grand public nomme « les codes secrets »).

- La Cryptographie regroupe les techniques de défense.

- La Cryptanalyse regroupe les techniques d'attaque.

- Les « trois piliers » de la Cryptographie sont : le chiffrement, les signatures et l'authentification.


Cryptologie
Cryptographie
Cryptanalyse
Intégrité
Confidentialité
Authentification
Signatures
Chiffrement

Le chiffrement à clé secrète

- Alice veut envoyer un message à Bob en utilisant une ligne que Charlie peut écouter. Comment faire ?

- Alice chiffre. Bob déchiffre. Charlie essayer de décrypter.

Charlie

Alice

K

Bob

K

Le chiffrement à clé publique

- Alice veut envoyer un message à Bob en utilisant une ligne que Charlie peut écouter. Comment faire ?

- Alice chiffre. Bob déchiffre. Charlie essayer de décrypter.

Alice

Charlie

Bob

K

Il est possible de chiffrer sans avoir de secrets. (Mais il en faut toujours pour déchiffrer).

L’authentification à clé secrète

- Alice veut prouver à Bob qu’elle est Alice (en utilisant une ligne que Charlie peut écouter). Comment faire ?

Charlie

Alice

Bob

K

K

Bob envoie un défi à Alice. Alice doit répondre au défi.

L’authentification à clé publique

- Alice veut prouver à Bob qu’elle est Alice (en utilisant une ligne que Charlie peut écouter). Comment faire ?

Alice

Charlie

Bob

K

Il est possible de vérifier qu’Alice est bien Alice sans avoir de secrets. Mais il faut toujours avoir un secret pour s’authentifier.

Les signatures à clé secrète
(MAC : Message Authentication Code)

- Alice veut envoyer un message signé à Bob (en utilisant une ligne que Charlie peut écouter). Comment faire ?

- Alice signe, Bob vérifie la signature.

Charlie

Alice

K

Bob

K

Les signatures à clé publique

- Alice veut envoyer un message signé à Bob (en utilisant une ligne que Charlie peut écouter). Comment faire ?

- Alice signe, Bob vérifie la signature.

Alice

Charlie

Bob

K

Il est possible de vérifier une signature sans avoir de secrets.

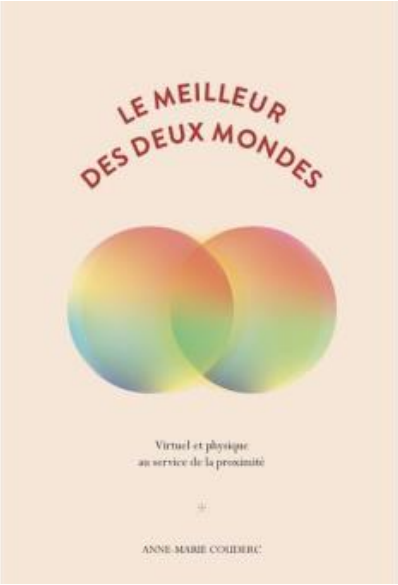
Mais il faut toujours avoir un secret pour pouvoir signer.

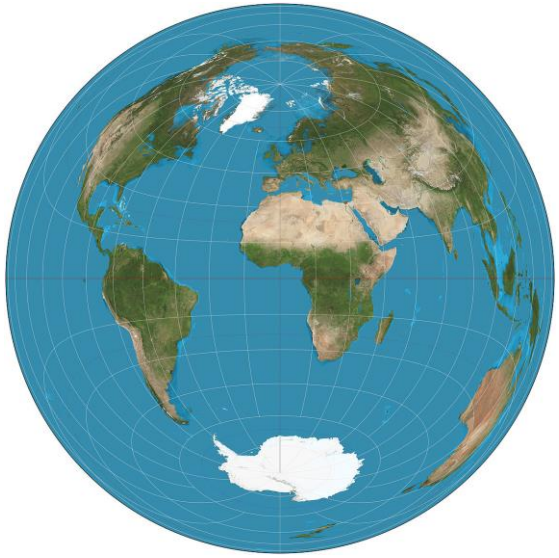
Système combiné : clé publique puis clé secrète

- Bien souvent on utilise le meilleur des deux mondes (les algorithmes à clé secrète sont plus rapides).

Typiquement :

- On transmet une clé K par RSA puis on utilise l'AES avec K.
- Ou bien : on génère une clé de session K via Diffie-Hellman, puis on utilise l'AES avec K.



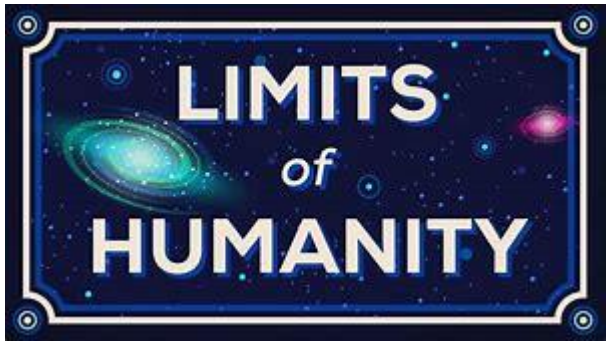


D’où vient la sécurité ? (1/3)

La cryptographie pose d’emblé aux mathématiques et à la physique des questions sur leurs limites.

Or il est souvent très difficile de connaître les limites de l’informatique et de la physique…

Il est aussi difficile d’évaluer les limites humaines…



D'où vient la sécurité ? (2/3)

- A priori, la sécurité peut venir :

1) De la théorie de l'information (< 1% des cas actuellement) : l'attaquant n'a pas assez d'information pour casser le système, même avec une puissance de calcul infinie.

2) De la théorie de la complexité (> 99% des cas actuellement) : l'attaquant pourrait casser le système s'il avait assez de puissance de calculs, mais cette puissance de calcul est irréaliste.

3) Des lois de la physique quantique (< 1% des cas actuellement).

D’où vient la sécurité ? (3/3)

Il existe en fait des attaques de types très différents :

- Attaques purement mathématiques, soit sur les algorithmes eux mêmes, soit sur la façon dont ces algorithmes sont utilisés (génération des clés, protocoles, variantes des algorithmes).
  (« Cryptanalyse »).

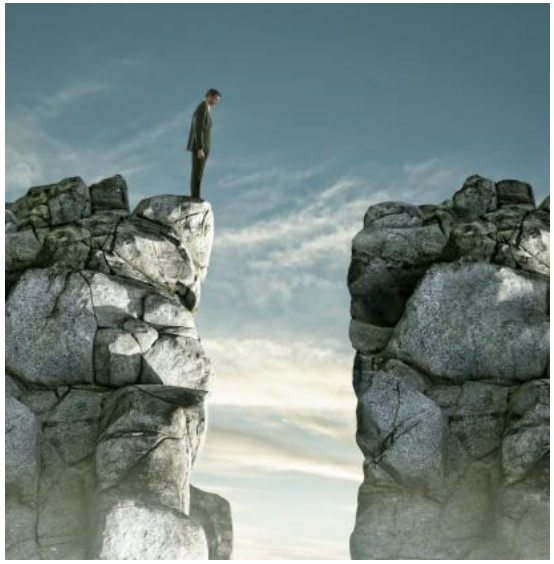
- Attaques physiques sur les composants (« Side channel attacks »).

- Exploitation de faiblesses humaines (« social engineering »).

2^{80} ou 2^{128} : le « standard de sécurité »

- D'après une des fameuses la « loi de Moore » la puissance de calcul des microprocesseurs double tous les 2 ans environ.

- Ainsi, en cryptographie basée sur la théorie de la complexité, en 1976 le « standard de sécurité » était-il de 2^{56} calculs, alors qu'actuellement il est entre 2^{80} et 2^{128} calculs.
- Les clés AES font : 128, 192 ou 256 bits.
- Les clés RSA font typiquement entre 1024 et 3000 bits.



Les puissances de 2

- $2^{10} = 1024$ (k : kilo)
- 2^{20} : environ 1 million (M : Mega)
- 2^{30} : environ 1 milliard (G : Giga) (US : « billion »)
- 2^{40} : environ 1000 milliards (T : Téra) (Fr : « billion », US : « trillion »)
- 2^{50} : env. 1 million de milliards (P : Peta) (Fr : « billiard », US : « quadrillion »)
- 2^{60} : environ 1 milliard de milliards (E : Exa) (Fr : « trillion », US : quintillion »)
- 2^{70} : environ 1000 milliards de milliards (Z : Zetta) (Fr : « trilliard », US : « sextillion »).

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
1	2	4	8	16	32	64	128	256	512	1024	2048

Exemples de puissance de calcul (1/2)

- Avec le PC le plus puissant de 2018 (1 seul PC boosté à 4,4 GHz sur 1 an de calcul en utilisant les 18 cœurs de façon optimale) : 2^{64} opérations.
- En faisant environ autant de calculs que ce qui a été fait en 2018 pour casser SHA_1 : 2^{70} opérations
- En utilisant la totalité des moyens de calcul des projets BOINC (311 000 participants à temps partiel) : $2^{78,3}$ opérations
- Avec un virus qui infecterait 2 millions de PC pour faire des calculs, ou bien avec le superordinateur le plus puissant du monde (93 PFlops) sur 1 an : $2^{81,3}$ opérations
- Avec les 500 superordinateurs les plus puissants (749 PFlops), ou bien en utilisant (ou piratant) toutes les Box Internet de la France : 1200 bits (avec $2^{83,3}$ opérations)

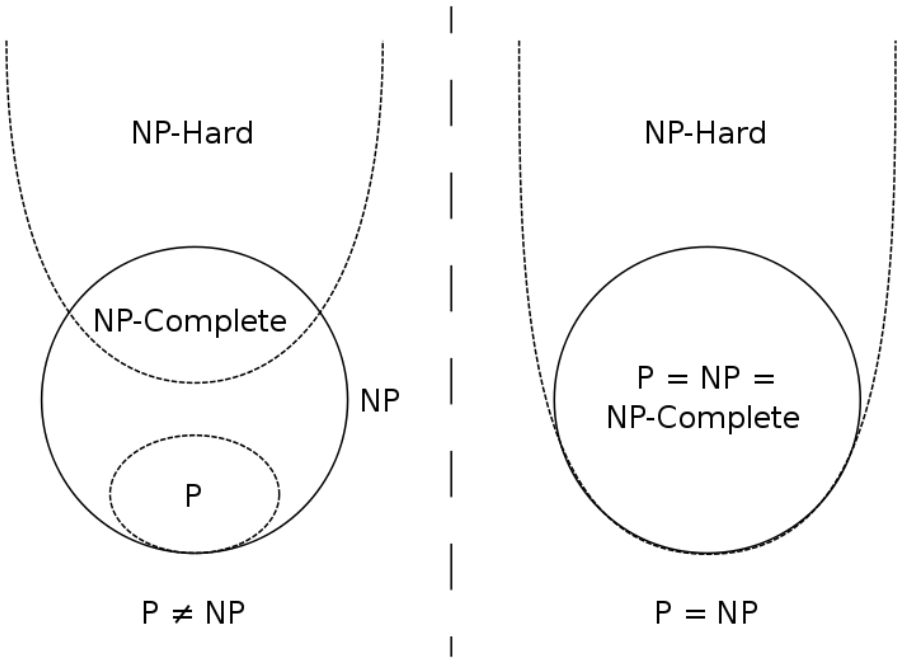
Exemples de puissance de calcul (2/2)

- Avec un superordinateur Exascale (disponible vers 2021) en une année : $2^{84,7}$ opérations
- Avec toute la puissance d'Internet de 2018 (tous les ordinateurs + tous les smartphones à pleine puissance durant 1 an) : 2^{95} opérations
- Si l'on utilisait toute la production mondiale d'électricité durant 1 an sur les meilleurs composants Turing complets de 2017 : 2^{99} opérations.
- En faisant 80 zettaflops sur 1 an (environ comme le Bitcoin mining en 2018, mais ce n'est pas Turing Complet) : 2^{101} opérations.

Le problème P ≠ NP

- Ce problème est le problème le plus célèbre de toute l'informatique théorique.

- Du fait qu'il n'est pas résolu, on ne connaît pas de système cryptographique prouvé sûr dans le cadre de la théorie de la complexité (c'est-à-dire pour plus de 99% des systèmes actuels).



Identification/Authentification/Signatures/Chiffrements

Un algorithme d'authentification est un algorithme qui permet à Alice de prouver à Bob qu'elle est Alice.

Un algorithme d'identification est un algorithme qui permet à Alice de prouver à Bob qu'elle est soit Alice, soit Bob.

A partir d'un algorithme d'Authentification (mais pas d'Identification) on peut construire des signatures à clé publique (via le procédé Fiat-Shamir).

Signatures

Chiffrement

Authentification → Identification