LA CRYPTOGRAPHIE ET LA SÉCURITÉ DE L'INFORMATION:

Quels enjeux éthiques?

Par Anne-Sophie Letellier

PLAN DE LA SÉANCE

- Mise en contexte
- Qu'est-ce que la cryptographie?
- Les crypto-wars
- Les cypherpunks
- Le dark web et les crypto-wars aujourd'hui
- La cryptographie pour tous

1- MISE EN CONTEXTE

- Savez-vous ce qu'est le chiffrement?
- Avez-vous des exemples de communications ou d'information qui sont chiffrées?

2- QU'EST-CE QUE LA CRYPTOGRAPHIE?

- La cryptographie « est l'étude et l'application de techniques, de méthodes, de principes et de systèmes qui protègent l'information d'adversaires » (Gill *et al.*, 2018, p.1)
- Le chiffrement des communications est un processus mathématique qui utilise un algorithme (cipher) dans l'objectif de modifier un texte (texte clair) ou une information en une série de caractères incompréhensibles (ciphertexte). Le processus de chiffrement requiert qu'une clé soit appliquée à l'algorithme pour le rendre unique.
- Le déchiffrement des communications est le processus inverse: la clé est utilisée afin de permettre à l'algorithme de retransformer le ciphertexte en texte clair.

chiffrement

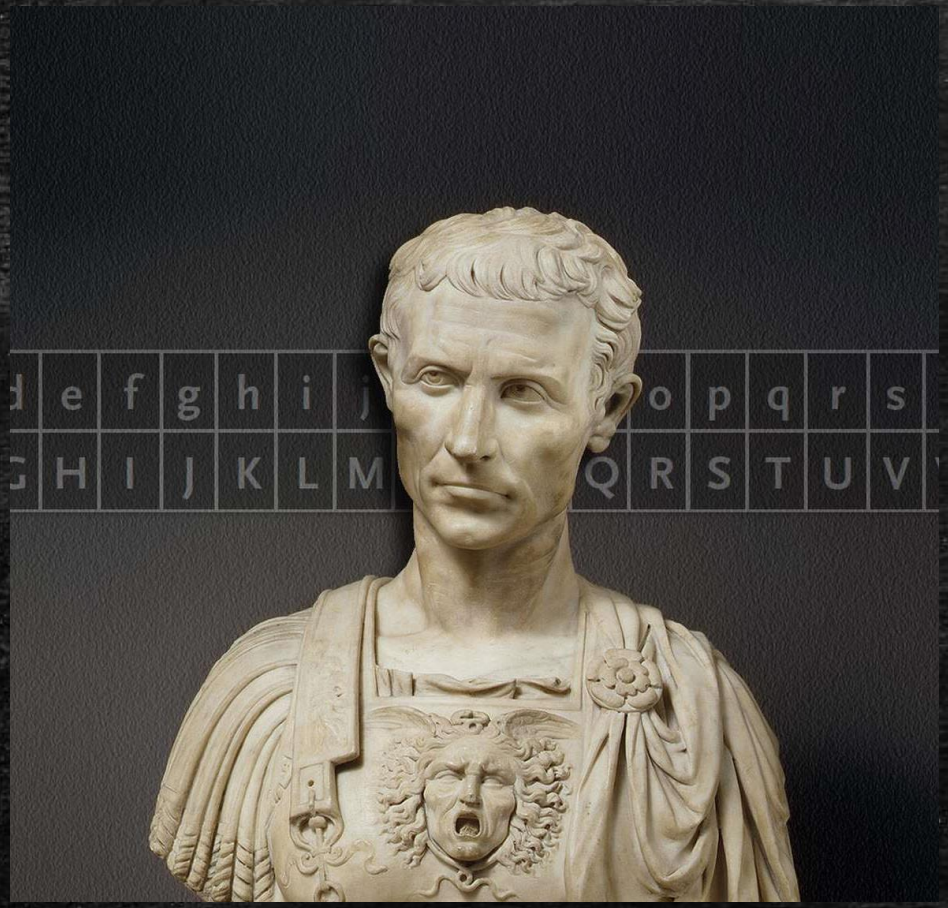
$$C = E_k(M)$$

déchiffrement

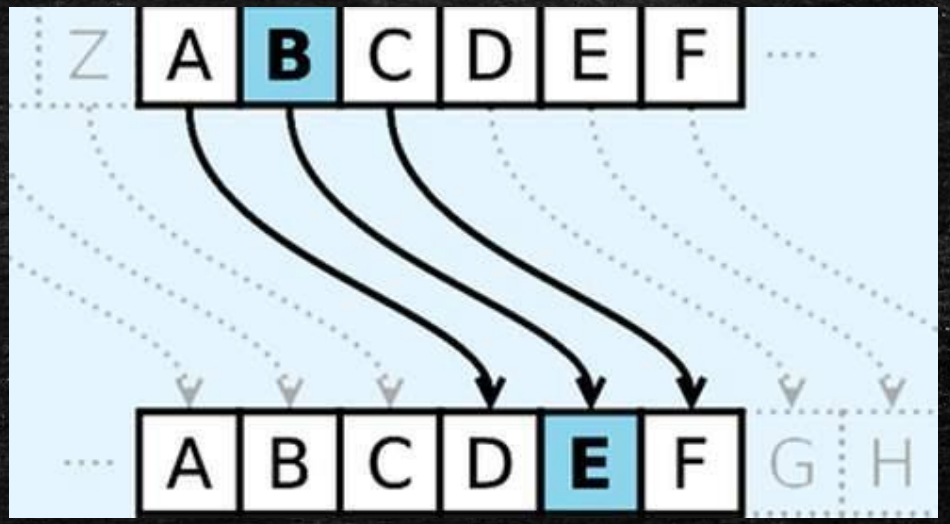
$$M = E_k(C)$$

C: message chiffré (ciphertext)
E: algorithme de chiffrement (cipher)
K: Clé de chiffrement
M: Texte clair

2- QU’EST-CE QUE LA CRYPTOGRAPHIE?



Le chiffre de César: l’un des premiers algorithmes de chiffrement



2- QU'EST-CE QUE LA CRYPTOGRAPHIE?

Qu'est-ce qui détermine la solidité d'un système cryptographique?

- Qualité des algorithmes
- Qualité des clés de chiffrement
- Qui possède les clés de chiffrement
  - Accès des intermédiaires
  - Chiffrement de bout-en-bout (en anglais: *end-to-end encryption* ou E2EE)

2- QU'EST-CE QUE LA CRYPTOGRAPHIE?

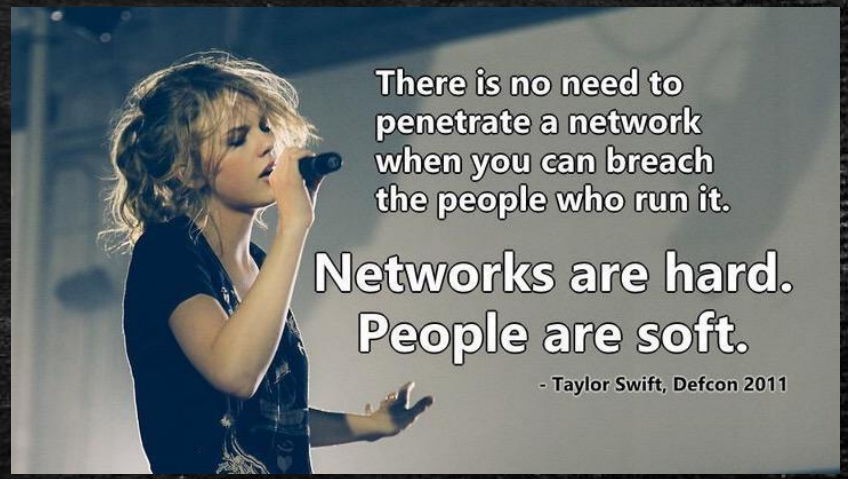
Est-il possible de déchiffrer un message chiffré?

- Les **attaques de forces brutes** font référence au fait qu'un tiers parti puisse déchiffrer un message sans préalablement posséder la clé en tentant de deviner systématiquement et « aléatoirement » des combinaisons alphanumériques jusqu'à ce la bonne combinaison soit trouvée.

- La **cryptanalyse** implique l'utilisation de techniques mathématiques dans le but d'identifier des erreurs, des faiblesses ou des *patterns* dans un système de chiffrement qui lui permettront de « deviner » ou trouver une clé plus rapidement qu'en utilisant une attaque de force brute.

- **Déchiffrement forcé/ divulgation des clés** fait référence au processus où une autorité oblige un individu ou une compagnie à déchiffrer les communications chiffrées

- **Ingénierie sociale** création d'un contexte où l'on dupe quelqu'un à révéler une clé pour permettre le déchiffrement de communications



3- LES CRYPTO-WARS: un peu d’histoire

Le chiffrement et l’Internet: une affaire d’État;

Rôle clé dans la Deuxième Guerre Mondiale

Les algorithmes et logiciels de chiffrement ont longtemps été considérés aux yeux de la lois comme des armes

3- LES CRYPTO-WARS: un peu d'histoire

Au début des années 1990, un point tournant:

Rivest, Shamir et Adleman utilisent pour la première fois l'analogie de l'envelope pour décrire l'impact des systèmes cryptographiques

- Déplace l'analogie du chiffrement depuis un enjeu militaire jusqu'à un enjeu « populaire »
- Le chiffrement devient (rapidement) un intérêt « populaire », établissant pour la première fois une tension avec la compréhension usuelle du terme associé au domaine militaire et au « secret de la guerre »

1976: Whitfield Diffie et Martin Hellman publient un article qui établit les fondements de la cryptographie à clé publique

- Un nombre grandissant de hackers et de cryptographes s'intéressent donc au chiffrement

3- LES CRYPTO-WARS: un peu d’histoire

Jusqu’en 1990, deux tendances se développent en tension

Les entreprises constatent que le chiffrement est un outil essentiel pour développer des nouvelles opportunités d'affaires et des activistes se soucient des enjeux de vie privée qui émergent alors que de plus en plus de communications transitent via les réseaux numériques

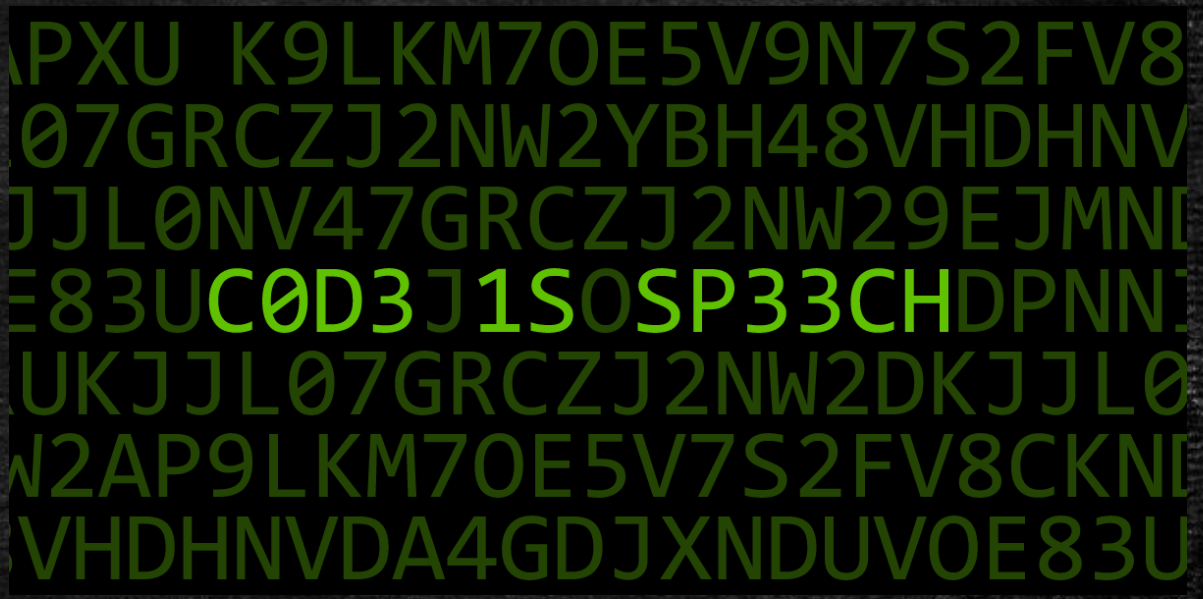
Le gouvernement américain est préoccupé que le développement d’algorithmes de chiffrement robustes nuise stratégiquement aux opérations des agences de renseignement américaines, tout en faisant perdre l’avantage d’avoir un accès facile aux communications électronique des citoyens dans le cadre d’enquêtes criminelles.

C’EST LE DÉBUT DES CRYPTO-WARS

3- LES CRYPTO-WARS: un peu d'histoire

DEUX FRONTS DES CRYPTO-WARS

1. Le contrôle des normes d'exportation des logiciels et algorithmes de chiffrement
   - Avant 1996 – toute technologie utilisant du chiffrement robuste légiférée sous le *international Traffic Arms Regulation (ITAR)*
   - Publier un algorithme en ligne était illégal
   - 1995: plusieurs décident de contester la loi devant les tribunaux
   - 1999: Dans le jugement de Bernstein v. US Department of Justice, on reconnaît que le code source d'un logiciel est une forme d'expression protégée par le 1e Amendement
2. Débats entourant l'introduction de portes dérobées dans les logiciels et services numériques

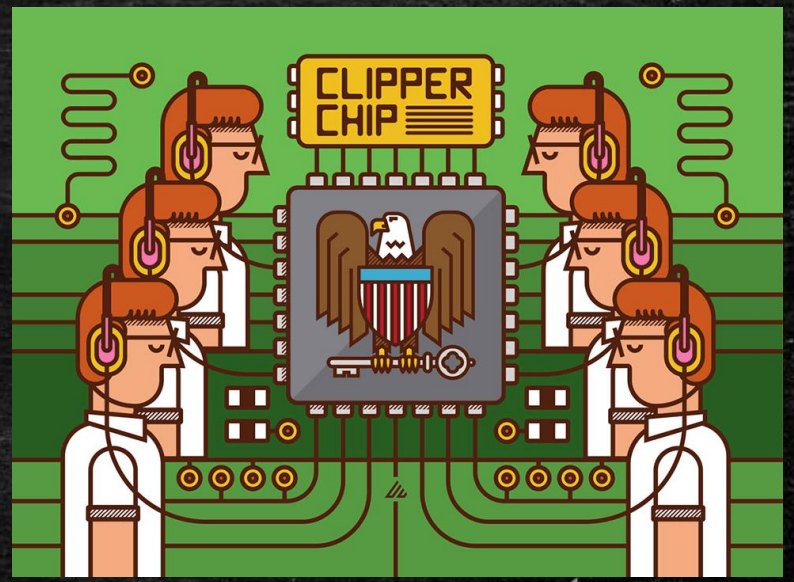


4- LES CRYPTO-WARS: un peu d'histoire

DEUX FRONTS DES CRYPTO-WARS

1. Le contrôle des normes d'exportation des logiciels et algorithmes de chiffrement
2. Débats entourant l'introduction de portes dérobées dans les logiciels et services numériques
   - Objectif de cadrer la cryptographie, dans l'imaginaire populaire, comme une épée à double tranchant
   - 1991 - proposition du « Anti-Crime Bill » - propose que les fournisseurs de services, les manufacturiers de systèmes de communications permettent au gouvernement d'obtenir le contenu de communications privées, lorsque requis par les forces de l'ordre
   - Le Clipper Chip
   - Débats sur la pertinence d'introduire des portes dérobées dans les systèmes cryptographiques

   https://www.youtube.com/watch?v=IgqJK2emrVI



5- LES CYPHERPUNKS

CYPHER: clin d'œil au texte chiffré
PUNK: clin d'œil au terme « cyberpunk »

Communauté libertarienne et anarchiste s'étant développé autour d'une liste d'envoi:

- Dans les années 1990, articulent l'idée selon laquelle la cryptographie devrait protéger les citoyens et non les secrets étatiques
- Protection de la vie privée par les mathématiques plutôt que par les "lois arbitraires et bureaucratiques"

5- LES CYPHERPUNKS

- Ce groupe s'intéresse aux politiques des technologies
- La promotion de la cryptographie et la protection de la vie privée des citoyens comme enjeu politique: « leur confiance en leur habileté de fabriquer des solutions technologiques pour des problèmes sociaux est basée dans une sensibilité éthique qui affirme la nature sacrée de la vie privée individuelle » (Coleman & Golub, p. 260)
- Communauté cypherpunk:
- « BlackNet croit que l'acte de garder un secret devrait uniquement relever de la responsabilité d'un individu » (Myers-West, 2019)
- « Privacy for the weak, and transparency for the powerful »

6- CRYPTO-WARS AUJOURD'HUI

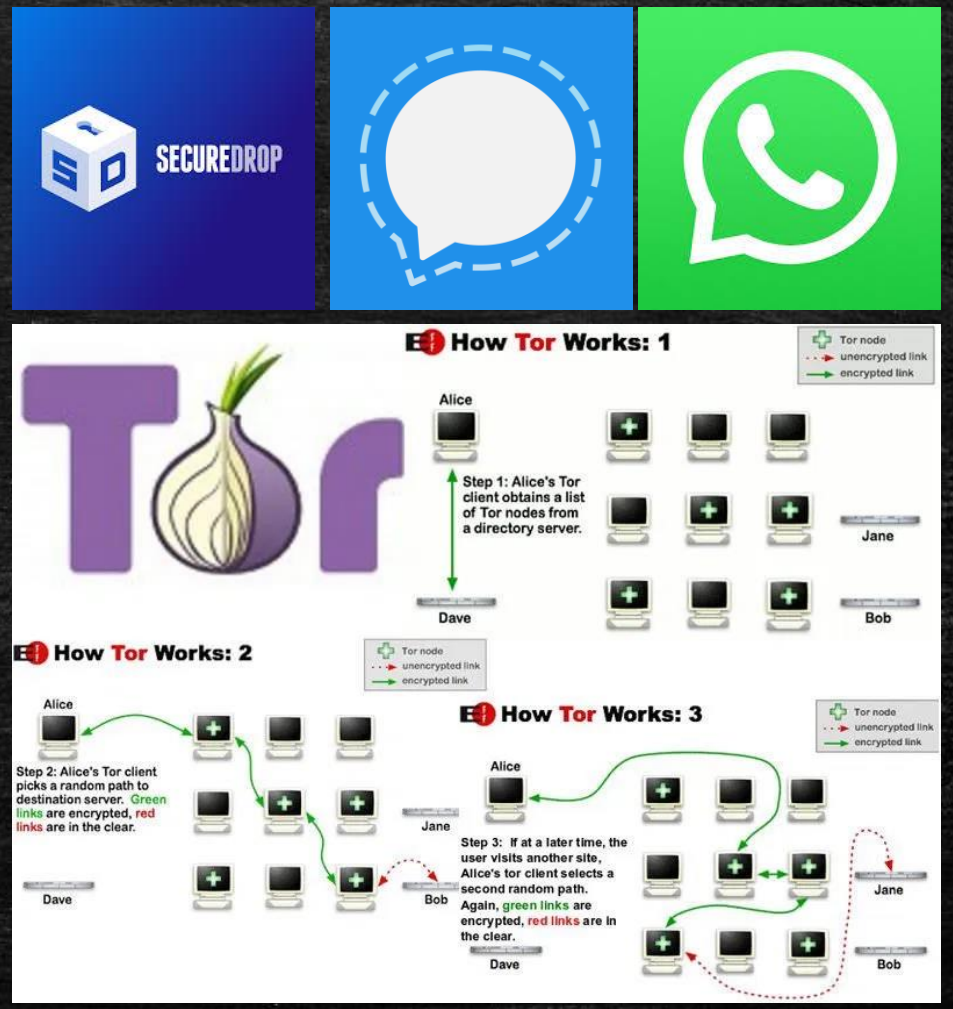
LES MILITANTS DE LA CRYPTOGRAPHIE

Lanceurs d'alerte

Batailles juridiques

Développement et popularisation d'outils de chiffrement au Canada et à l'étranger

- Vie privée
- Sécurité
- Détournement de la censure



6- CRYPTO-WARS AUJOURD'HUI

LES QUATRE CHEVALIERS DE « L'INFO-CALYPSE »

Selon Assange et al. (2010)

- Les trafiquants de drogue
- Les pédophiles
- Les terroristes
- Blanchisseurs d'argent

6- CRYPTO-WARS AUJOURD'HUI

« Les communautés de cryptographes persistent à dire qu'il est impossible d'implanter ce type d'accès sans compromettre significativement la sécurité des systèmes fait "autant l'unanimité que l'existence des changements climatiques chez les scientifiques environnementaux » (Gill et al. 2018, p. 108)

Plusieurs pays (Royaumes-Unis, Australie, Autriche, et plusieurs autres) ont ou sont en train d'adopter des lois qui:

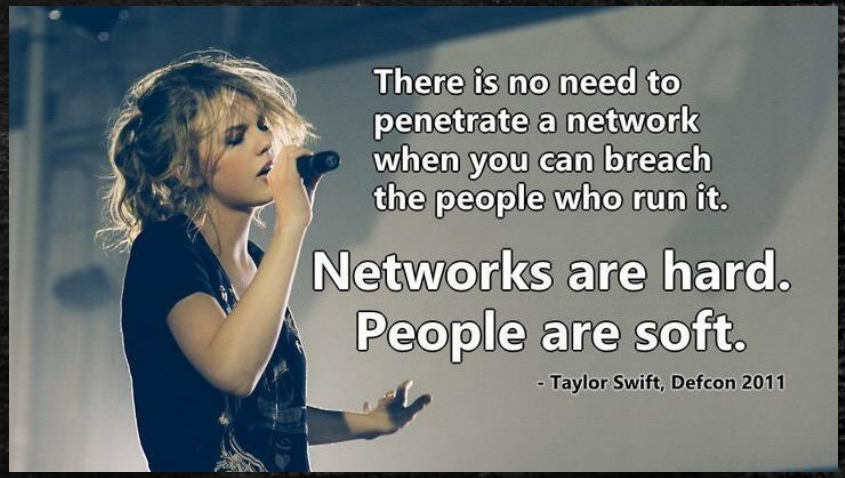
- Interdisent le chiffrement de bout-en-bout
- Pourraient obliger des compagnies à donner l'accès à des messages chiffrés.

RAPPEL

Est-il possible de déchiffrer un message chiffré?

- Les attaques de forces brutes font référence au fait qu'un tiers parti puisse déchiffrer un message sans préalablement posséder la clé en tentant de deviner systématiquement et « aléatoirement » des combinaisons alphanumériques jusqu'à ce la bonne combinaison soit trouvée.
- La cryptanalyse implique l'utilisation de techniques mathématiques dans le but d'identifier des erreurs, des faiblesses ou des *patterns* dans un système de chiffrement qui lui permettront de « deviner » ou trouver une clé plus rapidement qu'en utilisant une attaque de force brute.
- Déchiffrement forcé/ divulgation des clés fait référence au processus où une autorité oblige un individu ou une compagnie à déchiffrer les communications chiffrées
- Ingénierie sociale création d'un contexte où l'on dupe quelqu'un à révéler une clé pour permettre le déchiffrement de communications

L'introduction de portes dérobées représentent uniquement *une* solution qui s'applique au déchiffrement (cryptanalyse). Il reste donc 3 autres méthodes pour déchiffrer du contenu dans le cadre d'enquêtes.



Les critiques intersectionnelles

La compréhension des problématiques liées à la surveillance reflète les limites de leurs expériences personnelles comme hommes majoritairement blancs, occidentaux et soit libertariens, libéraux ou socialistes.

“Their articulation of civil liberties failed to recognize how certain kinds of bodies—such as black, brown, queer, trans and disabled bodies—are policed differently than others; both surveillance and the ability to speak are not evenly distributed and their vision failed to account for these differences. Ultimately, both the successes and failures of the cypherpunks serve as a rich historical case study. Those learning from it today represent a more diverse community of cryptography enthusiasts, who aim to achieve the radically inclusive project that cryptography makes possible.” (Myers-West, 2020, en ligne: https://hackcur.io/cypherpunks-write-code/)

Les critiques intersectionnelles

La différence des expériences devrait amener une différence des solutions.

- **Dans le milieu de la cryptographie:** “Ce nouvel imaginaire reconnaît que la surveillance n’est pas distribuée également dans la société – que la surveillance trouve son origine et est inséparable des pratiques de discriminations vécues par les communautés noires (Browne, 2015) et continue d’impacter de manière disproportionnelle des personnes qui se positionnent aux marges de la société. Cet imaginaire adopte également explicitement les différences au sein de la communauté et cherche à remettre en question les constructions normatives en matière de vie privée et, au lieu, mettent au centre de leurs pratiques la création d’espaces sécuritaires pour l’expression collective dans un contexte de surveillance de masse” (Myers West, 2020, p.16)
- **Dans le milieu de la cryptographie:** confusion fréquente entre la sécurité (security) et le bien-être (safety)

https://www.youtube.com/watch?v=yUqGVx-74Do