Cryptographie ancienne, moderne et future

Caesar défie l'ordinateur quantique ?!

Anca Nitulescu

Salon de la culture et des jeux mathématiques
18ème édition

Institut Henri Poincaré

UPMC SORBONNE UNIVERSITÉS

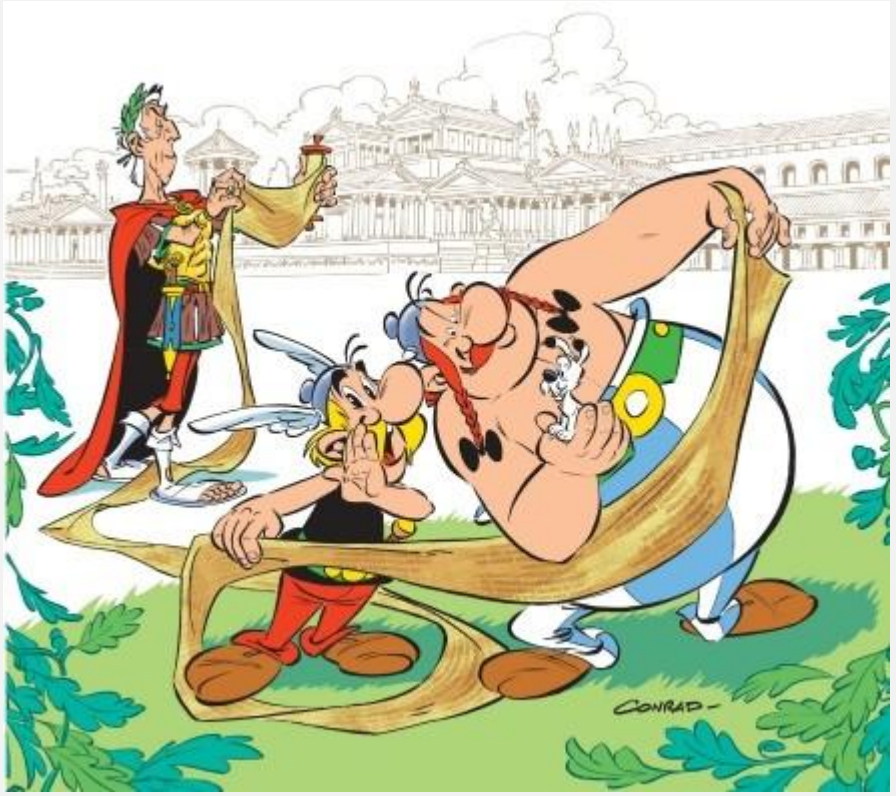
Qu'est-ce que c'est la crypto ?

La **cryptographie** est une science du codage des messages à la jointure des mathématiques, de l'informatique et même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : **le maintien du secret.**

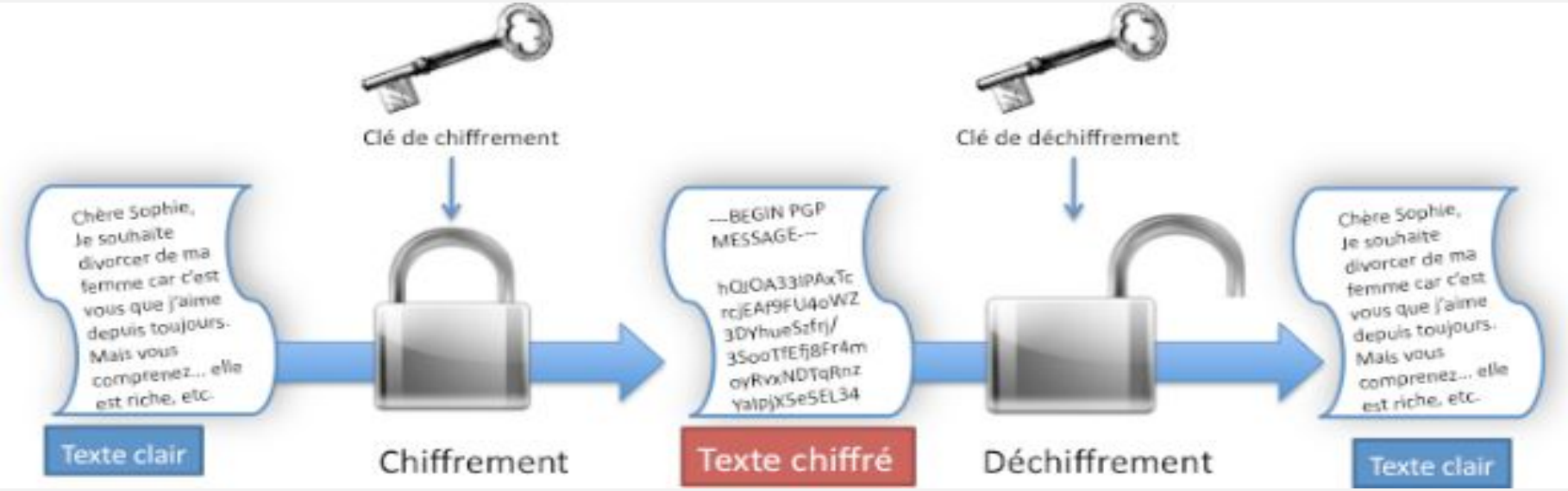
La cryptographie a pour but de protéger des informations confidentielles, limiter la lecture d'un message à son destinataire et empêcher des autres personnes à les modifier.

On parle des techniques permettant de chiffrer des messages afin de:

- les rendre incompréhensibles lors la transmission
- refuser l'accès à toute personne non autorisée
- garantir l'authenticité
- la confidentialité
- l'intégrité de l'information



Vocabulaire



Les termes utilisé dans ce domaine sont:

- **texte clair**: le message initial qui doit être chiffré
- **texte chiffré**: le message incompréhensible pour celui qui ne dispose pas de la clé de déchiffrement
- **chiffrement** : transformation à l'aide d'une clé d'un texte clair en un texte chiffré

Utilisation

L'envoi de messages sur Internet.

Les emails sont comme des cartes postales : n'importe qui se trouvant sur leur chemin peut les lire, parce qu'ils n'ont pas d'enveloppe pour cacher leur contenu !
Les chiffrer permet de garder ce contenu seulement pour l'expéditeur et le destinataire.

De manière générale, tout le monde utilise déjà la cryptographie tous les jours, souvent sans s'en rendre compte. Voici quelques activités qui l'emploient :

- lire ses emails ;
- acheter avec une carte bancaire ;
- téléphoner avec un téléphone portable.

Histoire

Utilisé depuis l'antiquité, l'une des utilisations les plus célèbres pour cette époque est le chiffre de César, nommé en référence à Jules César qui l'utilisait pour ses communications secrets. Ainsi, il pouvait empêcher que ses ennemis prennent connaissance de ses plans.

Mais la cryptographie est bien antérieure à cela : le plus ancien document chiffré date du xvie siècle av. J.-C.

Plus récemment, la cryptologie a joué un rôle important pendant les Guerres Mondiales. Churchill citait la cryptographie comme l'un des facteurs clefs de la victoire pendant le Second Guerre Mondial.

Histoire

Trois grandes étapes :

Chiffrements alphabétiques manuels (< 1500)

Chiffrements alphabétiques mécaniques (1930)

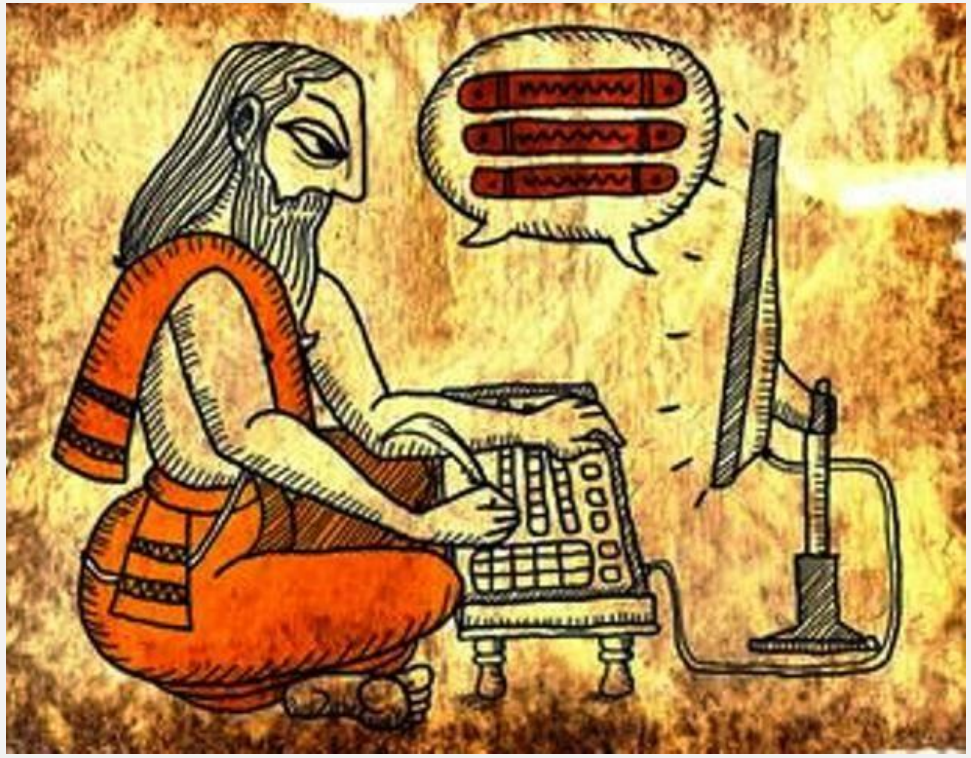
Chiffrements numériques (1990)

Futur : chiffrement quantique (> 2017)

Histoire

- **Le plus vieux document chiffré**

  Le premier « document » chiffré connu remonte à l'Antiquité. Il s'agit d'une tablette d'argile, retrouvée en Irak, et datant du XVIe siècle av. J.-C. Un potier y avait gravé sa recette secrète en supprimant des consonnes et en modifiant l'orthographe des mots.



- **La technique grecque**

  Le **scytale**, objet ancien utilisé pour le chiffrement :

- entre le Xe et le VIIe siècle av. J.-C,
- technique de chiffrement par transposition,
- utilise un bâton de diamètre déterminé appelé scytale.

Histoire

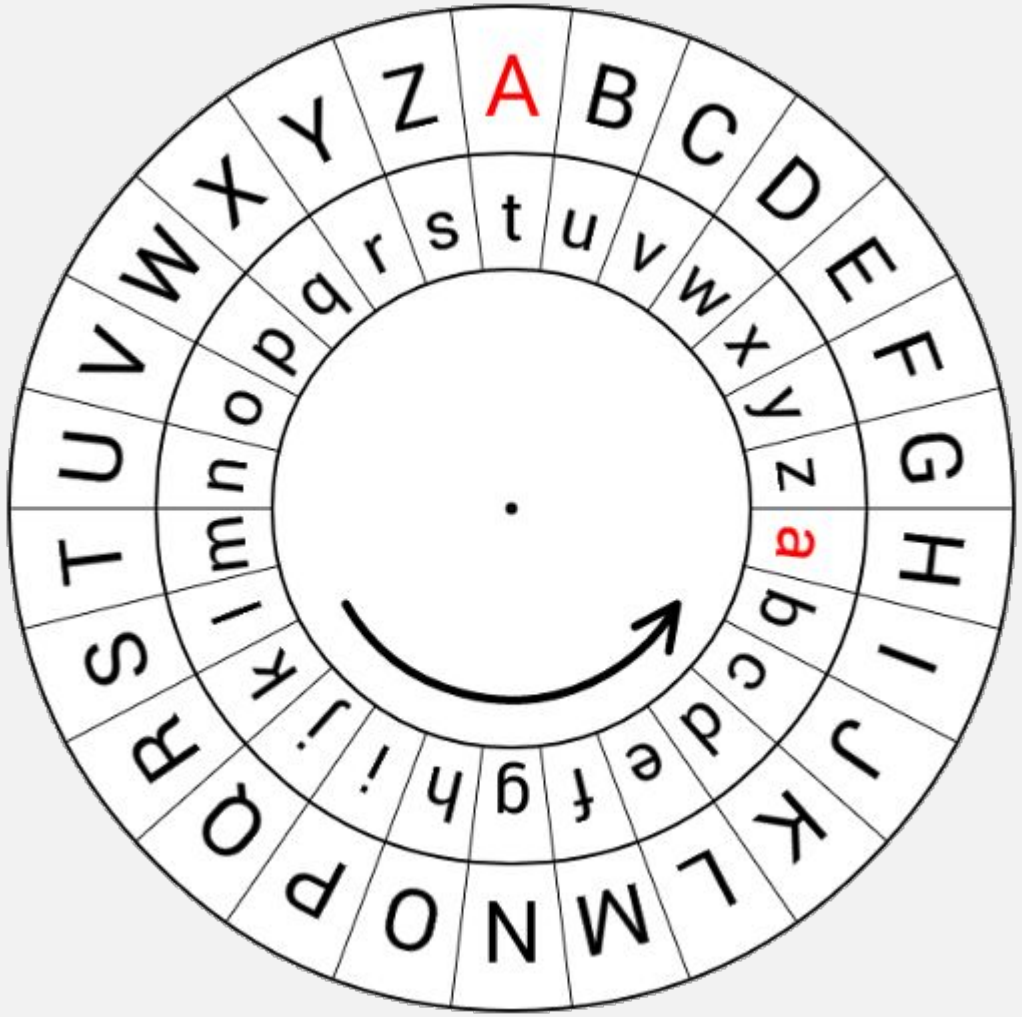
On enroulait en hélice une bande de cuir autour de la scytale avant d'y inscrire un message. Une fois déroulé, le message était envoyé au destinataire qui possédait un bâton identique, nécessaire au déchiffrement.

Le chiffre de César

Le code de César consiste en une substitution mono-alphabétique :

Chaque lettre est remplacée par une seule autre, selon un certain décalage dans l'alphabet ou de façon arbitraire.

Disque de César



VENI VIDI VICI


C D E F G H I J K L M N O P Q R S T U V W X
01 02 04 05 06 07 08 09 10 11 13 14 15 16 17 18 19 20 21 22 23 24
ENIGMA

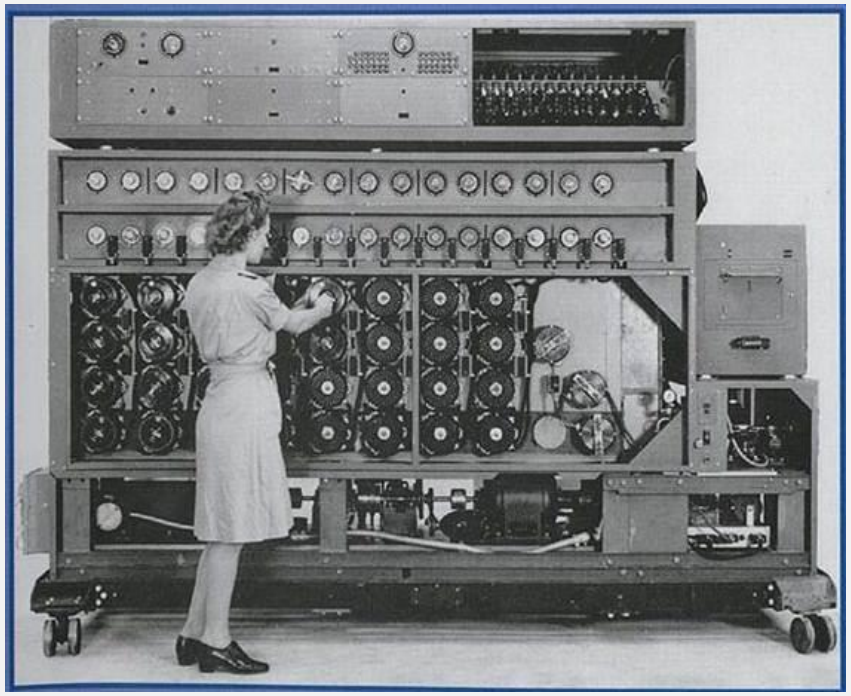
Histoire

La cryptologie a joué un rôle décisif pendant la Seconde Guerre mondiale. Les exploits des alliés en matière de cryptanalyse auraient permis d'écourter la guerre.

Machine Enigma

L'armée allemande chiffrait ses communications à l'aide d'une machine, Enigma.

Les alliées : Construction d'une machine à décrypter, « La bombe » (**Alan Turing**)



La machine Enigma

On écrivait les lettres du message avec son clavier et, à chaque lettre, une lampe s'allumait pour montrer quelle lettre chiffrée correspondait.

Enigma possédait généralement trois rotors : ces molettes permettaient de régler la machine pour chiffrer et déchiffrer les messages allemands, selon un ordre choisi par le gouvernement et changé régulièrement (pour des raisons de sécurité).

Les points forts

- 3 types de réglages (clés) : ordre d'installation des rotors
  rotation initiale des 3 rotors
  branchements entre les lettres appareillées (12 lettres).
- nombre presque infini de clés - peut atteindre 10^{110} !
  (il y a 10^{80} atomes dans l'univers observable)
- réversibilité : message clair <-> message chiffré (avec la même clé)

Évidence : des hommes ne peuvent pas tester tous ces cas à « la main » !

Histoire

La BOMBE

Pour décrypter les messages allemands, les Alliés ont alors commencé à construire les tous **premiers ordinateurs** : baptisés **Bombes.**

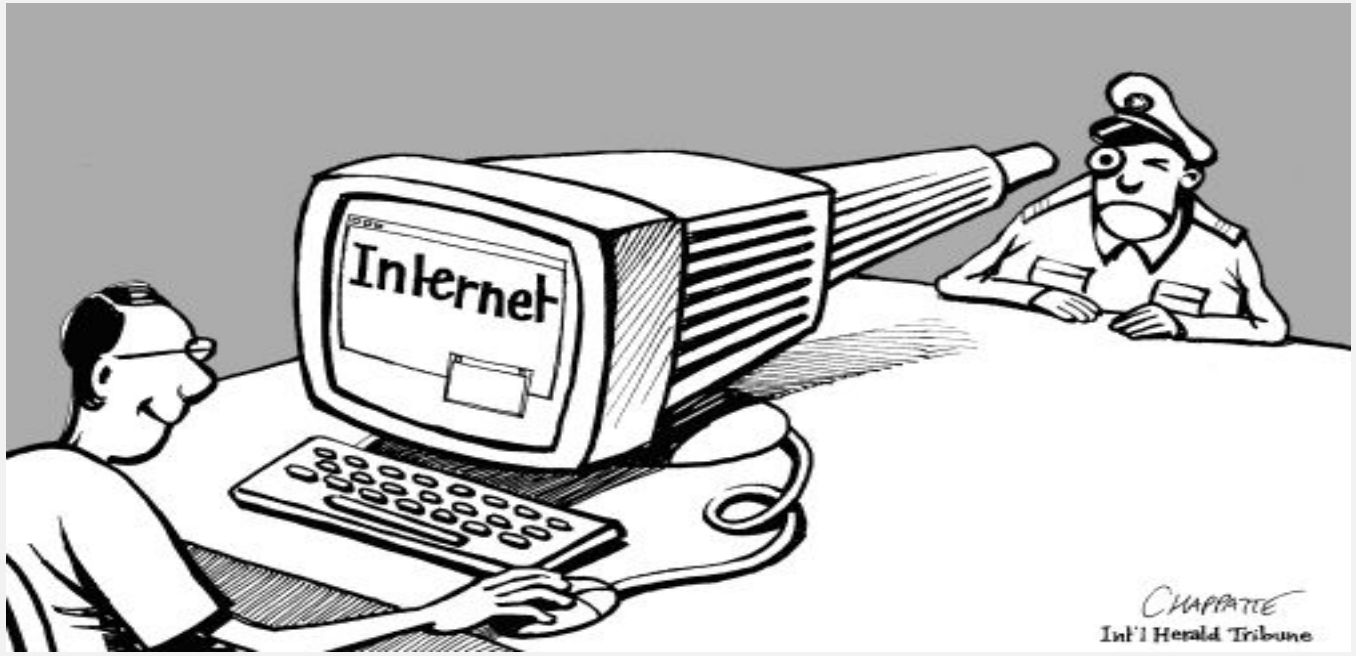
Ces machines essayaient toutes les possibilités à la place des humains.

Les méthodes de chiffrement dites « modernes » sont nettement plus sûres, pour résister à la puissance des ordinateurs qui peuvent tester énormément de possibilités dans une durée très courte.

Failles de Machine Enigma

- jamais la lettre A ne sera codée par un A
- deux lettres différentes frappées à la suite (ex. AB) ne donnent jamais, deux fois de suite, la même lettre chiffrée (ex. CC).
- les fautes des chiffreurs : certains messages du même format avec des mots récurrents.

Cryptographie moderne



Les applications de la cryptographie ne sont pas seulement militaires ou politiques.

Avec la croissance fulgurante d'Internet à la fin du XXième siècle, les communications nécessitent de plus en plus cette technologie afin de protéger la confidentialité d'un nombre croissant d'internautes.

Cryptographie moderne

Même s'il a été utilisé beaucoup des temps pendant l'histoire - jusqu'au Moyen Age, le chiffre de César représente un chiffrement très faible (facilement cassable).

Heureusement, les codes secrets actuels sont plus robustes que le code de César. Cependant, le principe de substitution d'un caractère par un autre est toujours d'actualité, il reste un composant essentiel des codes secrets.

Aujourd'hui, le chiffrement le plus largement utilisé s'appelle AES pour Advanced Encryption Standard et, à notre connaissance, personne n'a encore réussi à le casser.

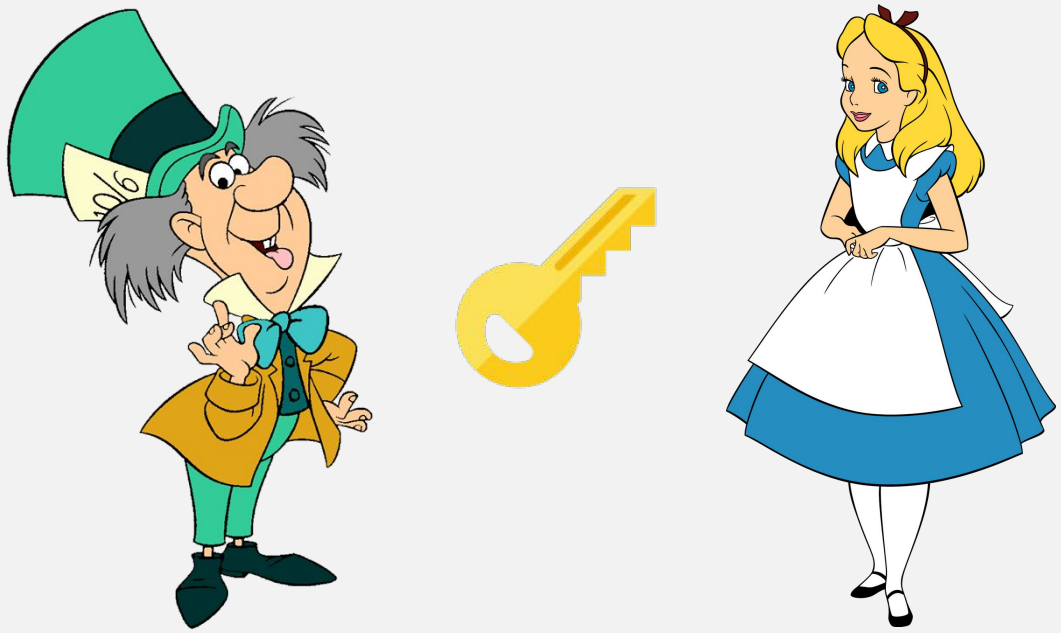
Cryptographie à clé secrète

Alice et Bob doivent utiliser une clé secrète pour chiffrer et déchiffrer les messages.

(par exemple pour les communication sur Internet)

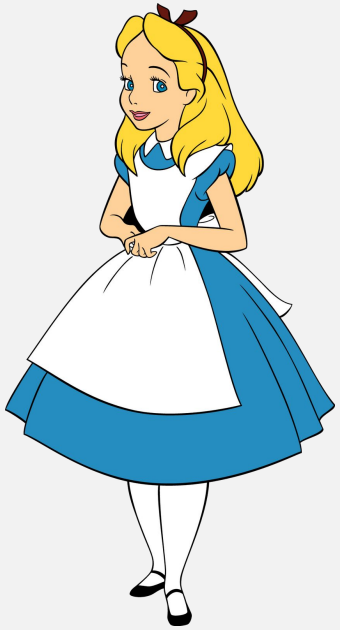
Échange de clé à distance

L'échange d'une clé secrète entre Alice et Bob est nécessaire et doit rester confidentiel.
Impossible si les deux personnes ne peuvent se rencontrer physiquement !?



Echange de clé Diffie-Hellman

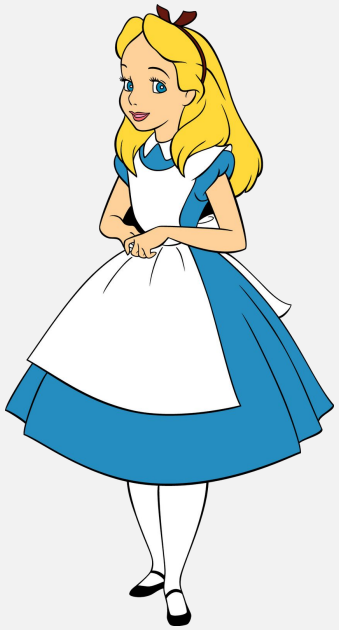
Diffie-Hellman en couleurs

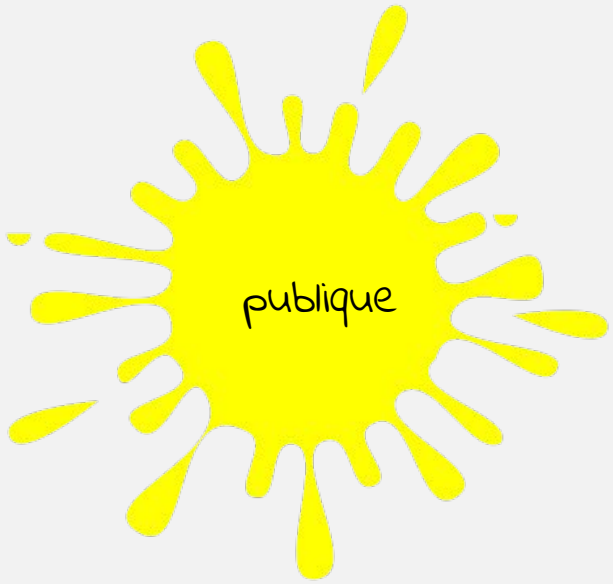


Diffie-Hellman en couleurs

+

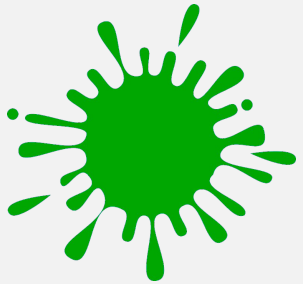
=



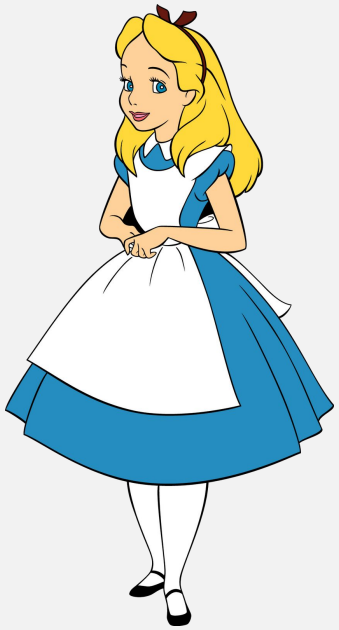


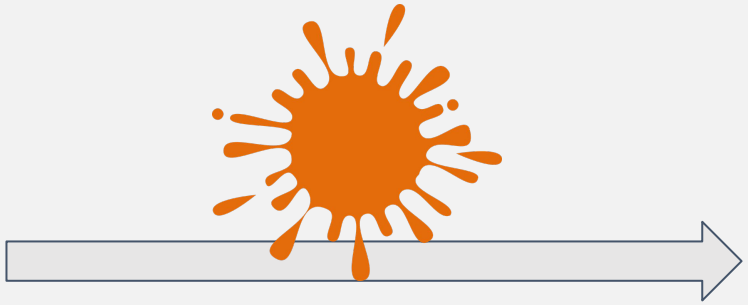
+

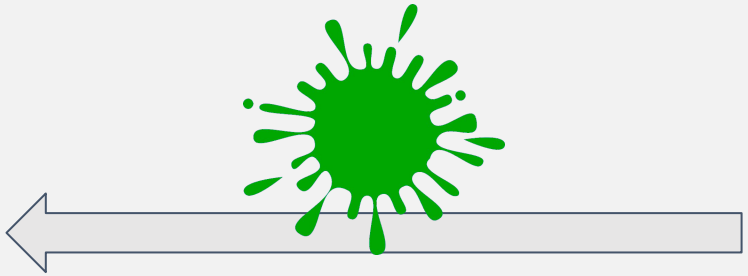
=

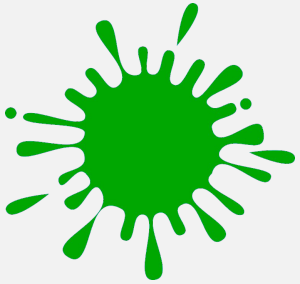


Diffie-Hellman en couleurs



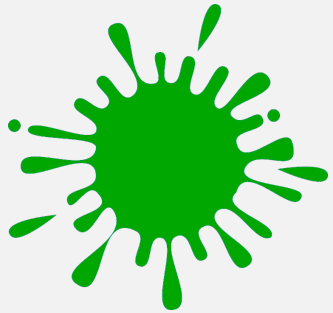




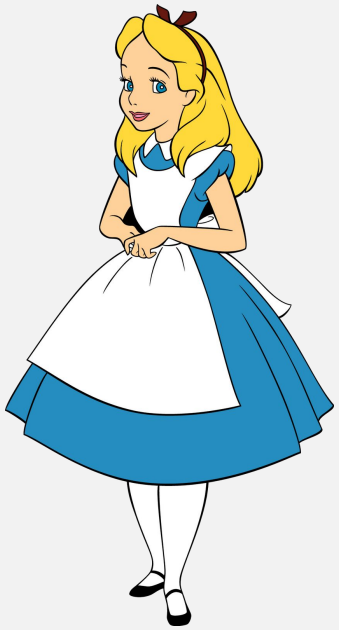


Diffie-Hellman en couleurs

+



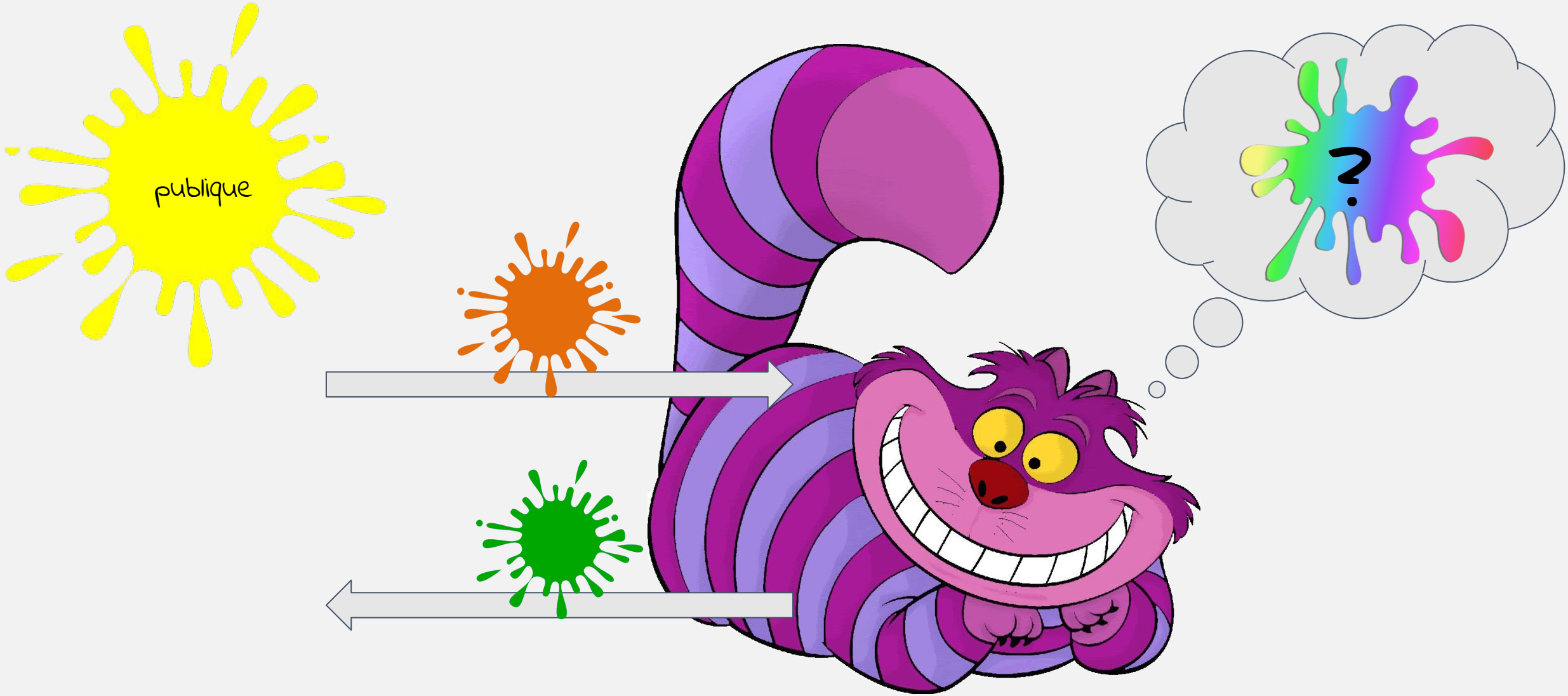
=



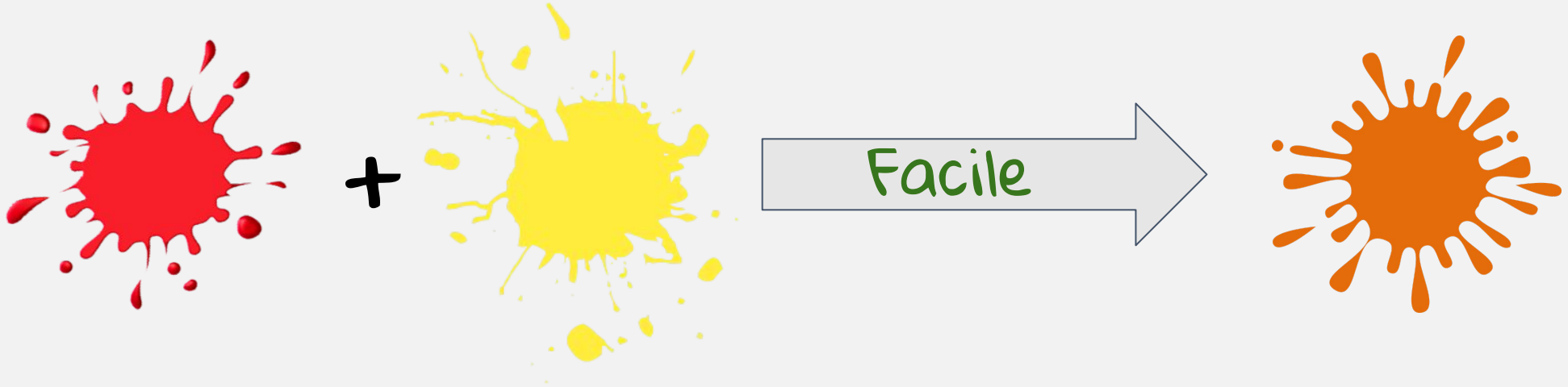
+

=

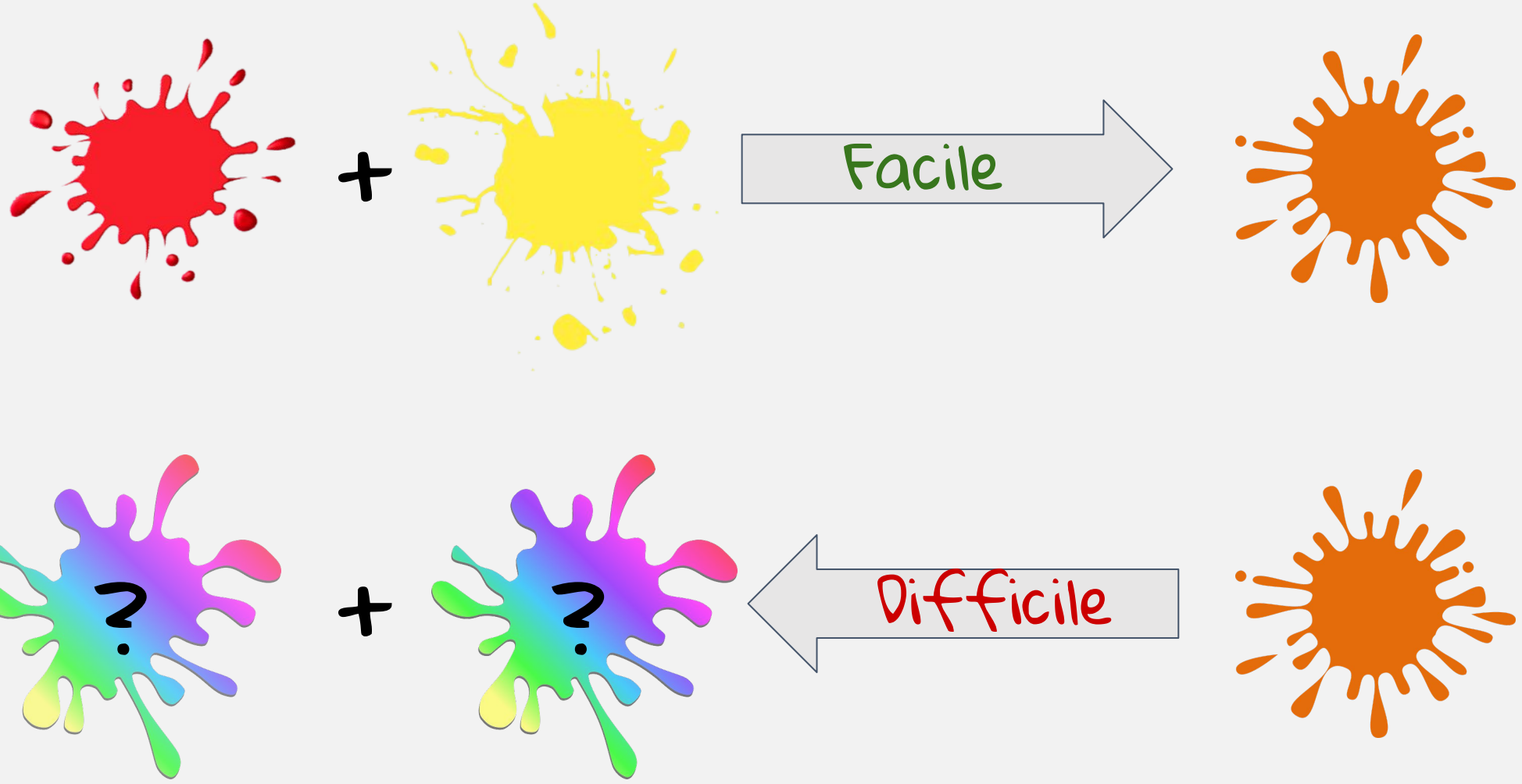
Diffie-Hellman en couleurs



Fonction à sens unique



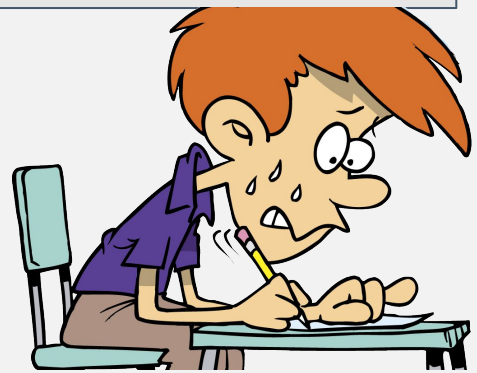
Fonction à sens unique



Factorisation

79 x 73 → Facile → 5767

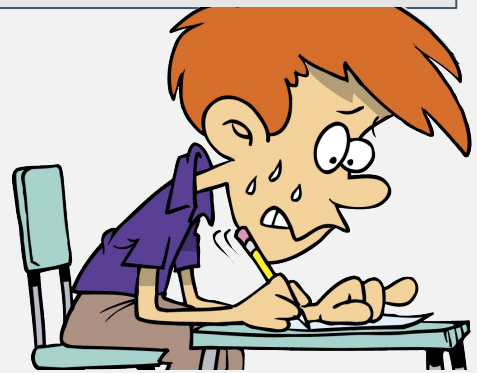
? x ? ← Difficile ← 5767



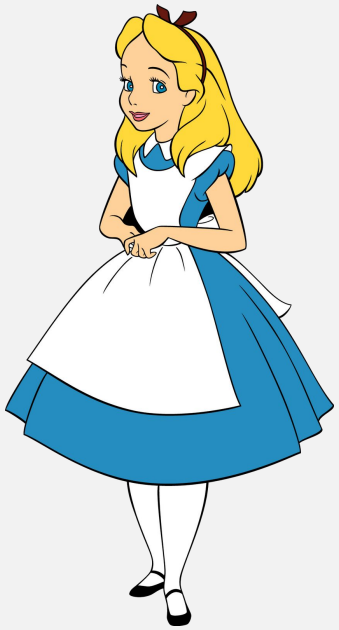
Logarithme discret

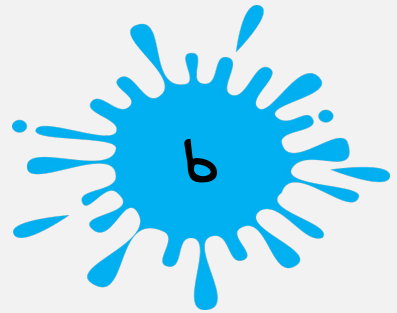
7^9 mod 13 → Facile → 8

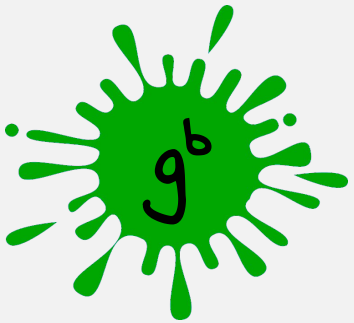
$7^?$ mod 13 ← Difficile ← 8



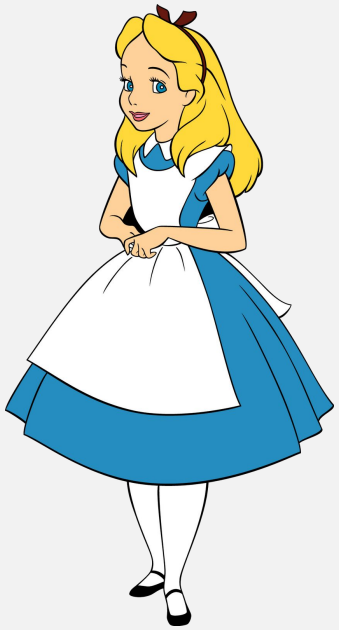
Diffie-Hellman modulo p

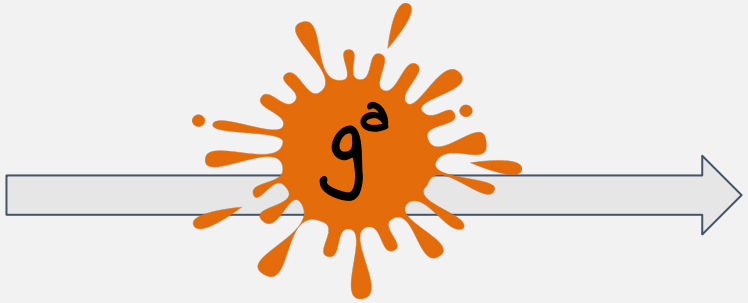


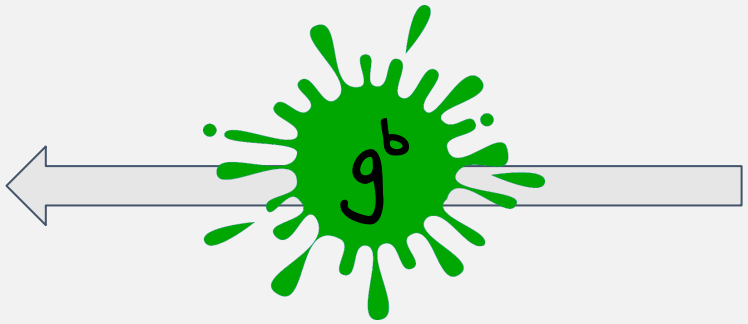


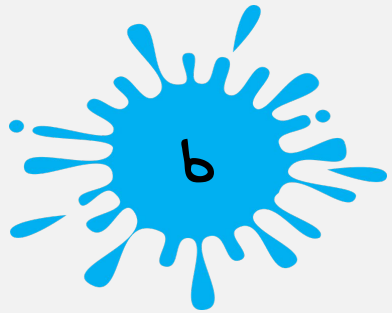


Diffie-Hellman

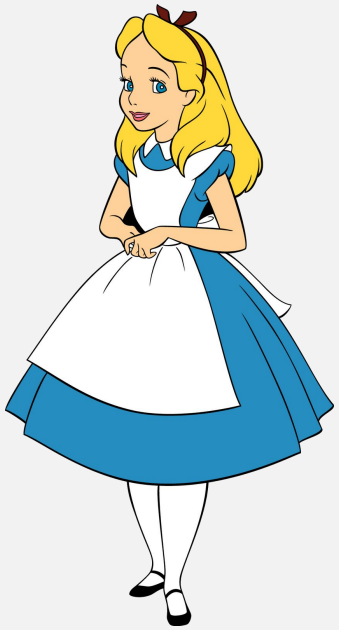


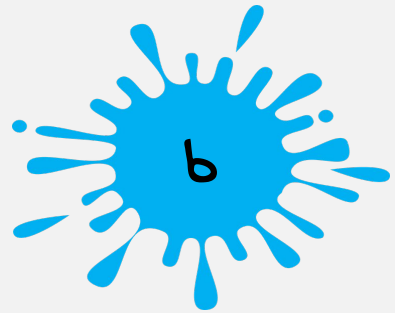


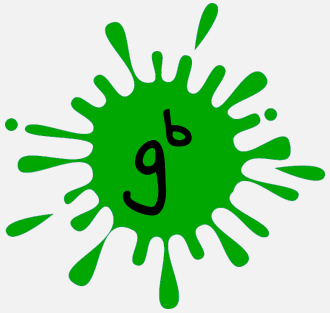




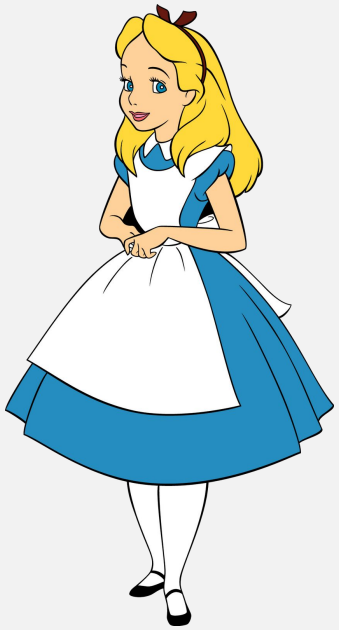
Diffie-Hellman

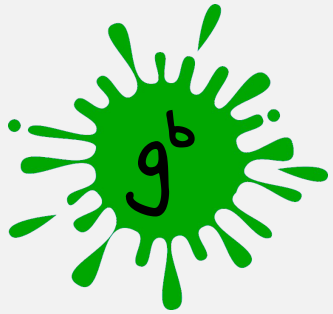


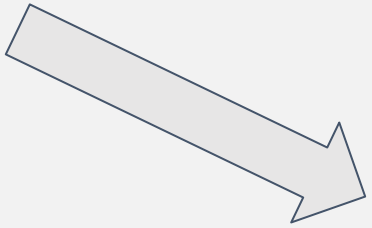


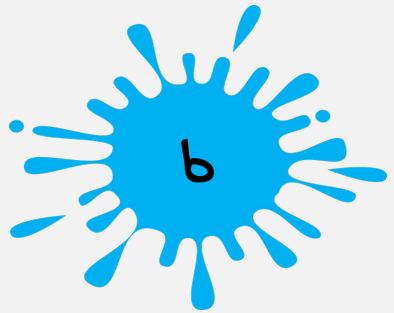


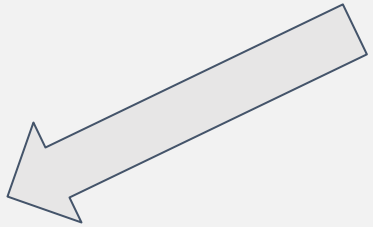
Diffie-Hellman





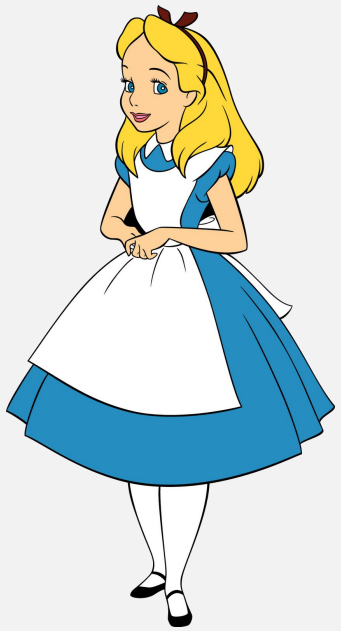






clé commune

Cryptographie à clé publique



Cryptographie à clé publique

Menace quantique

Les propriétés quantiques de la matière:

- la superposition
- l'intrication

Un ordinateur quantique, à la différence d'un ordinateur classique basé sur des transistors qui travaille sur des **données binaires** (des bits, valant 0 ou 1), le calculateur quantique travaille sur des **qubits** dont l'état quantique peut posséder plusieurs valeurs.

De petits calculateurs quantiques ont été construits à partir des années 1990. Jusqu'en 2008, la difficulté majeure concerne la réalisation physique de l'élément de base : le qubit.

L'algorithme de Shor conçu pour utiliser un circuit quantique, rend possible de nombreux calculs combinatoires hors de portée d'un ordinateur classique en l'état actuel des connaissances.

Le Monde quantique

Une particule peut posséder de **multiples états simultanés** : l'état de la particule est une superposition d'états possibles. Ce principe est illustrée par la métaphore du chat de Schrödinger.

Toutes les caractéristiques des particules peuvent être sujettes à cette **indétermination.**
La position d'une particule quantique est incertaine : Elle n'est ni au point A, ni au point B. Par contre, après la mesure, l'état de la particule est bien défini : elle est au point A ou au point B.

On peut faire une analogie avec un oeuf.
Le poussin sera soit doré, soit noir. Le moment de l'éclosion, on a la réponse. Mais avant, il y avait simplement une certaine **probabilité** d'être doré et une autre probabilité d'être noir.

Le Monde quantique

Pour représenter mathématiquement un **système quantique**, on dit que c'est la somme des systèmes potentiellement mesurables, pondérés par des **amplitudes de probabilité.**

Considérons par exemple le système quantique suivant :

$$|\text{Système quantique}\rangle = \alpha\ |\text{état } 1\rangle + \beta\ |\text{état } 2\rangle$$

Avant la mesure, le système est dans un **état indéterminé.**

Lors d'une mesure, on pourra observer soit l'état 1 (avec une probabilité de $|\alpha|^2$), soit l'état 2 (avec une probabilité de $|\beta|^2$).

En attendant, le système est dans un état superposé. On dit abusivement qu'avant la mesure, le système est à la fois dans l'état 1 et dans l'état 2.

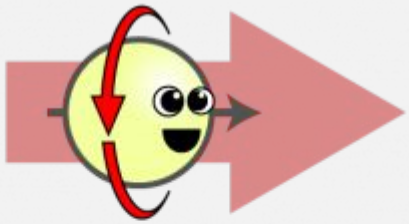
Ordinateur quantique

La mémoire d'un ordinateur classique est faite de bits. Chaque bit porte soit un 1 soit un 0.
Un circuit de calcul quantique travaille sur un jeu de qubits.
Un qubit peut porter soit un un, soit un zéro, soit une superposition d'un un et d'un zéro.
On n'a pas deux états en tout mais une infinité :

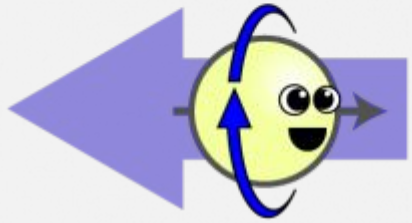
$$|q\text{-}bit\rangle = \alpha\,|1\rangle + \beta\,|0\rangle \qquad |\alpha|^2 + |\beta|^2 = 1$$

Pour un bit classique, on a

- $\alpha=0$ et $\beta=1$ (c'est l'état 0),
- $\alpha=1$ et $\beta=0$ (c'est l'état 1).



Un ordinateur quantique fait varier les coefficients grâce à des portes quantiques (l'analogue des portes logiques classiques).



Ordinateur quantique

L'intrication quantique : au lieu d'avoir une série de bits indépendants les uns des autres comme dans un ordinateur classique, on les intrique, de sorte à ce que l'ensemble des qbits dans l'ordinateur forme un unique système quantique, et non une série de systèmes isolés.

Deux qubits réunis sont dans une superposition d'états

$$\alpha \mid 00 > + \beta \mid 01 > + \gamma \mid 10 > + \delta \mid 11 >$$

avec $\mid \alpha \mid^2 + \mid \beta \mid^2 + \mid \gamma \mid^2 + \mid \delta \mid^2 = 1$

Il s'agit cette fois d'employer **la superposition** des quatre états pour le calcul. C'est pourquoi la puissance de calcul théorique d'un calculateur quantique double à chaque fois qu'on lui adjoint un qubit.

Avec dix qubits, on a 1024 états superposables, et avec n qubits, 2^n.

Conclusion

Nous avons vu que la cryptographie est l'art de concevoir des cryptosystèmes, et que les techniques de cryptage ont beaucoup évolué durant les âges et sont encore en perpétuelle évolution. La cryptographie est un champ de recherche très actif.

La sécurité d'un grand nombre d'applications en dépend : applications militaires, commerce en ligne, télécommunications ...

C'est pourquoi des chercheurs, les cryptologues, travaillent à construire des cryptosystèmes plus résistants et plus performants, mais ils travaillent également à les attaquer!

Cela peut sembler étrange, mais le meilleur moyen de savoir si un code secret peut être cassé est d'essayer soi-même.

Merci

http://www.di.ens.fr/~nitulesc

Sources

http://www.quantumdiaries.org/2011/08/23/the-spin-of-gauge-bosons-vector-particles/

https://cercle.institut-pandore.com/physique-quantique/informatique-ordinateur-quantique/

http://www.di.ens.fr/~nitulesc/files/crypto7.pdf