MINISTÈRE
CHARGÉ
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE

Liberté
Égalité
Fraternité

GREYC
Laboratoire de recherche
en sciences du numérique

cnrs

RÉGION
NORMANDIE

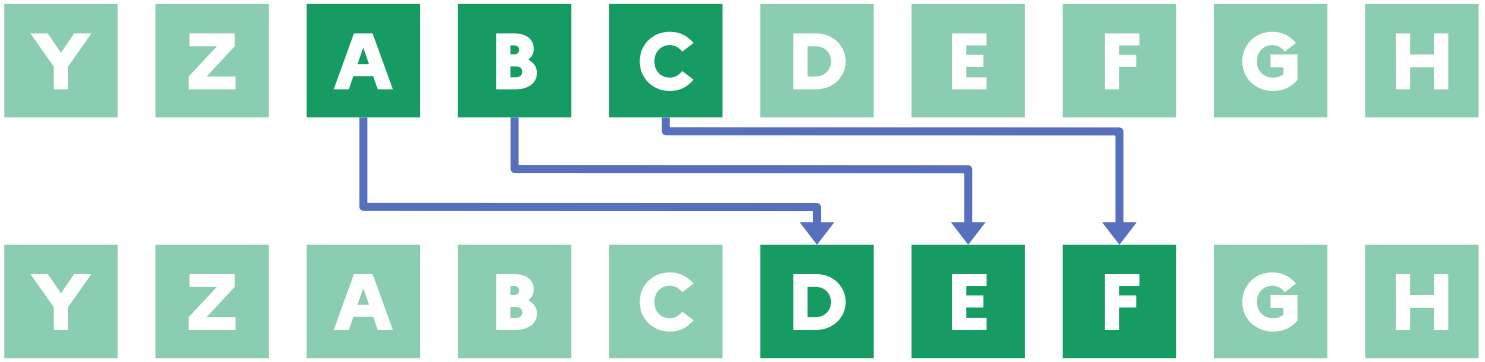
fête de la Science

lqwhooljhqfh(v)

- Qu'est ce que cela peut bien signifier ?
  - Il s'agit d'un message chiffré,
  - Par la méthode du chiffrement de J. César,
  - Il cache un vrai message (qui a du sens),
- Recherchons ce que cela veut dire ?

Chiffrement de César

- Cacher le contenu de ses correspondances,



- On remplace par une autre lettre, à chaque fois avec le même décalage, ici +3

Faisons de la cryptanalyse

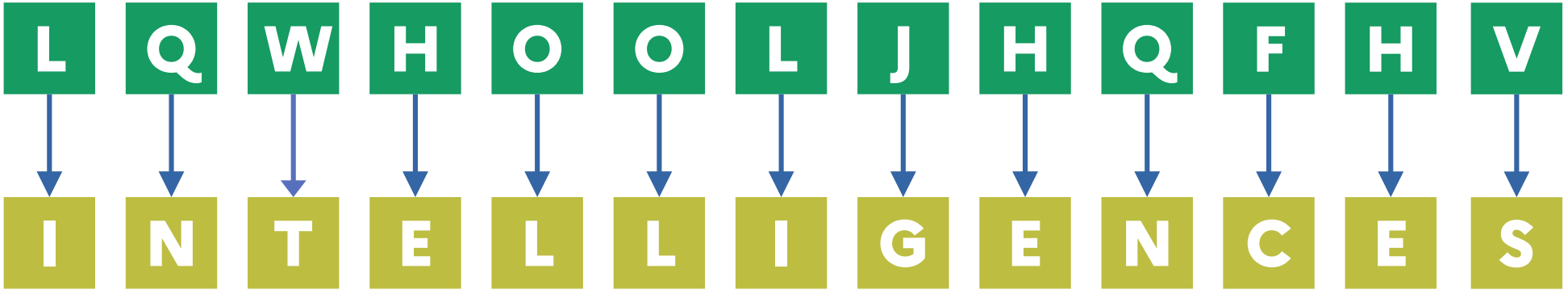
- La cryptanalyse, c'est casser la cryptographie
- Comment décrypter ce chiffrement de César ?

lqwhooljhqfh(v)

lqwhooljhqfh(v)

- Quelle est la lettre la plus utilisée dans l'alphabet français ? Le E
- Quelle est la combinaison de 2 lettres, appelée bigramme la plus fréquentes en fin de mot ? ES
- Substituons alors les 2 dernières lettres HV → ES
- Cela indique un décalage de -3 en arrière

Chiffrement de César



MINISTÈRE
CHARGÉ
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE

Liberté
Égalité
Fraternité

intelligence(s)

Nouvelles hypothèses autour de la cryptographie post-quantique

Antoine Douteau

Doctorant en Informatique au Laboratoire GREYC et au CNRS à Caen

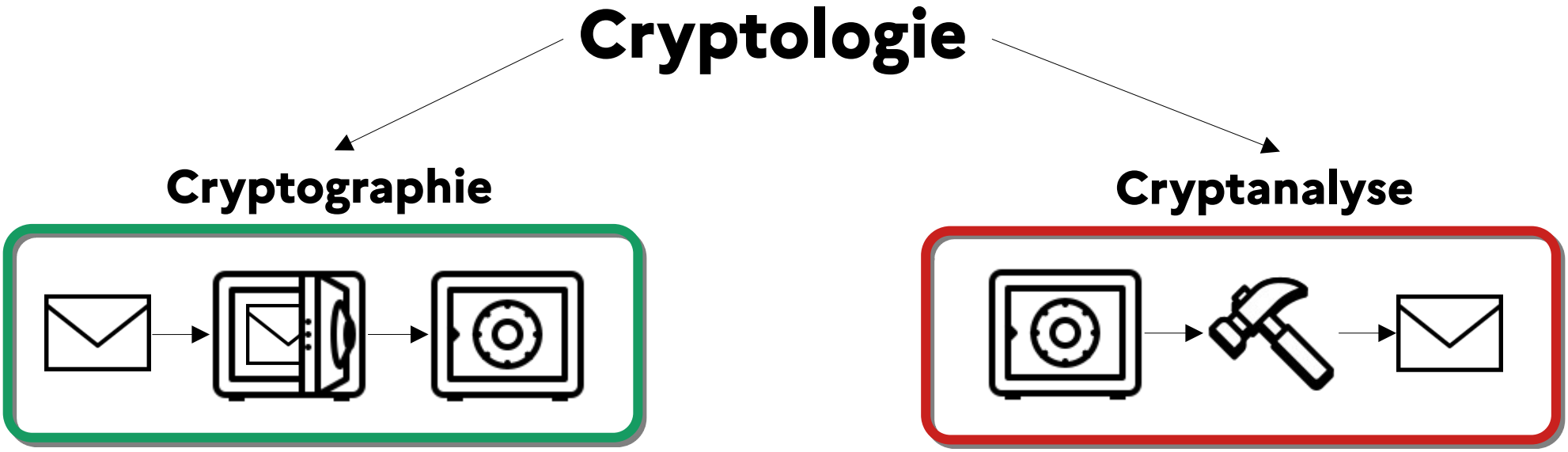
fête de la Science

GREYC
Laboratoire de recherche en sciences du numérique

cnrs

RÉGION NORMANDIE

Introduction à la cryptologie



Diapo la + importante : Vocabulaire

Chiffrement

chiffrer

Déchiffrement

déchiffrer

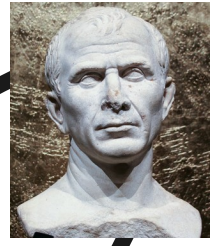
Décryptage

décrypter

Ne jamais dire : crypter/cryptage/chiffrage et autre

Un point d'histoire (passée)

-1500
1er cryptographie



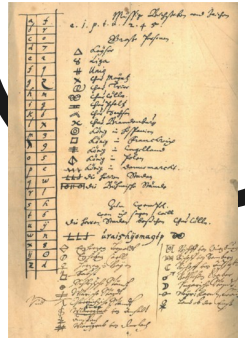
-50, J. César
1er cryptosystème

-400, Scytale

800, Al-Kindi
1ère cryptanalyse

Un point d'histoire (un peu passé)

Ère des cryptosystèmes « fastidieux »



Un point d'histoire (présent)

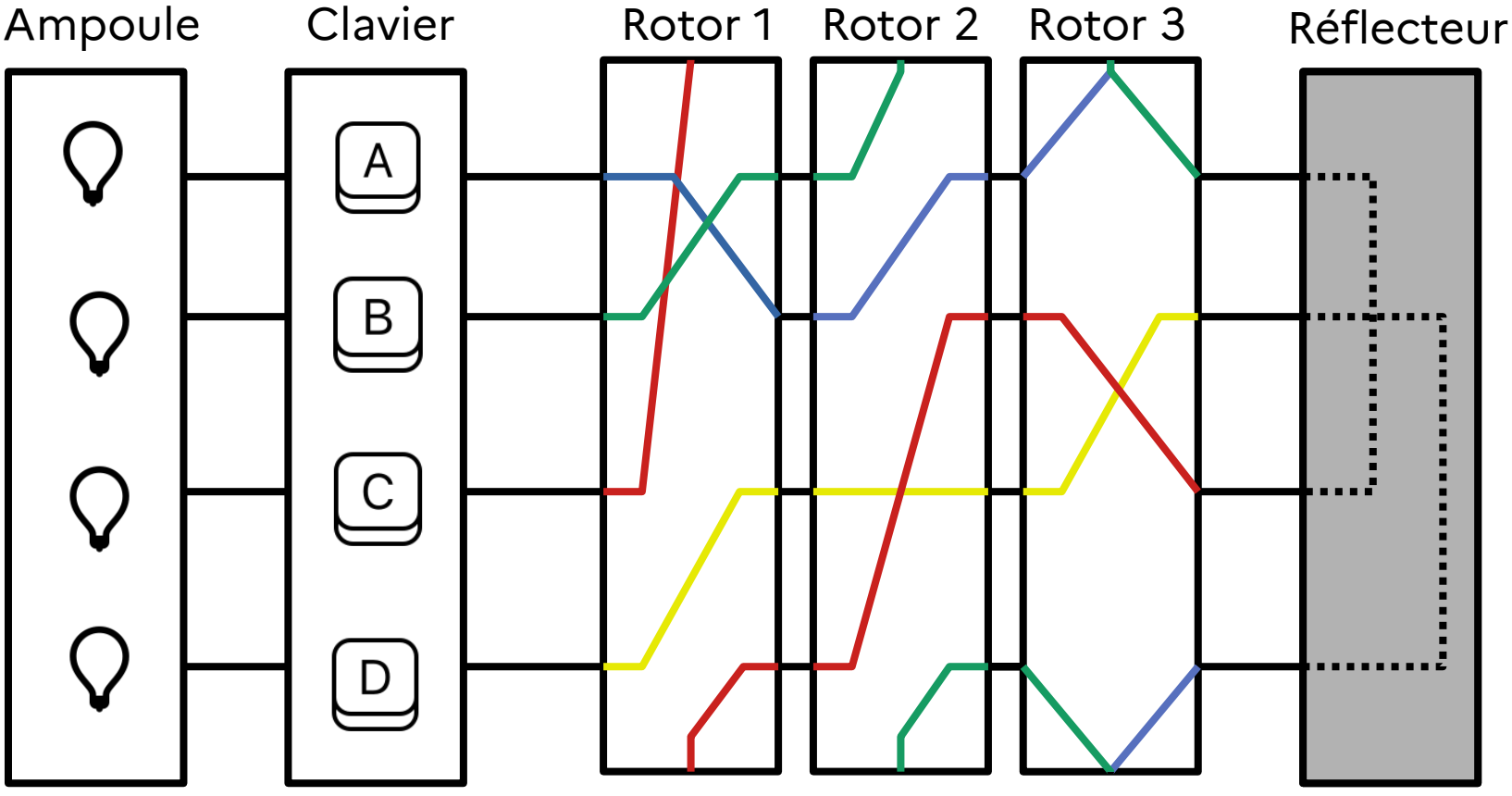
Besoin de cryptosystèmes efficaces

1791
1er télégraphe

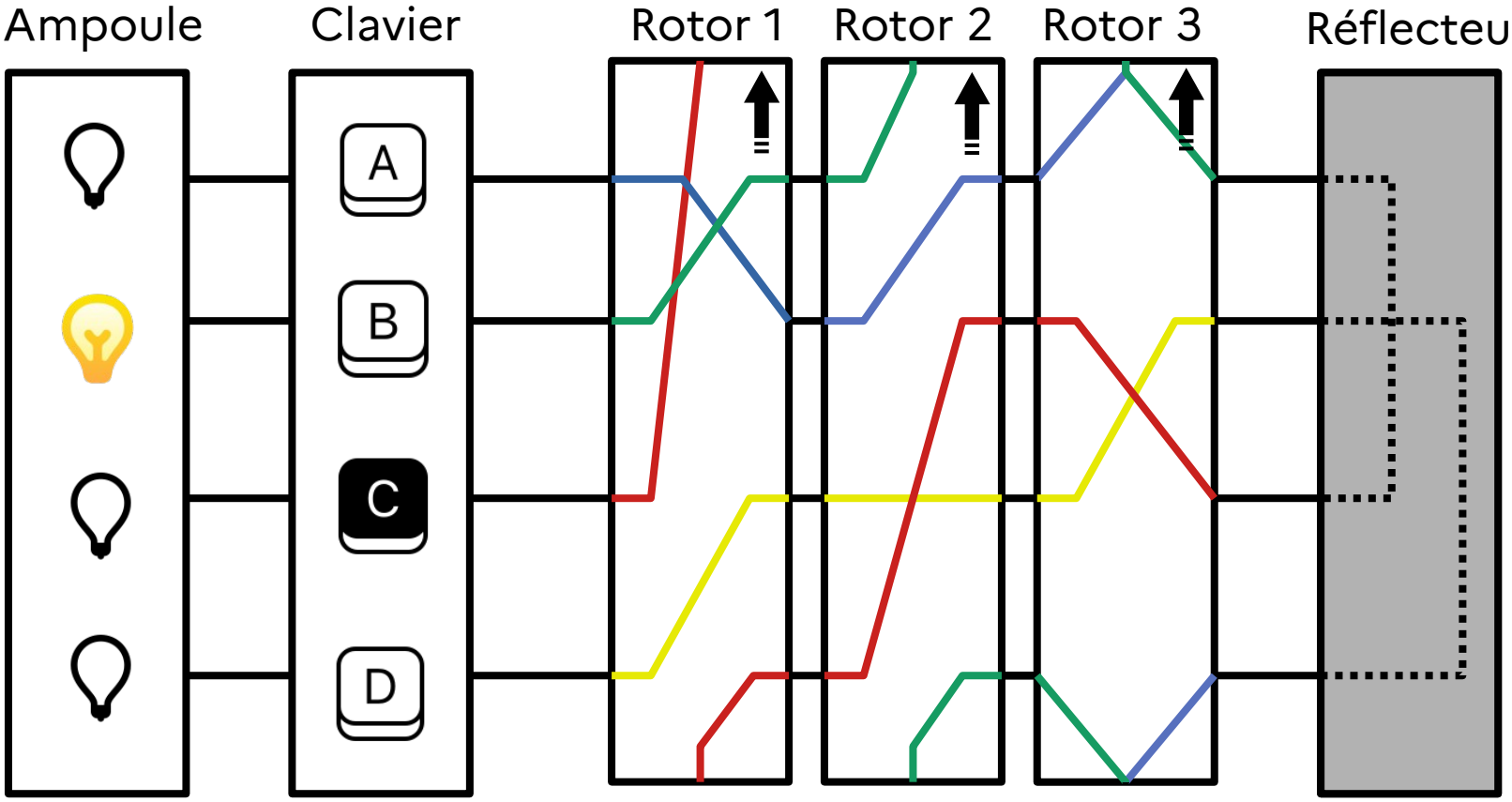
1918
Enigma

1943
Bombe de Turing

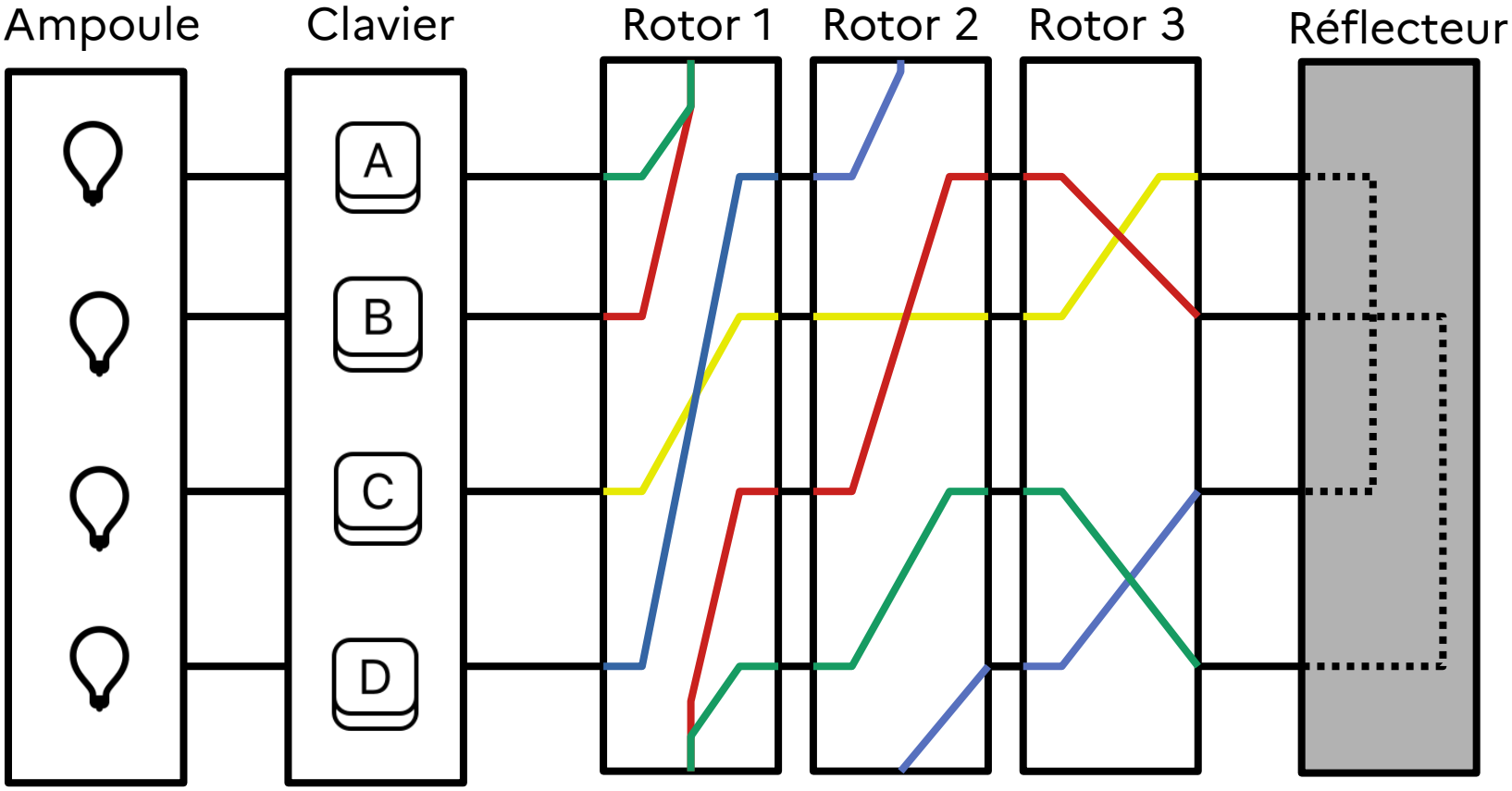
(mini-)Enigma



(mini-)Enigma



(mini-)Enigma



Un point d'histoire (présent)

Besoin de cryptosystèmes efficaces

1791
1er télégraphe

1918
Enigma

1943
Bombe de Turing

Et maintenant ?

Protocole symétrique

Un point d'histoire (présent)

Besoin de cryptosystèmes efficaces

1791
1er télégraphe

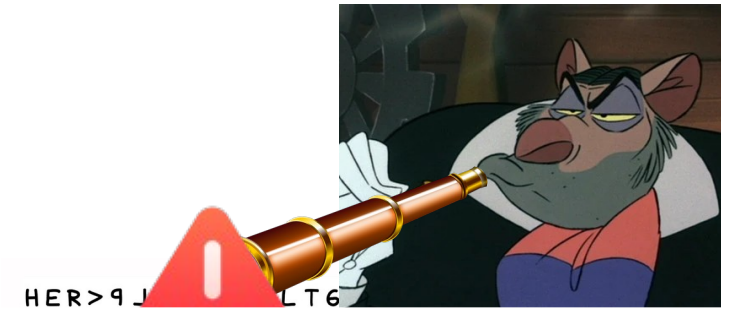
1943
Bombe de Turing

1976
La Révolution !

1918
Enigma

Protocole asymétrique

La sécurité cryptographique



Mais pas que !

Confidentialité
Contenu caché

Intégrité
Contenu non modifié

Authentification
Expéditeur est bien Alice

Du cadenas au cryptosystème

Il nous faut un « cadenas » :


Qui se ferme facilement


Qui s'ouvre facilement avec la bonne clé


Qui ne casse pas facilement

Il nous faut un « cryptosystème » :


Chiffrer se fait par un calcul simple


Déchiffrer se fait par un calcul simple avec connaissance d'une bonne clé


Décrypter le message est difficile et revient à résoudre un problème mathématique quasiment insoluble

Quand les mathématiques s'invitent

Trouvons alors un problème mathématique quasiment insoluble

1 – Multiplier 2 grands nombres entre eux,
2 – Diviser 2 grands nombres entre eux,
3 – Deviner les 2 facteurs tel que le produit donne un certain nombre,
4 – L'exercice 2 du dernier contrôle de Maths (il était trop dur).

919 x 787 =

x =

723253

Quand les mathématiques s'invitent

Ce nombre a 250 chiffres et est le plus grand nombre difficile factorisé :
- cela a mis 2700 années (cumulé),
- sur 10 000 ordinateurs,
- grosse consommation électr

641352894770715802787901901
705773890848250147429434472
081168596320245323446302386
235987526683477087376619255
85694639798853367

x

Mais il faut différencier deux aspects : non-fait et infaisable :
- 250 chiffres : fait,
- 251 chiffres : non-fait mais faisable,
- ...
- 900 chiffres : infaisable

333720273949781563562260106
0535551142279407603447675546
667845209870238417292100370
802574486732968818775657189
86258026932062711

=

<u>Infaisable en temps :</u>

Coopération entre les 8 milliards d'êtres humains sur Terre avec des ordinateurs récents
= + d'années que depuis le big bang

<u>Infaisable en énergie :</u>

- 250 chiffres : autant d'énergie pour bouillir 2 piscines olympiques
- 900 chiffres : à vous d'estimer !
Autant d'énergie que pour faire bouillir toute l'eau de ce système solaire (minimum)

2 140 324 650 240 744 961 264
423 072 839 333 563 008 614
715 144 755 017 797 754 920
881 418 023 447 140 136
643 145 519 695 804 679 610
992 851 872 470 914 587 687
396 261 921 557 363 047 454
770 520 805 119 056 493 106
687 691 590 019 759 405 693
457 452 230 589 325 976 697
471 681 738 069 364 894 699
871 578 494 975 937 497 937

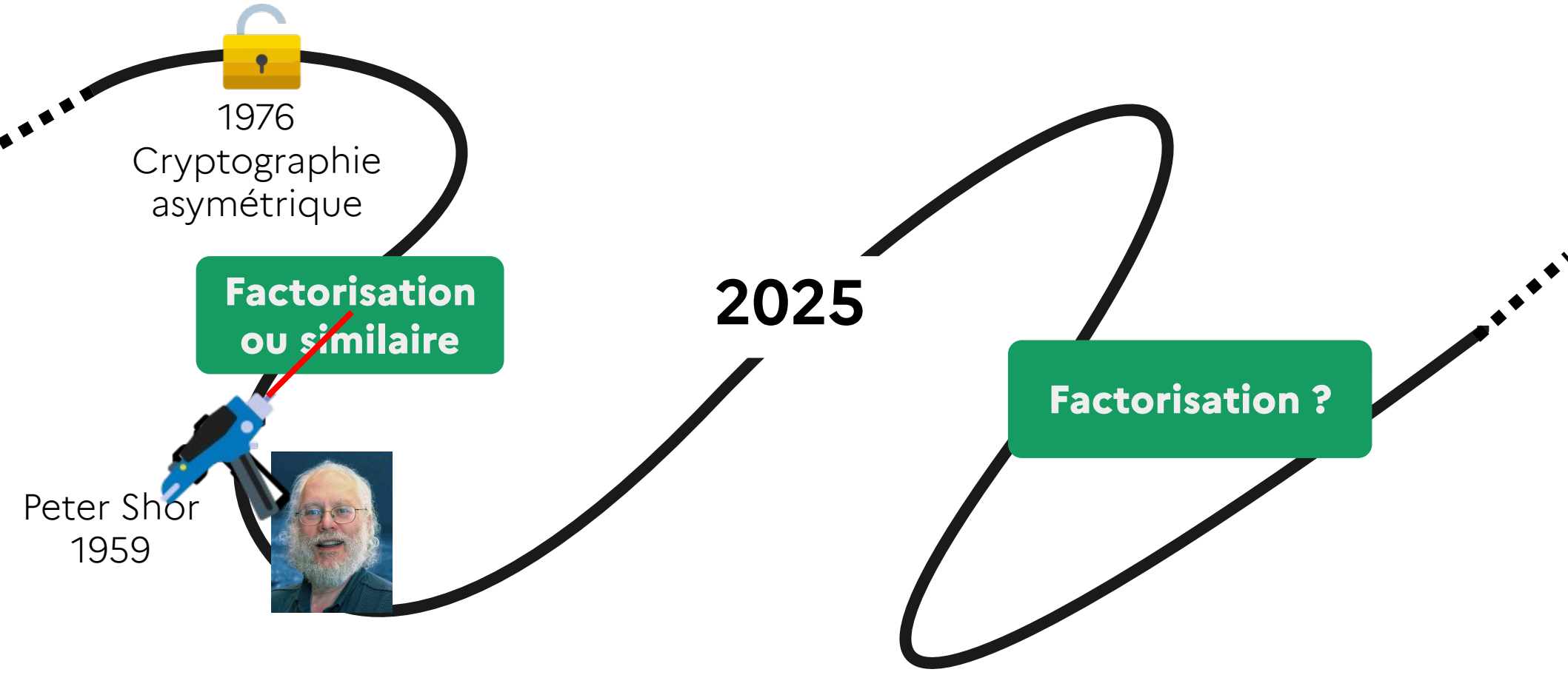
Estimation non rigoureuse pour montrer l'absurdité

Usage actuel

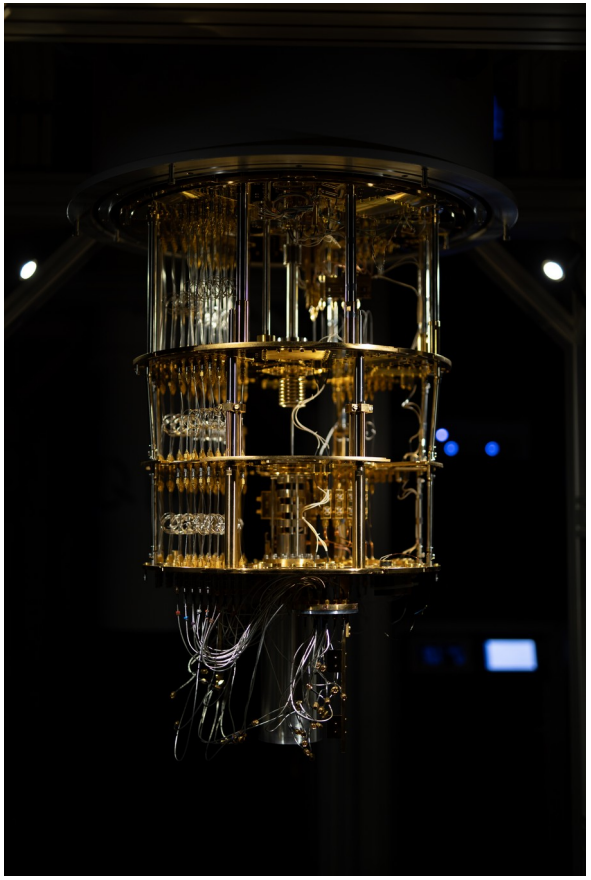
Militaire : sécurisation des communications

En quoi la cryptographie vous est utile ?

Un point d'histoire (future)



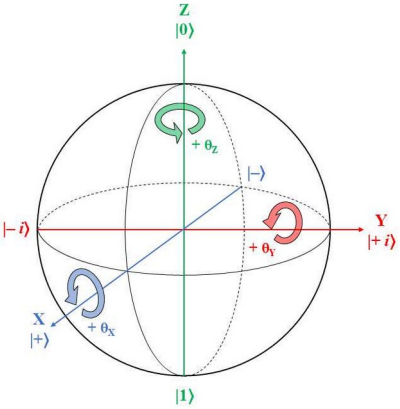
Ordinateur quantique



Autre type d'ordinateur :
- **Pas meilleur**
- **Pas moins bien**
- **Mais nouvelles règles de calcul**

Différents problèmes :
- **Quantité de données**
- **Correction d'erreurs diffici**
- **Protection difficile**
- **et surtout, ça n'existe pas (**

Un bit | Un qubit

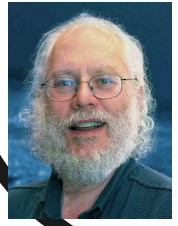


Cryptographie post-quantique

1976
Cryptographie
asymétrique

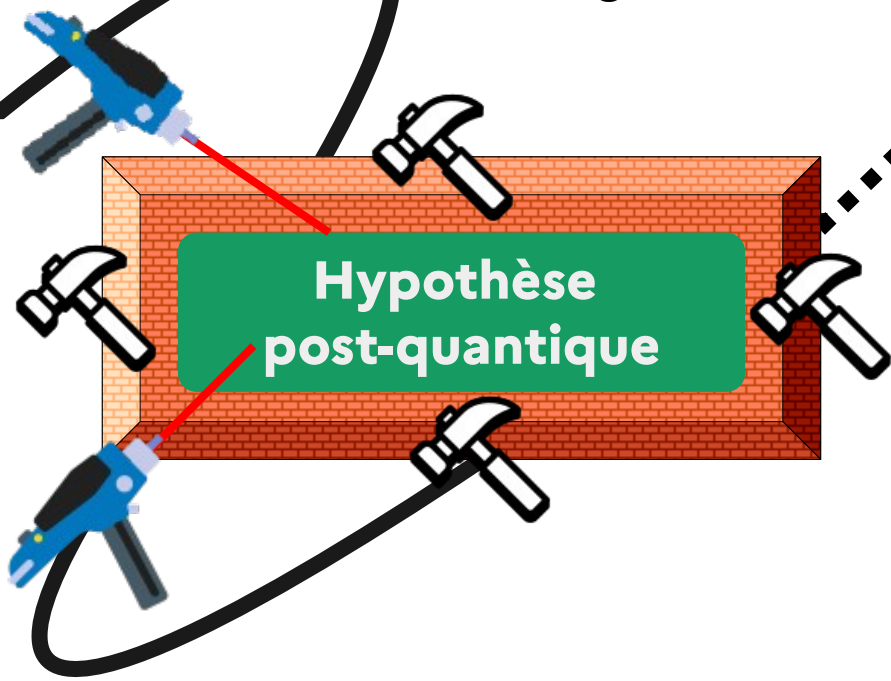
Factorisation ou similaire

1959
Peter Shor



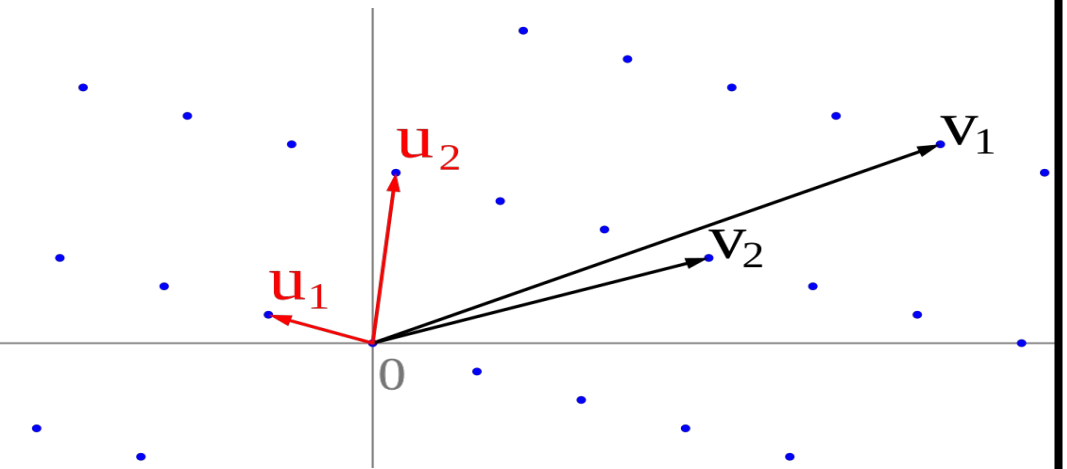
2025

2030
Recommandation
de migration



Réseaux euclidiens

Géométriquement (*ici en 2D*)



Ensemble de points régulièrement espacés dans un repère orthonormé

Calculatoirement (*ici en 64D*)

$$\begin{cases} 25x_1 + 32x_2 + \ldots + 100x_{64} \approx 12 \ [101] \\ 47x_1 + 72x_2 + \ldots + 13x_{64} \approx 67 \ [101] \\ 36x_1 + 7x_2 + \ldots + 87x_{64} \approx 41 \ [101] \\ \ldots \\ 21x_1 + 16x_2 + \ldots + 64x_{64} \approx 98 \ [101] \end{cases}$$

Nouveau problème mathématique quasiment insoluble :

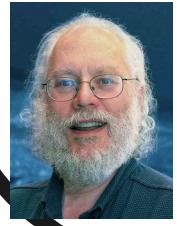
Trouvez une solution (x_1, x_2, …, x_{64}) au système d ‘équation bruitée ci-dessus

[101] signifie qu’on regarde tout nombre entre 0 et 100 en les réduisant si nécessaire

Cryptographie post-quantique

1976
Cryptographie asymétrique

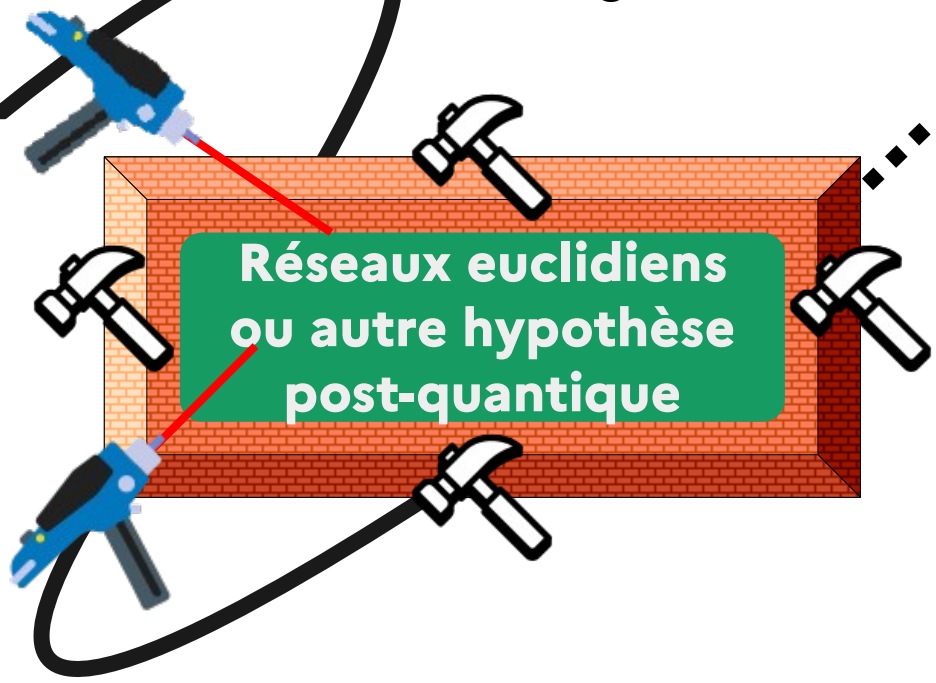
Factorisation ou similaire



1959
Peter Shor

2025

2030
Recommandation de migration



MINISTÈRE
CHARGÉ
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE

Liberté
Égalité
Fraternité

intelligence(s)

Je vous remercie pour votre écoute !

Antoine Douteau, Doctorant en Informatique

fête de la Science

GREYC
Laboratoire de recherche en sciences du numérique

cnrs

RÉGION NORMANDIE