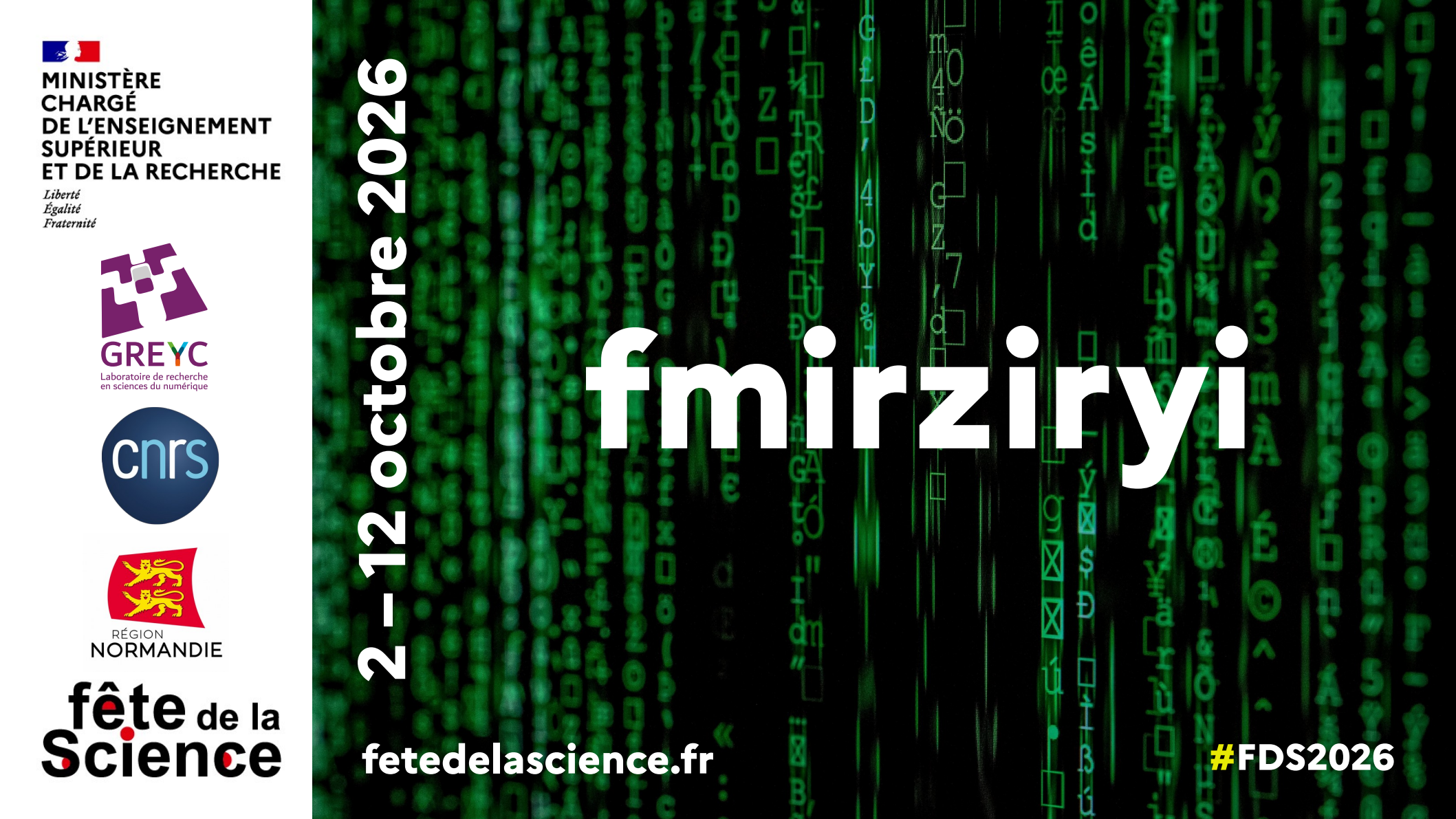
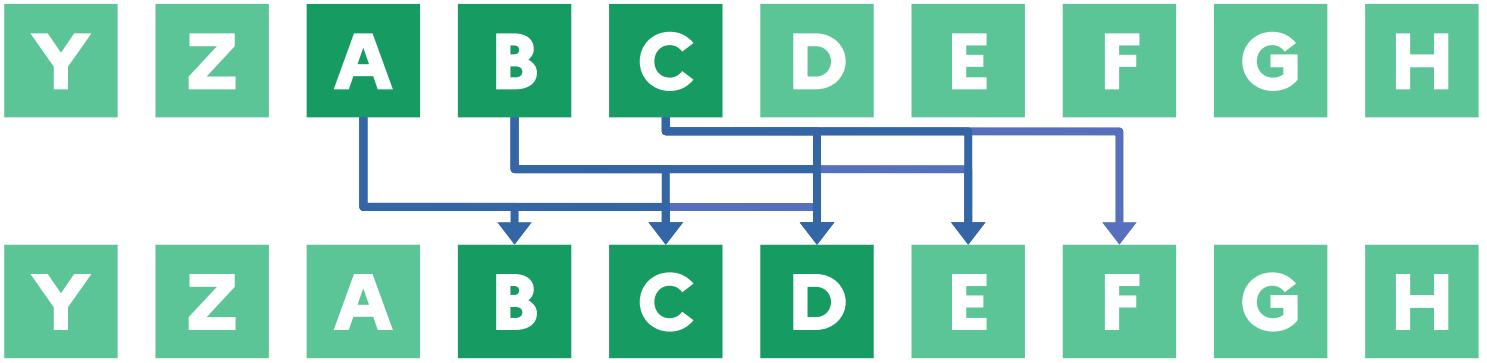

MINISTÈRE
CHARGÉ
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE
Liberté
Égalité
Fraternité
GREYC
Laboratoire de recherche
en sciences du numérique
cnrs
RÉGION
NORMANDIE
fête de la
Science
2 – 12 octobre 2026
fmirziryi
fetedelascience.fr
#FDS2026

fmirziryi

- 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 alors le message initial.

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

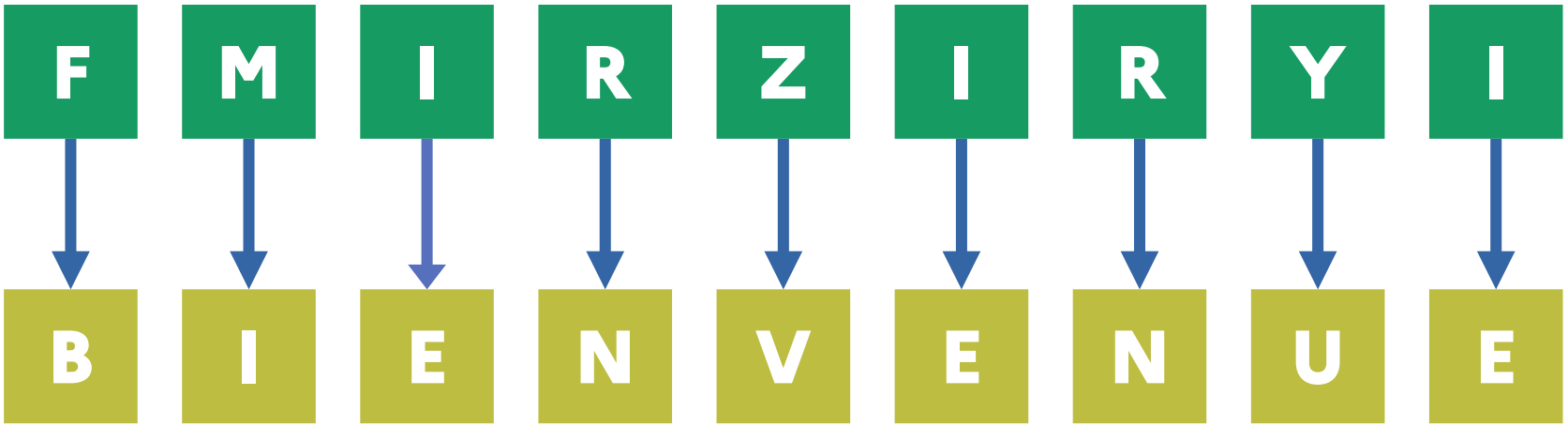
- La cryptanalyse, c'est casser un chiffrement
- Comment décrypter ce chiffrement de César ?

fmirziryi

fmirziryi

- Quelle est la lettre la plus utilisée dans l'alphabet français ? Le E
- Quelle est la lettre la plus fréquente dans mon mot chiffré ? Le
- Cela reviendrait à substituer : I → E
- Cela indique un décalage de 4 en arrière

Chiffrement de César



MINISTÈRE
CHARGÉ
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE

Liberté
Égalité
Fraternité

Bienvenue à toutes et tous

Quelle sécurité pour nos données ?

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

Un monde numérique

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

FINANCES PUBLIQUES

La Facturation électronique arrive en 2026

Doctolib

POUR DÉCLARER SUR IMPOTS.GOUV.FR	
VOTRE N° FISCAL POUR DÉCLARER EN LIGNE	SI VOUS N'AVEZ PAS ENCORE DE MOT DE PASSE
DÉCLARANT 1 1234567891234	N° D'ACCÈS EN LIGNE
DÉCLARANT 2	REVENU FISCAL DE RÉFÉRENCE : REPORTEZ-VOUS À VOTRE DERNIER AVIS D'IMPÔT SUR LE REVENU

MINISTÈRE
CHARGÉ
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE

Liberté
Égalité
Fraternité

Bienvenue à toutes et tous

Introduction à la cryptologie

Antoine Douteau

Doctorant en Informatique au Laboratoire GREYC et au CNRS à Caen

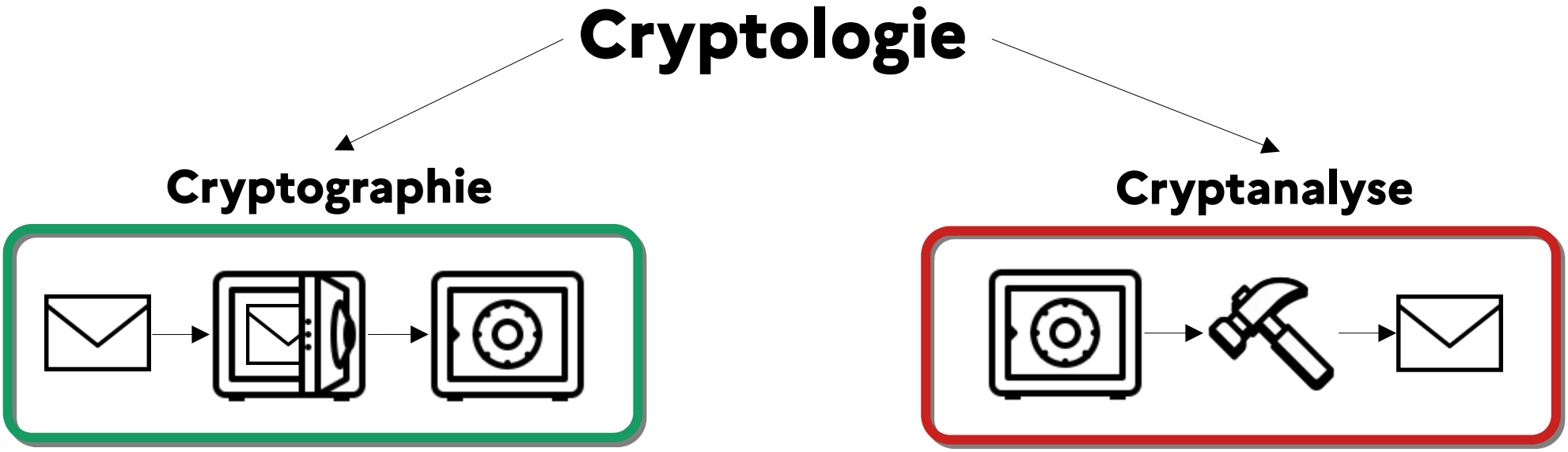
fête de la Science

GREYC
Laboratoire de recherche en sciences du numérique

cnrs

RÉGION NORMANDIE

Introduction à la cryptologie



Diapo la + importante : Vocabulaire



Chiffrement

chiffrer



Déchiffrement

déchiffrer



Décryptage

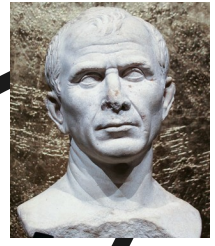
décrypter

Ne jamais dire : crypter/cryptage/chiffrage et autre

Un point d'histoire (passée)



-1500
1er cryptographie



-50, J. César
1er cryptosystème



-400, Scytale

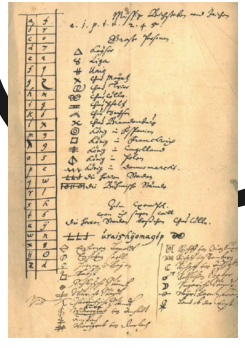


800, Al-Kindi
1ère cryptanalyse

Un point d'histoire (un peu passé)



Ère des cryptosystèmes « fastidieux »



Un point d'histoire (présent)

Besoin de cryptosystèmes efficaces

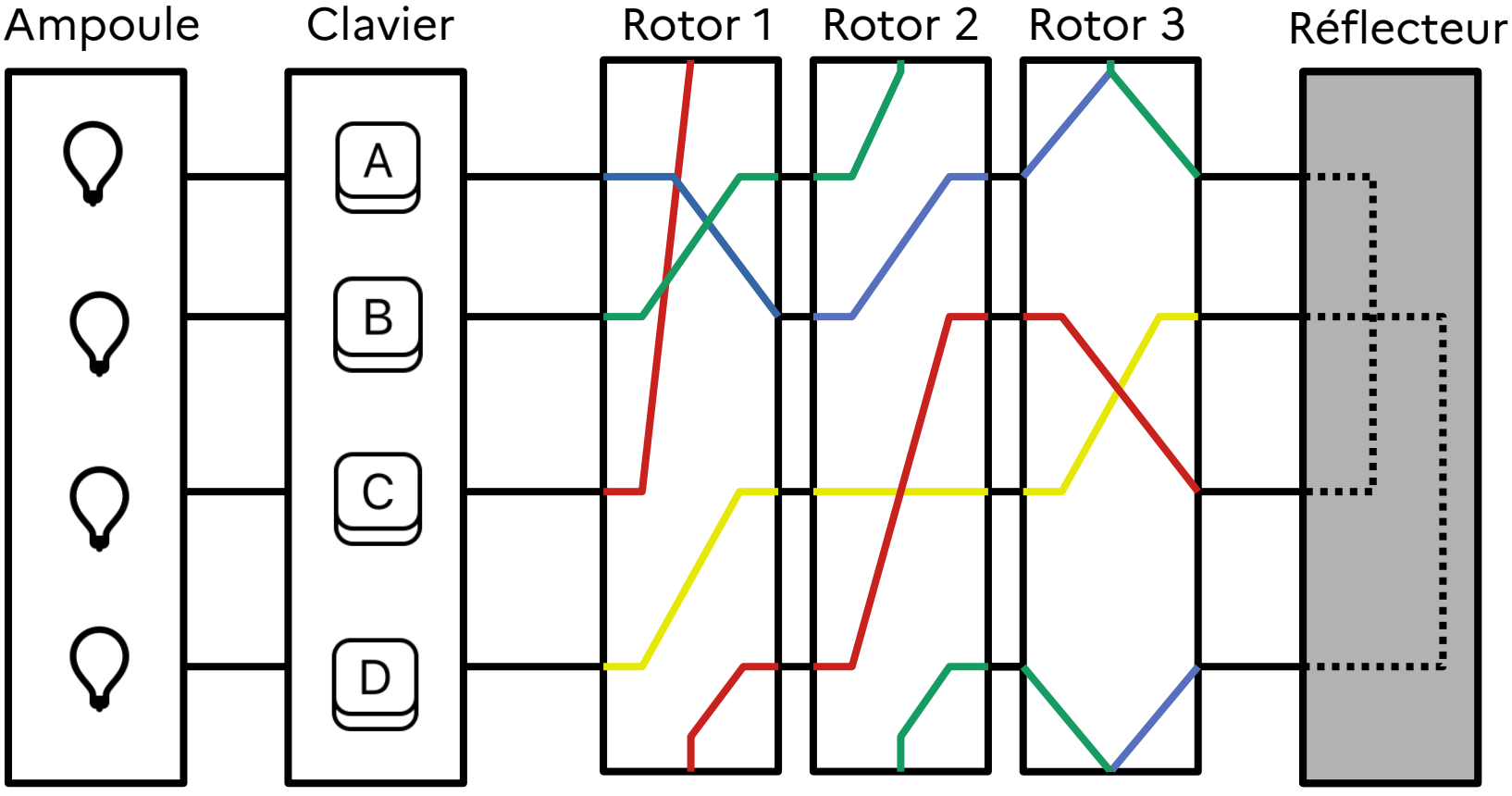
1791
1er télégraphe



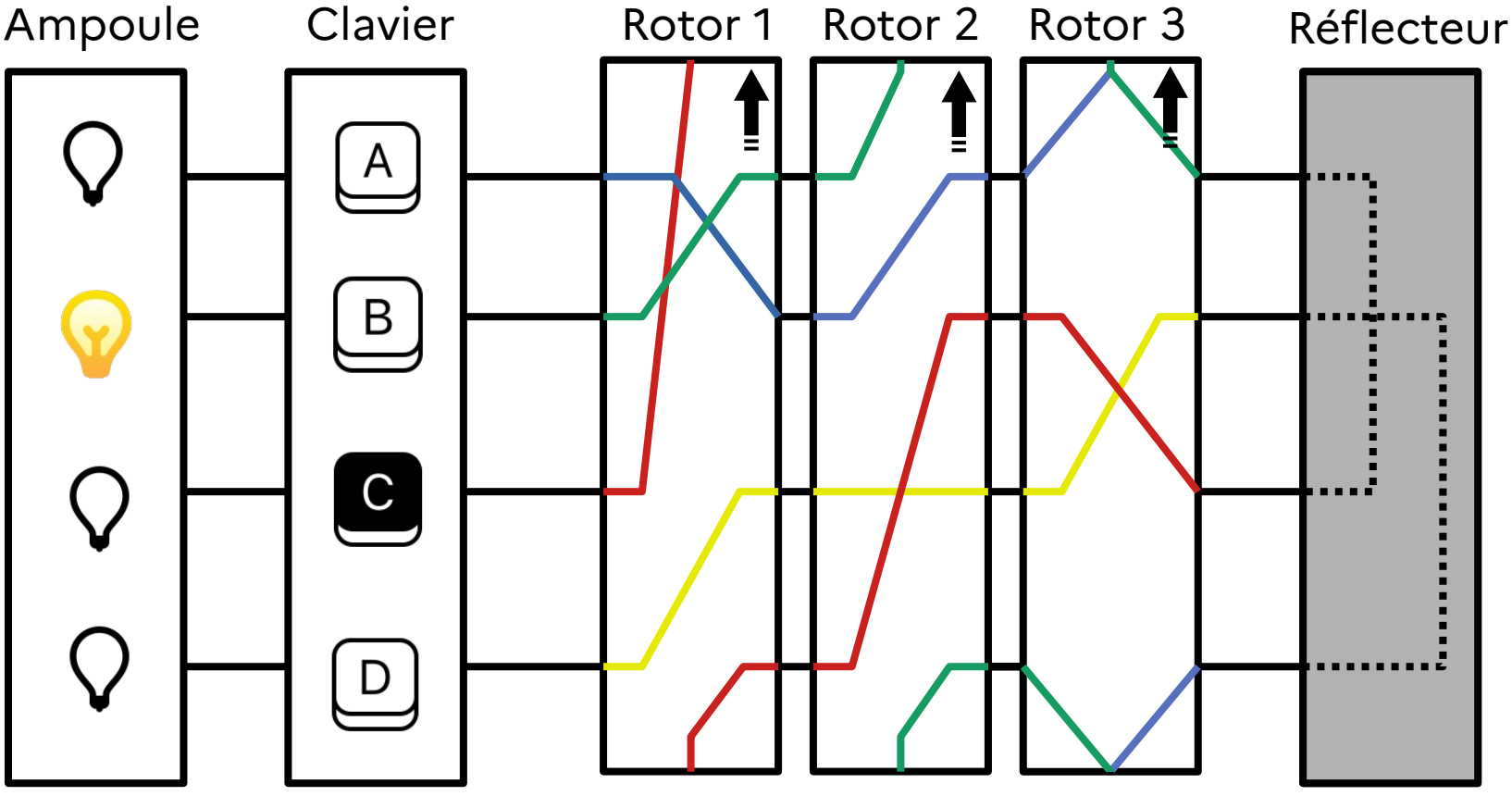
1918
Enigma



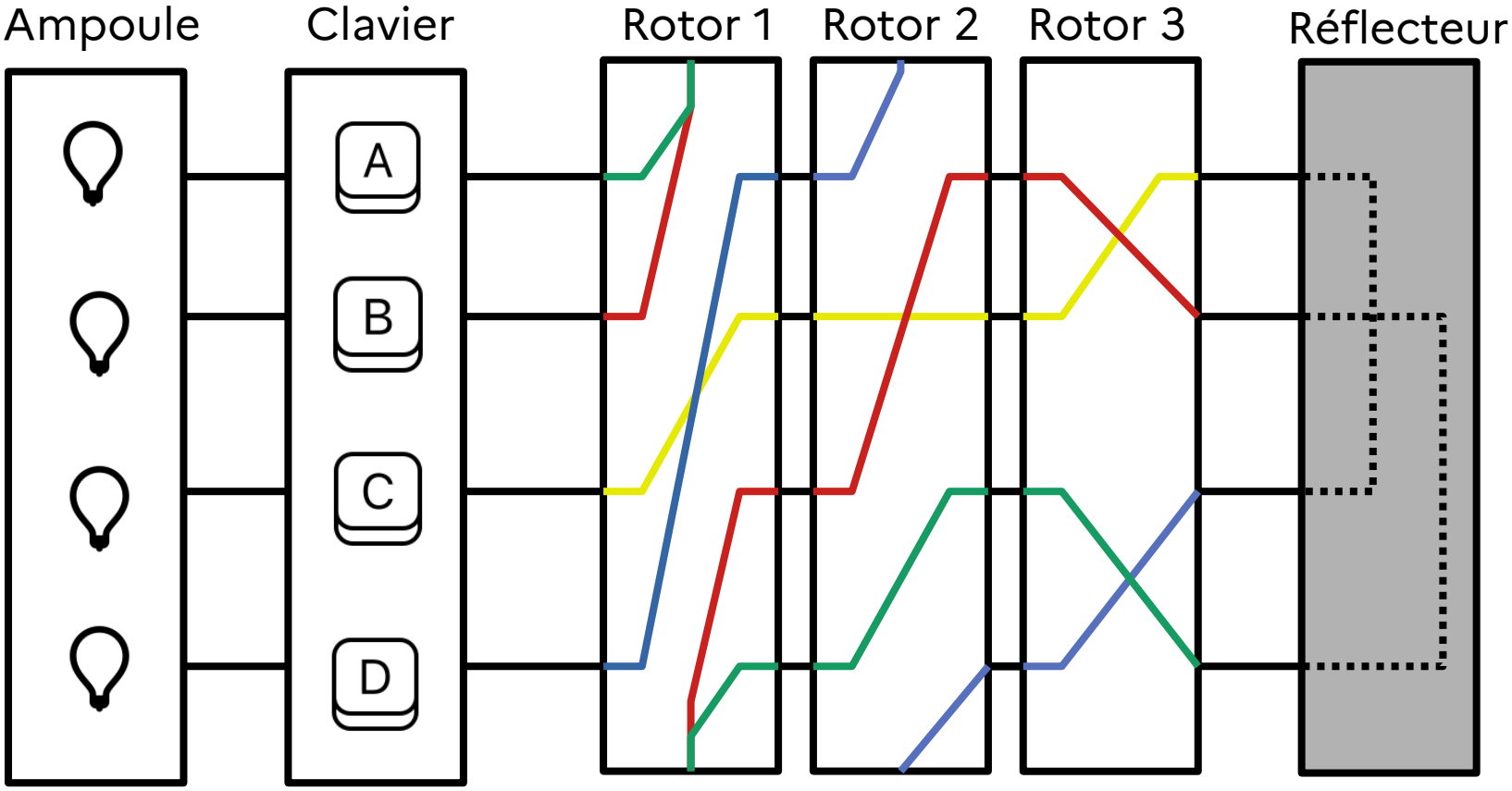
(mini-)Enigma



(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.rice 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 – Décomposer un nombre en un produit de 2 facteurs (≠ 1),
c'est-à-dire trouver les 2 nombres tel que leur multiplication do

On appelle ce problème : la FACTORISATION.

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 (cumulées),
- sur 10 000 ordinateurs,
- grosse consommation électrique

x

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

=

Infaisable en temps :

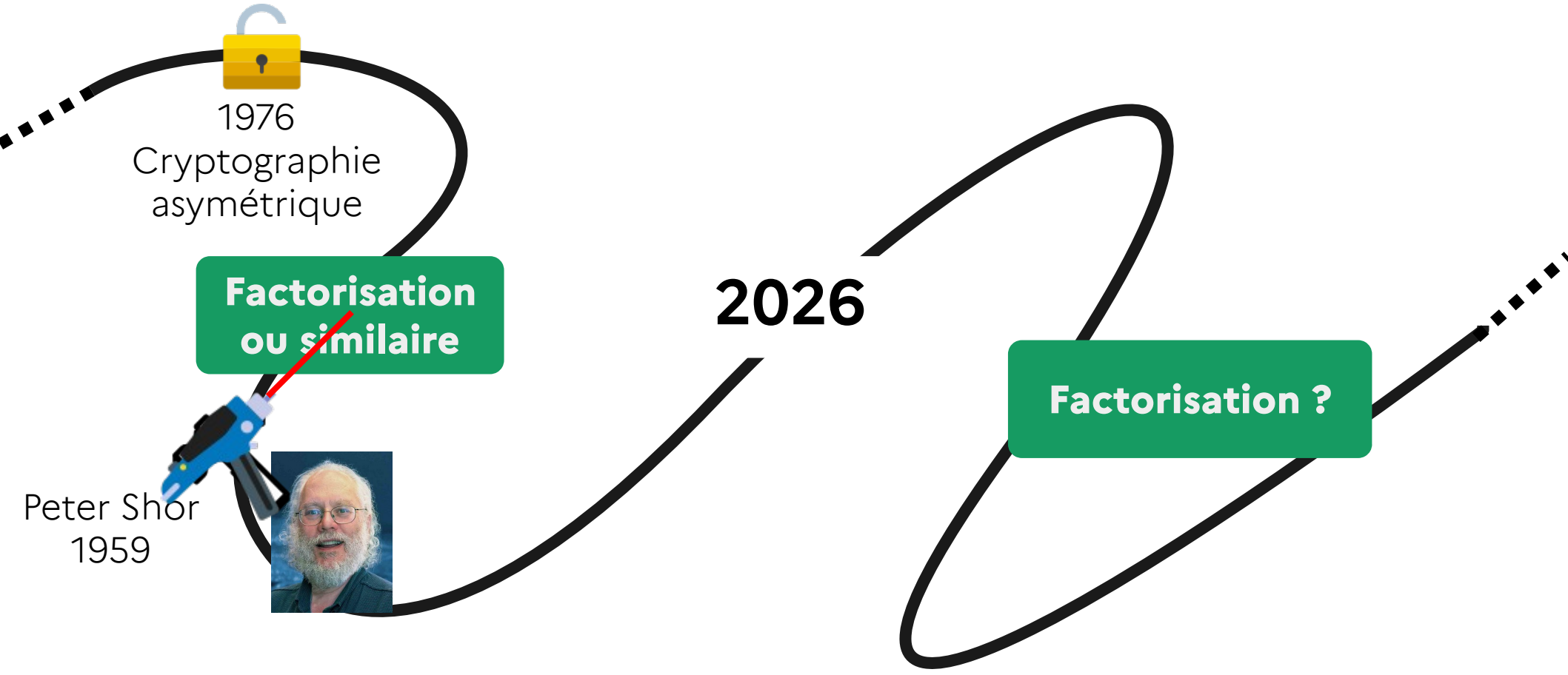
Coopération entre les 8 milliards d'êtres humains sur Terre avec des ordinateurs récents
= + d'années que depuis le big bang

Infaisable en énergie :

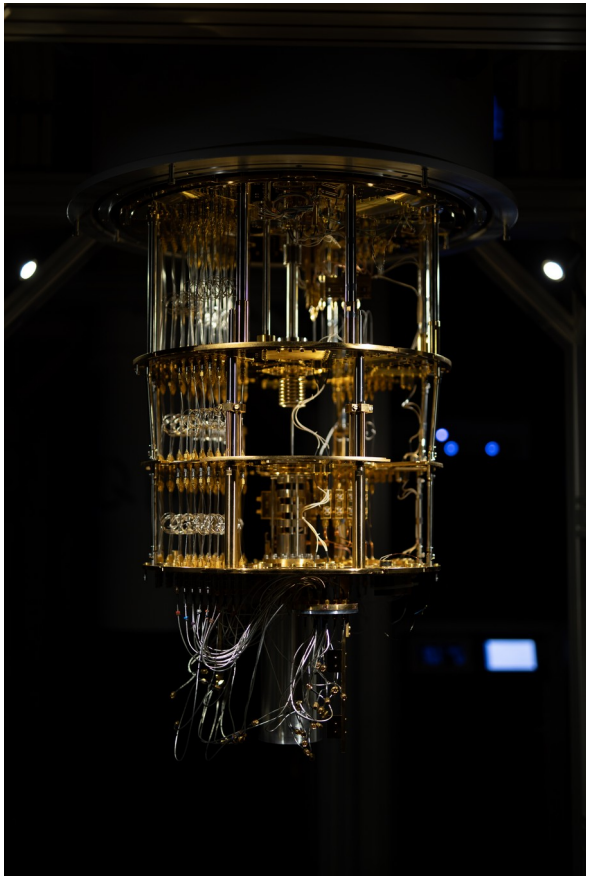
- 250 chiffres : autant d'énergie que pour évaporer 2 piscines olympiques
- 900 chiffres : autant d'énergie qu'il faut pour évaporer toute l'eau de ce système solaire (minimum)

Estimation non rigoureuse pour montrer l'absurdité

Un point d'histoire (future)



Ordinateur quantique



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

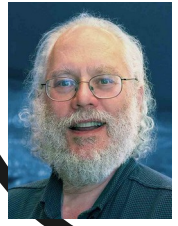
Différents problèmes :
- Quantité limitée de données en entrée,
- Correction d'erreurs difficile,
- Protection difficile,
- Et surtout, ça n'existe pas (encore)

Cryptographie post-quantique

1976
Cryptographie
asymétrique

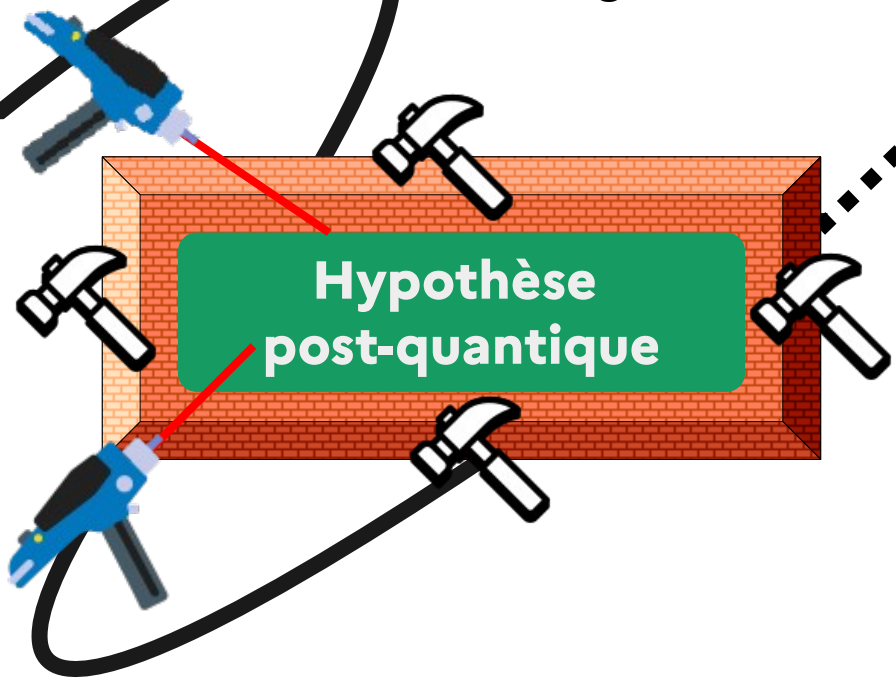
Factorisation ou similaire

1959
Peter Shor



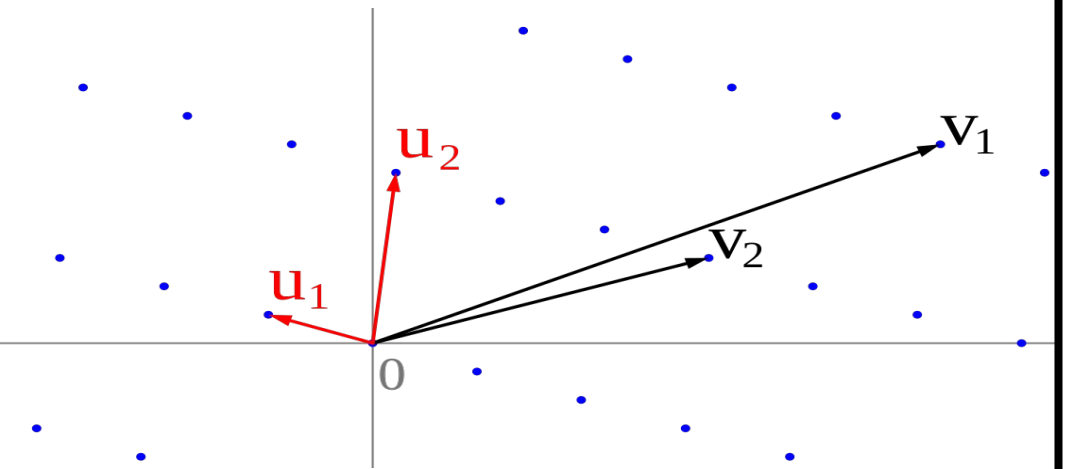
2026

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

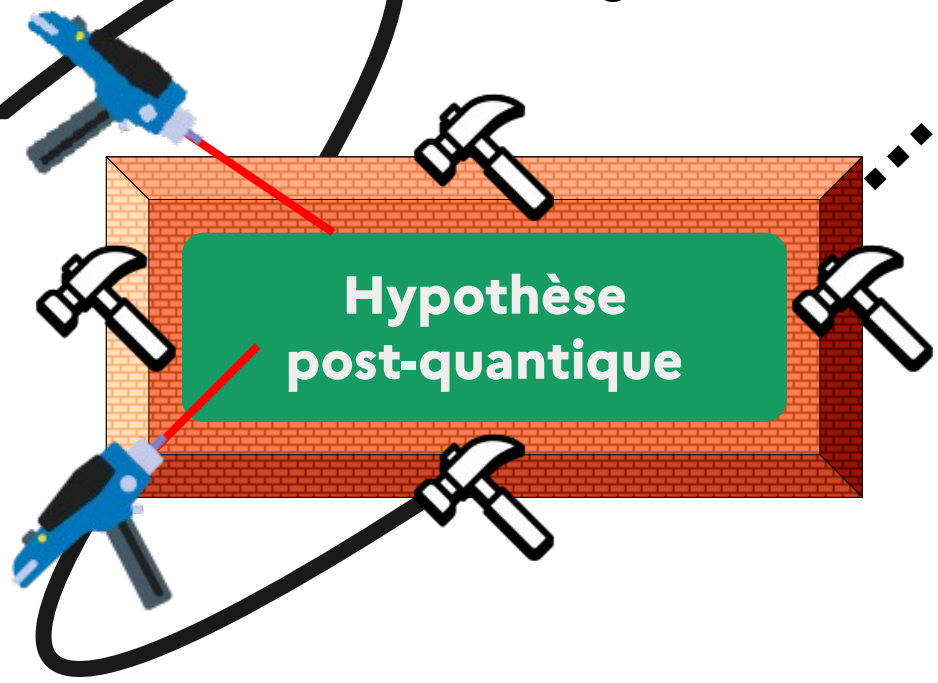
Factorisation ou similaire

1959
Peter Shor



2026

2030
Recommandation
de migration



Usage actuel

Militaire : sécurisation des communications



En quoi la cryptographie vous est utile ?



Prévention numérique

LES 10 RÈGLES D'OR

1. Séparez strictement vos usages à caractère personnel de ceux à caractère professionnel.

2. Mettez régulièrement à jour vos outils numériques.

3. Protégez vos accès par une authentification double-facteur lorsque c'est possible, ou a minima par des mots de passe robustes.

4. Ne laissez pas vos équipements sans surveillance.

5. Prenez soin de vos informations personnelles en ligne.

6. Protégez votre messagerie électronique.

7. Évitez les réseaux Wi-Fi publics ou inconnus.

8. Sauvegardez régulièrement vos données.

9. Protégez-vous des virus et autres logiciels malveillants.

10. Accordez le juste niveau de privilèges.



MINISTÈRE
CHARGÉ
DE L'ENSEIGNEMENT
SUPÉRIEUR
ET DE LA RECHERCHE

Liberté
Égalité
Fraternité

Merci pour votre attention

N'hésitez pas à poser des questions.

Antoine Douteau, Doctorant en Informatique

fête de la Science

GREYC
Laboratoire de recherche en sciences du numérique

cnrs

RÉGION NORMANDIE