FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

PROCESSEUR QUANTIQUE ET SÉCURITÉ INTERNET

JP Bonneau Novembre 2021

Sémantique

- On devrait utiliser le mot «processeur»
- Et non «d’ordinateur»
- Mais dans ce texte, ce sera utilisé indifféremment.

Plan de la présentation

- Qu’est ce que la physique quantique ?
- Qu’est-ce qu’un ordinateur «classique» ?
- Qu’est-ce qu’un ordinateur «quantique» ?
- Promesse de la supériorité d’un ordi quantique
- Une tentative d’explication de cette supériorité
- Internet et encodage (cryptologie)
- Comment briser l’encodage
- Désespoir
- Espoir

Les différentes sortes de «physiques»

- **Physique classique** …celle que l'on a apprise (et oubliée..?)
  - La physique de Newton….celle qui nous sert dans 99 % de nos vies.

- **Physique relativiste**: celle d'Einstein…les grosses choses qui vont vite…
  - Vitesse de la lumière et $E=mc^2$
  - C'est pas pour nous mais …***le GPS doit en tenir compte…***

- **Physique quantique**: cela se passe dans l'infiniment petit (niveau atomique et subatomique)

La physique quantique

- S’est développée au début des années 1900
- Surtout en Europe (Heisenberg, Schrödinger, Planck, Bohr…)
- Elle ne nous concerne pas …(pas encore)
- Des choses bien étranges se passent dans l’infiniment petit
- On ne parle plus de certitude mais de probabilité.
- Ce n’est plus 0 ou 1 mais «peut-être».
- Superposition, fonction d’onde, principe d’incertitude, décohérence, intrication.

Un ordinateur classique

- Basé sur des **0 ou 1…le bit…**
- Des opérateurs logiques : **Et ,Ou, Ou exclusif, Additionneur**
- Machine séquentielle…ie: une opération à la suite de l'autre
- La puissance a explosé….loi de Moore….
- Tous les 18 mois, on double la puissance (mémoire, vitesse)
- Mais on croit arriver à la limite ….
- Les derniers «chips» se butent aux phénomènes de l'infiniment petit (phénomène quantique ironiquement)

Un ordinateur quantique

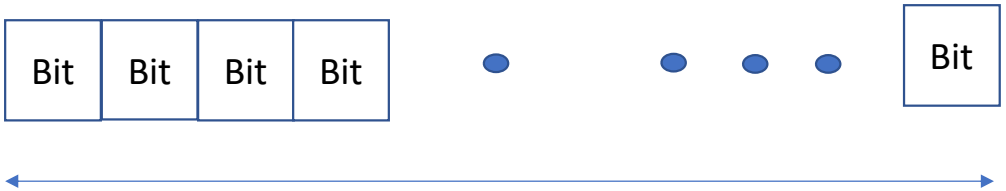
- C’est très expérimental…
- Cela coûte très cher…
- Ce n’est pas encore fiable…on est loin de la mise en marché
- Cela doit être refroidi (- 273 C …sinon cela ne fonctionne pas…)
- Mais les grands de ce monde y mettent des millions $ en recherche…

L'ordinateur quantique

- Basé sur le «bit quantique» ou «**qubit»…**
- On distingue les ordi quantique par le nombre de qubits qu'ils peuvent «cascader»…IBM annonce un ordi de 127 qubits.
- Un «qubit» : 0 ou 1 ou ***quelque chose entre les 2 (principe de la superposition en quantique)***

FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

Classique



32 ou 64

Bit

0 ou 1

Quantique

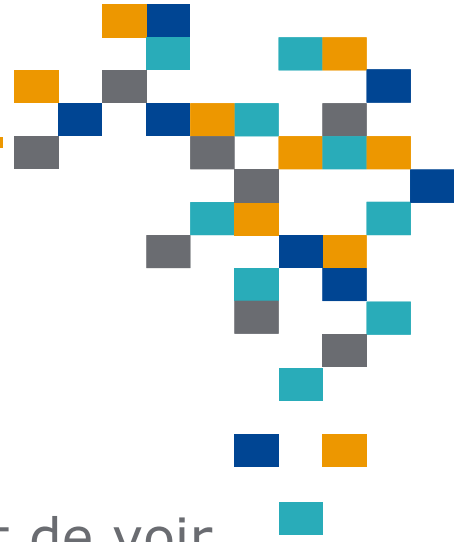
127 (En laboratoire)

Qbit

0 ou 1 ou «X»

X= n|1> + m|0> où n+m=1

Bit vs Qbit



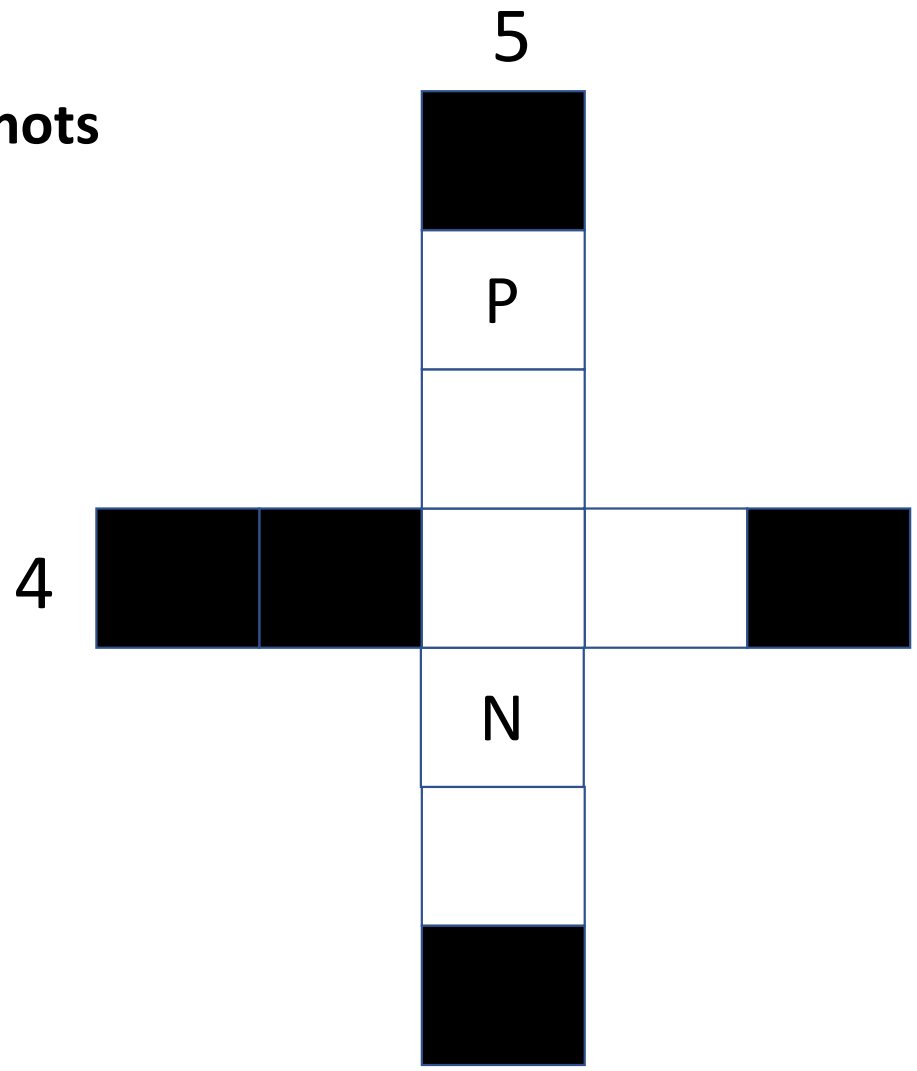
- Pourquoi un Qubit est-il supérieur à un Bit ?
- Exemple qui suit est sans doute boiteux mais il permet de voir la nouvelle dimension du Qubit.

Prenons l'exemple d'un mots croisés

Questions :

4 horizontal: Fin de verbe

5 vertical: Difficulté

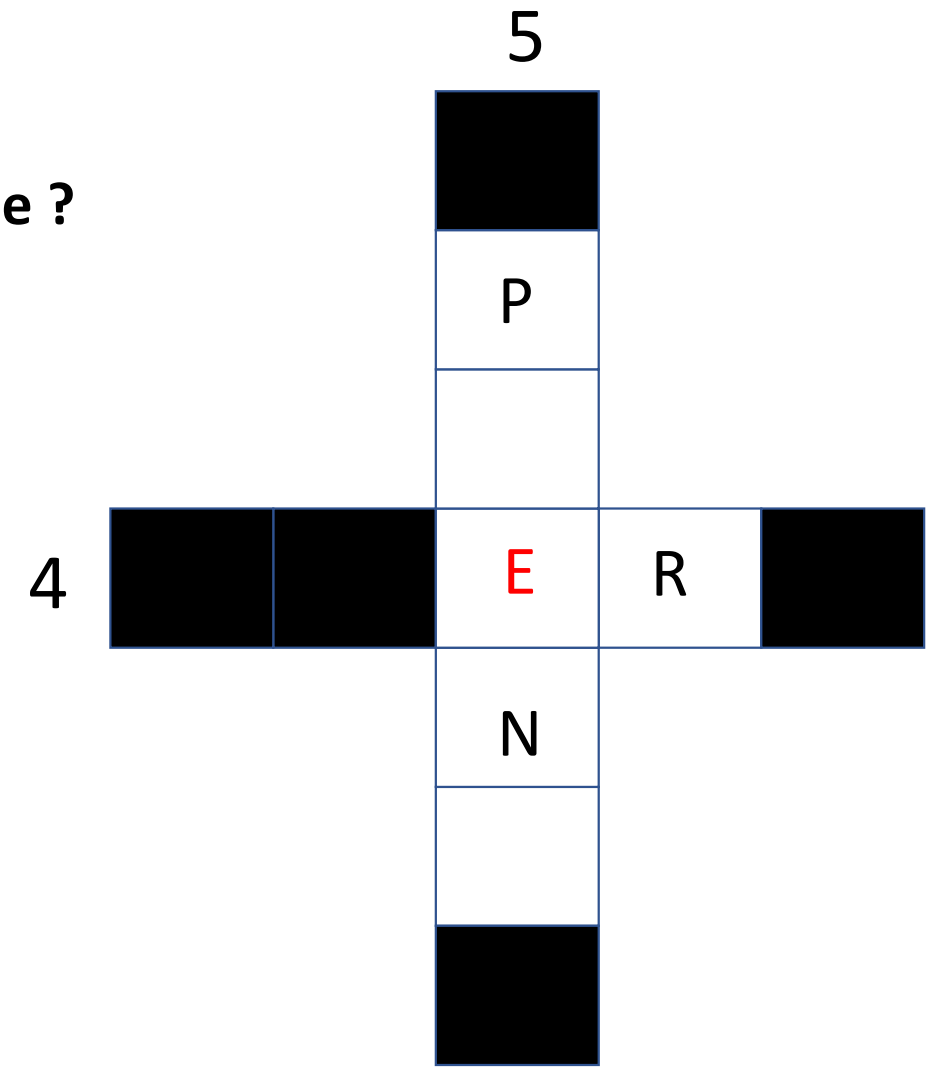


Que ferait un ordi classique ?

Questions :

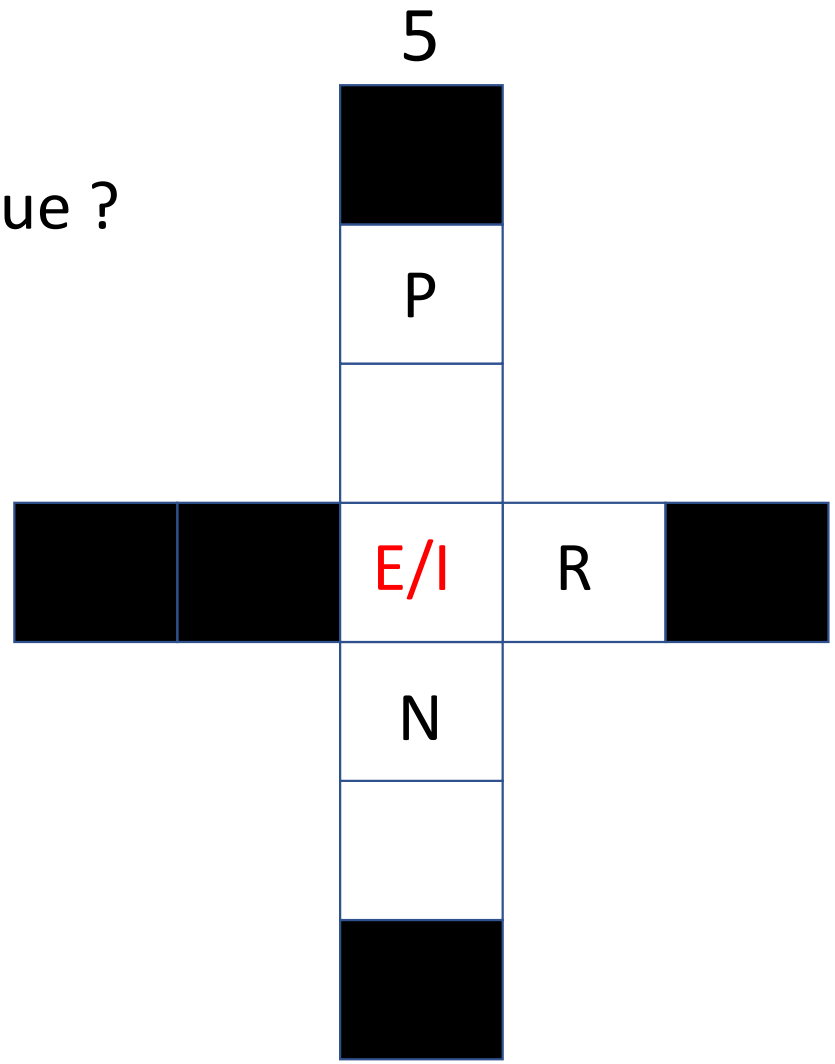
4 horizontal: Fin de verbe

5 vertical: Difficulté



Que ferait un ordi quantique ?

Questions :
4 horizontal: Fin de verbe
5 vertical: Difficulté

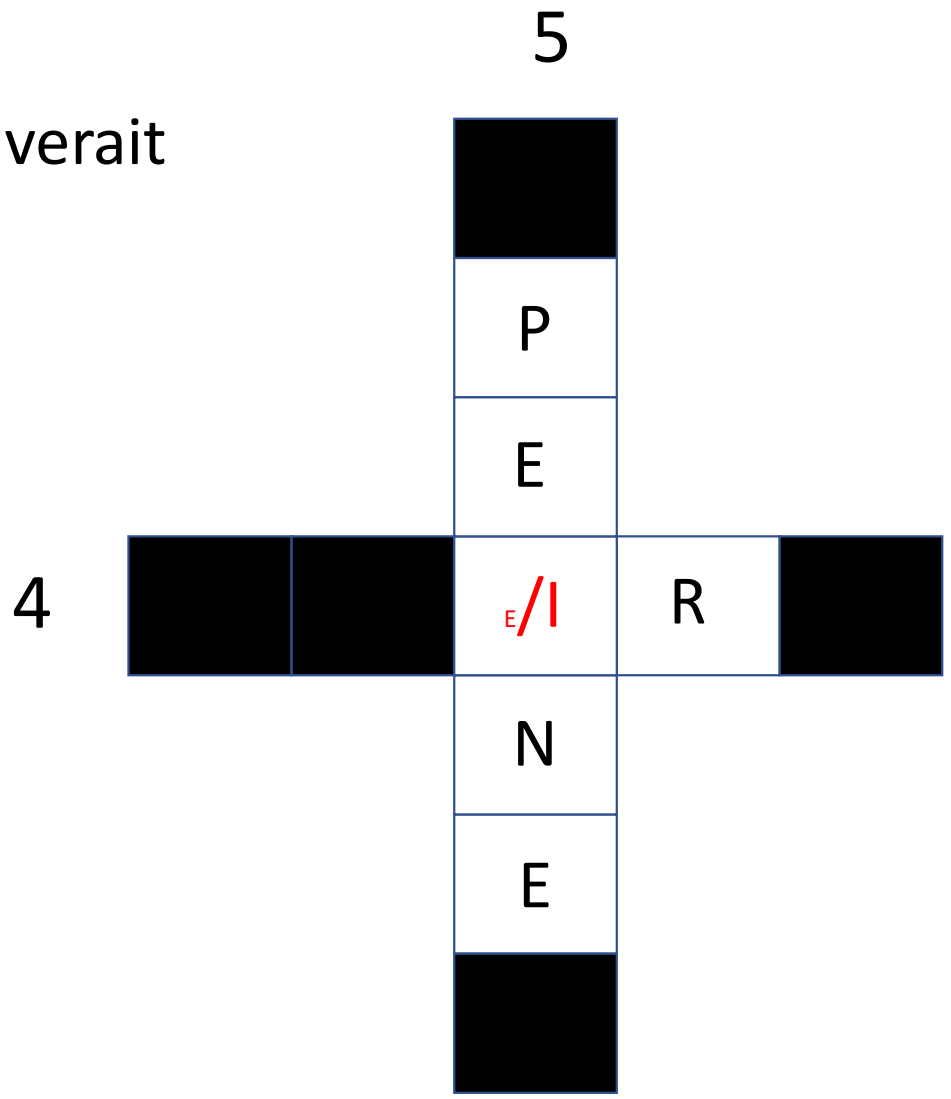


Ici l'ordinateur quantique trouverait la réponse plus rapidement…

Questions :

4 horizontal: Fin de verbe

5 vertical: Difficulté



Quelques percées à date …

- En Octobre 2019, Google annonce une percée (Sycamore 54 qubits)
- L'équivalent de 10,000 ans de calculs en quelques minutes.
- IBM a contesté ceci en disant que leur ordi classique aurait pris 3 jours.
- En juin 2021, une agence chinoise dit avoir fait l'équivalent de 8 ans de calcul en 72 minutes (66 qubits)
- En général ce sont des calculs théoriques qui n'ont rien de pratique.
- IBM a annoncé un processeur de 127 qubits cet automne.

Autres avantages de l'ordi quantique

- Il peut travailler en «parallèle» et non seulement en «séquence»
- Ce n'est pas le «multi tâches» (qui n'est que la séquence à tour de rôle) mais vraiment faire plusieurs opérations en même temps
- La programmation en parallèle: un défi de programmation…
- Exemple du livre marqué dans une bibliothèque

Mais ce n’est pas demain la veille.

- C’est très instable…
- Présentement, il faut répéter souvent un même calcul pour s’assurer que l’on a la même solution (convergence).
- Code correcteur d’erreurs.
- «Décohérence» à la moindre «anicroche».
- Certains scientifiques pensent que ce ne sera jamais stable.

Alors pourquoi tant d'intérêt ?

- Plusieurs labo de recherche y consacrent des fortunes
- (Google, IBM, AMZ, Intel, les universités)
- Les gouvernements…(USA, Russie, Chine…Canada..)
- Plusieurs domaines de recherches demandent de grandes puissances de calculs…
- Ex. : météorologie, recherche en biologie,
- Mais surtout: le **décodage des codes secrets**….

LA CRYPTOGRAPHIE

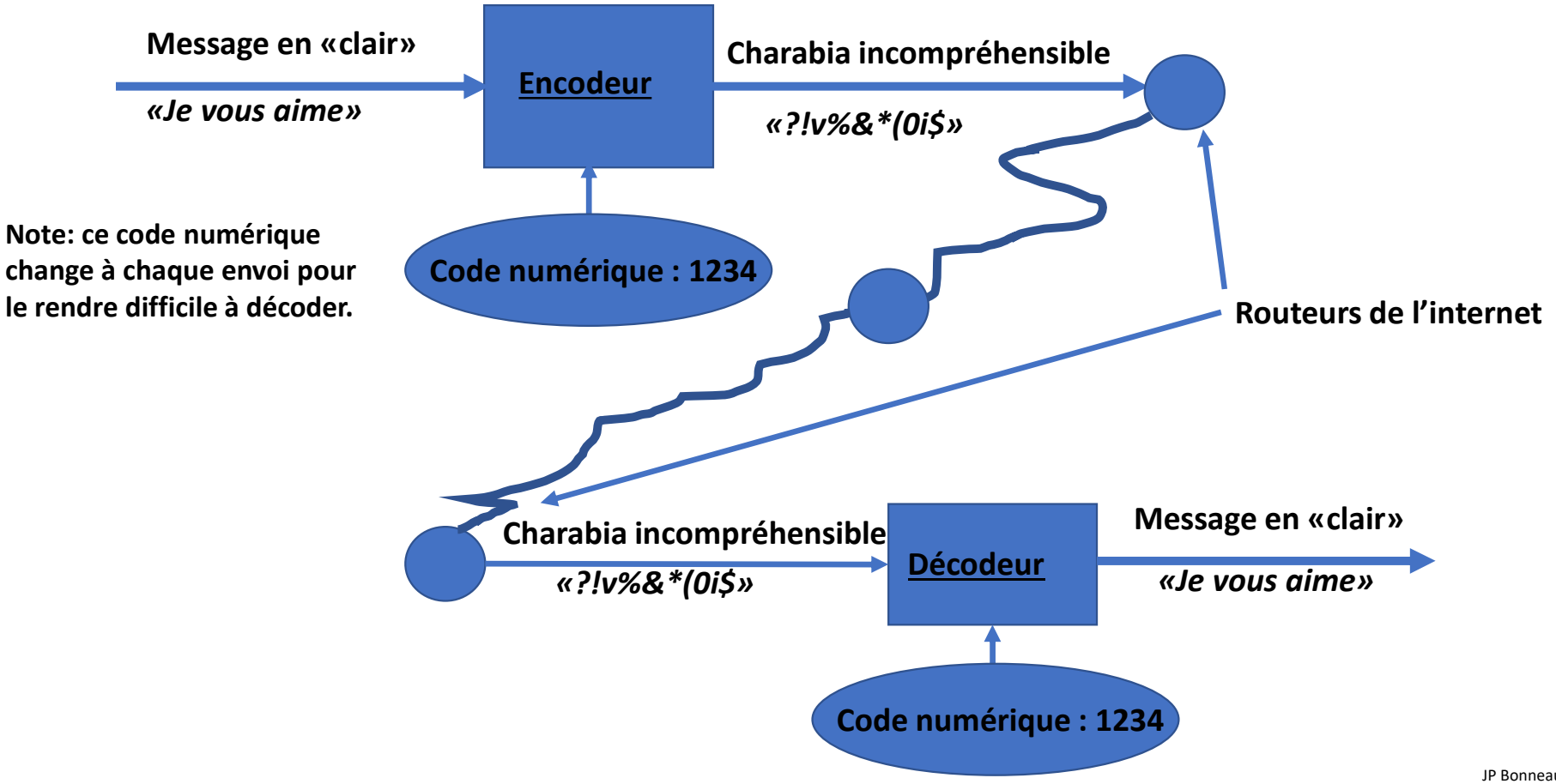
La cryptographie

- Un sujet aride et «plate»
- Mais combien nécessaire
- Toutes nos transactions bancaires… (https:/ …)
- Nos courriels contenants des infos personnelles.
- Documents personnels échangés sur le net

Comment cela fonctionne…

- Un processus qui transforme des données claires en «charabia » numérique
- Le «charabia» numérique est transmis sur le «net»
- Un processus inverse se fait à la réception…ie: décodage
- Une clé échangée entre TX et RX permet le codage et son décodage

Comment fonctionne l'encodage / décodage sur l'internet



JP Bonneau Octobre 2019

L’échange de clé

- En fait il y a 2 clés…
- La clé privée que le TX et RX doivent utiliser pour coder /décoder
- (1234 dans notre exemple)
- La clé «publique» échangée en «clair» entre TX et RX..
- Cette clé publique contient la clé privée mais bien cachée..
- Mais comment transmet-on cette clé «sous les yeux» de tous ?

L'astuce mathématique

Opération facile: multiplier 1234 ✖ 70 = **86380**

Opération facile : diviser **86380 / 70 = 1234**

Opération très difficile: décomposer en nbres premiers : 84675

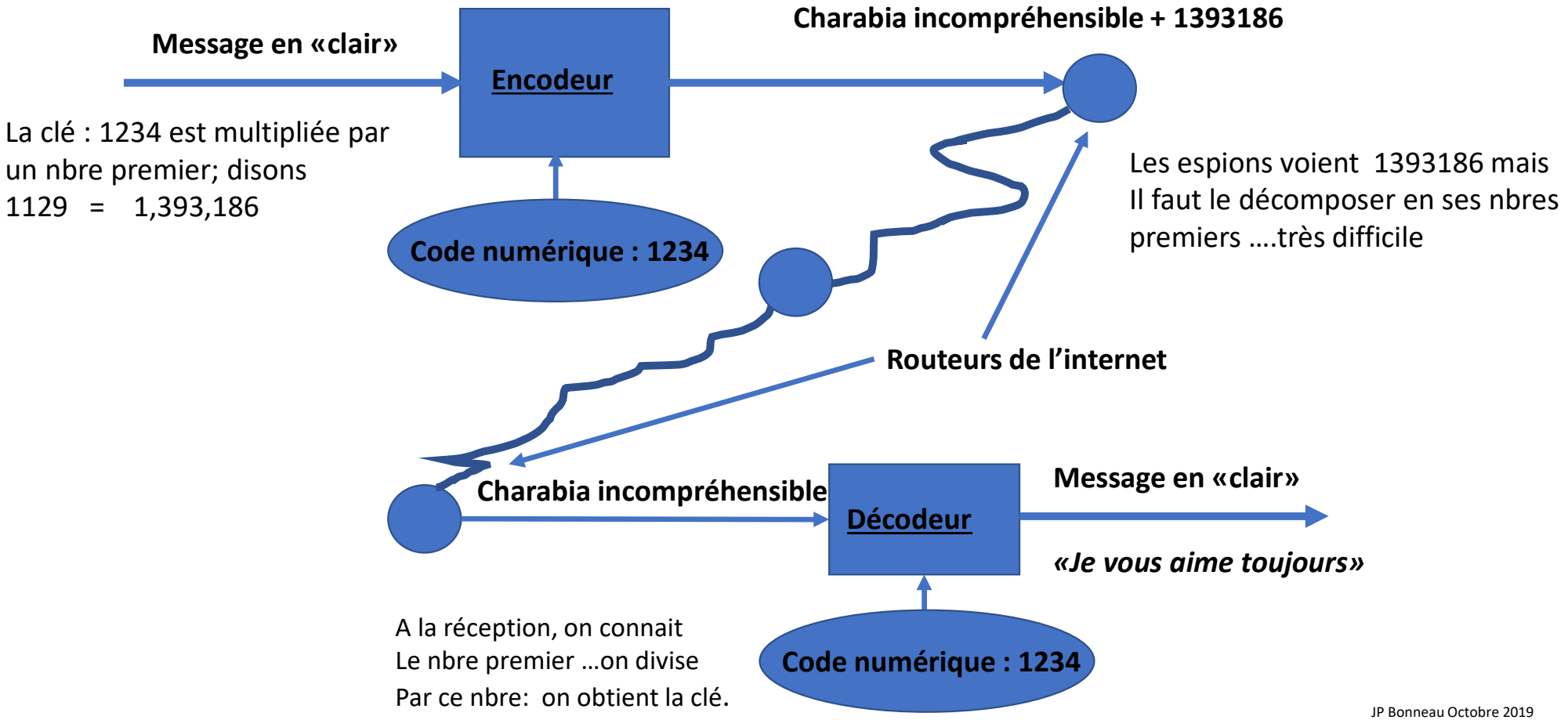
Réponse: 3 * 5 * 5 * 1129
Imaginez un nbre de 100 chiffres…de 1000 chiffres…

JP Bonneau Octobre 2019

La décomposition d'un nbre en ses nbres premiers

- Il est extrêmement difficile de décomposer un nombre (très grand) en ses nombres premiers
- Nombres qui sont très grands…ils sont écrits avec plus de 1000 chiffres..
- Il n'y a pas de «formule» pour les décomposer …«force brute»
- Un ordi classique peut prendre des années

Comment fonctionne l'encodage / décodage sur l'internet



JP Bonneau Octobre 2019

La décomposition d'un nbre en ses nbres premiers

- Un ordi classique peut prendre des années

- ***Mais un ordinateur quantique pourrait le décomposer en quelques minutes***
- ***Trouver la clé privée***
- ***et donc décoder le message.***

Les agences de renseignements en «bavent»

- Toutes nos communications seraient décodables…
- La seule façon de se prémunir est de multiplier par des nombres premiers encore plus grands…mais il y a un prix…
- Le doute subsistera toujours….est ce que l'autre peut me décoder ?
- Bien pire: nos échanges actuels sont tous enregistrés…
- On ne peut pas les lire présentement…mais dans le futur
- Des organismes pourront les lire….rétroaction qui viendra nous hanter…

Solution : l'encodage quantique

- Cela aussi c'est du «matériel» de laboratoire
- Ceci aussi est très complexe.
- Cela utilise un principe de base des effets quantiques..
- Quand on mesure un phénomène quantique , on le perturbe…
- Alors il s'agit d'associer un «phénomène quantique» à un message…et
- Si quelqu'un a essayé de le lire …on le saura à la réception
- Désolé c'est tout ce que j'ai compris

Merci de votre attention.