La cryptographie mathématique

La journée horizons mathématiques
28 avril 2017

Monica Nevins
Département de mathématiques et de statistique

Que sont les mathématiques ?

- Les nombres
- Les fractions
- L'arithmétique
- La probabilité
- L'analyse des données
- La géométrie
- L'algèbre
- …

- **La cryptographie**
- **L'analyse des réseaux sociaux**
- **L'imagerie résonance magnétique**
- **Les épargnes et le crédit**
- **La stratégie économique**

…

Ainsi que ses applications !

L’étude des mathématiques est …

- La résolution d’énigmes
- La découverte de motifs et de structures

$$1 + 2 + 3 + 4 + 5 + 6 = 3 \times 7$$

Les mathématiques et la statistique sont un sujet vivant et vibrant

La découverte de 0...

vers l'an 700, en inde

La découverte du calcul différentiel et intégral...

vers 1650

(la plus grande découverte scientifique du 2e millénaire!)

La cryptographie mathématique...

aujourd'hui !

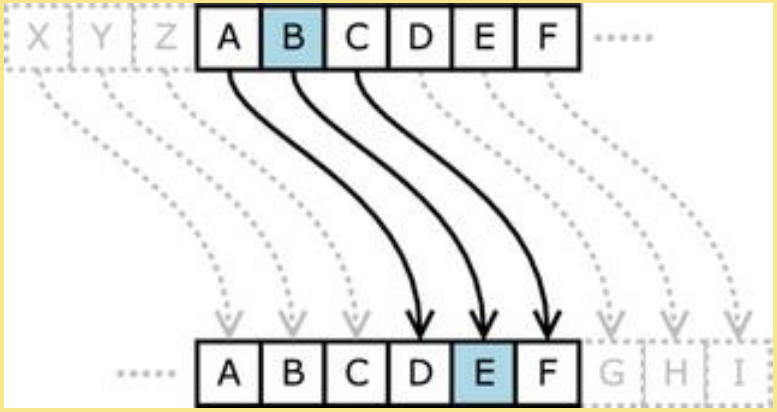
La cryptographie

…est l'**art** et la **SCIENCE** d'obscurcir les messages afin que personne, sauf le destinataire prévu, puisse les lire.

Quel est un **cryptosystème** ?

- **Un algorithme** pour chiffrer vos messages (et déchiffrer vos messages codés), plus
- **Une clef**, qui est le paramètre spécifique utilisé pour chiffrer un certain message

Chiffre de **César**: **Décaler chaque lettre par 3**



Exemple: VENI, VIDI, VICI

Devient: YHQL, YLGL, YLFL

La Seconde Guerre mondiale

Le cryptosystème :

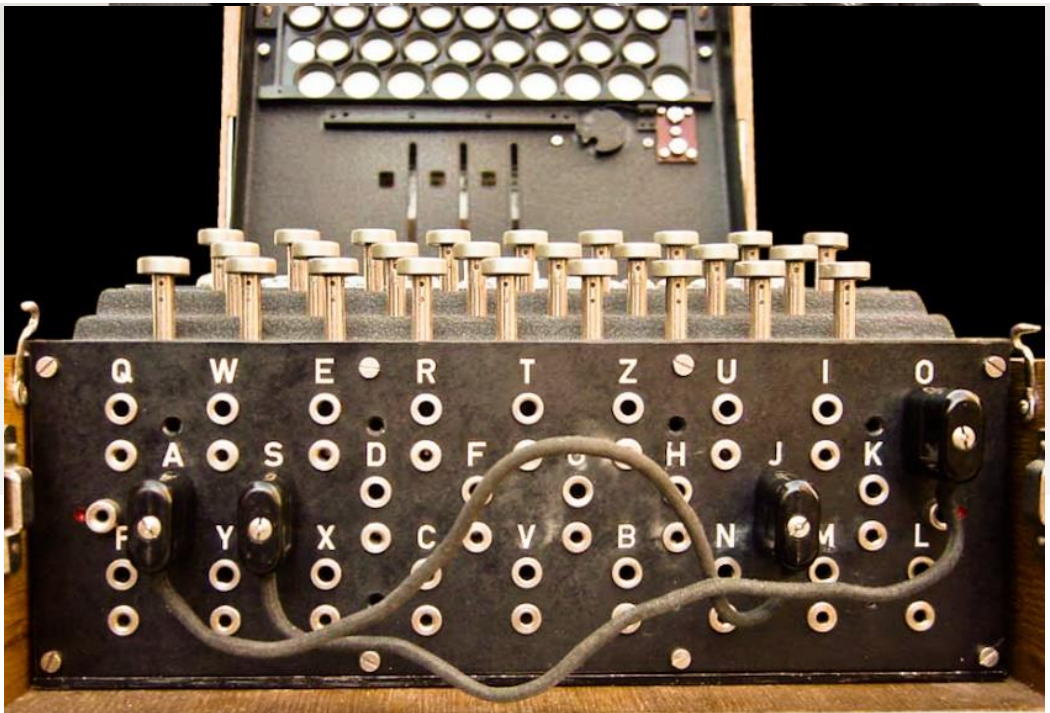
La machine Enigma

La clef :

Le réglage des rotors et les prises

Donc 10^{20} clefs possibles !

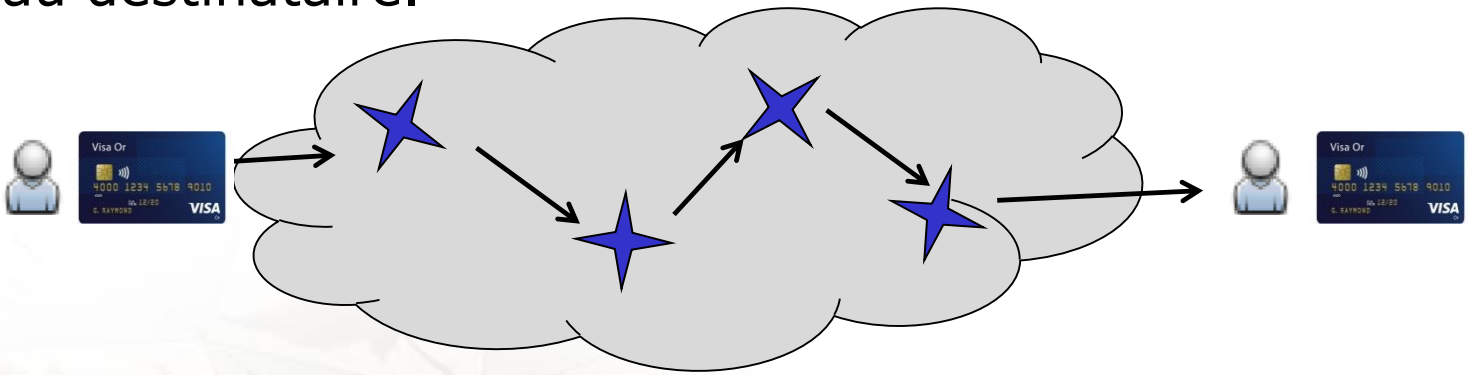
"Complètement incassable"



Craqué par une équipe de mathématiciens, 1940

La cryptographie de nos jours

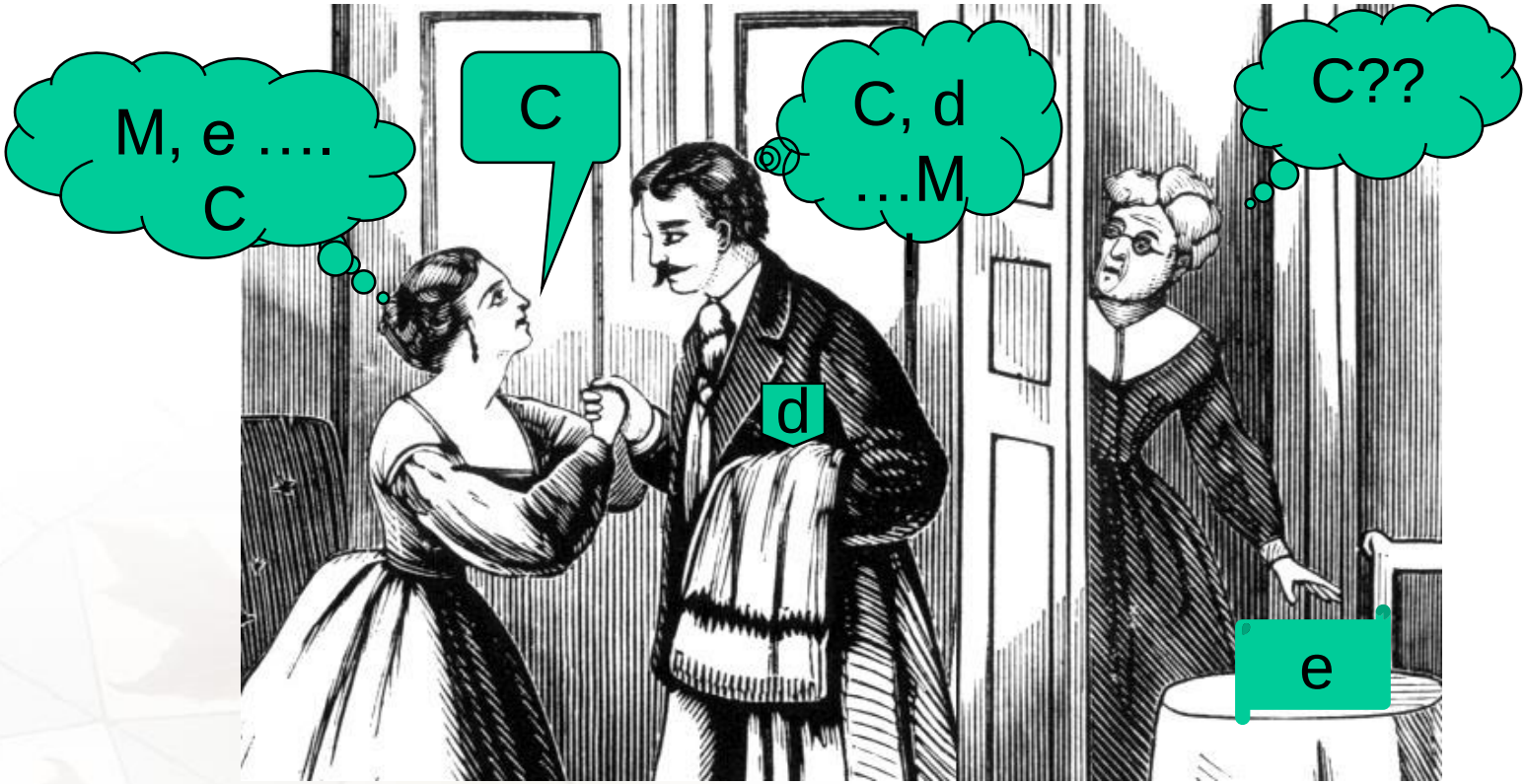
- Une nécessité: toute communication par l'internet est copiée et transmise à plusieurs serveurs avant d'arriver au destinataire.



- Pour mener une communication secrète, il faut avoir **déjà** partagé une clef secrète.

- Le **paradoxe** : si on était capable de partager une clef secrète, ne serait-on pas capable d'échanger nos informations secrètes sans en avoir besoin?

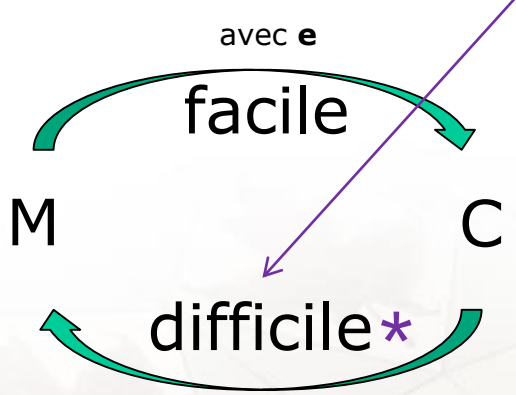
Le concepte revolutionnaire : la cryptographie asymétrique



Anne Bertrand Eve

Est-ce que c'est possible ?

On cherche une fonction qui satisfait les exigences:



Qui veut dire: qu'il faudra un temps énorme (l'âge de l'univers!) pour déchiffrer C.

Une telle fonction est dite une fonction à sens unique.

* Mais facile, si vous avez **d**

Une telle fonction est dite une fonction à porte dérobée.

Les nombres premiers

Définition: Un nombre p>1 est premier si sa seule factorisation est de la forme p=1xp.

Les premiers premiers sont

2, 3, 5, 7, 11, 13, 17, 19, …

Ce sont les atomes de la multiplication.

- Il y a une ∞ de nombres premiers
- Avec la théorie des nombres peut les repérer 'facilement'
- À date, on ne connait aucun patron dans leur distribution, ils semblent distribués aléatoirement parmi les nombres

L'HYPOTHÈSE DE RIEMANN

Problème no. 1 du prix du millénaire

Un exemple d'une fonction à sens unique

Multiplier:	Factoriser:
$5 \times 7 = 35$	$57 = 3 \times 19$
$11 \times 17 = 187$	$91 = 7 \times 13$
$17 \times 19 = 323$	$299 = 13 \times 23$

La multiplication est **facile** – mais la factorisation est **difficile**

C'est donc une fonction à sens unique, mais pas une fonction à porte dérobée…

L'arithmétique modulo n

Soit n un nombre fixe. Posons

$[a]_n$ = le reste (entre 0 et n-1) quand on divise a par n.

Exemples: $[27]_{10} = 7$ et $[257]_{10} = 7$ et $[-3]_{10} = 7$

Une meilleure définition: pour un b entre 0 et n-1

$[a]_n=b$ ssi $a = b + kn$ (pour un k en Z)

À votre tour: calculez

- $[17]_{15}$, $[32]_{15}$ puis
- $[17]_{15}x[32]_{15}$ et $[17x32]_{15}$.

$=[2]_{15}x[2]_{15}=[4]_{15}$ $=[544]_{15}=[4 + 15(36)]_{15}=[4]_{15}$

En fait: $(\mathbf{b}+kn) \times (\mathbf{b'}+k'n) = (\mathbf{bb'} + \underbrace{(kb'+k'b+kk'n)}_{k''n}n)$

Donc pour tout a, c nous avons: $[a]_n[c]_n= [ac]_n$

La multiplication modulo n

Donc c'est vrai que

$$[ac]_n = [a]_n[c]_n$$

Notons:

$[10 \times 6]_{15} = [60]_{15} = 0$ mais ni $[10]_{15}$ ni $[6]_{15}$ sont nuls (!!!)

Par contre, si a et c sont relativement premiers avec n (donc, n'ont aucun facteur en commun avec n),

alors

$$[ac]_n = 0 \quad \Leftrightarrow \quad [a]_n=0 \text{ ou } [c]_n=0$$

On préfère alors les nombres entre 1 et n-1 qui sont relativement premiers avec n.

Les entiers inversibles modulo n

On préfère alors les nombres entre 1 et n-1 qui sont relativement premiers avec n.

Exemple: $Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Est-ce que cet ensemble est fermé sous la multiplication?

Le *nombre* de tels nombres est dite

$\phi(n)$ --- *l'indicatrice d'Euler*.

Par exemple, si p est premier,

$\phi(p) = p-1$

$\phi(p^2) = p(p-1)$

$\phi(pq) = (p-1)(q-1)$ si $p \neq q$ sont premiers

Par exemple: $\phi(15)=2x4=8$. ✔

Les puissances modulo n

(Ici, n=15 et notre base est 8)

e	8^e	$[8^e]_{15}$
0	1	1
1	8	8
2	64	4
3	512	2
4	4096	1
5	32 768	8
6	262 144	4
7	2 097 152	2
8	16 777 216	1

… … …

Les puissances forment une suite qui est à la fois aléatoire et cyclique.

Astuce:

On n'a pas à faire le grand calcul; Il suffit de multiplier la ligne précédente par 8 à chaque fois.

Les puissances modulo n

Alors c'est facile de calculer le résultat de

$$C=[M^e]_n$$

Et la fonction réciproque?

- La fonction $f^{-1}(x)=x^{1/e}$ n'a aucune utilité, puisqu'on ne connait pas la *valeur* de M^e mais seulement sont *reste* modulo n.
- À peu près la seule méthode connue: créer un tableau de toutes les valeurs possibles $[a^e]_n$.

Si n est GRAND déchiffrer C est une tâche impossible.

GRAND comme $10^{80} \approx$ no. d'atomes dans l'univers

Donc: c'est une deuxième fonction à sens unique.

Mais où se trouve la porte dérobée ??

La porte dérobée : le théorème d'Euler

Soit n le modulus.

Théorème d'Euler: Pour tout M relativement premier à n,

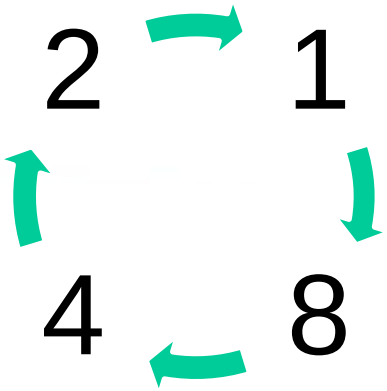
$$[M^{\phi(n)}]_n = 1.$$

Exemple:

$$\phi(15)=8 \text{ et } : \ [8^8]_{15}=1,\ [7^8]_{15}=1,\ [2^8]_{15}=1,\ \ldots$$

Donc, pour n'importe quel entier k, nous avons

$$\begin{aligned}[M^{\phi(n)k+1}]_n &= [(M^{\phi(n)})^k M^1]_n \\ &= [M^{\phi(n)}]^k [M]_n \\ &= M.\end{aligned}$$



La porte dérobée : le théorème d'Euler

Donc $[M^{\phi(n)k+1}]_n = M$ pour tout entier k.

Soient e et d deux nombres dont leur produit satisfait à

$$ed = \phi(n)k + 1 \quad \text{(pour un choix d'entier k)}$$

Exemple: Ex: $7 \times 7 = 49 = \phi(15) \times 6 + 1$

Donc si $M<n$ et M est relativement premier avec n et

$$C=[M^e]_n$$

Alors

$$\begin{aligned}[C^d]_n &= [(M^e)^d]_n \\ &= [M^{ed}]_n \\ &= [M^{\phi(n)k+1}]_n \\ &= M.\end{aligned}$$

Exemple: si $M=8$

$C=[8^7]_{15}=2$

alors

$[C^7]_{15}=[2^7]_{15}=8=M$!

RSA (Rivest, Shamir, Adleman, 1977)

Choisir en secret deux **très grands** nombres premiers

p et q.

La clef publique : $n = pq$. (Personne ne pourrait retrouver p et q!)

La clef privée : $\phi(n) = (p-1)(q-1)$. (Votre secret.)

Choisir e et d tel que $[ed]_{\phi(n)}=1$. (Facile.)

Publier au monde: n, e. Garder au privé: d. (Détruire p et q.)

Pour chiffrer **M**, Anne calcule

$\mathbf{C = [M^e]_n}$.

Pour déchiffrer **C**, vous calculez

$\mathbf{[C^d]_n = M}$.

À votre tour…

Choisir en secret deux **très grands** nombres premiers p et q. ($5<p,q<20$!)

Calculer $n=pq$ et $\phi(n) = (p-1)(q-1)$.

Choisir e relativement premier à $\phi(n)$ et puis trouver d tel que $[ed]_{\phi(n)}=1$.

(Astuce: e va diviser un des nombres $\phi(n)+1$, $2\phi(n)+1$, $3\phi(n)+1$, …)

Publier à votre équipe: n, e.

Garder au privé: d.

*Choisir M relativement premier à n

M=3	M=4	M=5	M=6	M=8
minuit	midi	jamais	8h15	17h20

L'heure de notre rencontre secrète :

Pour chiffrer **M**, Anne calcule

$\mathbf{C = [M^e]_n}$.

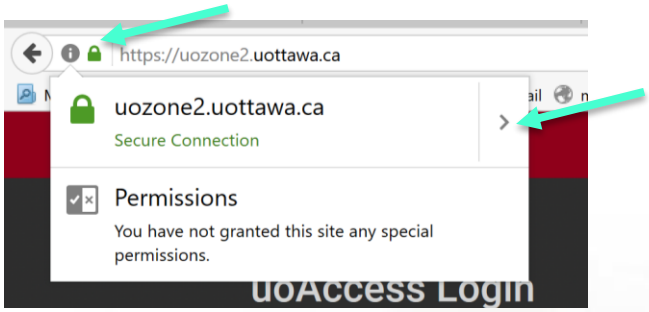
Pour déchiffrer **C**, vous calculez

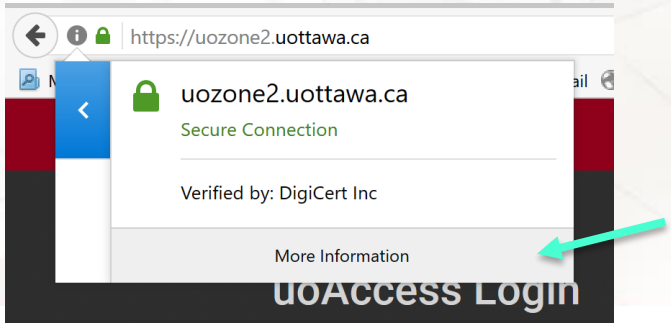
$\mathbf{[C^d]_n = M}$.

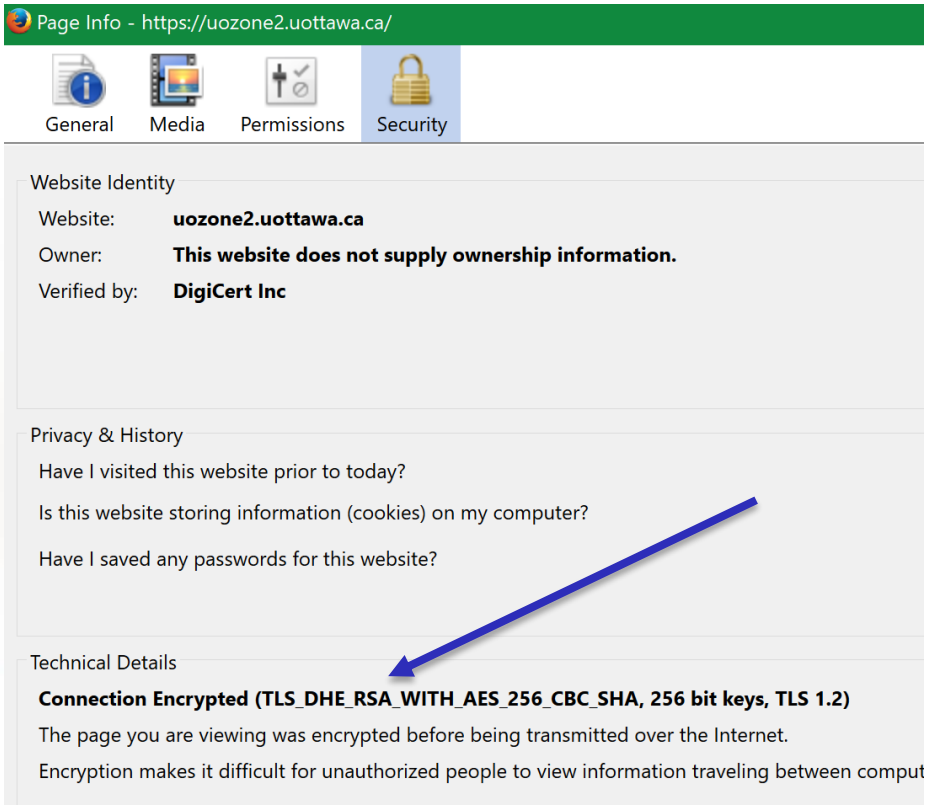
http://www.dcode.fr/calcul-exponentiation-modulaire

RSA est malin, et facile, mais qu’est ce que ça vaut ?

RSA est utilisé partout au monde – c’est la base du chiffrement de la majorité de pages web sécurisées.







Et la sécurité?

RSA est extrêmement forte, et nous assure d'une communication privilégié … à condition qu'on ne puisse factoriser n.

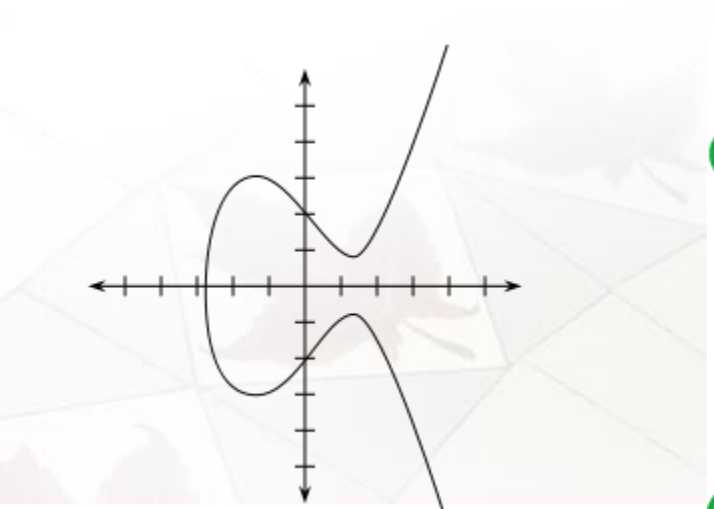
Son importance est tel qu'on investit énormément dans la recherche en théorie des nombres (et beaucoup d'autres domaines de mathématiques).

Par contre, un ordinateur quantique pourrait factoriser même un grand n facilement …

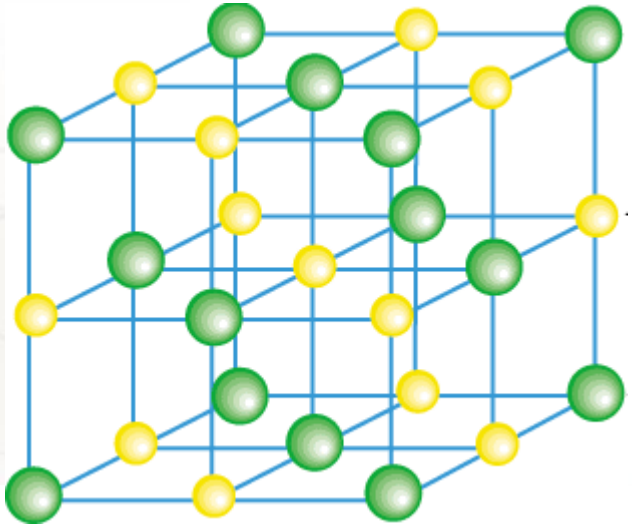
Et l'avenir ?

Il n'y a aucune manque de problèmes mathématiques difficiles qu'on puisse développer en cryptosystèmes puissants!

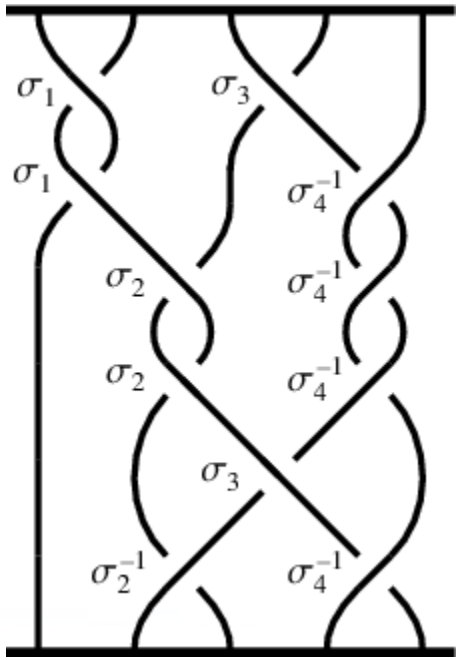
Quelques exemples:



Les courbes elliptiques (ECDHA)



Les réseaux intégraux (NTRU)



Les tresses mathématiques

Bibliographie

- Les images de cette présentation viennent de partout sur le web et souvent de Wikipédia.org.

- **Simon Singh** est un auteur très connu pour ses oeuvres de l'histoire et de la réalité moderne de la cryptographie.

- **Jean-Marie De Koninck**, un mathématicien québecois, a écrit plusieurs excellents livres, en particulier 'Introduction à la théorie des nombres'.

- Mon courriel: mnevins@uottawa.ca

L'idée de Diffie et Hellman (1978)

Prenons p=11, et la base 2.

5

6

Je choisi: a=4
Donc 2^a = **5** (mod 11)

Je choisi: b=9
Donc 2^b = **6** (mod 11)

Anne calcule:
$2^{ab} = (2^b)^a = 6^a = 9 \pmod{11}$

Bertrand calcule:
$2^{ab} = (2^a)^b = 5^b = 9 \pmod{11}$

???

L'échange de clefs secrètes de Diffie et Hellman

- Anne et Bertrand choisissent un nombre p et une base n publiquement.
- Puis, chacun choisit une puissance (a et b, respectivement), qu'il garde secrète.
- Anne calcule n^a (mod p) et publie le résultat : A.
- Bertrand calcule n^b (mod p) et publie le résultat : B.
- De A et B, personne ne peut déduire a ou b.
- Par contre, puisque $B^a = A^b = n^{ab}$ (mod p), Anne et Bertrand peuvent calculer cette valeur commune, qui sera leur clef secrète!