Mathématiques au XXIè siècle : pourquoi ?

Depuis 80 ans, nos connaissances bâtissent de nouveaux mondes

Le CNRS

Le CNRS, 80 ans de sciences

Maths en France

Les mathématiques en France

- 3300 chercheurs et chercheuses permanents
- 1800 chercheurs et chercheuses non permanents

- Des personnels des universités ou du CNRS
- Dans des laboratoires en partenariat

- 43 laboratoires en France

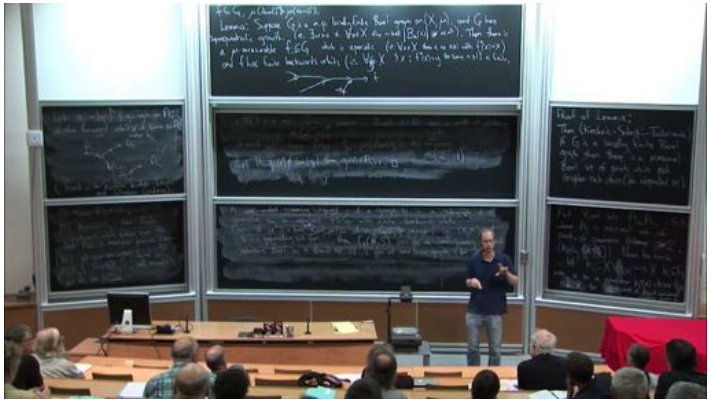
Les mathématiques en France

- 460 personnels d'accompagnement

- Des unités de soutien
  - Pour organiser des rencontres internationales ;
  - Pour diffuser les résultats ;
  - Pour collaborer avec les entreprises ;
  - Pour faire connaître les mathématiques

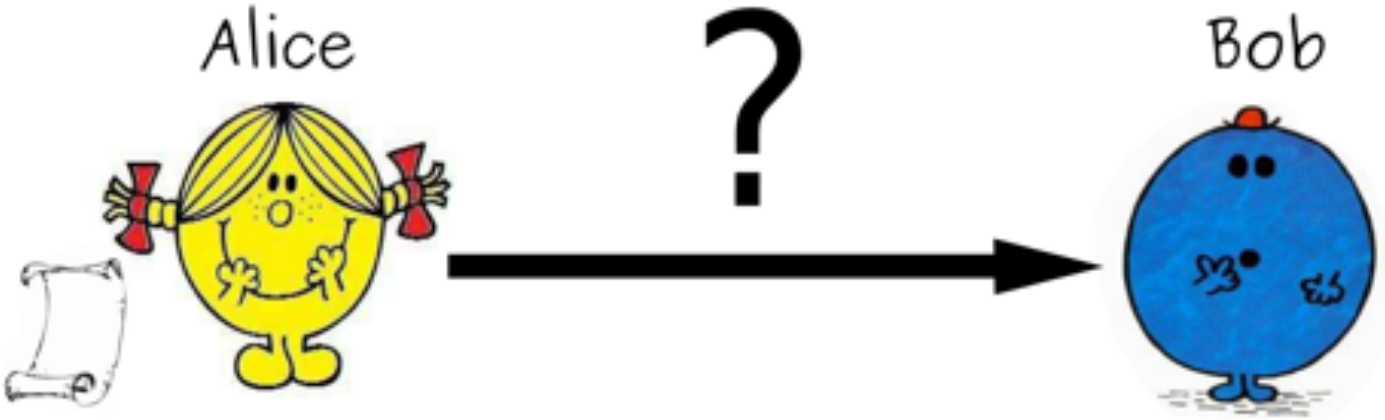
Les mathématiques en France

Un travail coopératif international



Un exemple : la cryptographie

La cryptographie



Cryptographie à clé secrète

- Chaque lettre de l'alphabet est remplacée par une autre
- Deux lettres différentes ne sont pas remplacées par des lettres identiques

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	R	Y	P	T	O	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

Cryptographie à clé secrète

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	R	Y	P	T	O	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

CE QUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT

YT LST G'JI YJIYJDQ RDTI N'TIJIYT YGCDMTHTIQ

Cryptographie à clé secrète

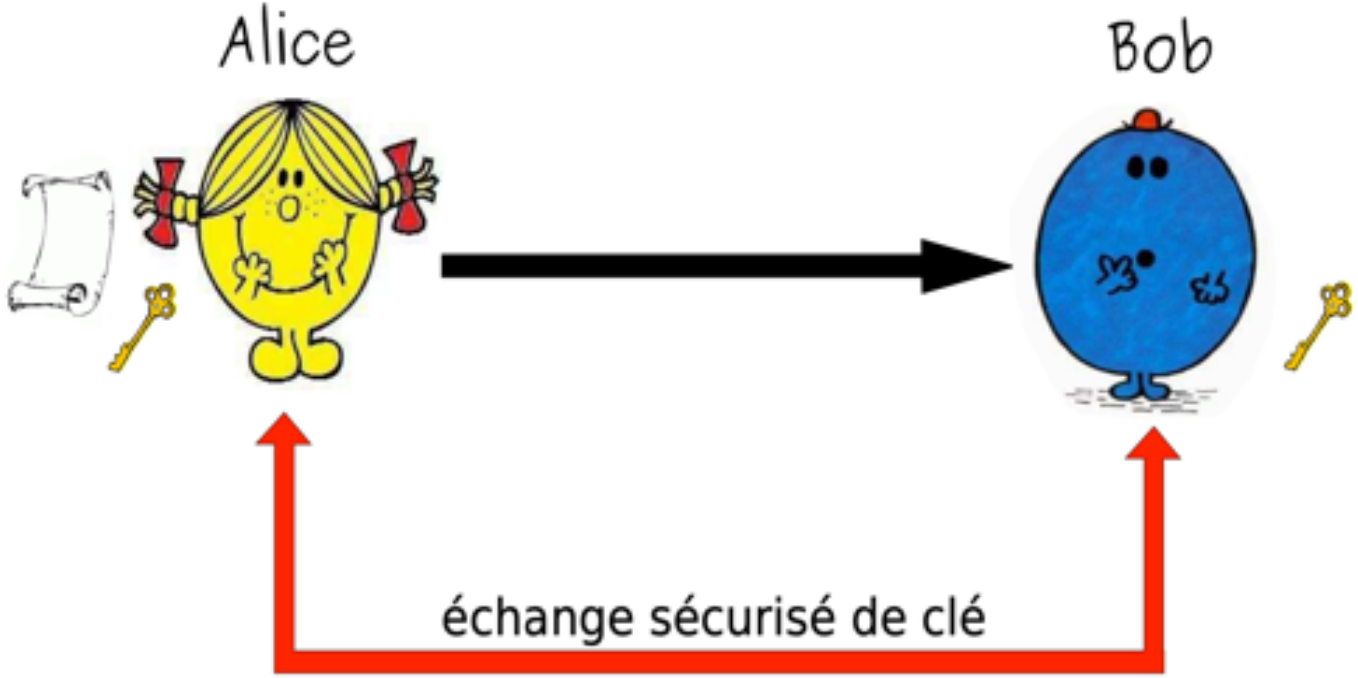
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	R	Y	P	T	O	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

YT LST G'JI YJIYJDQ RDTI N'TIJIYT YGCDMTHTIQ

CE QUE L'ON CONCOIT BIEN S'ENONCE CLAIREMENT

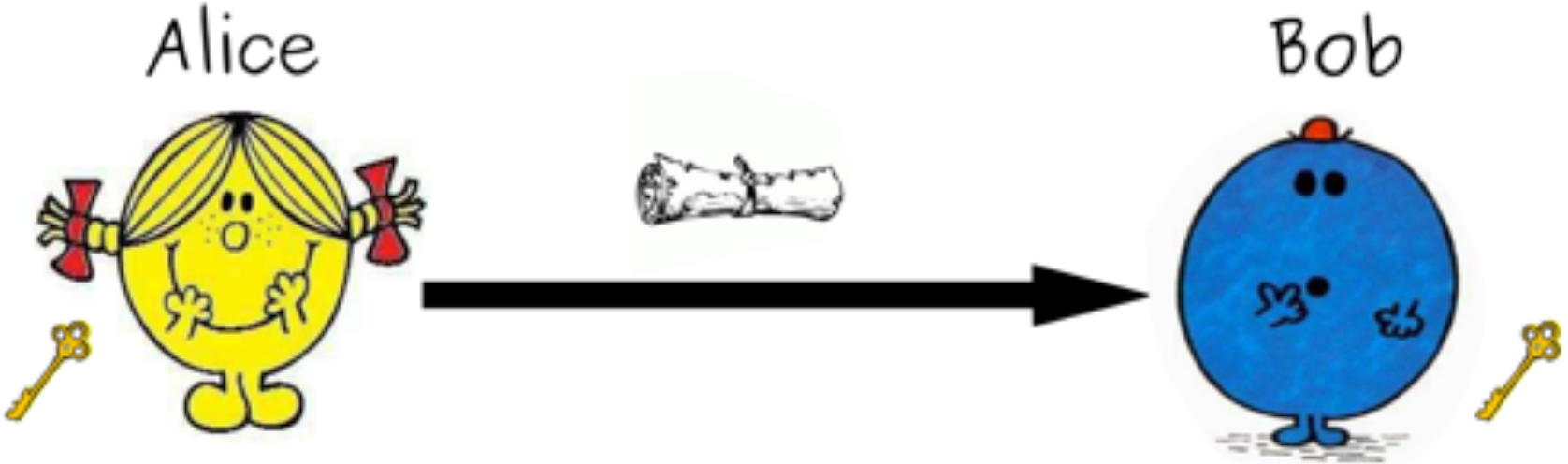
Cryptographie à clé secrète

- Alice et Bob échangent une *clé* de codage



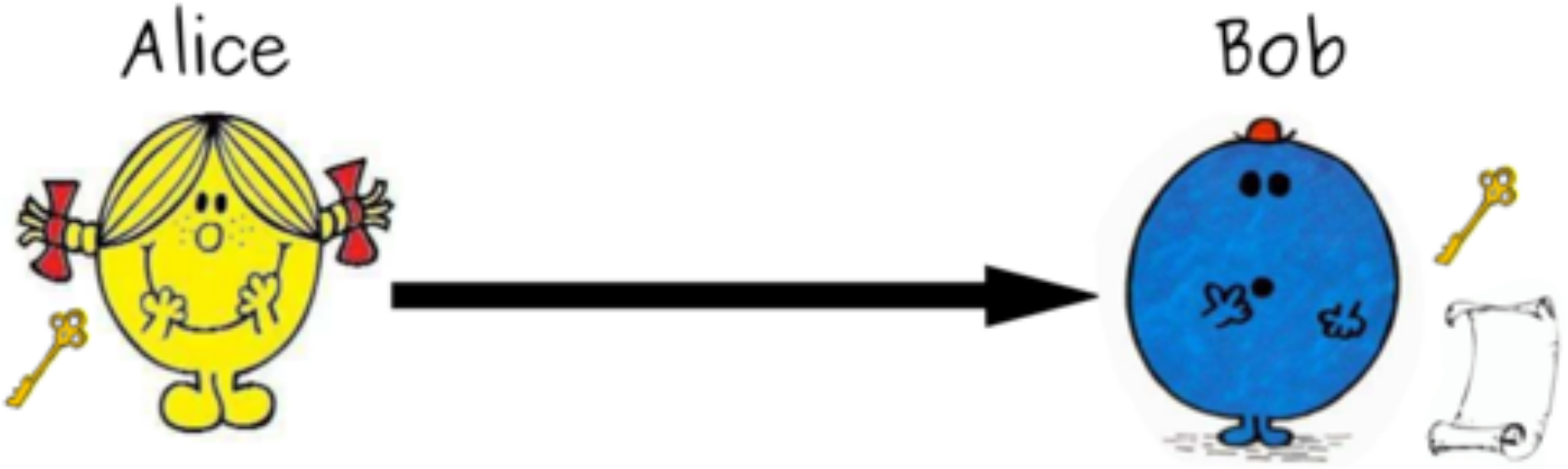
Cryptographie à clé secrète

- Alice *chiffre* son message et l'envoie à Bob



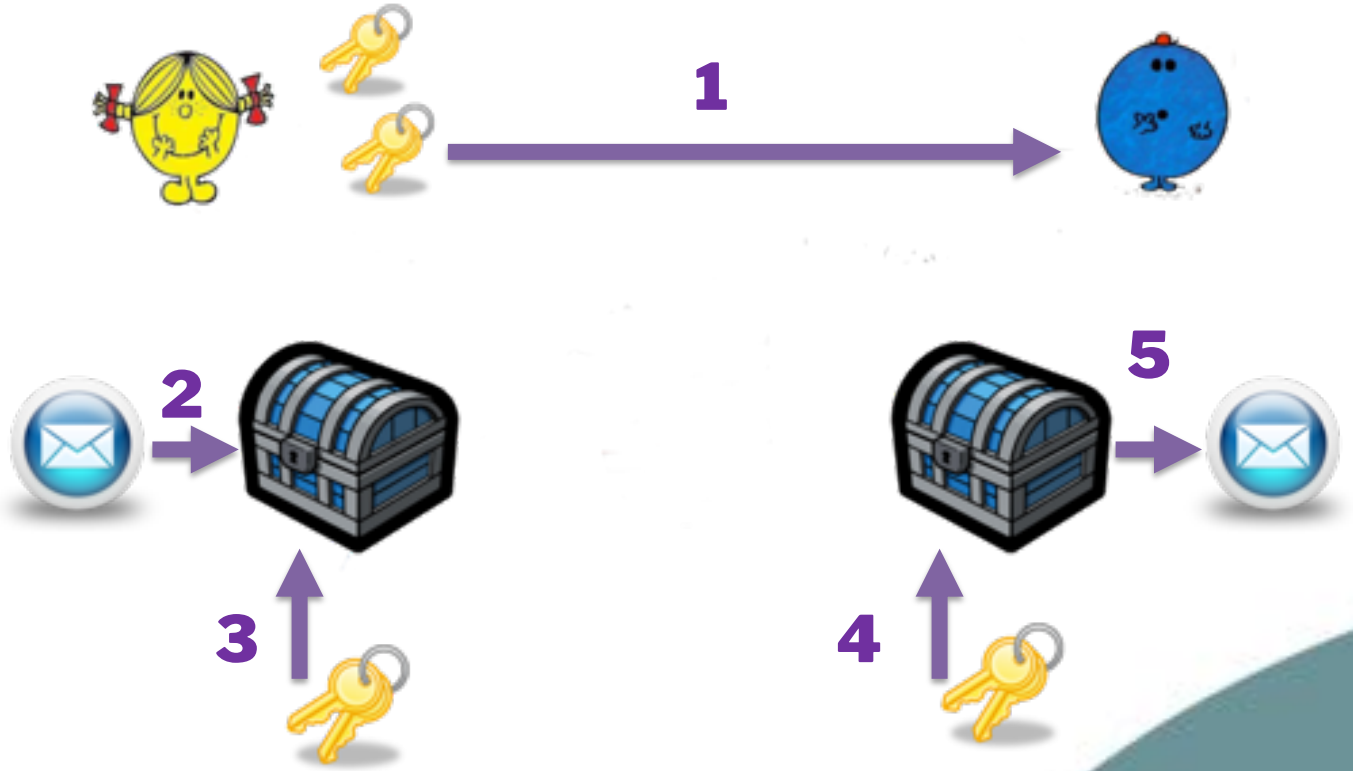
Cryptographie à clé secrète

- Bob dé*chiffre* son message



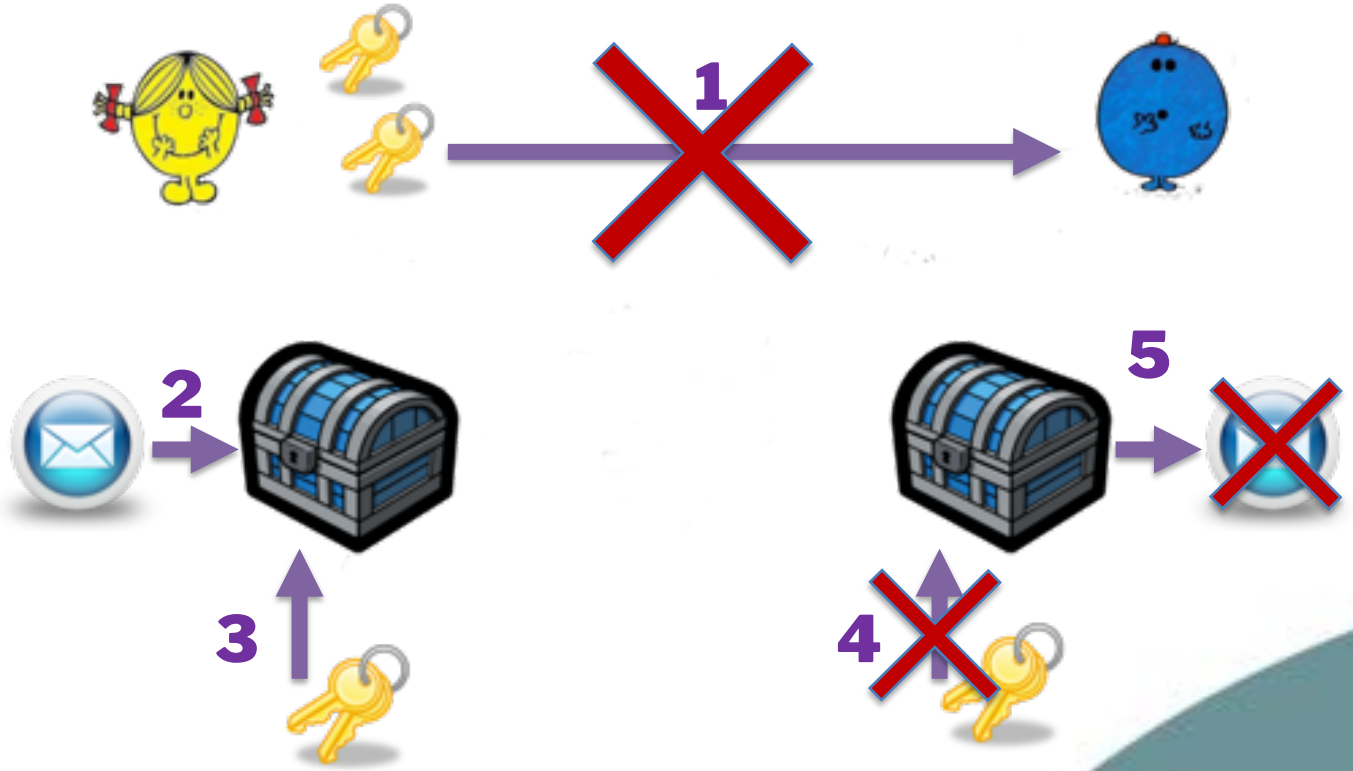
Cryptographie à clé secrète

- Une boîte à lettres, une clé pour tous



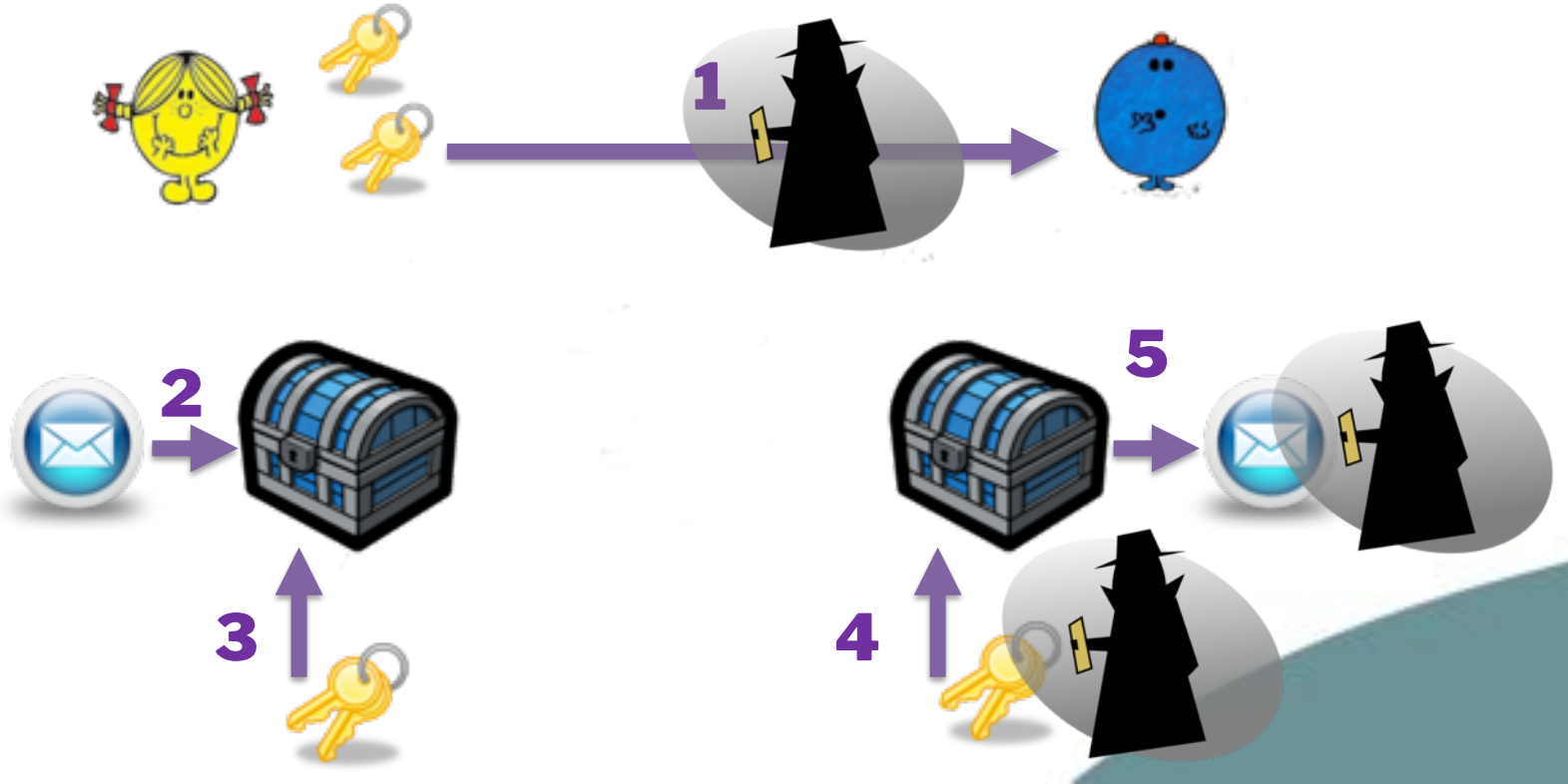
Cryptographie à clé secrète

- Et si Alice et Bob ne se rencontraient jamais



Cryptographie à clé secrète

- Et si un espion écoutait Alice et Bob ?



Cryptographie à clé publique

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

***Abstract*—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.**

Cryptographie à clé publique

- Bob dispose de deux méthodes
  - Une de chiffrement *C*
  - Une de déchiffrement *D*
- Chiffrer puis déchiffrer un texte clair, c'est ne rien faire

$$D\big(C(texte)\big) = texte$$

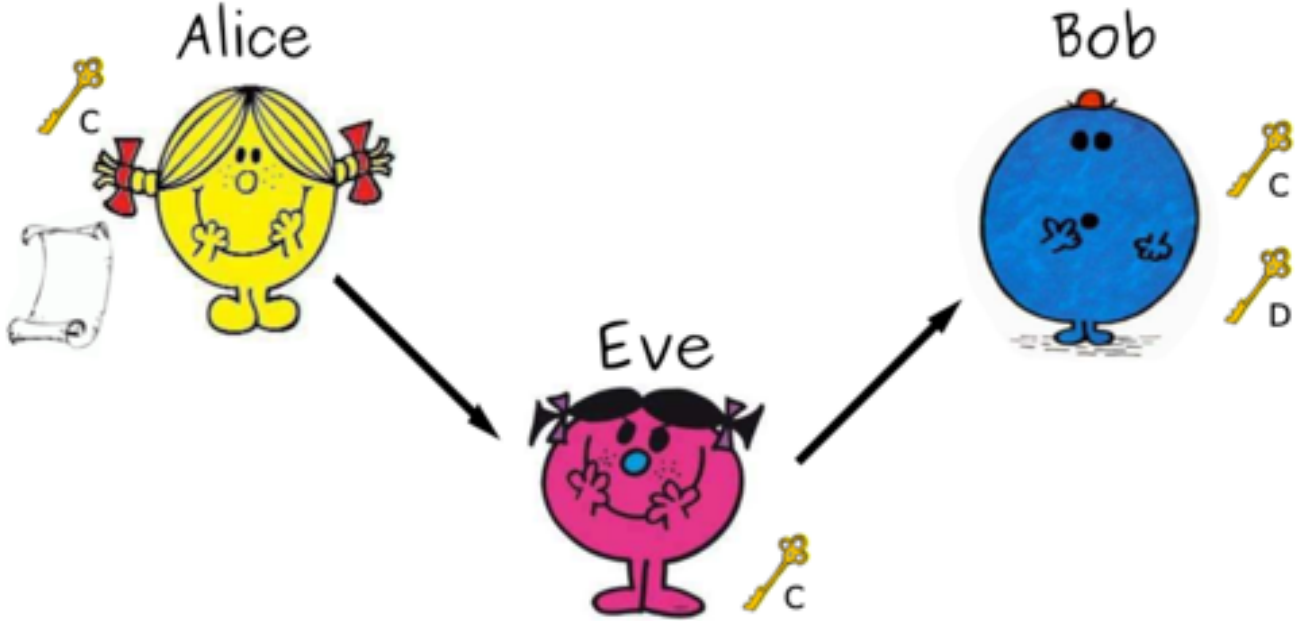
- Déchiffrer puis chiffrer un secret, c'est ne rien faire

$$C\big(D(secret)\big) = secret$$

- Bob rend la méthode de chiffrement publique mais garde secrète la méthode de déchiffrement
- Chiffrer et déchiffrer sont faciles mais savoir chiffrer n'aide pas à savoir déchiffrer.

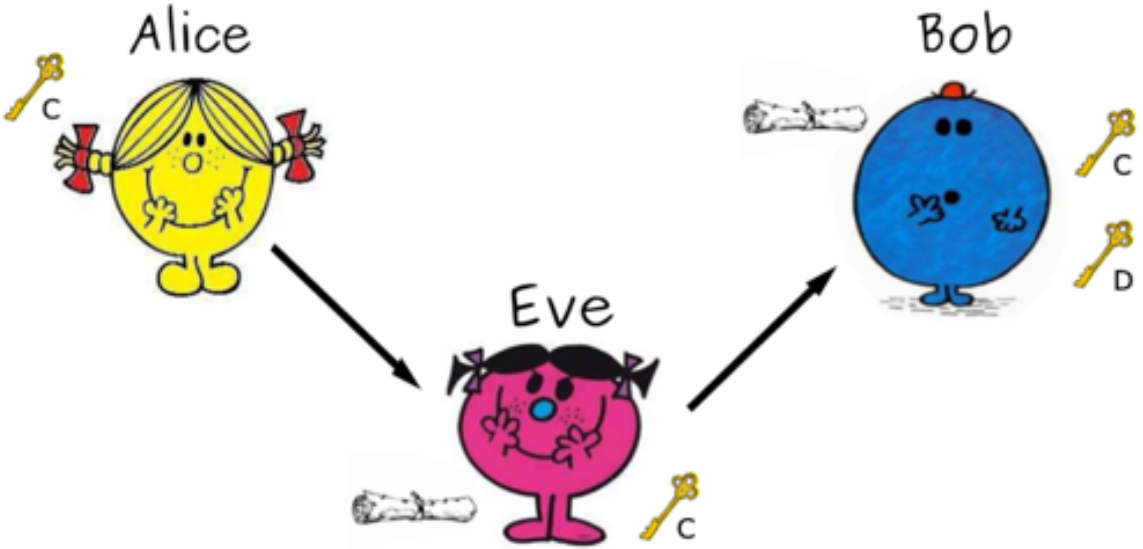
Cryptographie à clé publique

- Bob rend publique sa méthode de chiffrement



Cryptographie à clé publique

- Alice utilise cette méthode pour transformer son texte en secret

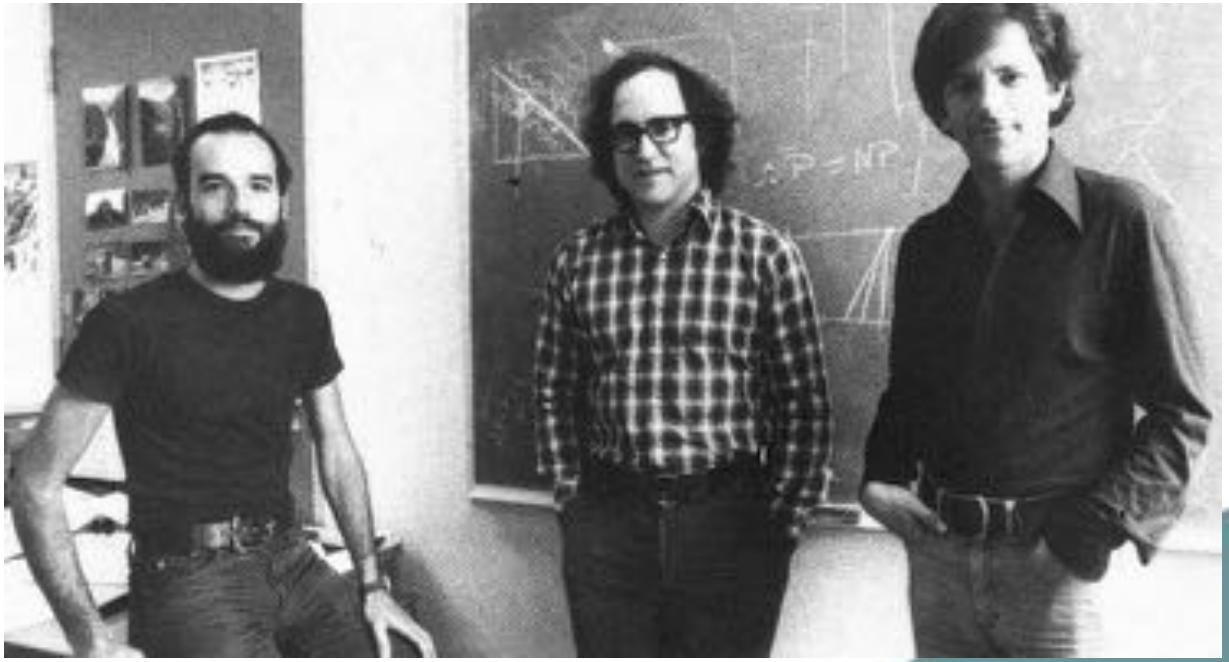


Cryptographie à clé publique

- Bob utilise la méthode de déchiffrement que lui seul connaît pour lire le secret

Cryptographie à clé publique

- En pratique, la première méthode est due à Rivest, Shamir & Adleman en 1977



Cryptographie à clé publique

- En secret
  - Construire deux nombres premiers p et q,
  - Calculer le produit n,
  - Calculer $\varphi = (p-1)(q-1)$,
  - Construire $e < \varphi$ premier avec n,
  - Calculer l'inverse d de e modulo φ ;
- Divulguer n et e ;
- Chiffrer $M \longmapsto M^e \pmod{n}$;
- Déchiffrer $M \longmapsto M^d \pmod{n}$.

Cryptographie à clé publique

- On connaît p et q, il est facile de calculer φ et d ;
- On ne connaît que n et e, il est difficile de calculer φ.

- Raison : on ne sait pas factoriser rapidement
- Inquiétude : est-ce vraiment impossible ?

Cryptographie à clé publique

- La méthode RSA, datant de 1977, toujours utilisée repose sur les découvertes de

Pierre de Fermat
Début XVII^{è} - 1665

Leonhard Euler
1707- 1783

Carl Friedrich Gauss
1777- 1855

Cryptographie à clé publique

- Petit théorème de Fermat (1640 : énoncé, 1741 : preuve)

Tout nombre premier mesure infailliblement une des puissances − 1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné − 1

$$\forall p \in \mathcal{P}\ \forall a \in \mathbb{Z} \quad p \nmid a \Longrightarrow a^{p-1} \equiv 1 (\mathrm{mod}\, p)$$

Cryptographie à clé publique

- Il existe d'autres méthodes de chiffrage et déchiffrage
- Elles reposent sur la notion de groupe, notion qui généralisent et place dans un cadre abstrait la notion d'addition d'entiers

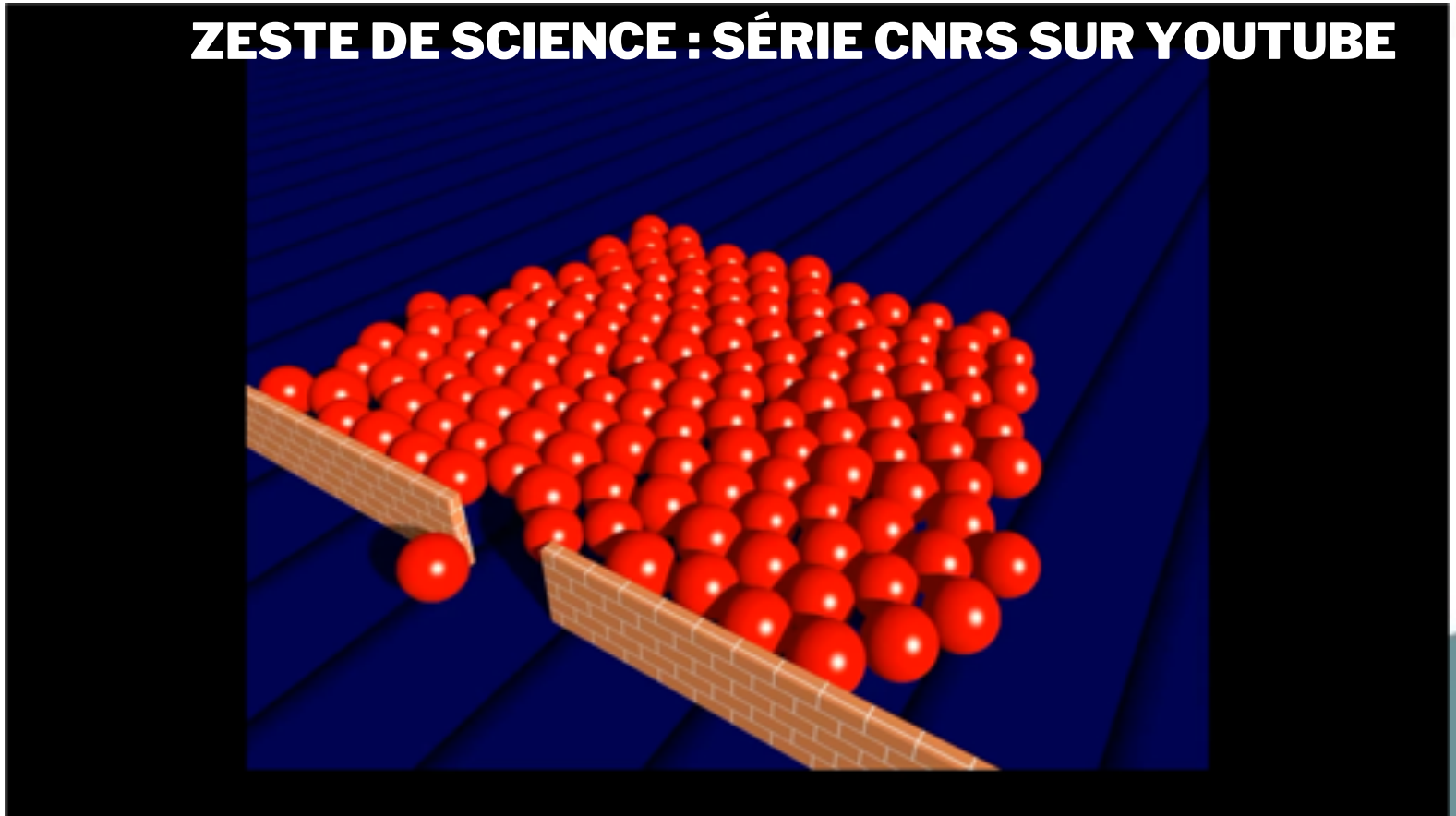
DÉFINITION 6. — *Soient* E *un magma unifère,* $\top$ *sa loi de composition, e son élément neutre, x et x′ deux éléments de* E. *On dit que x′ est* inverse à gauche (resp. inverse à droite, resp. inverse) *de x si l'on a* $x' \top x = e$ (resp. $x \top x' = e$, resp. $x' \top x = x \top x' = e$).

On dit qu'un élément x de E *est* inversible à gauche (resp. inversible à droite, resp. inversible) *s'il possède un inverse à gauche* (resp. *inverse à droite*, resp. *inverse*).

Un monoïde dont tous les éléments sont inversibles s'appelle un groupe.

D’autres exemples

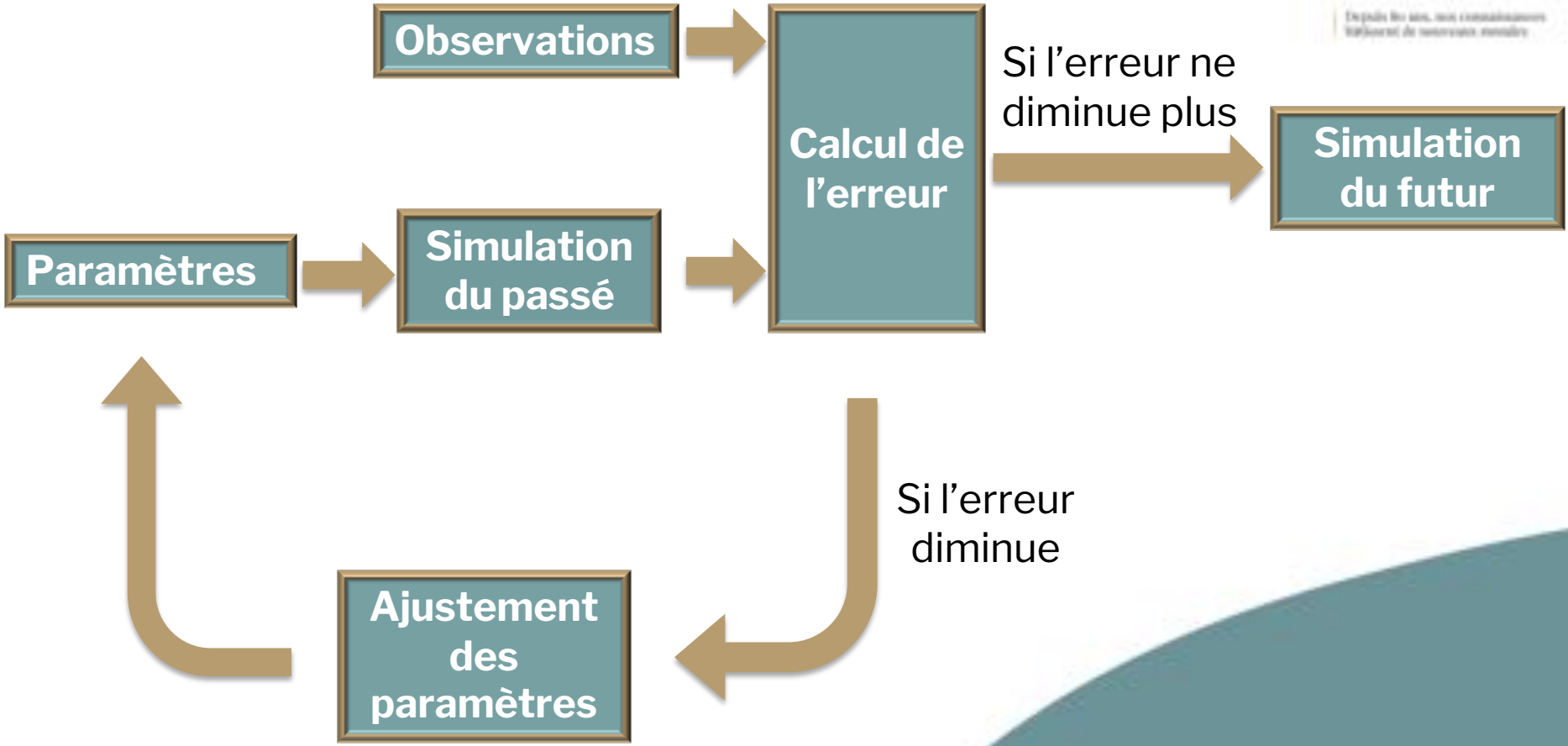
Déplacement de foules



Amélioration d'images

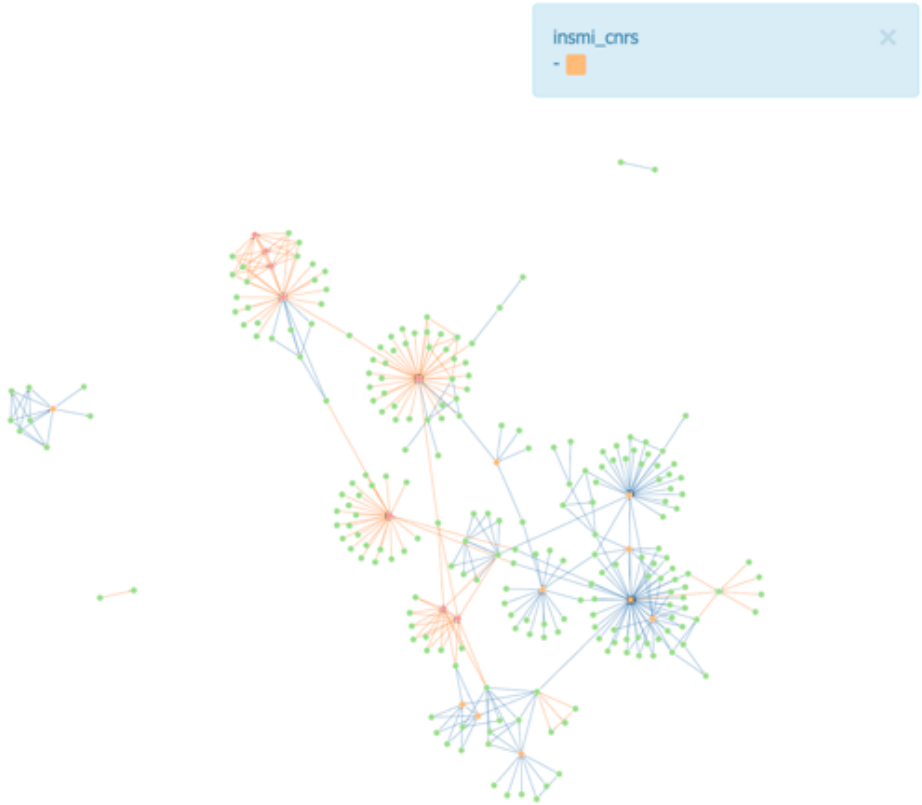
Julie DELON – 5 minutes Lebesgue

Prévision météorologique



Simulation des évolutions d'incendie

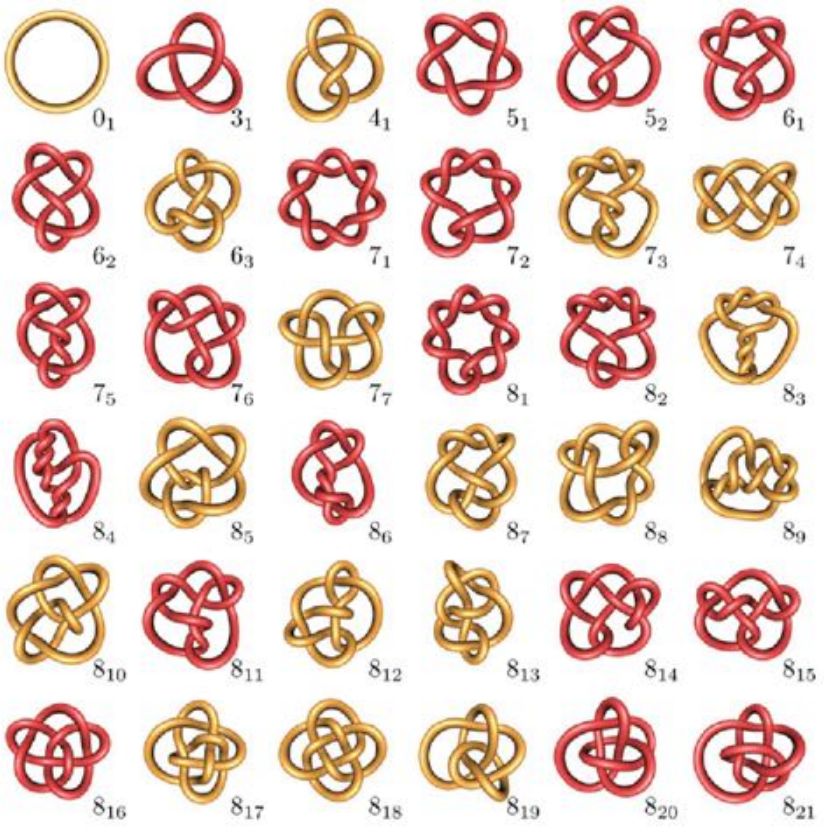
Internet : étude des relations

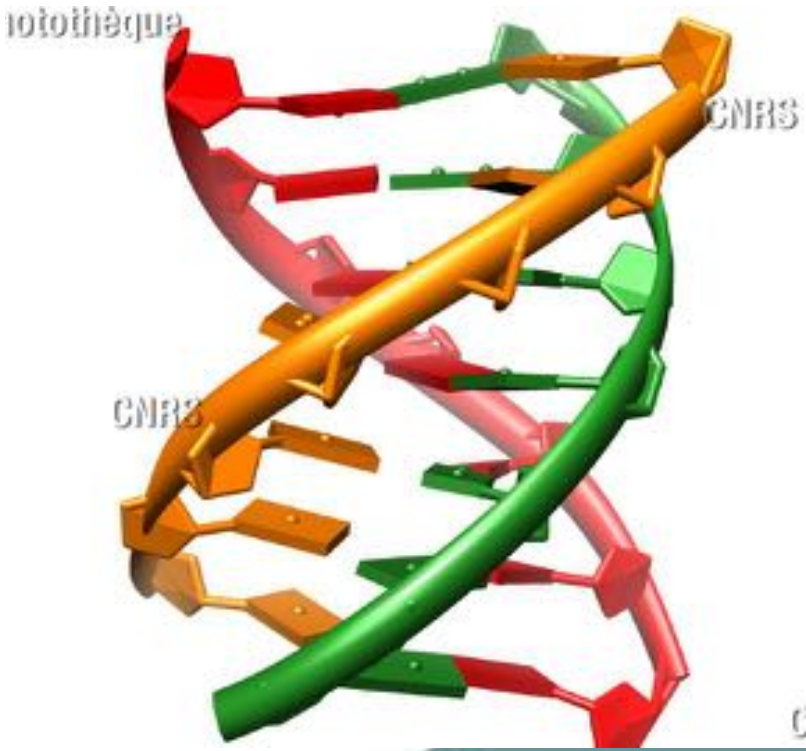


Exemple : Tweets #Maths2020 avec Linkage

Effacement du bruit

ADN et topologie

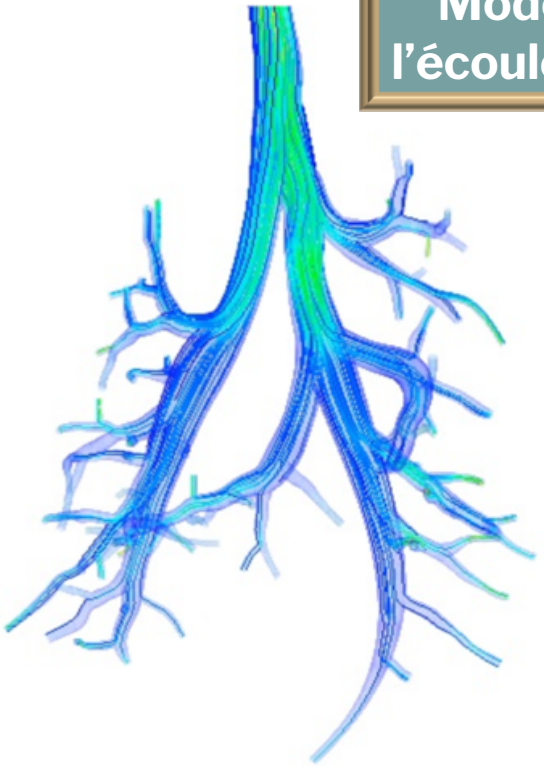




Optimiser une flotte

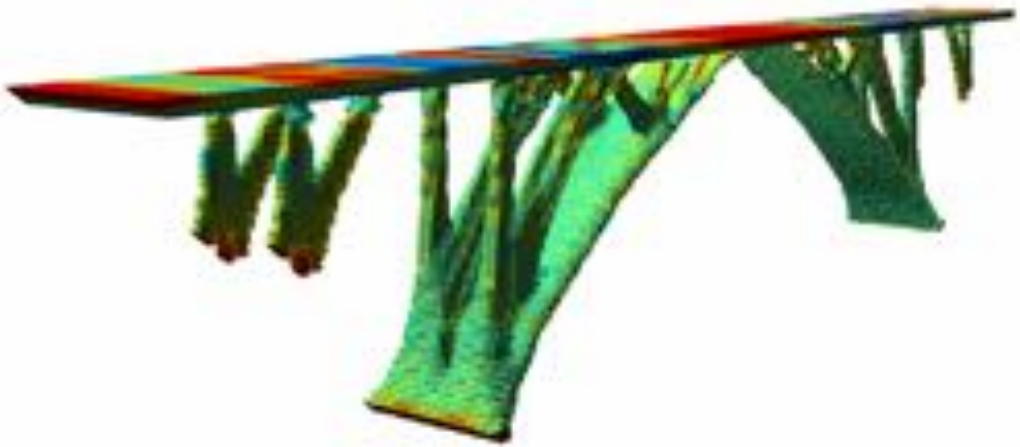
Modélisation du poumon

Modélisation de l'écoulement de l'air



Dépôt d'aérosol

Optimisation de formes



En conclusion...

Les mathématiques sont partout !