Les courbes en cryptographie

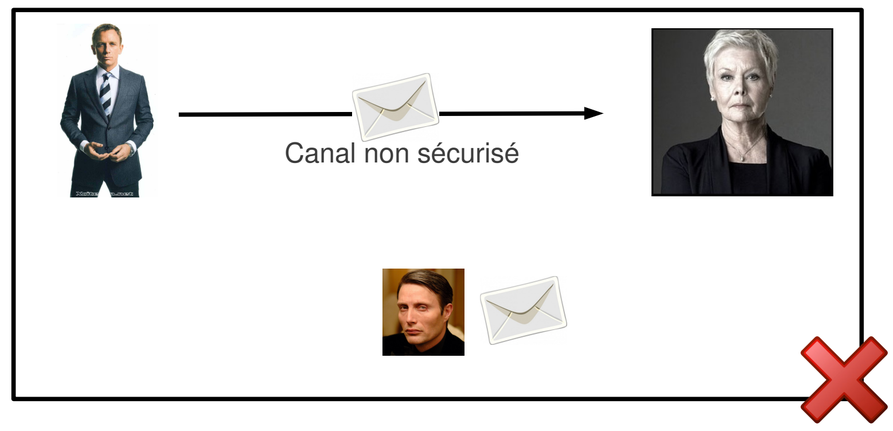
Cécile Gonçalves

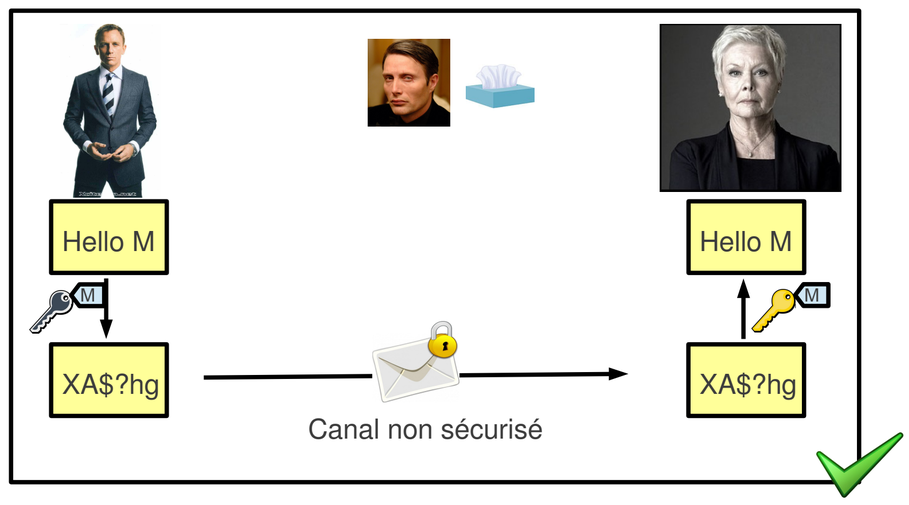
La cryptographie permet d'établir une communication secrète

La cryptographie permet d'assurer

- **La confidentialité des donnés :** seul le destinataire est capable de lire le message. Si un espion écoute la communication, alors il ne pourra pas retrouver le message d'origine.
- **L'authentification :** le destinataire a la garantie de l'identité de l'émetteur du message. Ainsi, un espion qui écoute la communication ne peut pas se faire passer pour l'émetteur du message.
- **L'intégrité des données :** le destinataire a la garantie que les données n'ont pas été modifiées. Ainsi, un espion qui écoute la communication ne peut pas substituer le message.

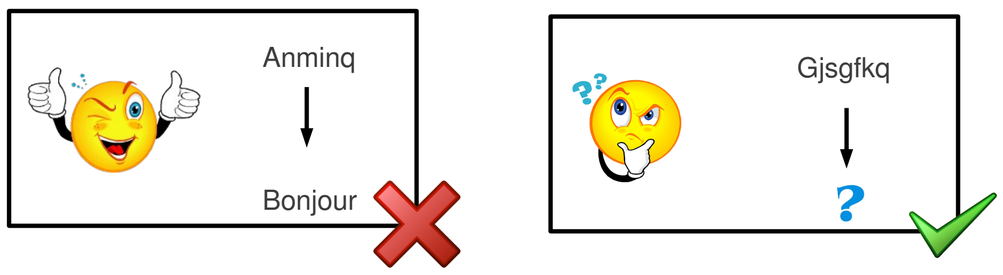
La **confidentialité** est assurée par le **chiffrement** des données.





La sécurité dépend du choix des paramètres du cryptosystème

La sécurité du système de chiffrement est assurée lorsqu'un espion ne peut pas retrouver le message d'origine m à partir du message chiffré c.



Les courbes fournissent de bons candidats pour le chiffrement

- Elles sont **compactes** : elles fournissent de plus petites clés
- Elles sont **efficaces** : le chiffrement et le déchiffrement peuvent s'effectuer rapidement.
- Elles sont **sûres** : les meilleures attaques connues sur une courbe aléatoire sont les attaques génériques, qui sont exponentielles (mois, voire années).

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 1: NIST Recommended Key Sizes

Le comptage de points permet d'assurer la sécurité du cryptosystème

Avant d'utiliser une courbe dans un cryptosystème, il faut s'assurer qu'elle soit **sûre**. Pour cela, il faut savoir **compter les points** sur les courbes.

Si l'on identifie le chiffrement à l'éclairage, alors les cryptosystèmes correspondent aux ampoules. Le cryptosystème que j'étudie correspond à un modèle d'ampoule et les courbes sont équivalentes à une ampoule d'excellente qualité parmi les ampoules de ce modèle (durée de vie, économie d'énergie, …).

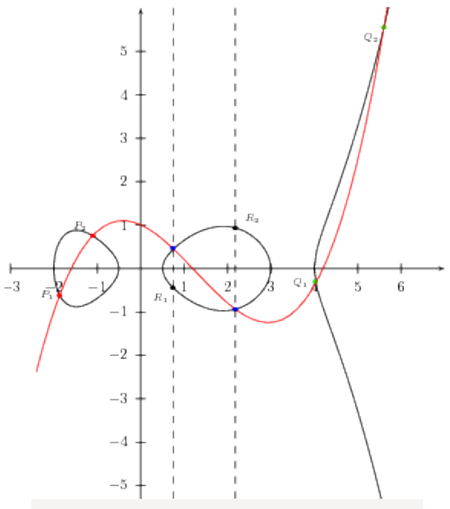
Le comptage de points permet de déterminer la puissance d'une ampoule donnée.

20W - 40W - 60W

Conception d'algorithmes de comptage de points efficaces

Il est facile de compter les points en énumérant les points rationnels sur la courbe. Le problème de cette technique est qu'elle est exponentielle en temps (résultats en mois, voire années).
Mes travaux de thèse consistent à concevoir des algorithmes efficaces (résultat en secondes).

Une manière plus efficace de compter les points consiste à **utiliser la géométrie de la courbe** ou bien des particularités comme certains endomorphismes explicites.
Cela se traduit par des particularités sur la cohomologie de la courbe et permet d'avoir un algorithme en temps **polynomial**.



$$y^2 = x^5 + ax^4 + bx^3 + cx^2 + dx + e$$