Courbes elliptiques et Cryptographie

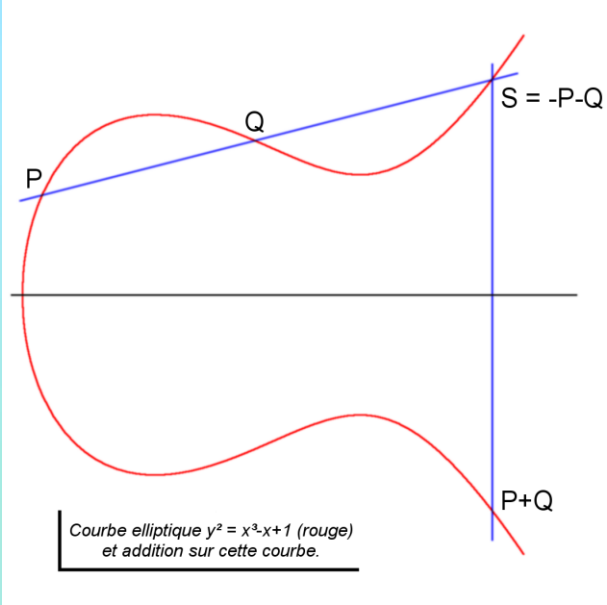
La cryptographie existe depuis des centaines d'années, des messages étaient déjà codés durant l'Antiquité. Les besoins sont aujourd'hui très nombreux (sécurité de paiement, protection des sites internet…) et les techniques de cryptanalyse (pour "casser" les codes) progressent également très vite avec l'augmentation de la puissance informatique.

Le chiffrement asymétrique a été proposé par Diffie et Hellman en 1976. Il repose sur l'utilisation de deux clés (contrairement au chiffrement symétrique) : une clé publique pour coder les messages et une secrète pour les déchiffrer. Nous allons ici nous intéresser à un système qui utilise les courbes elliptiques projectives.

On appelle courbe elliptique sur R toute courbe plane d'équation $y^2=x^3+ax+b$ (forme simplifiée).
Les mathématiciens ont défini la somme de deux points de cette courbe. Voici sa construction géométrique.

On prouve que la courbe possède un seul point à l'infini (dans le sens vertical). On note ce point 0.
La qualité essentielle d'une courbe elliptique est que la somme de trois points alignés est toujours 0.

Soient P, Q deux points de la courbe.
La droite (PQ) coupe la courbe en un 3ème point S (qui est éventuellement le point à l'infini 0).
Ainsi P, Q et S sont alignés donc P+Q+S=0, ie S = -P-Q.
Enfin, le point P+Q est le symétrique de S par rapport à l'axe des abscisses (0, S et P+Q sont alignés).



Courbe elliptique $y^2 = x^3-x+1$ (rouge) et addition sur cette courbe.

En cryptographie, on ne travaille pas dans le corps des réels mais sur des corps finis.


Mélina et Nikola choisissent publiquement une courbe elliptique et un point *P* sur la courbe.

Mélina veut envoyer secrètement à Nikola un point *M* de la courbe (correspondant à une partie du message).

Chacun de leur côté, ils vont choisir secrètement un entier : *m* (pour Mélina) et *n* (pour Nikola).

Nikola va alors envoyer le point *nP* (=*P*+*P*+….+*P*, *n* fois) de la courbe elliptique à Mélina.

Elle calcule les points *mP* et *M*+*mnP* et elle les transmet à Nikola.

A l'aide de sa clé secrète *n*, Nikola est le seul à pouvoir trouver le point *nmP*=*mnP* à partir de *mP*.
Pour retrouver le point *M* communiqué par Mélina, il lui suffit ainsi de calculer (*M* + *mnP*) – *nmP*.

Si un espion veut déchiffrer le message, il devra, pour retrouver n, effectuer la "division" de nP par P, mais une telle division n'existe pas ! C'est le problème du calcul du logarithme discret de base P.

Conception graphique : étudiants de L3 maths, LMA Poitiers, promotion 2013-2014