INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES ROUEN

Projet : Cryptage sur courbes elliptiques

Auteurs :
Hamza Fadili
Joachim Curtelin
Reda Bouzid

Enseignant :
Alexandrina Rogozan

Table des matières

1 Introduction

Le cryptage existe déjà depuis les années 90
La plupart des algorithmes de cryptage sur courbes elliptiques sont brevetés par Certicom, ce qui limite la cryptanalyse et l'étude

2 Bibliographie

2.1 Courbes elliptiques

Une courbe elliptique est l'ensemble

$$E = \{(x, y) \in \mathbb{R} | y^2 = x^3 + ax + b\}$$

avec a,b réels tels que $4a^3 + 27b^2 \neq 0$
- La courbe est symétrique avec l'axe des abscisse (selon x)
- La condition sur a,b est le discriminant de l'équation du troisième degré
- Presque toute les droites coupant par deux points la courbe passent par un troisième point (sauf droite à x constant)

![[exempleCourbe.png]] Exemple ici avec a=-3, b=1

On a besoin d'une loi de composition interne, notée + ($E \times E \to E$), pour former un groupe $(E, +)$

Rappel de la définition d'un groupe :
- la loi est associative : pour tout a,b,c de E, a+(b+c) = (a+b)+c
- E possède un élément neutre
- Les éléments de E possède un inverse dans E pour + (il existe un élément y dans E tel que x+y vaut l'élément neutre)

On définit + tel que, pour tout point P,Q de E
- Si P et Q sont symétriques, ils sont symétriques selon l'axe des abscisses, on a $(x_q, y_q) = (x_p, -y_p)$, alors $P + Q = N_e$, point neutre , on note $P = -Q$
- En général : La droite formée par P et Q coupe la courbe en un troisième point R, on a $P + Q = -R$
- Si P = Q, la droite est la tangente de la courbe en P, on note $P + P = 2P$

Difficulté du problème : Pour tout entier naturel n, calculer $S = nP$ est facile, mais retrouver n avec S et P est très difficile

2.2 Application au cryptage

On (Bob) choisit une clé privée n et un point P.
La clé publique est :
- $Q = nP$
- P
- la courbe (donc a et b)

Alice veut envoyer un message M. Elle choisit k entier > 1, et envoie à Bob les deux points kP et $M + kQ$

Bob connait n donc retrouve $M = (M + kQ) - nkP$

Le cryptage sur courbe elliptiques est un cryptage asymétrique : il y a une clé privée et une clé publique : Trouver la clé privée est difficile, vérifier la clé est facile. En théorie, on découpe le message à chiffrer en petits blocs qui sont chacun chiffré. En pratique on utilise le cryptage asymétrique pour chiffrer la clé d'un cryptage symétrique comme AES.

3 Algorithmes

3.1 Elliptic Curve Diffie-Hellman

3.2 ECDSA

4 Cryptanalyse

5 Conclusion