N° d'ordre :
N° de série :

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Superieur et de la Recherche Scientifique

UNIVERSITÉ ECHAHID HAMMA LAKHDAR EL OUED

FACULTÉ DES SCIENCES ET DE TECHNOLOGIE

Mémoire de fin d'étude

LICENCE ACADEMIQUE

Domaine: Mathématiques et Informatique
Filière: Mathématiques
Spécialité: Modélisation mathématiques & simulation numérique

Thème

Algèbre et Cryptographie

Sous la supervision de :
YOUMBAI Mouhamed Amine

Présenté par:
HAMIDATOU Kenza
GUEDDA Manel
LEGHDEMSI Rahil

Année universitaire 2014 – 2015

Remerciement

La louange est à Allah, qui nous a facilité l'accomplissement de ce travail de recherche chose ne peut étre qu'avec la volonté de Dieu -à lui la tout puissance et la Majesté- et que la louange initiale et finale appartieut à allah,Seigneur des mondes

*Aussi,il nous fait plaiser que nous,au commencement de ce travail,présentons nos grands remerciments,éstimations et reconnaissances à notre encadreur puissant " **YOUMBAI Mohamed Amine** " de nous avoir encourager moralement la durée de recherche et que ce travail est le fruit de ces encouragement*

Nous présentons nos veridiques remerciments à tout personne,du proche ou du loin ,qui nous adonné un coup de main,à fin de términer ce travail de recherche

En fin, nous remercions vivement notres familles pour l'aide matérielle et morale durant la période de préparation

Table des matières

Introduction Générale

La moitié de ce siècle est celle de la révolution numérique et de l'utilisation systématique de l'algèbre dans la transmission de données. L'information est précieuse lors de son stockage ou sa transmission, il est nécessaire de la protéger. Deux grands types de protection se distinguent: La protection contre les ennemis malicieux et la protection contre les altérations dues à des problèmes physiques (canaux bruitées). La théorie des codes correcteurs d'erreurs et la cryptologie sont les domaines de recherche associés à ces problématiques. La cryptologie, qui nous intéresse plus particulièrement ici, se divise en deux disciplines complémentaires et indissociables: la cryptographie : la conception de systèmes de protection et la cryptanalyse : l´étude des attaques des systèmes connus. Dans ce mémoire nous nous intéressons à la conception de quelque cryptosystèmes et l'étude de leurs sécurité élémentaire. Les systèmes ordinaires, les systèmes à base de courbes algébriques. Dans ce cadre la sécurité est liée au problème du logarithme discret dans des groupes ordinaires ou des groupes liés aux courbes.

0.1

Chiffrer: transcrire, à l'aide d'un algorithme un message clair en une suite incompréhensible de symboles.

texte en clair: le message à chiffrer.

texte chiffré: le résultat du chiffrement.

Déchiffrer: retrouver le texte en clair à partir du texte chiffréàl'aide d'un algorithme paramétrable.

cl: le paramètre des algorithmes de chiffrement et de déchiffrement.

Décrypter: retrouver le texte en clair à partir du texte chiffré sans la clé.

Cryptographie: science du chiffrement.

Cryptanalyse: science du décryptage.

Cryptologie: cryptographie et cryptanalyse.

Cryptosystème: ensemble des méthodes de chiffrement et de déchiffrement utilisables en sécurité.

Chapitre 1

Notions Fondamentales d'Algèbre

Dans ce chapitre on va acquérir les notions fondamentales utilisées dans les cryptosystémes, à partir des notions de groupes, corps, courbes algébriques plans.....

1.1 Structures algèbriques fondamentales

1.1.1 Goupes, Groupes cycliques

Définition 1.1.1 *un groupe est un couple formé d un ensemble G et d une loi de composition (x,y) → xy sur l ensemble G ces données d oivent vérifier les trois condition :*

$\forall x, y, z \in G : (xy)z = x(yz)(associativité)$;
$\exists 1 \in G$ telque $\forall x \in G$:
x1=1x=x (existance d un élement neutre)
$\forall x \in G, \exists x^{-1} \in G$ tel que
$x^{-1}x = xx^{-1} = 1$
(existance d un élément inverse pour tout élé,ent du groupe).
si la loi de groupe est commutative, le groupe est appélé groupe commutatif .

Définition 1.1.2 ***Notation 1.1.1*** *Les notations les plus utilisées sont : la notation additive avec* 0 *pour élément neutre,* $-x$ *pour le symétrique (dit aussi opposé) et la notation multiplicative où l'élément neutre est noté* 1, x^{-1}*pour le symétrique (dit aussi inverse).*

Exemple 1.1.1 (i) $\mathbb{Z}, \mathbb{R}$ *et* $\mathbb{Q}$*: sont des groupes additives commutatif*

(ii) $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe multiplicatif commutatif.
avec $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, 3, \ldots, (p-1)\}$, p : premier.

Définition 1.1.3 *Soit G un groupe fini. L 'ordre d'un groupe est son cardinal et on le note $|G|$ ou $O(G)$ ou $card(G)$.*

Définition 1.1.4 *Soit G un groupe fini et soit g un élément de G. L'ordre de g est l'ordre du groupe engendré par g.*

Définition 1.1.5 *On dit qu'un groupe G est monogéne s'il est engendré par un seul élément g et qu'il est cyclique si en plus il est fini.*

$$\begin{aligned} G &= < g >= \{g^0, g^1, g^2, \ldots\} \rightarrow monogéne \\ G &= < g >= \{g^0, g^1, g^2, \ldots, g^p\} \rightarrow cyclique \end{aligned}$$

Exemple 1.1.2 $((\mathbb{Z}/7\mathbb{Z})^*, .)$*est un groupe cyclique.*

$(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6\}; card((\mathbb{Z}/7\mathbb{Z})^*) = 6.$
$(\mathbb{Z}/7\mathbb{Z})^* = \langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\};$
3 est un générateur du groupe $((\mathbb{Z}/7\mathbb{Z})^*, .)$.

Théorème 1.1.1 *L 'ordre d'un élément d'un groupe fini divise l'ordre de G.*

Définition 1.1.6 *soint $(G.*), (H.\top)$deux groupes et f une application de G dans H. On dit que f est un morphisme de groupes, si :*

$$\forall a, b \in G; f(a * b) = f(a) \top f(b)$$

Si en plus f est bijective, on dit que f est un isomorphisme, si de plus $G = H$, on parle d'endomorphisme et d'automorphisme.

1.1.2 Anneaux, corps, corps finis

Définition 1.1.7 *Un anneau est un triplet $(A, +, .)$ où A est un ensemble, $+$ et $\cdot$ deux lois de composition interne tels que:*

$(A, +)$ soit un groupe commutatif, la loi $\cdot$ une loi associative, possédant un élément neutre noté 1 et distributive par rapport à la loi $+$.

Si de plus la loi $\cdot$ est commutative, on parle d'anneau commutatif.

Définition 1.1.8 *$K = (A, +, .)$ est un corps ssi :*

(i) $K = (A, +, .)$ est un anneau.

(ii) Chaque élément non nul de A possède un inverse pour l'opération $(\cdot)$.

$\star$ Si $a, b \in A$, alors: $a(-b) = (-a)b = -ab$ et $a.0 = 0.a = 0$.

Définition 1.1.9 *Un corps fini est un corps qui possède un nombre fini q d'éléments, et on le note par $\mathbb{F}_q$*

Définition 1.1.10 *Soient G, H deux anneaux et f une application de G dans H. On dit que f est un morphisme d'anneaux, si :*

$$\forall a, b \in G; f(a+b) = f(a) + f(b) et f(a.b) = f(a).f(b).$$

Proposition 1.1.1 *Deux corps finis ayant le même nombred 'éléments sont isomorphes.*

Théorème 1.1.2 (Wedderburn) *Tout corps fini est commutatif.*

La cardinalité d'un corps fini $\mathbb{F}_q$ est une puissance d'un nombre premier c-à-d: $q = p^m$ avec p est premier et $m > 0$.

Exemple 1.1.3 *Corps binaire $\mathbb{F}_2$.*

$\mathbb{F}_2 = \{0, 1\}$ est le corps binaire ; c'est le plus petit corps fini.

Exemple 1.1.4 *Corps binaire $\mathbb{F}_8$*

$\mathbb{F}_8$ $(8 = 2^3; p = 2$ et $m = 3)$. est de caractéristique 2,donc $\mathbb{F}_8$ est construit comme extension du corps premier $\mathbb{Z}/2\mathbb{Z}$. Soit le polynôme: $f(x) = x^3 + x + 1$; ce polynôme

est irréductible sur $\mathbb{F}_2$*,* $f(x)$ *est une cubique qui n'a pas de zéro dans* $\mathbb{F}_2$*, car* $f(0) = 1$ *et* $f(1) = 1$*.Comme* $f(x)$ *est de degré 3 sur* $\mathbb{F}_2$*, les éléments de* $\mathbb{F}_8$*sont de la forme:* ax^2+bx+c *avec* a, b, c *des éléments de* $\mathbb{F}_2$*.Donc :* $x^3 + x + 1 = 0 \mod(x^3 + x + 1)$*; Alors:* $x^3 = x + 1 \mod(x^3 + x + 1)$*; Et par conséquent :* $x^4 = x^2 + x \mod(x^3 + x + 1)$.

Calculons les puissances sucessives de X :

$$\begin{aligned} X^0 &= 1 \\ X^1 &= X \\ X^2 &= X^2 \\ X^3 &= X + 1 \\ X^4 &= X^2 + X \\ X^5 &= X^3 + X^2 = X^2 + X + 1 \\ X^6 &= X^3 + X^2 + X = X^2 + 1 \\ X^7 &= X^3 + X = 1 \end{aligned}$$

Donc: $\mathbb{F}_8 = \{0, 1, X, X^2, X + 1, X^2 + X, X^2 + 1, X^2 + X + 1\}$.

Exemple 1.1.5 *corps fini* $\mathbb{F}_9$*.*

$\mathbb{F}_9$ $(9 = 32; p = 3$ *et* $m = 2)$*.* $\mathbb{F}_9$ *est de caractéristique* 3*, donc* $\mathbb{F}_9$ *est construit comme extension du corps premier* $\mathbb{Z}/3\mathbb{Z}$*. Soit le polynôme:* $P(x) = x^2 + 1$*; ce polynôme est irréductible sur* $\mathbb{F}_3$*;* $P(x)$ *n'a pas de zéro dans* $\mathbb{F}_3$*, car:* $P(0) = 1, P(1) = 2$ *et* $P(2) = 2$*. Comme* $P(x)$ *est de degré 2, les éléments de* $\mathbb{F}_9$ *sont de la forme:* $ax + b$ *avec* $a, b \in \mathbb{F}_3$*, donc:* $x^2 + 1 = 0 \mod(x^2 + 1)$*; alors:* $x^2 = 2 \mod(x^2 + 1)$*; et par conséquent :* $x^3 = 2x \mod(x^2 + 1); x^4 = 1 \ldots$

Alors $\mathbb{F}_9 = \{0, 1, 2, x, 2x, x + 1, 2x + 1, x + 2, 2x + 2\}$.

1.2 Courbes Elliptiques

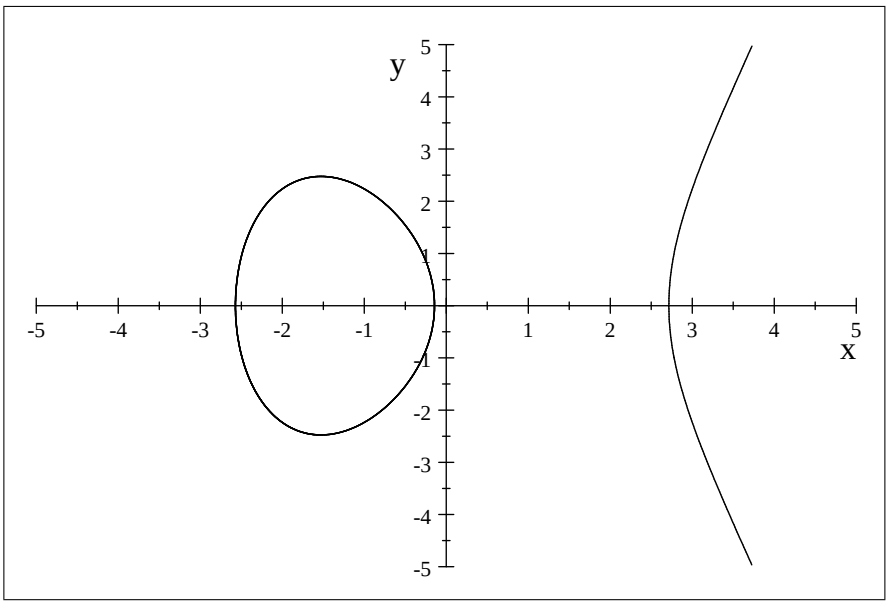
1.2.1 Définition d'une courbe elliptique

Cette partie définira ce qu'est une courbe elliptique et le groupe topologique d'une telle courbe il sera également montré qu'une courbe elliptique peut s'écrire sous une forme particulière appelée équations de Weierstrass

Définition 1.2.1 *Une courbe elliptique est une cubique plane E non singulière, d'équation de la forme*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Les cinq coefficients a_i sont des éléments d'un corps commutatif quelconque $\mathbb{K}$. les deux variables $x$et y sont des zéros de cette équation. L'équation de dessus est dite L'équation de Weierstrass.



1.2.2 Invariants de courbes elliptiques

Une courbe elliptique E possède plusieurs invariants: Un discriminant, un invariant modulaire, un invariant différentiel, un conducteur , un régulateur , ...

Définition 1.2.2 *Le discriminant d'une courbe elliptique E, sur un corps $\mathbb{K}$, est le polynôme "homogène "de l'anneau $\mathbb{K}[b^2, b^4, b^6, b^8]$, égal à:*

$$\Delta(E) = 9b_2b_4b_6 - 8(b_4)3 - 27(b_6)^2 - (b_2)^2b_8$$

avec: $b_2 = (a_1)^2+4a_2, b_4 = a_1a_3+2a_4, b_6 = (a_3)^2+4a_6$, $4b_8 = b_2b_6-(b_4)^2$ *et* $car(K) \neq 2, 3$.

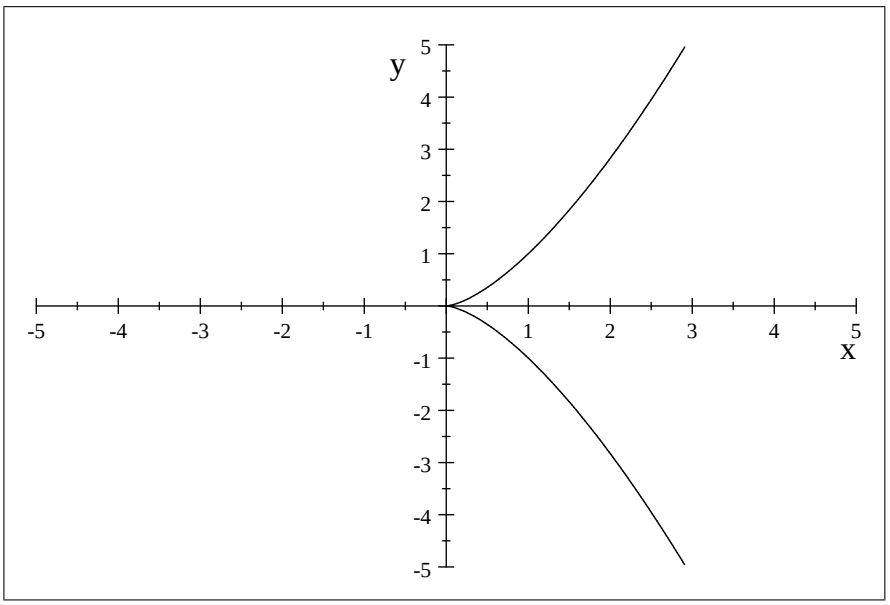
L'équation d'une courbe elliptique définie sur le corps de nombres réels peut être mise sous la forme simple:

$$y^2 = x^3 + ax + b$$

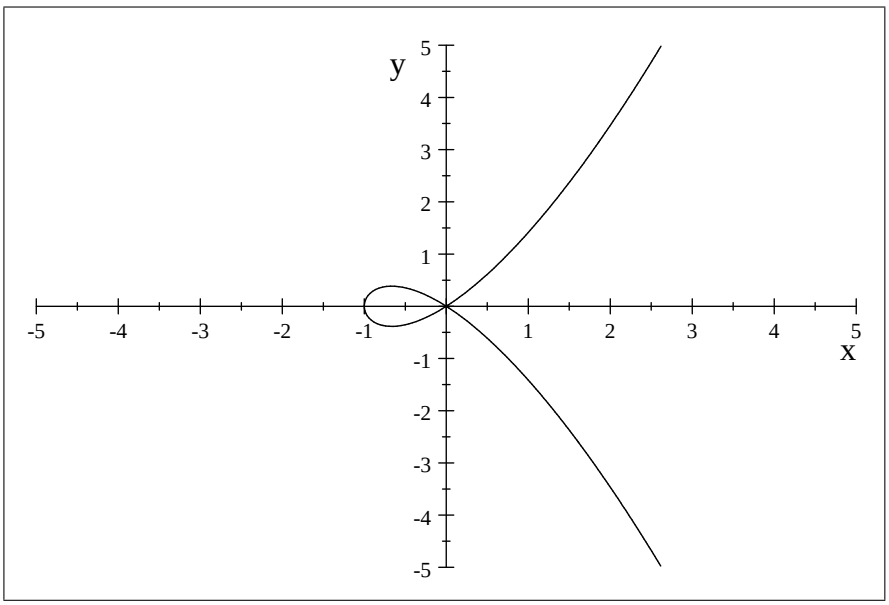
Où les coefficients a, b sont des nombres réels. Selon le choix de ces coefficients, les graphes correspondants ont des formes variées.

Et le discriminant devient : $\Delta(E) = -16(4a^3 + 27b^2)$.

Si $\Delta(E) = 0$: la cubique plane E est **singulière** (n'est plus une courbe elliptique), son graphe est l'une des formes suivantes:

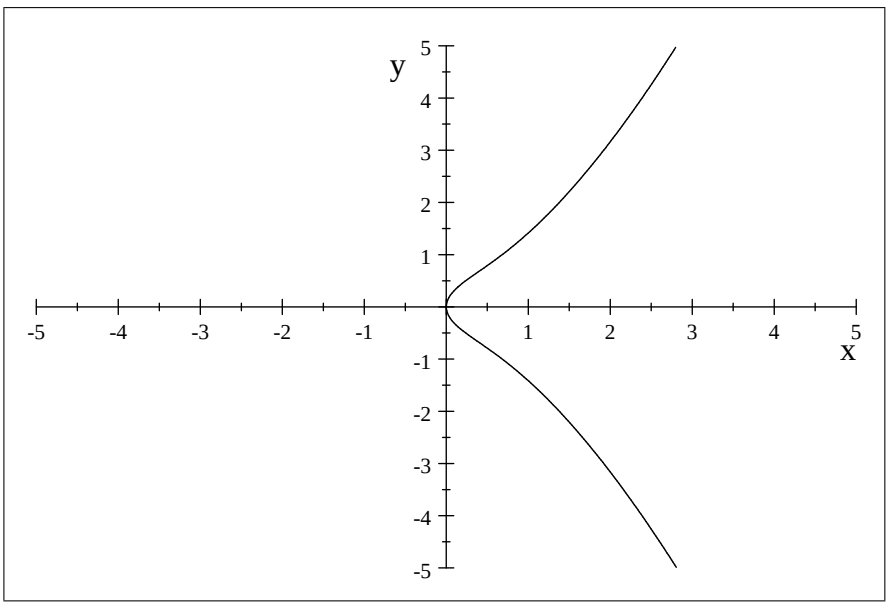


courbe d'équation $y^2 = x^3$ qui admet un point de rebroussement



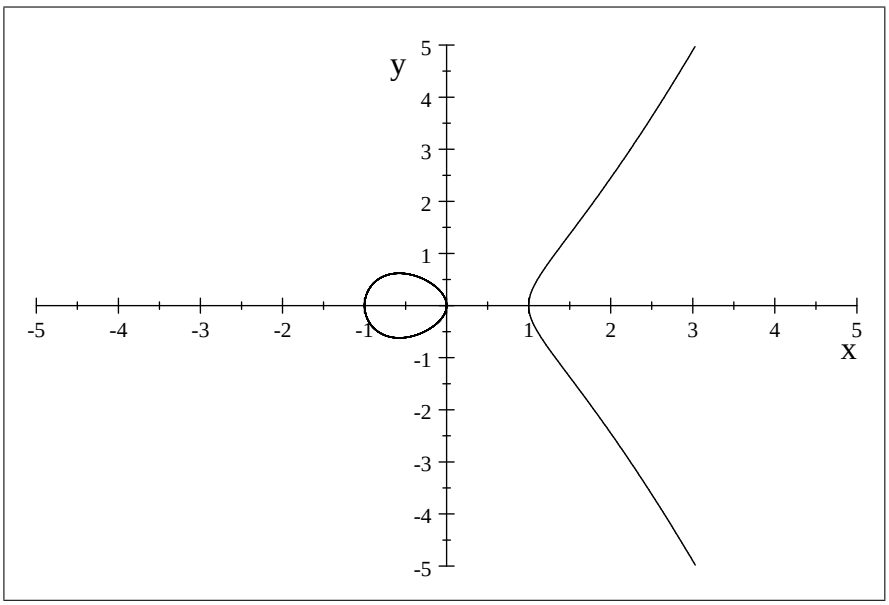
courbe d'équation $y^2 = x^3 + x^2$ qui adment un noeud

Définition 1.2.3 *Si $\Delta(E) \neq 0$: la cubique plane E est non singulière (c'est une courbe elliptique), son graphe de la forme:*



Courbe Elliptique d'équation $y^2 = x^3 + x$

ou bien :



Courbe Elliptique d'équation $y^2 = x^3 + x$

1.2.3 Groupe de Mordell-Weill

Les points de la courbe sont tous ceux dont les coordonnées (réelles) vérifient l'équation, ainsi qu'un point à l'infini. Comprendre comment et pourquoi ce point doit être pris en compte nécessite de se placer dans le cadre de la géométrie projective.

Ce point à l'infini est essentiel car ce sera l'élément neutre (le zéro) pour plus de détails consulter les ouvrages de la géométrie algèbrique.

pour l'addition des points de la courbe. Intuitivement, il suffit ici de l'imaginer comme le point d'intersection de toutes les droites verticales.

1.2.4 Loi de Groupe : résumé et justification

Considérons l'ensemble $E(K)$ des points K-rationnels d'une courbe elliptique E et le point à l'infini $O(\infty, \infty)$ de E.

Construisons sur l'ensemble $E(K)$ une loi de groupe abélien d'élément neutre le point à l'infini .

Proposition 1.2.1 *L'application $f : E(K) \times E(K) \to E(K)$ de valeur $f(P, R) = P + R$ munit l'ensemble $E(K)$ d'une structure de groupe abélien d'élément neutre O avec la règle*

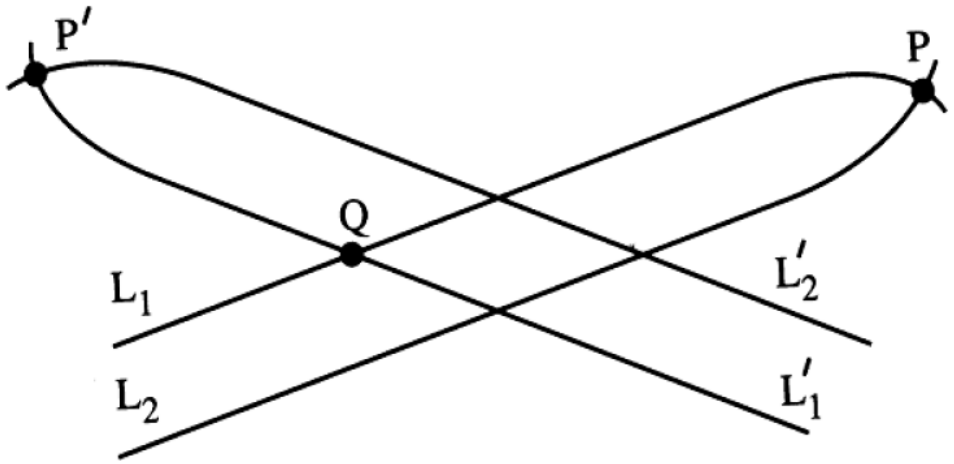


Figure 1: Intersection de droites parallèles.

géométrique : trois points colinéaires de la courbe E ont une somme nulle :

$$P + R + S = O$$

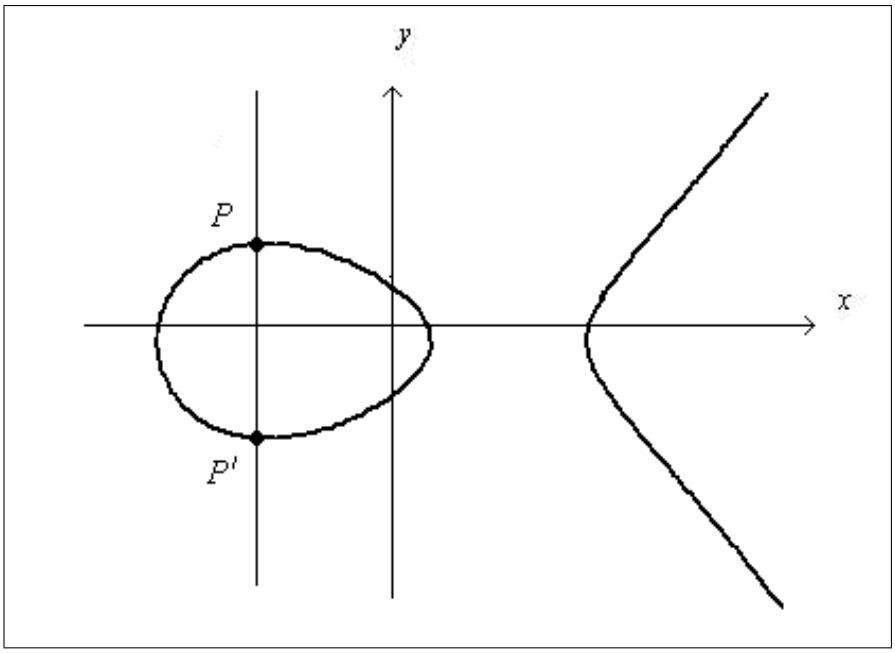
Formules du symétrique $-P$

Soit un point $P(x; y)$ sur une courbe elliptique $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Son symétrique est l'intersection P' de la courbe E par la parallèle à Oy passant par P.

Pour $P = (x_p, y_p)$ alors

$$-P \quad = \quad P' = (x_p, -y_p - a_1 x_p - a_3)$$



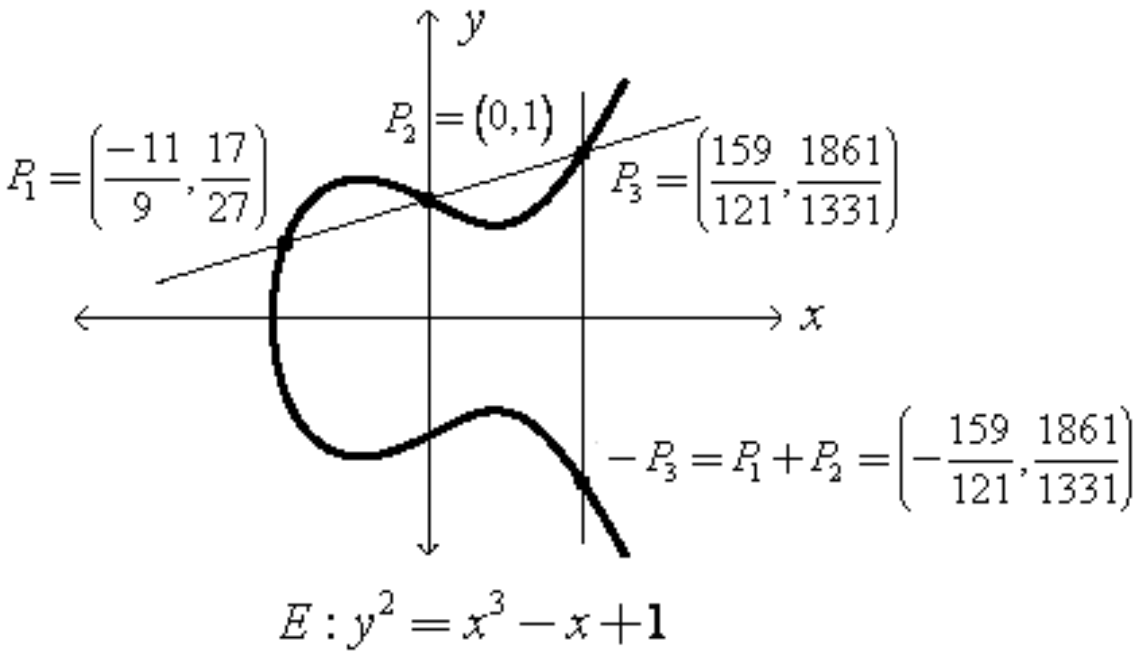
Formules de la somme $P_1 + P_2$ avec $P_1 \neq \pm P_2$

Soient $P = (x_P; y_P)$ et $Q = (x_Q; y_Q)$ deux points distincts d'une courbe elliptique $E(K)$ tels que $P \neq -Q$. Pour trouver les formules donnant les coordonnées du point $R = P + Q$ avec $R = (x_R; y_R)$, nous cherchons à résoudre le système de deux équations formé par l'équation de la droite (PQ) et l'équation de la courbe elliptique. Ce système traduit exactement le fait que $-(P+Q)$ est le troisième point d'intersection de la courbe elliptique et de la droite (PQ). Nous obtenons les formules

$$P + Q = \begin{cases} \lambda = \frac{y_P - y_Q}{x_P - x_Q} \\ x_R = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q \\ y_R = \lambda^3 + a_1\lambda - \lambda\left(a_2 + 2x_P - x_Q\right) - y_P \end{cases}$$

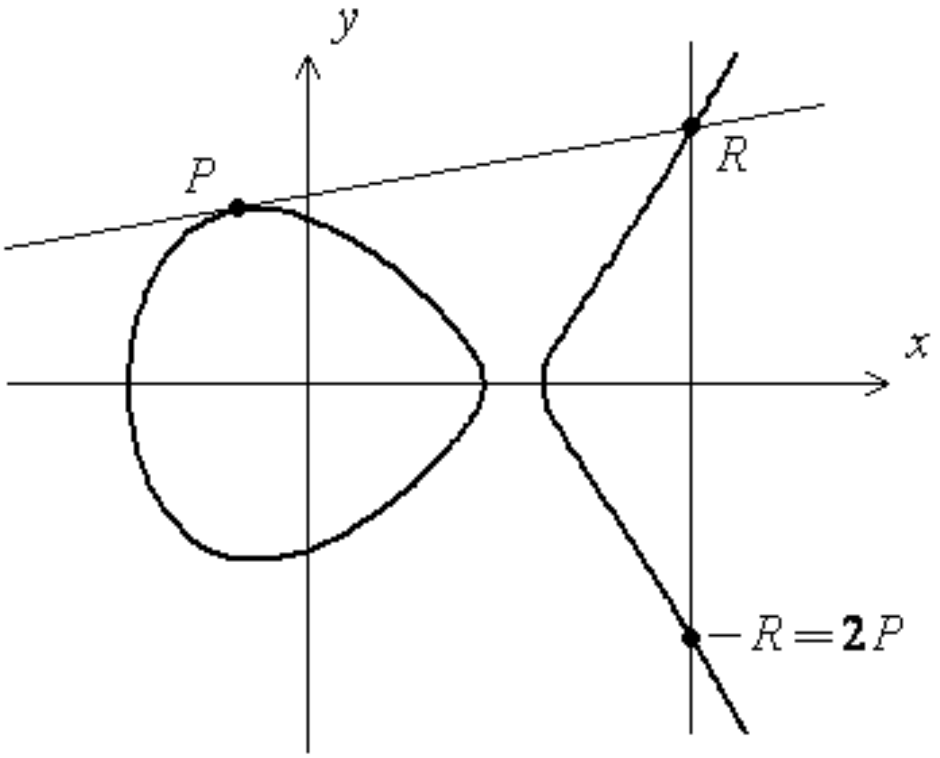
Formules de la somme $P + P$

Pour trouver les formules donnant les coordonnées du point $R = 2P$, nous utilisons le fait que $-2P$ est le second point d'intersection de la courbe E et de la tangente en E au point



P. L'équation de la tangente et celle de la courbe elliptique forment un système dont la résolution nous donne les formules pour obtenir les coordonnées de point $R = 2P$. Nous obtenons les formules, où λ représente la pente de la tangente au point$P$ de la courbe elliptique :

$$2P = \begin{cases} \lambda = \frac{3x_P^2 + a}{2y_P} \\ x_{2P} = \lambda^2 - 2x_P \\ y_{2P} = \lambda\left(x_P - x_R\right) - y_P \end{cases}$$



1.2.5 Cardinalité d'une courbe elliptique sur un corps fini

Soit $K = \mathbb{F}_q$ un corps fini à q éléments et E une courbe elliptique définie sur ce corps. Un premier résultat important concernant le nombre de points d'une courbe elliptique sur un corps fini, est le suivant:

Théorème 1.2.1 (Hasse) *Si E est une courbe elliptique définie sur le corps fini $\mathbb{F}_q$ alors:*

$$q + 1 - 2\sqrt{q} \leq cardE(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$

Compter les points d'une courbe elliptique sur un corps fini:

Dans cette partie nous allons montrer qu'il est facile de calculer le cardinal d'une courbe $E(\mathbb{F}_{q^n})$ si nous connaissons son cardinal pour $E(\mathbb{F}_q)$.

Ensuite nous allons donner un algorithme qui nous permet de calculer $CardE(\mathbb{F}_p)$ pour un p premier.

Théorème 1.2.2 *Soit* $CardE(\mathbb{F}_q) = q+1-\varepsilon$*; avec* ε *est un entier. Posons:* $X^2-\varepsilon X+q = (X-\alpha)(X-\beta)$*, ou* α *et* $\beta \in C$*. Alors:* $CardE(\mathbb{F}_{q^n}) = q^n+1-(\alpha^n+\beta^n)$*, pour tout* $n > 0$*.*

Exemple 1.2.1 *Considérons la courbe elliptique* $E : y^2 = x^3 + 2$*, définie sur* $\mathbb{F}_7$*, alors un simple calcul montre que:*

$$E(\mathbb{F}_7) = \{O, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}$$

Ainsi $CardE(\mathbb{F}_7) = 9$ *et* $\varepsilon = 7+1-9 = -1$ *et nous avons le polynôme suivant:*

$$x^2 + x + 7 = \left(x - \frac{-1+\sqrt{-27}}{2}\right)\left(x - \frac{-1-\sqrt{-27}}{2}\right)$$

Nous pouvons donc calculer le cardinal de tout groupe $E(\mathbb{F}_{7^n})$.
Par exempel pour $n = 60$: $\left(x - \frac{-1+\sqrt{-27}}{2}\right)^{60} + \left(x - \frac{-1-\sqrt{-27}}{2}\right)^{60} = 180498585261198848060064 98$
et donc:

$$\begin{aligned} cardE(F_{7^{60}}) &= 7^{60} + 1 - 180498585261198848060064 98 \\ &= 508021860739623365322188179602357975652549718829504. \end{aligned}$$

Grâce à ce théorème nous pouvons très vite calculer la cardinalité d'un groupe $E(\mathbb{F}_{P^n})$ du moment que nous connaissons $CardE(\mathbb{F}_p)$.

1.2.6 L'algorithme de Schoof

C'est un algorithme due à René Schoof qui permet de calculer $CardE(\mathbb{F}_p)$ pour tout nombre premier p.

Ainsi nous pourrons calculer $CardE(\mathbb{F}_{p^n})$.

Schoof a évalué l'ordre d'un groupe $E(\mathbb{F}_p)$ sous la forme : $p+1-t$, ou t est une racine d'une équation dite de Frobenius.

q	$E(F_q)$	Card $E(F_q)$	Temps (sec)
11	$y^2 = x^3 + 8x + 1$	17	0.164835
13	$y^2 = x^3 + 2x + 9$	17	0.000000
17	$y^2 = x^3 + 9x + 5$	11	0.054945
19	$y^2 = x^3 + 5x + 12$	19	0.054945
23	$y^2 = x^3 + 2x + 6$	29	0.000000
29	$y^2 = x^3 + 22x + 16$	37	0.054945
31	$y^2 = x^3 + 5x + 3$	41	0.054945
37	$y^2 = x^3 + 8x + 14$	47	0.000000
41	$y^2 = x^3 + 8x + 4$	43	0.274725
43	$y^2 = x^3 + 27x + 22$	29	0.000000
47	$y^2 = x^3 + 38x + 6$	37	0.054945
53	$y^2 = x^3 + 5x + 12$	43	0.054945
59	$y^2 = x^3 + 4x + 49$	53	0.000000
61	$y^2 = x^3 + 31x + 49$	61	0.054945
67	$y^2 = x^3 + 2x + 56$	37	0.000000
71	$y^2 = x^3 + 57x + 14$	47	0.054945
73	$y^2 = x^3 + 33x + 34$	79	0.000000
79	$y^2 = x^3 + 75x + 6$	61	0.054945
83	$y^2 = x^3 + 3x + 78$	67	0.000000
89	$y^2 = x^3 + 54x + 52$	103	0.054945
97	$y^2 = x^3 + 32x + 33$	97	0.054945

Table: Programme Performance De schoof [13].

Chapitre 2

Logarithme Discret Ordinaire(D-L)

Soient a, x, y des entiers.

Dans ce chapitre on va étudier l'équation $y = a^x$, donc trouver y (avec x donné) c'est Le problème d'exponentiation, réciproquement le calcul de x est difficile.

2.1 Définition du probléme D-L

Soit le groupe multiplicatif cyclique $(\mathbb{Z}/p\mathbb{Z})^*$ avec p premier. Soit g un générateur de ce groupe (tous les éléments du groupe sont des puissances de g).

Le problème du logarithme discret de base g dans $(\mathbb{Z}/p\mathbb{Z})^*$ est le suivant :

Problème 2.1.1 *Étant donné un élément x de $(\mathbb{Z}/p\mathbb{Z})^*$, trouver l'entier y tel que l'on ait :*

$$x = g^y \bmod (p)$$

On note parfois cet entier y, $log_g(x)$**,** avec $0 \leq y \leq (p-1)$.

donc: $log_g(x) : (\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$

$$x \rightarrow log_g(x) = y$$

Exemple 2.1.1 $(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6\}$. *Remarquant que* 3 *et* 5 *sont des générateurs de ce groupe.*

Donc on peut définir un logarithme discret à la base 3 et à la base 5 comme suit:

x	1	2	3	4	5	6
$\log_3(x)$	6	2	1	4	5	3
$\log_5(x)$	6	4	5	2	1	3

2.2 Algorithmes pour calculer le D-L

Il est toujours possible, pour calculer **logarithme discret** de x, d'énumérer les éléments : $g^0, g^1, g^2, \ldots,$ jusqu'a ce que l 'on rencontre x. Cependant, si cette méthode est tout à fait raisonnable pour les petits groupes, elle est totalement imaginable quand la cardinalité du groupe augmente.

Il y a plusieurs algorithmes pour calculer le *D-L* :

1 L 'algorithme baby-step giant-stepdû de Shanks.

2 L 'algorithme ζ de Pollard.

3 L 'algorithme de Pohlig-Helman.

4 L 'algorithme de calcul d'index.

On va indiquer dans la suite l'un de ces algorithmes qui est L'algorithme de baby-step giant-step dû à Shanks.

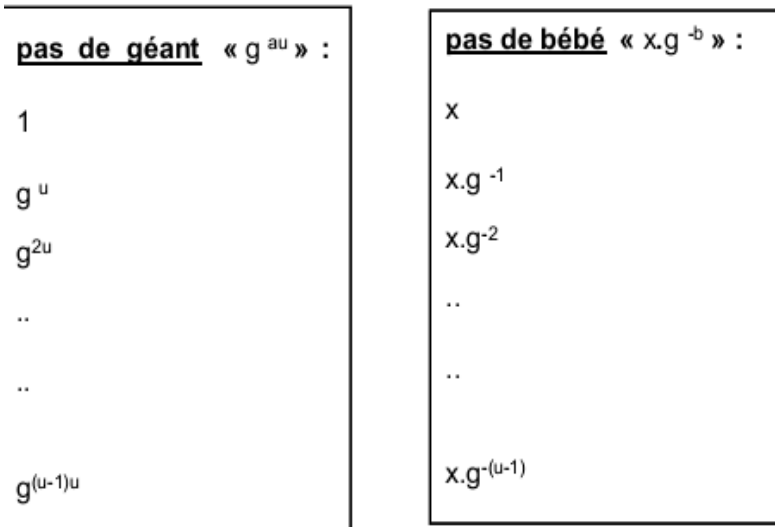
Soit l'équation: $g^y = x \bmod(p)$, (on cherche y).

La résolution de cette équation se fait d'après Shanks comme suit :

On écrit : $y = au + b$, avec: $u = \left[\sqrt{p}\right]$ et : $0 \leq a, b \leq u - 1$,où $\left[\sqrt{p}\right]$est le plus petit entier rationnal p:

L 'équation devient : $g^{au} = xg^{-b} \bmod(p)$.

On crée alors deux listes, constituant ainsi la méthode dite ''pas de géant, pas de bébé".



La création des listes utilise $o(\sqrt{p})$ opérations et leur consultation a un coût de $o(\sqrt{p}\log p)$.

Exemple 2.2.1 $p = 23, g = 11, x = 14$. *Alors* $u = 5$*, les deux listes sont alors:*

$$\begin{aligned} Suite\ g^{au} &: 1, 5, 2, 10, 4 avec : 0 \leq a \leq 4 \\ Suite\ x.g^{-b} &: 14, 18, 10, 3, 17 avec : 0 \leq b \leq 4 \end{aligned}$$

Il ya égalité pour $a = 3$ et $b = 2$ d'où $y = 17$.

2.3 Cryptosystéme d'Algamel

2.3.1 L'algorithme d'Algamel avec l'organigramme

En 1985, Algamal a proposé un algorithme de chiffrement à clé publique. Cet algorithme concerne le problème de la confidentialité des messages envoyés, et son efficacité est aussi basée sur la difficulté du problème du logarithme discret, une personne, Ahmed, demande à Bilal de lui envoyer des messages confidentiels.

Une description est donnée ci-dessous:

Algorithme d'Algamal

Soient p un nombre premier et g un générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^*$.

$*$ Données communes: p et g

$*$ Clé privée d'Ahmed: $x \in (\mathbb{Z}/p\mathbb{Z})^*$.

$*$ Clé publique d'Ahmed: $y = g^x \bmod p$.

Chiffrement :

soit m un message à chiffrer par Bilal.

Ce message m est codé comme un élément de $(\mathbb{Z}/p\mathbb{Z})^*$.

Bilal choisit un élément k de $(\mathbb{Z}/p\mathbb{Z})^*$ puis il calcule R et S:

$$R = g^k \bmod p \quad et \quad S = m.y^k \bmod p$$

Un chiffré de m est la paire $(R; S)$.

Déchiffrement:

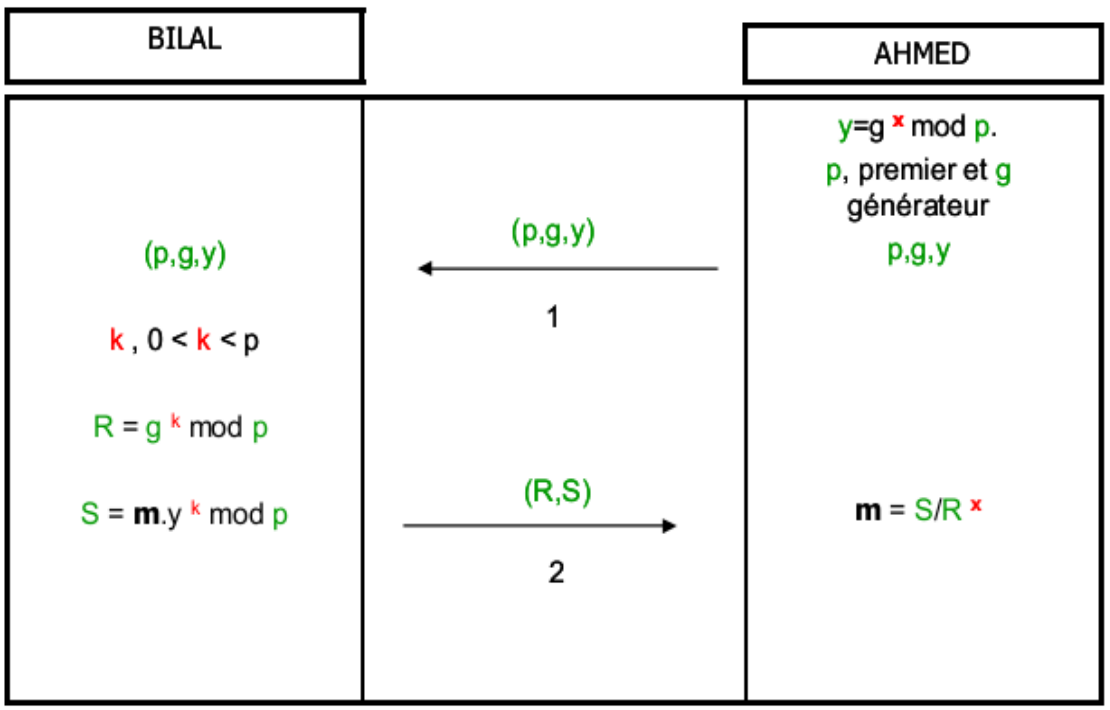
Seule Ahmed est capable de retrouver m à partir du chiffré, grâce à sa connaissance de x.

En effet,

$y^k = g^{xk} = (g^k)^x = R^x \bmod p$

Ainsi, $m = \frac{S}{R^x} \bmod p$.

l'organigramme:



m: le message à envoyer.

Les symboles en vert sont publiques.

Les symboles en rouge sont secrets.

Exemple 2.3.1 *Soit le dictionnaire suivant:*

A	B	C	D	E	F	G	H	I	J
01	02	03	04	05	06	07	08	09	10

K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20

U	V	W	X	Y	Z	.	espace	?
21	22	23	24	25	26	27	28	29

Première étape:

Ahmed choisit $p = 31$, premier.

Et soit $g = 11$ un générateur du groupe $(\mathbb{Z}/31\mathbb{Z})^*$.

$y = g^x \bmod 31 = (11)^{10} = 5$, pour $x = 10$(x clé secrète de Ahmed).

Donc Ahmed publie $(p, g, y) = (31, 11, 5)$ et garde sa clé secrète $x = 10$.

Deuxième étape:

Bilal veut envoyer à Ahmed le message suivant:

→Il fait beau.

Chiffrement:

Il convertit ce message à une suite d'entier m de $(\mathbb{Z}/31\mathbb{Z})^*$ Donc m = Il f**a**it **b**eau = 091228060**1**09202**8**0**2**05012127

Bilal choisit un élément $k = 8$ de $(\mathbb{Z}/31\mathbb{Z})^*$ puis, il calcule R et S :

$$\begin{aligned} R &= g^k mod 31 = 11^8 mod 31 = 19 \\ S &= m.y^k \bmod 31 \\ &= 091228060109202802050121 27.\mathbf{5}^8 \bmod 31 \\ &= 091228060109202802050121 27.\mathbf{25} \bmod 31 \\ &= 082118262508041821012529 24 \end{aligned}$$

Bilal envoi à Ahmed le chiffré de paire ($\mathbf{R}$; $\mathbf{S}$).

Déchiffrement

Ahmed déchiffre le message m en utilisant sa clé secrète $x = 10$ en calculant : $\frac{S}{R^x}$

d'où :

$$\begin{aligned} \frac{S}{R^x} &= S/19^{10} \bmod 31 \\ &= S/25 \bmod 31 \\ &= S.5 \bmod 31 \\ &= (082118262508041821012529 24).5 \bmod 31 \\ &= \mathbf{09122}8060109202802050121 27 \\ &= \text{il fait beau.} \rightarrow \text{le message initial} \end{aligned}$$

Chapitre 3

Cryptographie basé sur les Courbes Elliptiques

3.1 introduction

Dans ce chapitre en va donner un exemple sur les cryptosystèmes symétriques qui utilisent la même clé pour le chiffrement et le déchiffrement,

donc il nous faut un moyen pour transporter cette clé commune, il faut l'échanger en toute sécurité.

3.2 Le protocole d'échange de clé de Diffie-Hellman

Il s'agit d'un échange de clé par une courbe elliptique (définie sur un corps fini).

1 Ahmed et Bilal se mettent d'accord ensemble publiquement sur une courbe elliptique $E : y^2 = x^3 + ax + b$, sur un corps fini: $K = \mathbb{F}_P = \mathbb{Z}/p\mathbb{Z}$, p : premier.

Ils se mettent aussi d'accord sur un point P de $E(K)$.

2 Secrètement:

Ahmed choisit un entier K_A et Bilal un entier K_B.

3 Ahmed envoie à Bilal le point K_AP , et Bilal envoie à Ahmed le point K_BP.

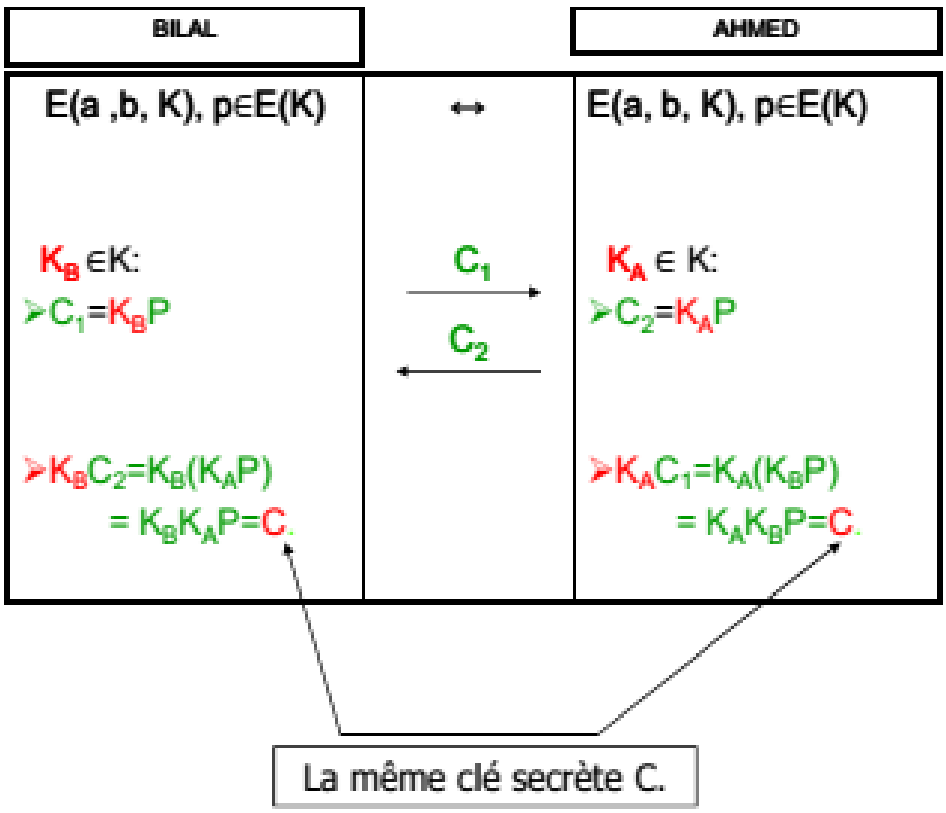
4 Chacun d'eux est capable de calculer $K_A(K_BP) = K_B(K_AP) = (K_AK_B)P$ qui est un point de la courbe $E(K)$, ce dernier constitue leur clé secrète.

Si quelqu'un a espionné leur échange, il doit connaître $E(a, b, K)$, P, K_AP, K_BP pour pouvoir calculer K_AK_BP et il faut résoudre un problème semblable au problème du logarithme discret mais sur une courbe elliptique, ce qui n'est pas évident en effet

Il faut pouvoir calculer $K_A$connaissant P et K_AP.

Le logarithme discret est déjà difficile à résoudre dans les groupes bien connues $(\mathbb{Z}/p\mathbb{Z})^*$. Pour les groupes des courbes elliptiques, c'est encore plus difficile...

3.2.1 l'organigramme



3.2.2 Exemple (le protocole de Diffie-Hellman)

Soit la courbe elliptique $E(\mathbb{F}_{23}) = E((\mathbb{Z}/23\mathbb{Z})^*)$ d'équation $y^2 = x^3 + x + 1$, et soit le point $P = (3, 10) \in E$

$$\begin{aligned} E(F23) &= \{0E, (0,1), (0,22), (1,7), (1,16), (3,10), (3,13), (4,0), \\ &\quad (5,4), (5,19), (6,19), (6,4), , (7,12), 7,11), (9,7), (9,16), \\ &\quad (11,3), (11,20), (12,4), (12,19), (13,16), (13,7), (17,3), \\ &\quad (17,20), (18,3), (18,20), (19,5), (19,18)\}. \end{aligned}$$

1 Pour $K_A = 4$, Ahmed calcule et envoit à Bilal :

$C_2 = K_A P = 4P = 4(3,10) = (17,3) = C_2$.
Pour $K_B = 2$, Bilal calcule et envoit à Ahmed :
$C_1 = K_B P = 2P = 2(3,10) = (7,12) = C_1$.

2 Ahmed et Bilal calculent chacun d'eux:

Ahmed : $K_A C_1 = K_A(K_B P) = 4(7,12) = (13,16) = C$
Bilal : $K_B C_2 = K_B(K_A P) = 2(17,3) = (13,16) = C$

3 Donc $C = (13,16)$ est un point de la courbe $E(\mathbb{F}_{23})$ qui est un point secret commun de Ahmed et Bilal. Alors la clé secrète commune sera par exemple la première composante du point C c-à-d :

$$K_C = \textit{clé secrète commune} = 13$$

3.3 Cryptosystème basé sur le Protocole Diffie-Hellman

3.3.1 L'algorithme

On suppose que Ahmed et Bilal ont suivi le protocole d'échange de clé de Diffie-Hellman.

Bilal veut envoyer à Ahmed un message m.

1 Il convertit tout d'abord son message à une suite de points m sur la courbe elliptique $E(a,b,K)$.

2 Il choisit secrètement un entier β et envoi à Bilal le chiffré (m_1, m_2) avec : $m_1 = \beta.P$ et $m_2 = m + \beta.K_C P$.

P : point quelconque de la courbe E

K_C : la clé secrète commune échangée suivant le protocole

3 Ahmed déchiffre le message initial en calculant:

$m_2 - K_C m_1 = m$.

Car :

$$\begin{aligned} m^2 - K_C.m_1 &= (m + \beta.K_c P) - K_C(\beta.P) \\ &= m + \beta.K_C P - K_C \beta.P = m. \end{aligned}$$

m : le message à envoyer.

Les symboles en vert sont publiques.

Les symboles en rouge sont secrets.

3.3.2 Exemple numérique

Supposant que la clé secrète commune échangé suivant le protocole de Diffie-Hellman est $K_C = 13$ donné dans l'exemple précédent.

Ahmed veut envoyer à Bilal le message m= (12,4) qui est un point de la même

Courbe $E(\mathbb{F}_{23}) = E((\mathbb{Z}/23\mathbb{Z})^*)$ d'équation : $y^2 = x^3 + x + 1$, et soit le même point $P = (3, 10)$.

★Le message $m = (12, 4)$ qui est un point de la même courbe.

★Il choisit secrètement un entier $\beta = 2$ et envoi à Bilal le chiffré (m_1, m_2) avec $m_1 = \beta.P = 2P = 2(3, 10) = (7, 12)$ et $m_2 = m + \beta.K_C P = (12, 4) + 2.13.(3, 10)$ ce qui donne :

$$\begin{aligned} m_2 &= (12, 4) + 26.\,(3, 10) \\ &= (12, 4) + (7, 11) \\ &= (17, 3) \end{aligned}$$

Car :

$$\begin{aligned}
26P &= 13(2P) \\
&= 13P\prime, pour P\prime = 2P = 2(3,10) = (7,12). \\
&= P\prime + 12P\prime = P\prime + 6(2P\prime) \\
&= P\prime + 6P", pour P" = 2P\prime = 2(7,12) = (17,3) \\
&= P\prime + 3(2P") = P\prime + 3P"\prime, pour P"\prime = 2P" = 2(17,3) = (13,16) \\
&= P\prime + P"\prime + 2P"\prime = (P\prime + P"\prime) + P"", pour P"" = 2P"\prime = 2\prime 13,16) = (5,19) \\
&= (6,4) + (5,19) = (7,11).
\end{aligned}$$

★Bilal déchiffre le message initiale en calculant :

$$\begin{aligned}
m_2 - K_c m_1 &= (17,3) - 13(7,12) \\
&= (17,3) - (7,11) \\
&= (17,3) + (7,12) \\
&= (12,4) = m.
\end{aligned}$$

3.3.3 Rappel sur les règles de calculs

★ $P = (x, y)$ $donc : -P = (x, -y)$.

★ $P = (x, y), P' = (x', y')$ donc : $P + P' = (x'', y'') = (t^2 - x - x', -t^3 + t(2x + x'') - y)$, avec $t = (y' - y).(x' - x)^{-1}$

★ $P = (x, y) doncP + P = 2P = (x_{2P}, y_{2P}) = (t^2 - 2x, -t^3 + t(x - x_{2P}) - y)$, avec $t = (3x^2 + a).(2y)^{-1}$.

3.3.4 Conclusion

La cryptographie à courbes elliptiques est une alternative à la cryptographie classique à clé publique.

La taille des clés permet de réserver un espace mémoire au niveau de processeur.

La cryptographie à courbes elliptiques est une approche appelée à se répandre dans les applications pratiques.

Il existe d'autres constructions basées sur les courbes elliptiques (courbes hyperelliptiques de Kobler).

3.4 Algorithmes pour les exemples précédents

À l'aide d'un langage de programmation, notre objectif est de donner un programme qui avait la capacité de crypter et de décrypter un message en utilisant le protocole d'Algamel, le protocole des courbes elliptiques.

L'étude des propriétés des courbes elliptique, des fonctions mathématiques et de la programmation a permit d' arriver à un résultat concluant.

Le programme a la capacité de crypter et de décrypter un message de longueur variable.

L'usage que l'on fait aujourd'hui de l'informatique dans nos communications et dans nos transactions bancaires, entre autres, exige un niveau de sécurité de plus en plus élevé. Les paiements de factures à l'aide du réseau Internet constitue un excellent exemple de ce besoin de sécurité.

message de longueur variable.

3.4.1 Algorithme d'AlGamel

Declaration des variables:

p, g, x, y, r, s, k, m, m1, m2, i :des entiers positives.

début

*donner la valeur de p: un nombre premier.

* donner la valeur de g: un générateur du groupe Z/pZ .

*donner la valeur de x: un élément quelconque de ce groupe.

*calculer $y = g^x$ **mod** p.

y= g *g*g…….*g **mod** p; x: fois

*Donc x: la clé secréte de recpteur ;

p, g, y: la clé publique.

Fin.

----------***L'émméteur***----------

début

* donner la valeur du méssage m.

* donner la valeur de k.

*calculer r, s **mod** p:

r = g*g*g……..*g **mod** p ; k: fois.

s = m.(y*y*y…..*y) **mod** p, k: fois.

*envoyer le chiffré: r et s.

Fin.

```
----------Le récepteur----------
Début
    calcul er:
        m1=r*r*r…….*r mod p;  x fois.
    calculer m2  l'inverse de m1:
    Début
        Pour  i de 1 à  (p-1)  faire :
        Début
            Si:  i*m1 = 1 mod p
            alors: m2= i;
            Sinon: i:=i+1
        fin
    fin
        calculer
    m= s*m2 =m.
    le même message initiale.
Fin.
```

3.4.2 Algorithme pour le cryptage par courbe elliptique

Declaration des données:

p, T, T', a, b, m, xp, yp, x2p, y2p, xq, yq, Ka, Kb, xKa, yKa, xKb, yKb, xkaKb, ykaKb, xkbKa, ykbKa, i, j , β, xm1, xm2, ym1, ym2,:xm, ym: des entiers positives.

données communes

lire : p, a, b, xp, yp

*calculer l'entier m:

début

pout i=1 à p faire:

si: i*2*yp= 1 **mod** p

alors m=i;

sinon: i:= i+1

fin

*calculer les cordonnées du point 2P :

début

T= [(3*xp*xp + a)*m] **mod** p.

x2p= [(T*T) -2*xp] **mod** p.

y2p= [-(T*T*T) -yp + 3*T*xp] **mod** p.

fin

***création de la clé commune:**

Ou protocole de **Diffie-Hellman**

```
----------émetteur-récepteur----------
lire Ka; (resp Kb)
*calculer le point Ka*P=(xKa, yKa) (resp : Kb*P=(xKb, yKb))……..@
début
  Ka*P= 2P + (Ka -2) *P= 2P+ (P+ P+……..+P); (Ka -2) fois .
   calculer l'entier m:
  début
  pour i=1 à p faire:
    si:  i*(xp- x2p)= 1 mod p
    alors m=i;
    sinon: i:= i+1
  fin
  début
  pour j=1 à (Ka -2) faire
    T'= [(yp- y2p)*m] mod p.
    x= [(T'*T') – xp –x2p] mod p.
    y= [-(T'*T'*T') -yp + (2*xp +x2p)*T'] mod p.
    x:=x2p; y:=y2p
  fin
    donc: xKa= x, yKa= y. (resp xKb= x, yKb= y. )
Fin.
Le récepteur- envoit à l'émméteur le point Ka*P=(xKa, yKa):
L'émméteur - envoit au récepteur le point Kb*P=(xKb, yKb):
```

----------émetteur-récepteur----------

Le récepteur- recoit le point *Kb*P=(xKb, yKb):*

L'émméteur - recoit le point *Ka*P=(xKa, yKa):*

* *calculer le point Ka(Kb*P)=(xKaKb, yKaKb) par le récepteur;*

*(resp le point Kb(Ka*P))=(xKbKa, yKbKa) par L'émméteur -).*

début

Ka(Kb*P)= 2(Kb*P)+* (Ka -2) **(Kb*P).*

Kb(Ka*P)= 2(Ka*P)+* (Kb -2) **(Ka*P).*

* utiliser le même algorithme précédent @ ;

remplissant le point P par le point (KbP);

(resp remplissant P par (KaP)).

fin

Donc :

*Ka(Kb*P)= Kb(Ka*P)*

soit xKaKb= xKbKa= k.

k est suposé comme une clé secrète commune.

----------L'émméteur/ chiffrement----------

***soit le point M =(xm, ym): le méssage voulu envoyer**

*** lire xm, ym, β ;entiers .**

***calculer les deux points M1 =(xm1, ym1) et M2=(xm2, ym2)**

début

*M1= β*P (utiliser le même algorithme précédent @) ;*

*M2= M + β *k*P =M + M'*

*utiliser le même algorithme précédent @ pour calculer β *k*P = M';

*utiliser le même algorithme précédent @ pour calculer M +M'.

(remplissant le point P par le point M ; le point 2P par le point M', et répéter l'opération un seul foi.)

fin

----------Le récepteur/ déchiffrement----------

***recoit les deux points M1 =(xm1, ym1) et M2=(xm2, ym2)**

début

calculer

*Msg=M2 – k*M1 = M 2 + k*(-M1) ; (-M1)= - (xm1, ym1) = (xm1, - ym1)*

Msg *= M 2 + k*M1'=M2 + M1".*

*utiliser le même algorithme précédent @ pour calculer k*M1 = M1';

*utiliser le même algorithme précédent @ pour calculer M2 +M1".

(remplissant le point P par le point M2 ; le point 2P par le point M1", et répéter l'opération un seul foi.)

fin

Conclusion Générale

Dans le monde de la cryptographie, le niveau de difficulté d'un problème se mesure au temps de calcul informatique nécessaire pour le résoudre : plus ce délai est long, et plus un « attaquant » aura du mal à accéder aux données secrètes. Jusque-là, le temps de résolution nécessaire aux meilleurs algorithmes pour résoudre le logarithme discret était "sous-exponentiel". Autrement dit, ce temps augmentait très rapidement en fonction de la taille de l'objet mathématique utilisé pour créer le logarithme discret, garantissant ainsi la presque inviolabilité des données qu'il protégeait. la résolution du log discret est en théorie à la portée des calculateurs actuels. Il est donc inutilisable pour protéger les données, un attaquant pouvant en trouver la clef à condition d'y mettre les moyens.« Le problème du logarithme discret était considéré comme l'un des "graals" de la théorie algorithmique des nombres, (Cryptologie, Arithmétique : Matériel et Logiciel). Nous sommes donc particulièrement fiers d'avoir contribué à ce sujet.

Bibliographie

[1] D-J. Mercier. Codage et cryptage, APMEP 421 , pages 219-232, 1999.

[2] Gilles Zemor : Cours de cryptographie.

[3] Husemoller, Dale, Elliptic Curves, Springer-Verlag, New York, 1987.

[4] J-Y. Enjalbert. Jacobiennes et cryptographie. Thèse de Doctorat de l'université de limoges, 2003.

[5] Marc Joye., Introduction élémentaire de la théorie des courbes elliptiques. Université catholique de louvain. Belgique.

[6] Silverman Joseph H. John Tate, Rational Points on Elliptic Curves, Undergraduate texts on mathematics.

[7] Silverman, J.H., The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.