République Algérienne Démocratique et Populaire

Ministère De L'enseignement Supérieur Et De La Recherche Scientifique

Université Mustapha STAMBOULI
Mascara

جامعة مصطفى اسطمبولي
معسكر

Département d'informatique

Mémoire en vue de l'obtention du Diplome de Magister

sujet du memoire

étude et implémentation d'un systéme de chiffrement asymétrique basé sur les courbes elliptiques

Présenté par :

MR BOUDAOUD ABDELKADER

Devant le jury composé de :

Présidente : **M^me^ DEBBAT FATIMA** (M.C.A, Univ.Mascara)

RAPPORTEUR **: M^R^ A. ALI PACHA** (professeur, USTO-MB)

Examinateur : **M^R^ MEFTAH BOUDJLAL** (M.C.A, Univ.Mascara)

Examinateur : **M^R^ Debakla Mohammed** (M.C.B, Univ.Mascara)

Examinateur : **M^R^ FAKIR ABDELKADER** (M.C.B, Univ.Mascara)

Année universitaire : 2016_2017

République Algérienne Démocratique et Populaire

Ministère De L'enseignement Supérieur Et De La Recherche Scientifique

Université Mustapha STAMBOULI
Mascara

جامعة مصطفى اسطمبولي
معسكر

Département d'informatique

Mémoire en vue de l'obtention du Diplome de Magister

sujet du memoire

étude et implémentation d'un systéme de chiffrement asymétrique basé sur les courbes elliptiques

Présenté par :

MR BOUDAOUD ABDELKADER

Devant le jury composé de :

Présidente : **M^me^ DEBBAT FATIMA** (M.C.A, Univ.Mascara)

RAPPORTEUR **: M^R^ A. ALI PACHA** (professeur, USTO-MB)

Examinateur : **M^R^ MEFTAH BOUDJLAL** (M.C.A, Univ.Mascara)

Examinateur : **M^R^ Debakla Mohammed** (M.C.B, Univ.Mascara)

Examinateur : **M^R^ FAKIR ABDELKADER** (M.C.B, Univ.Mascara)

Année universitaire : 2016_2017


بسم الله الرحمن الرحيم

Remerciement

Remerciement

Je remercie Allah tout puissant de nous avoir donné la volonté et le courage de mener à bien ce travail.

Pour une patience sans limites et un dévouement personnel sans égal je voudrais remercier mon encadreur, Mr A. ALI PACHA pour ses critiques qui m'a beaucoup aidé à apprécier ce travail et ont mieux éclairé mes perspectives .Je suis reconnaissant à lui tous particulièrement pour la confiance qu'il m'a témoignée et la liberté qu'il m'a laissée.

Ma gratitude va également à Mme .N.HADJ SAID pour m'avoir prodigué de précieux conseils, ainsi que pour avoir guidé et encouragé mes premiers pas dans ce travail.

Je tiens à exprimer ma parfaite considération aux membres de jury pour avoir accepté de me consacrer une partie de leurs temps, afin d'examiner et de juger ce modeste travail.

Je remercie également tous ceux qui, tous au long de ces années d'étude, m'encadre, observé, aidé, conseillé et même supporté, et surtout à mes parents, sans qui je ne serais jamais arrivés à ce stade.

Enfin, je remercie mes frères sœurs pour leur indéfectible soutient tout au long des nombreuses années. Merci à tous qui sont chers de près ou de loin.

Abdelkader Boudaoud

Dédicace

Dédicaces

Je dédie ce modeste travail :

A celle qui m'a donné la vie, qui m'a bercée mes nuits, celle qui n'a vécu que pour me voir un jour réussir, ma très chère mère.

«الله يرحمها و يدخلها فسيح جنانه و يجعل قبرها روضة من رياض الجنة»

A celui qui a puisé sa vie et sa jeunesse et qui n'a jamais su dire non pour subvenir, à mon très cher père.

A mes frères et mes sœurs et à toute la famille .....

A tous ceux qui ont beaucoup compté dans ma vie

A la mémoire de tous les être chères perdue

A tous mes amis .....

ABDELKADER BOUDAOUD

Sommaire

Sommaire

Chapitre II : les courbes elliptiques et notions

Chapitre III : algorithme de cryptage par les courbes elliptiques

Chapitre *IV* : implémentation de logiciel

Liste des abréviations

Abréviation

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programmation Interface
A5	Audio 5
BC	Bouncy Castle
CA	Certification Authority
CBC	Cipher-Block Chaining mode of operation
CFB	Cipher Feedback mode of operation
CPU	Computer Processing Unite
CRL	liste de révocation de certificat
CRT	Chinese Remainder Theorem
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
DH	Diffie-Hellman
DL	Discrete Logarithm
DLP	Discrete Logarithm Problem
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECB	Electronic Codebook mode of operation
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme

EDI	Environnement de Développement Intégré
FIPS	Federal Information Processing Standards
GF(p)	Corps fini (Galois Field) premier à p éléments
GF(2n)	Corps fini (Galois Field) binaire à 2n éléments
GSM	Global System for Mobile
HMAC	Hash-based Message Authentication Code
IBM	International Business Machines
IDEA	Norme internationale de cryptage de données
IEEE	Institute of Electrical and Electronics Engineers
IPSec	Internet Protocol Security
ISO	Organisation internationale de normalisation
IV	Initialization Vector
JCA	Java Cryptography Architecture
JCE	Java Cryptography Extension
JRE	Java Runtime Environnement
JVM	Machine Virtuelle Java
KDF	Key Derivation Function
MAC	Message Authentication Code
MD4	Message Digest 4
MD5	Message Digest 6
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PBE	Password Based Encryption
PKCS	Public Key Cryptography Standards

PKI	Public-Key Infrastructure
PRNG	Random Number Generator
RC4	Rivest Cipher 4
RC6	Rivest Cipher 6
RSA	Rivest-Shamir-Adleman
SEC	Standards for Efficient Cryptography
SECG	Standards for Efficient Cryptography Group
SET	Transaction électronique sécurisée
SHA-1	Secure Hash Algorithm 1
SSL	Secure Sockets Layer
SPI	Service Provider Interface
S/MIME	extension de messagerie Internet multi-usages
TLS	Transport Layer Security
TDES	Triple Data Encryption Standard
WEP	Wired Equivalent Privacy
XOR	eXclusive OR

Liste des Figures

Liste des figures

Liste des tables

Liste des Tables

Introduction

Générale

Introduction Général :

La cryptologie a connu une rapide évolution à notre époque surtout en ce qui concerne ces deux facteurs essentiels: l'irruption des mathématiques et de l'informatique et le développement des moyens de télécommunication, qui ont eu pour effet de multiplier les activités où intervient la cryptologie.

Le rôle de la cryptologie a évolué au fil des siècles. Auparavant, elle n'avait pour rôle que de protéger un texte écrit. Actuellement, la cryptologie s'étend dans différents domaines tels que la téléphonie, le télétraitement, le stockage des données, les communications avec les satellites...etc.

Mais la cryptographie à elle seule ne prend pas en charge tous les besoins de sécurité et n'est donc pas la seule discipline qui intervienne dans la sécurité des communications. La cryptographie est composée de la cryptographie symétrique et de la cryptographie asymétrique.

La cryptographie symétrique consiste à échanger des données chiffrées à partir d'un secret (appelé clé) connu uniquement par les parties concernées, le chiffrement comme le déchiffrement nécessitant la clé. Pour cela, il paraît nécessaire d'avoir un protocole d'échange de clés sûr et efficace.

De l'antiquité jusque dans les années 1970, tous les systèmes de cryptographie étaient symétriques (donc la principale préoccupation était la confidentialité) et il n'existait pas de méthode sûre pour échanger les clés secrètes.

Historiquement la cryptographie symétrique est le premier type de chiffrement utilisé et elle fournit le seul chiffrement théoriquement indéchiffrable (chiffrement de Vernam ou one-time pad) d'après la théorie de Shannon (1949). Elle est d'une grande efficacité en terme de temps de calculs. C'est en 1976 que deux chercheurs White Diffie et Martin Hellmann à l'université de Stand- ford, dans leur papier "New Direction In Cryptography", ont donné une solution au problème de l'échange des clés et ont proposé en même temps le modèle théorique de la cryptographie à clé publique qui est appelé modèle de cryptographie asymétrique
Depuis une quarantaine d'années, la cryptologie s'est enrichie de plus en plus vers une structure mathématique. Notamment d'une part l'algèbre linéaire comme par exemple corps fini, matrices, polynômes primitifs et fonctions à sens unique, d'autre part on trouve aussi énormément de notion de théorie de nombre comme par exemple nombre premier, congruence ou modulo.

Les cryptosystémes a clés publiques sont généralement construits sur des problèmes mathématiques difficile à résoudre.

Le premier problème utilisé fut le problème de la factorisation d'un entier qui donna naissance au cryptosystéme RSA.
Un second problème important est le problème du logarithme discret.
En 1987, Miller et Koblitz ont indépendamment propose l'utilisation des courbes elliptiques pour implanter les protocoles cryptographiques basés sur le problème du logarithme discret.
Ils ont justifie ce choix en argument que les courbes elliptiques assuraient une plus grande robustesse, en évitant les attaques sous-exponentielles.
Ces cryptosystémes sont aujourd'hui communément appelés ECC.

Durant les dix dernières années ECC à gagner popularité, il a été introduit dans de nombreux standards informatiques comme NIST ou IEEE.
Les protocoles cryptographiques doivent s'exécuter très rapidement afin de ralentir le moins possible les échanges de données.

Pour les protocoles basés sur le problème du logarithme discret, cela suppose que la multiplication scalaire se fait rapidement dans le groupe.

Il est donc important d'avoir une arithmétique efficace sur les courbes ainsi que sur le corps de définition de ces courbes.

) L'intérêt particulier qu'ils suscitent s'explique essentiellement par leur niveau de sécurité très élevé.

En effet, contrairement aux autres systèmes existants, aucune attaque en temps sous exponentiel n'est connue à ce jour contre les ECC, sauf en des cas particuliers rares et bien identifiés.

s'explique essentiellement par leur niveau de sécurité très élevé.

En effet, contrairement aux autres systèmes existants, aucune attaque en temps sous exponentiel n'est connue à ce jour contre les ECC, sauf en des cas particuliers rares et bien identifiés.

Une autre raison qui peut expliquer l'intérêt grandissant pour ces cryptosystèmes est le fait qu'ils offrent le même niveau de sécurité que d'autres cryptosystèmes largement utilisés pour la signature et l'authentification (comme RSA et DSA), mais avec des clés de taille nettement inférieure. Ceci les rend très attractifs pour les applications qui nécessitent des ressources très limitées (mémoire, puissance, bande passante...) telles que cartes à puces, téléphonie mobile ou communication par satellite.

Le travail qu'on compte réaliser s'insère dans cette tendance, il s'intitule : « étude et implémentation d'un système de chiffrement asymétrique basé sur les courbes elliptiques».

L'organisation de ce mémoire est comme suit :

1. Dans le premier chapitre on a donné une introduction et l'historique de la cryptographie et les différents cryptosystemes. On a fait un survol sur la cryptographie à clé secrète et la cryptographie à clé publique et les preuves de sécurité. Dans cette partie, nous avons parlé des systèmes de cryptographie et de la sécurité
2. Dans le deuxième chapitre nous avons présenté les notions algébriques et les courbes elliptiques. Il est destiné aux notions de base sur les courbes elliptiques et à titre d 'illustration des nouvelles formes de courbes elliptiques étudiées récemment et différentes de la forme de Weierstrass
3. le troisième chapitre représente les algorithmes de cryptographie basés sur les courbes elliptiques ici nous avons abordé quelques notions sur les protocoles : généralités sur les protocoles, protocoles cryptographiques et présentation de quelques protocoles d'échange de clés
4. Le quatrième chapitre c'est l'implémentation du logiciel ,Dans ce chapitre on a deux parties

    a. La première partie est consacrée à la représentation et a la description de notre logiciel
    b. La deuxième est consacrée aux résultats de la simulation

5. Une conclusion générale.
6. Une bibliographie.
7. Et en dernier une annexe.

Chapitre I

Cryptographie

Définition et concept

I-1 Introduction :

Il parfois sage de cacher certain choses,

Depuis l'aube du temps, le mystère ne cesse d'attirer l'homme doué de raison, il questionne la nature et lui demande ses papiers, ce qui est dissimulé ou cacher l'intéresse énormément, car sa soif de savoir est sans limite , mais si celui qui sait possède une forme de pouvoir , ce lui qui dissimule en possède un taux aussi grand.

La cryptologie est une véritable science qui étudie le chiffrement et le déchiffrement d'information; tandis que la cryptographie est l'utilisation de systèmes mis au point par des cryptologues , elle intéresse de plus en plus les informaticiens dans la mesure où l'on manipule des données croissants et qui sont nécessaire à protéger.

I-2 Généralités sur la cryptographie

Le cryptage ou chiffrement (encryption) peut être défini comme une fonction réversible de transformation des données en envisageant la protection d'information contre toute prise de connaissance du contenu (confidentialité) ou modification indue (intégrité) .

Le décryptage ou déchiffrement (decryption) est l'opération inverse du cryptage, il a pour but de récupérer l'information masquée [12].

Le message à crypter est également appelé texte en clair (plaintext) et le résultat du cryptage d'un texte en clair est appelé texte crypté (ciphertext). Le texte en clair est noté P, qui peut être une suite de bits, un fichier de texte, un enregistrement de voix numérisé, ou une image numérique. Du point de vue de l'ordinateur, P n'est rien d'autre que de l'information binaire. Le texte en clair peut être transmis ou stocké [29].

Le texte crypté est noté C , c'est aussi de l'information binaire, parfois de la même taille que P et parfois plus grande. La fonction de cryptage, notée E_{Ke} , transforme P en C

comme suit $C = E_{Ke}(P)$

Où Ke est la clé de cryptage. La fonction de décryptage, notée D_{Ke} , transforme C en P

comme suit : $P = D_{Kd}(C)$

où Kd est la clé de décryptage. La sécurité d'un système cryptographique ne doit pas reposer sur la clé de décryptage. La figure 1.1 présente un schéma block d'un tel système cryptographique.

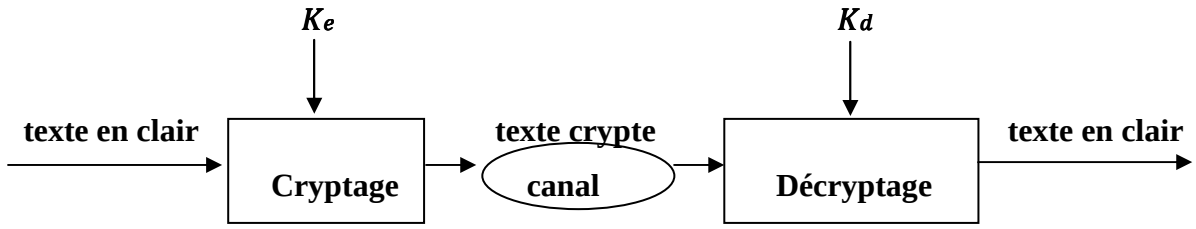


Figure I-1 : Principe d'un système cryptographique

La cryptographie est l'étude des techniques mathématiques qui sont utilisées pour accomplir plusieurs objectifs pour garantir la sécurité de communication, ces objectifs sont [14], [16]

- La confidentialité des données.
- L'intégrité des données.
- L'authentification des données et des communicants.
- La non-répudiation des données.

La confidentialité permet de protéger les informations contre tout accès non autorisé. Une partie indésirable de communication, appelée ennemi ne doit pas accéder au matériel de communication. Ceci nécessite une identification précise du destinataire, et une méthodologie permettant de rendre inutilisable l'information à tout autre qu'à ce destinataire. Cet objectif de la cryptographie est une base qui a toujours été traitée et exécutée dans toute l'histoire de la pratique cryptographique.

L'intégrité des données garantit que les informations n'ont pas été manipulées de manière non autorisée. Si l'information est modifiée pendant son passage dans le réseau, toutes les parties communicantes peuvent détecter cette modification.

L'authentification permet d'assurer que les données reçues et envoyées proviennent bien des entités déclarées. Les méthodes d'authentification sont étudiés en deux groupes ; l'authentification de l'entité et l'authentification des messages. L'authentification d'entité est le processus par lequel une partie est assurée de l'identité d'une deuxième partie impliquée dans un protocole, et que le second a effectivement participé immédiatement avant le moment où la preuve est acquise. L'authentification

des messages est un terme utilisé par analogie avec l'authentification d'origine des données. Il assure l'authentification d'origine des données par rapport à la source du message d'origine et l'intégrité des données.

La non répudiation consiste à éviter que, par la suite, les communicants nient leurs actions : l'émetteur nie avoir envoyé un message et le récepteur nie avoir reçu un message.

Heureusement, la cryptographie moderne a développé des techniques pour traiter tous les quatre buts de la cryptographie. [13], [20]

I-3 Cryptage Et Décryptage:

Les données lisibles et compréhensibles sans intervention spécifique sont considérées comme du texte en clair. La méthode permettant de dissimuler du texte en clair en masquant son contenu est appelée le cryptage. Le cryptage consiste à transformer un texte normal en charabia inintelligible appelé texte chiffré.

Cette opération permet de s'assurer que seules les personnes auxquelles les informations sont destinées pourront y accéder. Le processus inverse de transformation du texte chiffré vers le texte d'origine est appelé le décryptage.

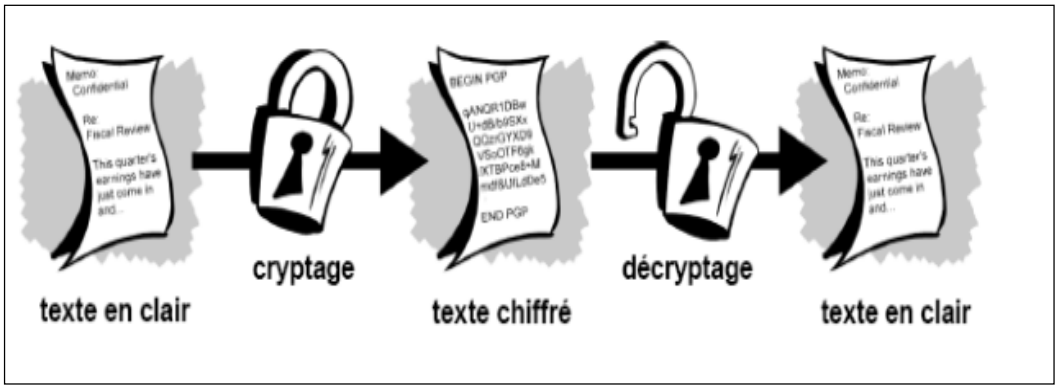


Figure I-2: cryptage et décryptage

I-3-1 Définition de la cryptographie :

a. La cryptographie est la science qui utilise les mathématiques pour le cryptage et le décryptage de données.

Elle vous permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire.

Alors que la cryptographie consiste à sécuriser les données,

b. La cryptanalyse est l'étude des informations cryptées, afin d'en découvrir le secret. La cryptanalyse classique implique une combinaison intéressante de raisonnement analytique, D'application d'outils mathématiques, de recherche de modèle, de patience, de détermination et de chance.

Ces cryptanalyses sont également appelés des pirates.

c. La cryptologie englobe la cryptographie et la cryptanalyse.

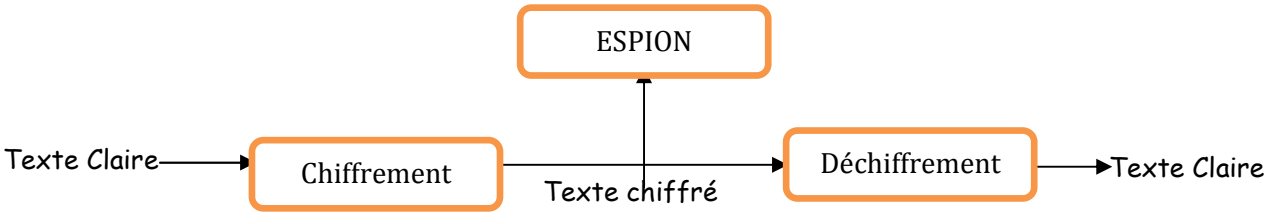


Figure I-3 : cryptage dans un canal non sécurise

I-3-2 Classes de cryptosystèmes :

La cryptographie peut être invulnérable ou vulnérable, comme décrit précédemment.

Cette vulnérabilité se mesure en termes de temps et de ressources nécessaires pour récupérer le texte en clair.

Une cryptographie invulnérable pourrait être définie comme un texte crypté particulièrement difficile à déchiffrer sans l'aide d'un outil de décodage approprié.

Mais, alors, comment déterminer cette difficulté ?

Etant donné la puissance informatique et le temps machine actuellement disponibles, il devrait être impossible de déchiffrer.

Le résultat d'une telle cryptographie avant la fin du monde (même avec un milliard d'ordinateurs effectuant un milliard de vérifications à la seconde).

On pourrait donc penser qu'une cryptographie évoluée résisterait même aux assauts d'un cryptanalyse particulièrement acharné.

Qui peut vraiment l'affirmer ?

Personne n'a encore prouvé que le meilleur niveau de cryptage pouvant être obtenu de nos jours tiendra la route avec la puissance informatique de demain. [12]

I-3-3 Mécanismes de la cryptographie :

Un algorithme de cryptographie ou un chiffrement est une fonction mathématique utilisée lors du processus de cryptage et de décryptage. Cet algorithme est Associé à une clé (un mot, un nombre ou une phrase), afin de crypter le texte en clair. Avec des clés différentes, le résultat du cryptage variera également.

La sécurité des données cryptées repose entièrement sur deux éléments :

- ✓ L'invulnérabilité de l'algorithme de cryptographie
- ✓ et la confidentialité de la clé.

Un système de cryptographie est constitué d'un algorithme de cryptographie, ainsi que de toutes les clés et tous les protocoles nécessaires à son fonctionnement.

I-4 Cryptographie symétrique et asymétrique:

En cryptographie on distingue deux approches

I-4-1 Cryptographie symétrique :

I-4-1-1 Définition :

En cryptographie symétrique, également appelée cryptage de clé secrète, ou de cryptographie conventionnelle, consiste à utiliser la même clé pour le chiffrement et le déchiffrement (Figure I-3). Le chiffrement consiste alors à effectuer une opération entre la clé privée et les données à chiffrer afin de rendre ces dernières inintelligibles. Le déchiffrement consiste à réaliser l'opération inverse c'est-à-dire récupérer le message d'origine à partir du message chiffré en utilisant la clé secrète.

Les algorithmes symétriques sont plus rapides et facilement implémentés sur le matériel. Ils sont des simples opérations de substitution et de transposition et sont mieux adaptés pour une utilisation sur le réseau Internet filaire et en mobilité. Cependant ces systèmes ne sont pas entièrement adéquats pour résoudre tous les problèmes de sécurité.

Le processus de chiffrement et déchiffrement dépend de la même clé secrète partagée entre l'émetteur et le récepteur. L'émetteur et le récepteur doivent donc se mettre d'accord sur la clé secrète avant qu'ils puissent communiquer d'une façon sécurisée. Un canal sûr d'échange de clé est difficile à établir.

Les crypto systèmes symétriques ont un problème de gestion de clé. En effet lorsqu'un grand nombre de personnes désirent communiquer ensemble, le nombre de clés augmente de façon importante et la situation devient impraticable. Pour n participants à la communication,

Il y a deux catégories de systèmes à clé privée : les chiffrements par blocs et les chiffrements de flux. [18]

I-4-1-2 Chiffrement par bloc (Block Cipher) :

C'est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique. Il consiste à un découpage des données en blocs de taille généralement fixe (souvent une puissance de deux comprise entre 32 et 512 bits). Les blocs sont ensuite chiffrés les uns après les autres. Il est possible de transformer un chiffrement de bloc en un chiffrement par flot en utilisant un mode d'opération comme ECB (chaque bloc chiffré indépendamment des autres) ou CFB (on chaîne le chiffrement en effectuant un XOR entre les résultats successifs).

Un exemple de taille de bloc et de clé utilisés par les algorithmes les plus connus:

- DES : blocs de 64 bits, clé de 56 bits.
- IDEA : blocs de 64 bits, clé de 128 bits.
- AES : blocs de 128 bits, clé de 128 à 256 bits.

Pour cette catégorie, nous allons présenter deux algorithmes très connus DES et AES en mettant l'accent sur l'AES car il est devenu le standard recommandé pour le chiffrement symétrique [04].

DES (Data Encryption Sandard) :

DES a été développé à la fin des années 1970s comme un standard du gouvernement US pour protéger l'information sensible. Le DES est officiellement défini dans la publication FIPS 46-3 et il est public. DES est encore supporté dans des outils de cryptographie pour les O.S des dispositifs mobiles et les cartes à puce. C'est un chiffrement qui transforme des blocs de 64 bits avec une clé secrète de 56 bits. Il a une conception basée sur le schéma de Feistel

au moyen de permutations et de substitutions. L'attaque de force brute est possible sur une clé DES. Cette attaque a été réalisée par DES Cracker de EFF-Electronic Frontier Fondation en juin 1998 (Elle a trouvé une clé DES dans moins de 3 jours).

Avec la technologie actuelle (des CPU très rapides et moins chers), il est hautement possible de cracker DES. La solution a été au premier temps d'adopter le triple DES (TDES ou 3DES) : 3 applications de DES à la suite avec 2 clés différentes (112 bits) (Figure I.3).

Figure I-4:Algorithme TDES

TDES utilise une taille de blocs est 64 bits et de clé comprise entre 128 bits et 192 bits.
TDES est suffisant en sécurité mais il est trois fois plus lent que DES. Un nouvel algorithme remplace DES, c'est l'AES (Advanced Encryption Standard). [08]

AES (Advanced Encryption Standard) :

En 1997, le NIST (National Institue of Standards and Technology) a lancé un appel d'offre pour un algorithme de chiffrement symétrique avec un bloc de taille 128 bits et supporte des clés de 128, 192 et 256 bits. Les critères d'évaluation de l'offre comprenaient la sécurité, la puissance de calcul, les contraintes de la mémoire des petits dispositifs (comme la carte à puce), la plateforme logicielle et matérielle et la flexibilité. Un total de 15 algorithmes ont été envoyés et 5 ont été sélectionné parmi ces 15 algorithmes [07].

L'algorithme de Rijndael a été sélectionné pour devenir l'AES en 2001. Rijndael a été conçu par Joan Daemen et Vincent Rijmen, deux chercheurs de la Belgique. Les autres algorithmes sont : Serpent, Twofish, RC6, et MARS. L'AES n'utilise pas le schéma de Feistel mais il utilise des opérations mathématiques comme des substitutions, des permutations et des XORs. Il a plusieurs rounds identiques (de 10 à 14) et leur nombre dépend de la taille de la clé. L'AES opère au niveau octet ce qui permet une implémentation efficace au niveau matérielle et logicielle. L'AES est un standard, donc libre d'utilisation, sans restriction d'usage ni brevet. NIST spécifie actuellement AES dans le document FIPS 197, comme le nouveau

standard de chiffrement symétrique. AES est approuvé pour utilisation par les organisations du gouvernement U.S pour protéger l'information sensible non classifiée.

AES a trois niveaux forts de sécurité : 128 bits, 192 bits et 256 bits. La sécurité 128 bits fournira au mois 30 ans de protection. AES ne fournit pas seulement une sécurité supérieure à TDES mais il délivre aussi une meilleure performance.

Une meilleure sécurité et une meilleure performance rendent l'AES une alternative plus attractive que TDES et un bon choix pour un algorithme de chiffrement symétrique [07].

AES est également un candidat particulièrement approprié pour les dispositifs mobiles limités en ressources de calcul et de stockage. Le monde de la 3G (3ème génération de dispositifs mobiles) a adopté l'algorithme AES pour son schéma d'authentification.

Autres finalistes d'AES :

Durant la compétition avec AES, Serpent et Twofish avaient une performance faible comparée à Rijndael. RC6 et MARS ont des problèmes de sécurité et d'efficacité. RC6 a été cassé à au moins de 17 rounds sur 20 pendant la compétition avec AES. MARS était plus couteux en calcul pour l'implémenter comparé aux autres finalistes d'AES [08].

I-4-1-3 Chiffrements de flux (StreamCipher) :

Les algorithmes de chiffrement de flux peuvent être définis comme étant des algorithmes de chiffrement par blocs, où le bloc a une dimension unitaire (1 bit, 1 octet, etc.) ou relativement petite. Leurs avantages principaux viennent du fait que la transformation (méthode de chiffrement) peut être changée à chaque symbole du texte clair et du fait qu'ils soient extrêmement rapides. De plus, ils sont utiles dans un environnement où les erreurs sont fréquentes car ils ont l'avantage de ne pas propager les erreurs (diffusion). Ils sont aussi utilisés lorsque l'information ne peut être traitée qu'avec de petites quantités de symboles à la fois [09].

Quelques algorithmes de cryptographie symétrique par flot:

- A5 : utilisé dans les téléphones mobiles de type GSM pour chiffrer la communication par radio entre le mobile et l'antenne-relais la plus proche.
- RC4, le plus répandu, conçu par Ronald Rivest, utilisé notamment par le protocole WEP, un algorithme récent de Eli Biham – E0 utilisé par le protocole Bluetooth.

une seule clé suffit pour le cryptage et le décryptage.

La norme de cryptage de données (DES) est un exemple de système de cryptographie conventionnelle largement utilisé par le gouvernement fédéral des Etats-Unis.

Le chiffrement de substitution est un exemple extrêmement simple de cryptographie conventionnelle. Il substitue une information par une autre. Cette opération s'effectue généralement en décalant les lettres de l'alphabet. Le code secret de Jules César est à la base de la cryptographie conventionnelle. Dans ce cas, l'algorithme constitue à décaler les lettres de l'alphabet et la clé correspond au nombre de caractères de décalage.

Par exemple :

si vous codez le mot « SECRET » à l'aide de la valeur 3 de la clé de César, l'alphabet est décalé de manière à commencer à la lettre D.

Ainsi, l'alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

si vous décalez le début de 3 lettres, vous obtenez

DEFGHIJKLMNOPQRSTUVWXYZABC

où D = A, E = B, F = C, etc.

Avec ce procédé, le texte en clair « SECRET » est crypté en « VHFUHW ».

Pour autoriser un autre utilisateur à lire le texte chiffré, indiquez-lui que la valeur de la clé est égale à 3.

Evidemment, ceci est considéré comme une cryptographie extrêmement vulnérable de par les standards actuels. Mais, cette méthode convenait à César et illustre le mode de fonctionnement de la cryptographie conventionnelle.

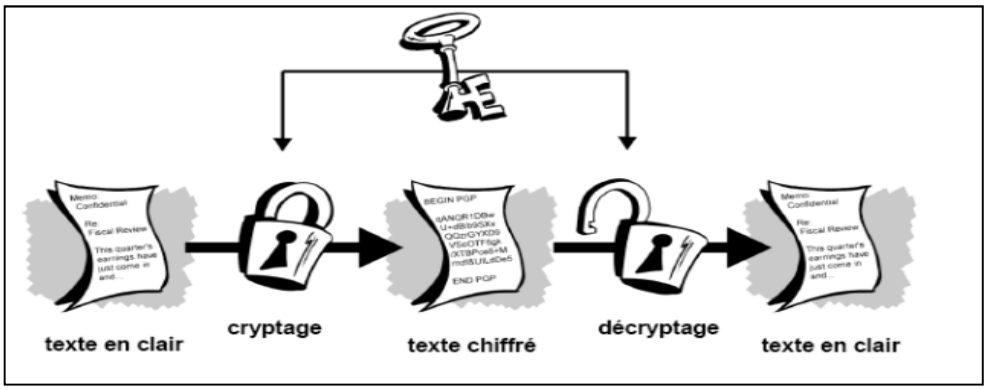


Figure I-5 : cryptage a clé privé

I-4-1-4 Gestion des clés et cryptage symétrique:

Le cryptage symétrique comporte des avantages. Il est très rapide. Mais, il s'avère particulièrement utile pour les données véhiculées par des moyens de transmission sécurisés.

Toutefois, il peut entraîner des coûts importants en raison de la difficulté à garantir la confidentialité d'une clé de cryptage lors de la distribution.

Un expéditeur et un destinataire souhaitant communiquer de manière sécurisée à l'aide du cryptage symétrique doivent convenir d'une clé et ne pas la divulguer.

S'ils se trouvent à des emplacements géographiques différents, ils doivent faire confiance à un coursier, au téléphone de Batman ou à tout autre moyen de communication sécurisé pour éviter la divulgation de la clé secrète lors de la transmission. Toute personne interceptant la clé lors d'un transfert peut ensuite lire, modifier et falsifier toutes les informations cryptées ou authentifiées avec cette clé.

De la norme de cryptage de données DES au code secret de Jules César, la distribution des clés reste le problème majeur du cryptage symétrique.

Autrement dit, comment faire parvenir la clé à son destinataire sans qu'aucune personne ne l'intercepte?

I-4-1-5 Avantages de la cryptographie symétrique :

Les avantages de la cryptographie symétrique sont:

- ✓ Système rapide du chiffrement/déchiffrement;
- ✓ Clés relativement courtes (128 ou 256 bits);
- ✓ Bonnes performances et sécurité bien étudié;

I-4-1-6 Inconvénients de la cryptographie Symétrique :

Les inconvénients de la cryptographie symétrique sont:

- ✓ Gestion des clés difficiles (nombreux clés) ;
- ✓ Point faible = l'échange de la clé secrète ;
- ✓ Dans un réseau de N entités susceptibles de communiquer secrètement il faut distribuer N*(N-1)/2 clés.

I-4-1-7Considérations de sécurité pour la cryptographie symétrique :

Lorsqu'on utilise la cryptographie à clé symétrique, nous devons considérer certains principes qui constituent les critères de base pour implémenter une sécurité fiable et efficace.

Choix de l'algorithme de chiffrement symétrique, la taille du bloc et la clé symétrique

Il y a plusieurs méthodes d'attaques pour trouver des vulnérabilités dans les crypto systèmes symétriques en mode bloc. Les problèmes de collision sont plus dominants dans les cryptages de bloc de 64 bits comparés à ceux de 128 bits [08]. Il est donc fondamental d'utiliser des chiffrements de bloc de 128 bits.

L'utilisation de la clé symétrique n'est pas la même pour chaque crypto système, et certaines initialisations des clés peuvent casser la sécurité offerte par l'algorithme. Par exemple, DES a un problème de clé faible et semi-faible (weak and semi-weak key). DES a 4 clés faibles et 16 clés semi-faibles. Le développeur est obligé de tester pour voir si la clé utilisée est faible ou non.

Un autre algorithme symétrique RC4 a une contrainte : la même clé ne doit jamais être utilisée pour chiffrer deux suites d'octets différentes parce que la sortie du générateur est XORé avec la suite d'octets. On trouve cette faiblesse de sécurité dans le standard WEP (Wired Equivalent Privacy) qui utilise RC4 pour chiffrer les communications sans fil sur les réseaux 802.11. Le problème avec le WEP est la taille faible de la clé. Les produits WEP implémentent une clé partagée de 64 bits, 40 bits pour la clé secrète et 24 bits pour le vecteur d'initialisation

(IV-Initial Vector). Le WEP n'alloue pas suffisamment de bits pour le vecteur d'initialisation, donc la même valeur de l'IV sera réutilisée, et plusieurs paquets seront chiffrés avec la même clé[08].

Donc une règle fondamentale dans les crypto systèmes symétrique : Chaque crypto système symétrique utilise une structure de clé différente.

L'AES est l'algorithme le plus efficace et le plus rapide pour les plateformes logicielles et matérielles, et est le mieux approprié sur les dispositifs mobiles et PDAs. Il est donc recommandé d'utiliser l'AES pour le chiffrement/déchiffrement symétrique.

I-4-1-8 Authentifier le chiffrement symétrique :

Les modes de chiffrement protègent les données de l'écoute mais ils ne fournissent aucune authentification. La fonction de déchiffrement déchiffre juste les données, elle peut déchiffrer un texte chiffré déjà modifié, en un certain plaintext qui est différent du plaintext d'origine. Dans un tel cas, il est recommandé de produire un code d'authentification du message MAC (Message Authentication Code), du texte chiffré et ajouter ce MAC au texte chiffré.

Utiliser le chiffrement en mode bloc au lieu du chiffrement par flot : Il est recommandé

d'utiliser le mode de chiffrement en bloc (CBC ou CTR) avec un vecteur d'initialisation générée d'une manière aléatoire. Un vecteur d'initialisation mal choisi peut causer une faiblesse de sécurité (le cas de RC4 avec le protocole WEP).

I-4-2 Cryptographie asymétrique (de clé publique) :

I-4-2-1 Définition :

Les problèmes de distribution des clés sont résolus par la cryptographie de clé publique. Ce concept a été introduit par Whitfield Diffie et Martin Hellman en 1975.

La cryptographie de clé publique est un procédé asymétrique utilisant une paire de clés pour le cryptage : une clé publique qui crypte des données et une clé privée ou secrète correspondante pour le décryptage.

Vous pouvez ainsi publier votre clé publique tout en conservant votre clé privée secrète.

Tout utilisateur possédant une copie de votre clé publique peut ensuite crypter des informations que vous êtes le seul à pourvoir lire. Même les personnes que vous ne connaissez pas personnellement peuvent utiliser votre clé publique.

D'un point de vue informatique, il est impossible de deviner la clé privée à partir de la clé publique. Tout utilisateur possédant une clé publique peut crypter des informations, mais est dans l'impossibilité de les décrypter. Seule la personne disposant de la clé privée correspondante peut les décrypter.

La cryptographie de clé publique présente un avantage majeur : en effet, elle permet d'échanger des messages de manière sécurisée sans aucun dispositif de sécurité. L'expéditeur et le destinataire n'ont plus besoin de partager des clés secrètes via une voie de transmission sécurisée. Les communications impliquent uniquement l'utilisation de clés publiques et plus aucune clé privée n'est transmise ou partagée.

Elgamal (d'après le nom de son inventeur, Taher Elgamal),

RSA (d'après le nom de ses inventeurs, Ron Rivest, Adi Shamir et LeonardAdleman), Diffie-Hellman (également d'après le nom de ses inventeurs) et DSA, l'algorithme de signature numérique (élaboré par David Kravitz), sontdes exemples de systèmes de cryptographie de clé publique.

La cryptographie symétrique étant auparavant la seule méthode pour transmettre des informations secrètes, les coûts de transmission et de distribution sécurisée des clés ont relégué son utilisation aux institutions disposant de moyens suffisants, telles que des gouvernements et des banques.

Le cryptage de clé publique représente une révolution technologique qui offre à tout citoyen la possibilité d'utiliser une cryptographie invulnérable.

Le cryptage symétrique est environ 1 000 fois plus rapide que le cryptage de clé publique.

De plus, le cryptage de clé publique résout non seulement le problème de la distribution des clés, mais également de la transmission des données. Utilisées

Conjointement, ces deux méthodes améliorent la performance et la distribution des clés, sans pour autant compromettre la sécurité. [19], [21]

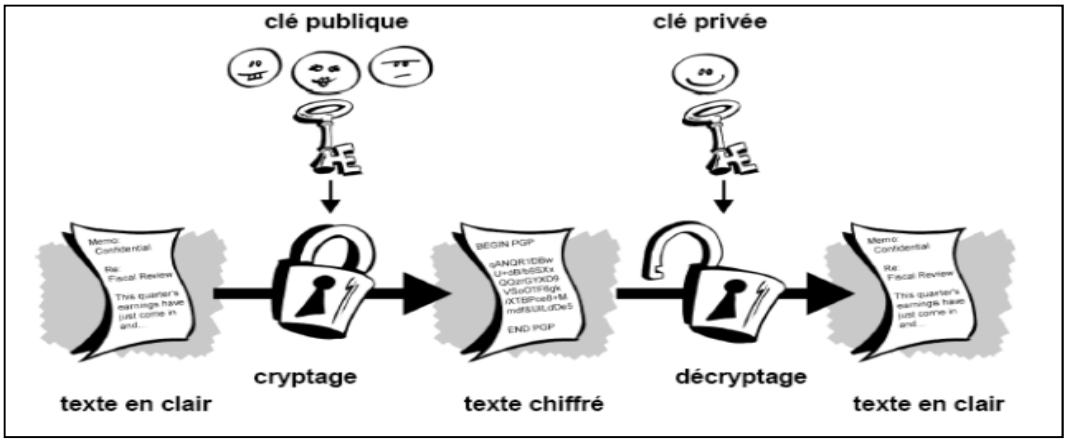


Figure I-6: cryptage a clé publique

I-4-2-2 Les Clés :

Une clé est une valeur utilisée dans un algorithme de cryptographie, afin de générer un texte chiffré. Les clés sont en réalité des nombres extrêmement importants.

La taille d'une clé se mesure en bits et le nombre correspondant à une clé de 1 024 bits est gigantesque. Dans la cryptographie de clé publique, plus la clé est grande, plus la sécurité du texte chiffré est élevée.

Cependant, la taille de la clé publique et de la clé secrète de cryptographie symétrique sont complètement indépendantes.

Une clé symétrique de 80 bits est aussi puissante qu'une clé publique de 1024 bit. De même, une clé symétrique de 128 bits équivaut à une clé publique de 3 000 bits.

Encore ne fois, plus la clé est grande, plus elle est sécurisée, mais les algorithmes utilisés pour chaque type de cryptographie sont très différents.

I-4-2-3 Avantages de la cryptographie asymétrique :

Les avantages de la cryptographie asymétrique sont:

- ✓ Gestion de la secrète facilitée ;
- ✓ Pas de secrète à transmettre ;
- ✓ Nombre de clés à distribuer est réduit par rapport aux clés symétriques ;
    1. Très utile pour échanger les clés ;
    2. Permet de signer des messages facilement ;

I-4-2-4 Inconvénients de la cryptographie asymétrique

Les inconvénients de la cryptographie asymétrique sont:

- ✓ La relation clé publique /clé privée impose :
- ✓ Des clés plus longues (1024 à 4096 bits) ;
- ✓ Gestion de certificats de clés publiques ;
- ✓ Lenteur de calcul;
- ✓ Pas d'authentification de la source.

I-4-3 Notions élémentaires de cryptographie :

Même si les clés publiques et privées sont liées par une relation mathématique, il est très difficile de deviner la clé privée uniquement à partir de la clé publique.

Cependant, la déduction de la clé privée est toujours possible en disposant de temps et de puissantes ressources informatiques. Ainsi, il est très important de sélectionner des clés de tailles correctes, suffisamment grandes pour être sécurisées, mais suffisamment petites pour être utilisées assez rapidement.

De plus, vous devez tenir compte du profil des utilisateurs tentant de lire vos fichiers, connaître leur détermination, le temps dont ils disposent, ainsi que de leurs ressources.

Plus la clé est grande, plus sa durée de sécurisation est élevée. Si les informations que vous souhaitez crypter doivent rester confidentielles pendant plusieurs années, vous pouvez utiliser une clé correspondant à un nombre de bits extrêmement élevé. Qui sait combien de temps sera nécessaire pour deviner votre clé avec la technologie de demain ? Il fut un temps où une clé symétrique de 56 bits était considérée comme extrêmement sûre. [31]

I-5 Fonctions et moyens de la cryptologie :

I-5-1 LE Cadre :

Deux interlocuteurs, A et B, échangeant des données sur un canal de communication public ou une seule personne archivant puis lisant des données stockées sur un support. La cryptographie va permettre d'empêcher les mésactions de l'environnement E, que celui-ci soit un espion ou simplement du bruit qui vient altérer les communications.

Fonction	Description	Moyen
Confidentialité	Empêcher E de consulter	Chiffrement
Intégrité	Empêche E de modifier	Production d'un condensat du message
Authentification	Permet à A d'être sûr de communiquer avec B et non E	Signature par B d'un nombre aléatoire (condensat de son message, challenge de A, etc.)
Notariat / Non-répudiation	Empêche A de se défausser comme émetteur du message	Signature du message : A est le seul à pouvoir signer le message d'une certaine façon
Certification	Confirmation par C de l'identité de A pour B (en cas de vol par E de tous les secrets de B)	Signature d'un certificat

TABLEAU I-1 : Les principaux techniques en cryptographie

I-5-2-1 Définition des termes employés dans le tableau ci-dessus :

Condensat : Partant d'une quantité d'information, un condensat est un résumé, mais tel qu'il soit difficilement possible de trouver deux informations correspondant au même condensat

Signature : Chiffrement d'une information avec une clé privée

Certificat : Signature avec une clé privée délivrée par un organisme certificateur d'une identité

I-5-2-2 Remarque :

Notons que l'on peut combiner les "moyens" pour garantir qu'une communication satisfait plusieurs fonctions. Par exemple, si l'on désire une communication confidentielle, intègre et authentifiée, on peut utiliser un algorithme de chiffrement à clé publique et un calcul de condensat.

Le protocole est le suivant :

A chiffre son message avec la clé publique de B : ceci assure la confidentialité de la communication, puisque seul B est capable de déchiffrer le message.

A envoie avec le message chiffré un condensat du message clair : ceci permet à B de vérifier que le message qu'il a déchiffré est bien le même que celui qui a été émis par A (du moment que les deux condensats sont égaux).

A 'envoie en fait pas le condensat du message clair, mais le chiffrement de ce condensat avec sa clé privée : ceci permet à B de vérifier que le condensat à été "signé" par A, car lui seul est un mesure de chiffrer avec sa clé privée. On assure donc l'authentification de A. Notons que comme le condensat change à chaque message envoyé, la "signature" ne peut pas être copiée telle quelle par E pour prétendre être A.

I-6 CRYPTOGHRAPHIE EN FUTUR :

Dans l'histoire, beaucoup de codes étaient considérés comme inviolables mais ont été cassés (Vigenère, Enigma, ...). Les systèmes actuels à clés publiques sont-ils alors menacés ? Quoi qu'il en soit, on se tourne maintenant vers une nouvelle sorte de cryptographie, ne reposant pas sur l'aspect déterministe des mathématiques, mais sur l'aspect probabiliste de la physique, donc sur les lois-mêmes de la nature, et non pas sur l'ignorance de l'homme sur certains points. Ces travaux se basent sur les recherches de Stephen Wiesner dans les années 60, qui inventa le principe de cryptographie quantique.

Mais, chose que l'on peut considérer surprenante, leur publication avait été rejetée.

Les fondements de la cryptographie quantique ont été établis, entre autres, par les travaux de 1984 de Charles H. Bennett et Gilles Brassard.

I-7 Conclusion

Un concepteur de système cryptographique est toujours entrain d'essayer d'élaborer un système de chiffrement plus sure mais en même temps des intrus essayent de casser ce dernier, ils se livrent constamment une bataille mais les enjeux sont énorme : c'est la sécurité de nos transmissions qui est menacée.

Dans ce chapitre nous avons présenté une introduction générale sur la cryptographie, en a retrouver deux grandes classes des méthodes de chiffrement, les cryptographies symétriques à clé secrète et le cryptage asymétrique à clé publique, je suis intéressé dans mon mémoire par laFR Cryptographie asymétrique (de clé publique) .

Chapitre II

Les courbes Elliptiques

Et Notions Algébrique

II-1 Introduction:

En cryptographie, les courbes elliptiques, les objets mathématiques, peuvent être utilisés pour des opérations asymétriques comme des échanges de clés sur un canal non-sécurisé ou un chiffrement asymétrique, on parle alors de cryptographie sur les courbes elliptiques ou ECC (de l'acronyme anglais Elliptic curve cryptography).

L'usage des courbes elliptiques en cryptographie a été suggéré, de manière indépendante, par "Neal Koblitz" et " Victor Miller " en 1985.

Nous verrons qu'il existe des tests de primalité et des algorithmes de factorisations utilisant les courbes elliptiques et finalement nous verrons comment compter les points sur certaines courbes elliptiques. Ces derniers aspects sont indissociables de ce genre de systèmes de cryptage.

II-2 Notions algébriques :

II-2-1 La structure de groupe :

Un groupe G est un ensemble muni d'une loi de composition interne : $(x, y) \rightarrow x * y$ qui possède les propriétés suivantes :

1. Elle est associative, c'est-à-dire que, si x, y, z sont des éléments de G, on a :

$(x * y) * z = x * (y * z)$.

2. Elle admet un élément neutre, c'est-à-dire qu'il existe un élément $e \in G$ tel que, pour tout $x \in G$: $x * e = e * x = x$.

3. Tout élément x de G admet un symétrique, c'est-a-dire qu'il existe un élément de G,

Noté x^{-1} , tel que : $x^{-1} * x = x * x^{-1}. = e$

Un groupe est dit abélian (commutatif), si la loi de composition est commutative, c'est-à-dire

si $x * y = y * x$ pour tout couple d'éléments de G. [17]

II-2-2 Ordre d'un élément dans un groupe :

Si x est un élément d'un group G, l'ordre de x étant le plus petit entier positif n tel que

$$x^n = \underbrace{x*x*\ldots\ldots*x}_{n \text{ fois}}$$

, (on écrit $nx = e$, si la loi de G est noté additivement). Si un tel entier n n'existe pas on dit que l'ordre de x est infini.

Notons aussi que le nombre des éléments de G (si G est fini) est appelé l'ordre du groupe G. [04], [10]

II-2-3 Définition d'un anneau :

Un anneau $\mathbf{k}$ est un ensemble muni de deux lois (+) et (*) telles que :

1. ($\mathbf{k}$,+) est un groupe abelien;
2. la loi (*) est associative et admet un neutre 1;
3. la multiplication est distributive par rapport à l'addition

$x * (y + z) = x * y + x * z$; $(y + z) * x = y * x + z * x$.

II-2-4 Qu'est-ce qu'un corps ?

Un corps est un anneau dans lequel tout les éléments non nul sont inversibles par rapport à la multiplication. Il revient au même dire : $\mathbf{k}$ est un corps s'il est muni de deux lois (+) et (*) , satisfaisant les propriétés suivants:

1) ($\mathbf{k}$, +) est un groupe abelien (avec l'addition) et l'élément neutre est 0.

2) ($\mathbf{k} \setminus \{0\}$, *) est un groupe dans lequel l'élément neutre est noté 1 .

3) La loi (*) est distributive par rapport à (+)

$x * (y + z) = x * y + x * z$ et $(y + z) * x = y * x + z * x$ pour tout x, y, z $\in \mathbf{K}$

Si l'ensemble $\mathbf{K}$ est fini, alors le corps est dit fini

Notons que le groupe multiplicative d'un corps fini est toujours abelian, d'après un théorème bien connue de Wedderburn. Dans un corps $\mathbf{k}$, l'ordre de 1 dans le groupe additive de $\mathbf{k}$ est appelé la caractéristique de $\mathbf{k}$. La caractéristique d'un corps est soit infinie ou soit un nombre premier. Les corps de caractéristique 2 sont appelés les corps binaires. Il en résulte que la caractéristique d'un corps fini $\mathbf{k}$ est forcément égale à un nombre premier p. Dans ce cas, q le nombre des éléments de $\mathbf{k}$ est une puissance de p, c.à.d $q=p^m$ pour certain entier positif m.

La notation utilisée pour un tel corps est $\mathbf{F_q}$,

Puisque il existe un seul corps qui a q éléments (à isomorphisme prés). En particulier $\mathbf{F_q}$ est appelé le corps premier de caractéristique p. [11]

II-2-5 Définition d'un corps fini:

un corps fini appelé aussi un corps de Galois noté GF(p) tel que p est un nombre premier est un corps à p éléments dans lequel on définit deux opérations : l'addition et la multiplication modulo p. [04]

II-2-6 Théorème1 :

Soit p un nombre premier ($p \geq 2$) et r un entier ($r \geq 1$), pour toutes valeurs de $q = p^r$ Il existe un et un seul corps fini GF(q). [10]

II-2-7 Théorème 2:

Soit un entier ($p \geq 2$), l'ensemble Zp = {0, 1, 2, 3,…, p-1}, muni de l'addition et de la multiplication définis modulo p, est un corps si et seulement si p est un nombre premier. [17]

Exemple :

Soit p=5, Zp= {0, 1, 2, 3, 4}, les opérations de l'addition et de la multiplication dans GF(5) sont définit par les tableaux suivants :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table II-1 : La multiplet dans le corps de Galois GF(5)

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	2	0
3	0	3	2	1	0
4	0	4	0	0	0

Table II-2 : L'addition dans le corps de Galois GF(5)

II-2-8 Propriétés sur les corps:

- Si un corps K est de caractéristique nulle, il contient une copie de Q. S'il est de caractéristique p, il contient une copie de Z/pZ
- Comme pour tout anneau intègre, la caractéristique de K est soit nulle soit un nombre premier p. Dans le premier cas, l'unique homomorphisme d'anneaux unitaires $\mathbb{Z} \longrightarrow \mathbb{K}$ est injectif ; comme K est un corps, il induit une injection du corps des fractions de Z, à savoir le corps des rationnels Q (par définition des rationnels). Dans le deuxième cas, l'unique homomorphisme d'anneaux unitaires $\mathbb{Z} \longrightarrow \mathbb{K}$induit une injection de Z/pZ dans K. Or, comme p est premier, Z/pZ est un corps fini ; c'est l'unique corps fini Fp à p éléments.
- Tout corps fini a pour cardinal une puissance d'un nombre premier, qui en est sa caractéristique.
- Si K est un corps fini, pour des raisons de cardinalité, il ne peut pas contenir une copie de Q. Par ce qui précède, il est de caractéristique finie p et contient donc une copie du corps Fp. De fait, K est un espace vectoriel sur Fp ; sa dimension est nécessairement finie. Donc son cardinal est p à la puissance sa dimension.[17]

II -3 les courbes elliptiques :

Les courbes elliptiques destinées aux applications cryptographiques doivent être définies sur un corps premier F_p ou sur un corps binaire fini F_2^n.

Les crypto systèmes utilisant les courbes elliptiques définies sur F_2^n doivent se plier à certaines exigences pour garantir une meilleure sécurité. De telles courbes sont de moins en moins utilisées car le corps F_2^n est considéré comme trop structuré. Cependant les calculs sur de tels crypto systèmes ont l'avantage d'être plus faciles à implémenter.

Les crypto systèmes utilisant les courbes elliptiques définies sur les corps finis de la forme F_p peuvent être compromis par l'attaque (eg : MOV). La taille des clés utilisées doit alors respecter les critères de sécurité appliqués au problème du logarithme discret dans un corps fini, on perd alors l'intérêt d'utiliser les courbes elliptiques [15].

II-3-1 Propriétés générales des courbes elliptiques :

II-3-1-1 Définition1:

Soit K un corps, on appelle équation de Weierstrass sur K une équation du type

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

Avec $a_1 \in K$. Une courbe donnée par une telle équation est dite lisse si le système suivant n'admet pas de solution. [06]

$$a_1y = 3x^2 + 2a_2x + a_4$$

$$2y + a_1x^2 + a_3 = 0$$

Autrement dit si les dérivées partielles en x et en y de

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

Ne s'annulent pas en même temps.

Une courbe elliptique E définie sur K est une courbe lisse donnée par une équation de Weierstrass définie sur K à laquelle on a rajouté un point " à l'infini ", noté O ;

$$E = \{(x,y)2K^2: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{o\}$$

Si la caractéristique de K (char(K)) n'est pas 2 ni 3, alors en faisant les deux changements de variables successifs $y \leftarrow \frac{1}{2}(y - a_1x - a_3)$ et ensuite

$(x,y) \leftarrow (\frac{x-3b_2}{36}, \frac{y}{216})$ dans E, ou $b_2 = a_1^2 + 4a_2$, nous obtenons

$$E: y^2 = x^3 - 27c_4x - 54c_6 ,$$

Avec $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$, $c_4 = b_2^2 + 24b_4$,

$c_6 = -b_2^3 + 36b_2b_4 - 216b_6$.

II-3-1-2 Définition2:

Le discriminant Δ de l'équation de Weierstrass est la quantité

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

et le j-invariant de la courbe elliptique E est la quantité [05]

$$j(E) = \frac{c_4^3}{\Delta}$$

II-3-1-3 Corollaire:

soit un corps K de caractéristique p. une courbe E définie sur K donnée par une équation de Weierstrass prend alors une forme simplifiée.[7]

1. si $p \neq 2$ et $p \neq 3$,

$y^2 = x^3 + a_4x + a_6$ $\quad \Delta = -16(4a_4^3 + 27a_6^2)$

$$j(E) = 1728(\frac{4a_4^3}{4a_4^3+27a_6^2})$$

2- si $p = 2$ et si $j(E) \neq 0$,

$y^2 + a_1xy = x^3 + a_4x^2 + a_6$ $\quad \Delta = a_6$, $\quad j(E) = \frac{1}{a_6}$,

Si $p = 2$ et si $j(E) = 0$,

$y^2 + a_3y = x^3 + a_4x + a_6$, $\quad \Delta = a_3^4$ $\quad j(E) = 0$,

3- si $p = 3$et si $j(E) \neq 0$,

$y^2 = x^3 + a_2x^2 + a_6$, $\quad \Delta = -a_2^3a_6$ $\quad j(E) = \frac{a_2^3}{a_6}$;

Si $p = 3$ et si $j(E) = 0$,

$y^2 = x^3 + a_4x + a_6$, $\quad \Delta = a_4^3$ $\quad j(E) = 0$,

Preuve:

(1) Si $p \neq 2$, nous pouvons remplacer y par $(y - \frac{1}{2}(a_1x + a_3))$.

nous obtenons alors

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} .$$

de surcroît, si $p \neq 3$, alors nous remplaçons x par $(x - \frac{b_2}{12})$pour obtenir

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}.$$

(2) l'invariant (en caractéristique2) de l'équation générale de Weierstrass

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

Vaut $j(E) = \frac{a_1^{12}}{\Delta}$. Si $j(E) = 0$, et donc si $a_1 = 0$, alors la substitution

$x \leftarrow (x + a_2)$ Donne

$y^2 + a_3y = x^3 + (a_2^2 + a_4)x + (a_2^3 + a_4a_2 + a_6)$; sinon, nous remplaçons (x, y)par $((a_1^2x + \frac{a_3}{a_1}), a_1^3y + \frac{(a_1^2+a_3^2)}{a_1^3})$ pour avoir

$$y^2 + xy = x^3 + (\frac{(a_1a_2+a_3)}{a_1^3})x^2 + \frac{a_1^4a_4^2+a_3^4+a_1^5a_3a_4+a_1^3a_3^3+a_1^4+a_2+a_3^2+a_1^6a_6}{a_1^{12}}.$$

(3) en (1), nous avons montré que si $p \neq 2$, alors $y^2 = x^3 + a_2x^2 + a_4x + a_6$. L'invariant de cette courbe (en caractéristique 3) vaut $j(E) = \frac{a_2^2}{\Delta}$. Si $j(E) = 0$, alors $a_2 = 0$ et nous avons l'expression demandée ; sinon il suffit de remplacer x par $(x + \frac{a_4}{a_2})$ pour obtenir $y^2 = x^3 + a_2x^2 + \frac{(2a_2^2a_4^2+a_2^3+a_4^3)}{a_2^3}$ [02]

Remarque :

Si char(p) ≠2, 3, nous pouvons toujours travailler avec des courbes elliptiques de la forme

$$E: y^2 = x^3 + Ax + B.$$

Dans ce cas la courbe est lisse si $4A^3+27B^2 \neq 0$.

Modifier ces coefficients va modifier la forme de la courbe, voici deux possibilités parmi une infinité :

On remarque que ces courbes ne s'intersectées jamais avec elles-mêmes. C'est la définition géométrique de la non-singularité. Algébriquement, cela nécessite de calculer le discriminant de la courbe :[03]

$$\Delta = -16(4a^3 + 27b^2)$$

Un discriminant différent de zéro indique une courbe non-singulière.

Le facteur (-16) peut paraître inutile à ce stade mais il intervient dans l'étude plus avancée des courbes elliptiques.

Une courbe non-singulière peut dès lors prendre deux formes :

- discriminant positif, la courbe présente deux composantes (image Fig. II.1) avec deux courbes séparées et un discriminant de 13392)

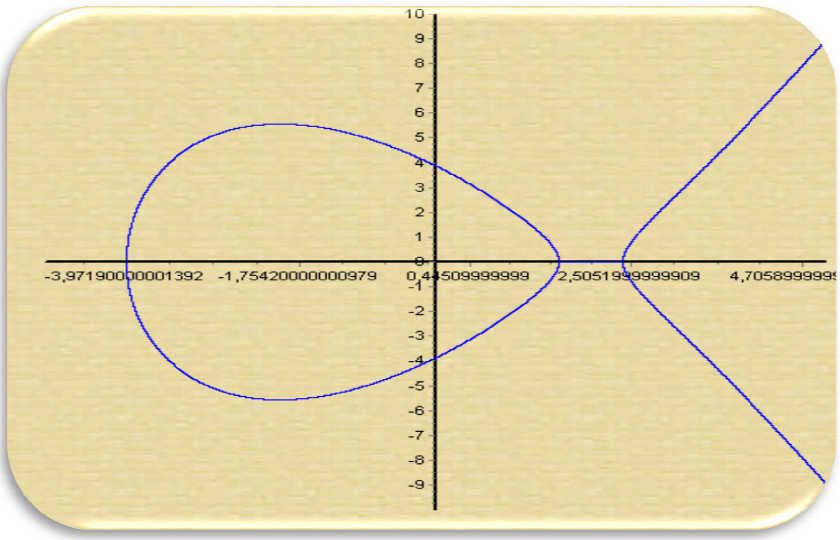


Figure II-1 : Courbe elliptique d'équation $y^2 = x^3 - 12x + 15$.

- discriminant négatif, la courbe présente une seule composante (image (Fig.II.2), discriminant de -2800)

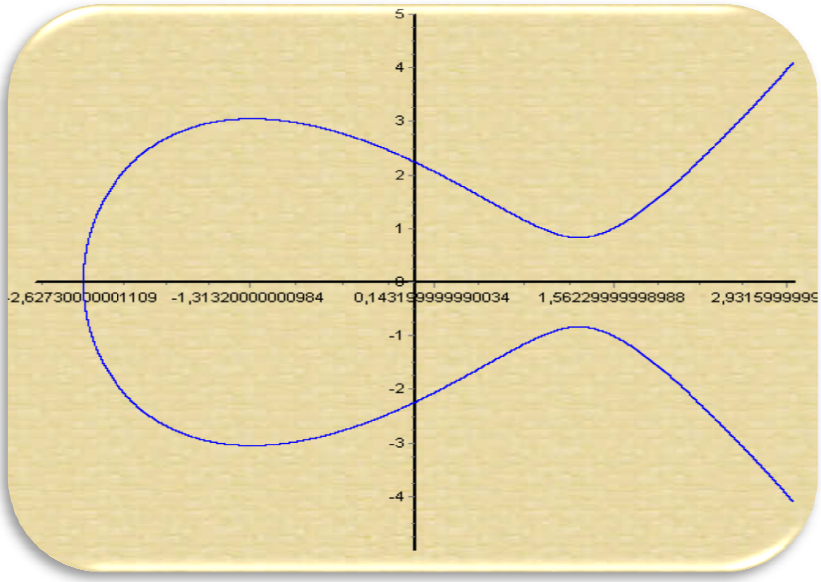


Figure II-2 : Courbe elliptique d'équation $y^2 = x^3 - 5x + 5$.

- Un discriminant égale a Zéro indique que le courbe et singulière image(Fig.II.3).

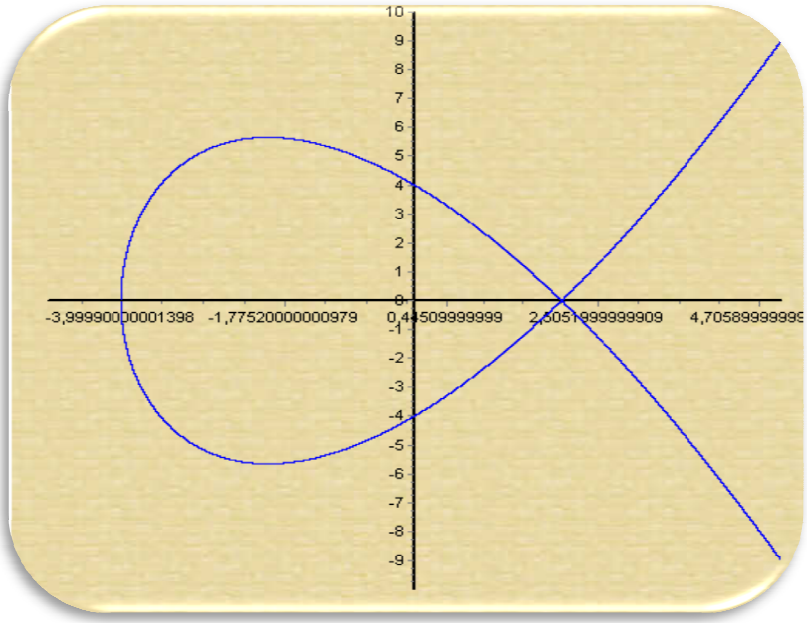


Figure II-3 : Courbe elliptique d'équation $y^2 = x^3 - 12x + 16$

II-3-2 La structure de groupe:

Soient E une courbe elliptique définie sur un corps K,

Et deux points $P_1, P_2 \in E(K)$, L la droite reliant P_1 à P_2 (la tangente à E si $P_1 = P_2$) et R le troisième point d'intersection de L avec E. Soit L0 la droite verticale passant par R.

On définit $P_1 + P_2 \in E(K)$ comme étant le deuxième point d'intersection de L0 avec E. Muni de cette loi de composition (E(K), +) est un groupe abélien dont l'élément neutre est le point à l'infini (O).[08]

Regardons géométriquement ce qui se passe lorsque nous additionnons deux points sur une courbe elliptique sur R.

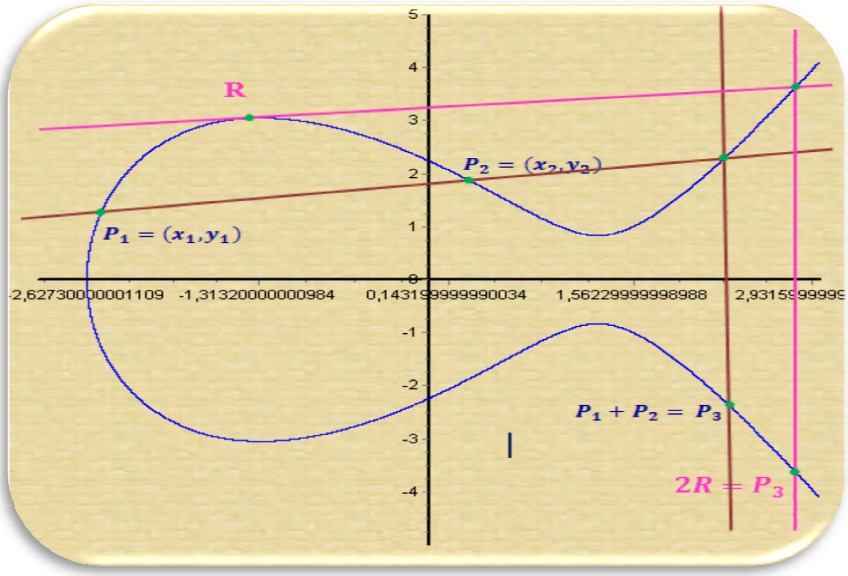


Figure- II-4 : Courbe elliptique d'équation $y^2 = x^3 - 5x + 5$

II-3-2-1 Loi de groupe:

Nous allons donner une manière explicite de calculer la somme de deux points d'une courbe elliptique.

Avec cette définition l'opération est bien commutative, associative, ayant O pour élément neutre.

Supposons que la courbe soit donnée par son équation générale de Weierstrass.[06]

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x_2 + a_4 x + a_6 .$$

Si $P_1 = (x_1, y_1) \neq O$ alors. $-P_1 = (x_1, -y_1 + a_1 x_1 + a_3)$ On se rend compte aussi que $P_1 + P_2 = -R'$.

Posons $P_2 = (x_2, y_2) \neq -P_1$ et $R = (P_1 + P_2) = (x_3, y_3)$.

$$\begin{cases} x_3 = -a_2 + \lambda^2 + a_1\lambda - x_1 - x_2 \\ y_3 = -(\lambda x_3 + \gamma) - a_1 x_3 - a_3 \end{cases}$$

$\gamma = y_1 - \lambda x_1$

1) si $P_1 = P_2$ $\qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1}$

2) si $P_1 \neq P_2$ $\qquad \lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}$

II-3-2-2 Caractéristique $\neq 2, 3$:

Soient E : $y^2 = x^3 + Ax + B$ une courbe elliptique

Si $P_1 = (x_1, y_1)$ et$P_2 = (x_2, y_2)$ alors$-P_1 = (x_1, -y_1)$, si

$P_1 = -P_2$ Alors$P_1 + P_2 = o$, sinon $P_1 + P_2 = P_3 = (x_3, y_3)$ où

1. Si $P_1 \neq P_2$ alors

$x_3 = (\lambda^2 - x_1 - x_2) \bmod p$, $y_3 = (\lambda(x_1 - x_3) - y_1) \bmod p$,

Ou $\lambda = \left((y_2 - y_1) * (x_2 - x_1)^{-1}\right) \bmod p$

2. Si $x_1 = x_2$ mais $y_1 \neq y_2$, alors $P_3 = o$.

3. Si $p_1 = p_2$ et $y_1 \neq 0$, alors

$x_3 = (\lambda^2 - 2x_1) \bmod p$, $y_3 = (\lambda(x_1 - x_3) - y_1) \bmod p$,

ou $\lambda = \left((3x_1^2 + A) * (2y)^{-1}\right) mod\ p$.

4. Si $p_1 = p_2$ et $y_1 = 0$, alors $P_3 = O$.

De plus, on a $P + o = P$ pour tout P sur E.

II-3-2-3 caractéristique 2 :

Soient E: $y^2 + xy = x^3 + ax^2 + b$ une courbe elliptique

Si $P_1 = (x_1, y_1)$, et $P_2 = (x_2, y_2)$ alors $-P_1 = (x_1, x_1 + y_1)$,

si $P_1 = -P_2$ alors $P_1 + P_2 = o$,

sinon $P_1 + P_2 = P_3 = (x_3, y_3)$ où

$$x_3 = (\lambda^2 + \lambda + x_1 + x_2 + a) \bmod p$$

$$y_3 = (\lambda(x_1 + x_3 + x_3 + y_1) \bmod p$$

Avec $\lambda = \left((y_1 + y_2) * (x_1 + x_2)^{-1}\right) \bmod p$ si $P_1 \neq P_2$

Et $x_3 = (\lambda^2 + \lambda + a) \bmod p$

$y_3 = (x_1^2 + \lambda x_3 + x_3) \bmod p$

Avec $\lambda = \left(x_1 + \frac{y_1}{x_1}\right) \bmod p$

II-3-2-4 caractéristique 3 :

1) Cas non-super singulier :

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

$$\begin{cases} x_3 = (\lambda^2 - x_1 - x_2) \bmod p \\ y_3 = (-\lambda(x_1 + x_3) - y_1) \bmod p \end{cases}$$

si $P_1 \neq P_2$ $\lambda = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) \bmod p$

si $P_1 = P_2$ $\lambda = \left(\frac{ax_1}{y_1}\right) \bmod p$

2) Cas super singulier :

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

$$\begin{cases} x_3 = (\lambda^2 - x_1 - x_2) \bmod p \\ y_3 = (-\lambda(x_1 - x_3) - y_1) \bmod p \end{cases}$$

si $P_1 \neq P_2$ $\quad \lambda = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) \bmod p$

si $P_1 = P_2$ $\quad \lambda = \left(\frac{a}{2y_1}\right) \bmod p$

Remarque :

Nous allons dans tout ce qui suit, sauf mention contraire, uniquement considérer des corps ayant une caractéristique différente de 2 et 3, pour pouvoir écrire une courbe elliptique sous la forme de Weierstrass simplifiée.

Prenons un exemple.

Soit la courbe $y^2 \, mod \, 11 = (x^3 + x + 2) \, mod \, 11$.

Calculons $d \cdot P$, avec $d = 3 \; et \; P = (4, 2)$. On peut vérifier que le point P appartient bien à la courbe elliptique.

On peut remplacer $(3 \cdot P)$ par $(P + P + P)$

Calculons d'abord $P + P$.

D'après la règle 3: $P + P = (4, 2) + (4, 2) = (8, 4) = 2 \cdot P$.

D'après la règle 1: $2P + P = (8, 4) + (4, 2) = (2, 10) = 3P$

Il est intéressant de noter, que dans ces formules, nous n'avons jamais utilisé B pour calculer les coordonnées de P_3.

Nous allons donner quelques propriétés sur les points de torsion d'une courbe elliptique E définie sur un corps quelconque K [22], [06]

II-3-2-5 Théorème de HASSE : Soit E une courbe elliptique définie sur un corps fini Fq.

Alors $\quad |q + 1 - \#E(Fq)| \leq 2\sqrt{q}$.

Pour ce qui suit, posons $a = q + 1 - \#E(F_q)$. [08]

Ce théorème ne fournit qu'un encadrement du nombre de points de la courbe. Or en cryptographie, il est essentiel de connaître le nombre précis de points de la courbe elliptique manipulée. Des algorithmes ont donc été construits dans le but de connaître le nombre exact de points d'une courbe elliptique.

II-3-2-6 Arithmétique modulo p :

II-3-2-6-1 Définissons l'arithmétique modulo p:

Z_p symbolise l'ensemble {0, ..., p-1} muni de deux opérations + et x. L'addition et la multiplication dans Z_p fonctionnent exactement comme l'addition et la multiplication usuelles, excepté le fait que tous les résultats sont réduits modulo p. [S10]

Supposons par exemple : que l'on veuille calculer 11 x 13 dans Z16. Comme entiers ordinaires, on a 11 x 13 = 143. Pour réduire 143 modulo 16, on fait une division euclidienne : 143 = 8 x 16 + 15, donc 143 mod 16 = 15, et, donc, 11 x 13 = 15 dans Z16.

Ces définitions de l'addition et de la multiplication satisfont la plupart des règles familières en arithmétique. On rappelle la liste de ces propriétés sans les démontrer:

1. l'addition est interne: si a et b appartiennent à Z_p,
   alors a + b appartient à Z_p
2. l'addition est commutative: si a et b appartiennent à Z_p,
   alors a + b = b + a
3. l'addition est associative: si a, b et c appartiennent à Z_p,
   alors (a + b) + c = a + (b + c)
4. 0 est le neutre pour l'addition: si a appartient à Z_p,
   alors a + 0 = 0 + a = a
5. l'opposé de tout a appartenant à Z_p est p - a:
   a + (p - a) = (p - a) + a = 0 (sauf pour a = 0 qui est son propre opposé)

Puisque les opposés existent dans Z_p, on peut aussi faire des soustractions. On définit a - b dans Z_p comme étant a + p - b mod p. De manière équivalente, on peut calculer l'entier a - b et le réduire modulo p. Par exemple, pour calculer 11 - 18 dans Z31, on peut évaluer 11 + 13 mod 31 = 24. On peut aussi retrancher 18 de 11, obtenir -7 et calculer -7 mod 31 = (-7 + 31) mod 31 = 24.

6. la multiplication est interne: si a et b appartiennent à Z_p, alors ab appartient à Z_p
7. la multiplication est commutative: si a et b appartiennent à Z_p, alors ab = ba
8. la multiplication est associative: si a, b et c appartiennent à Z_p,
   alors $(ab)c = a(bc)$

9. 1 est le neutre pour la multiplication: si a appartient à Z_p,

alors $a * 1 = 1 * a = a$

10. la multiplication est distributive sur l'addition: si a, b et c appartiennent à Z_p, alors $(a + b)c = ac + bc \; et \; a(b + c) = ab + ac$

11. $a^n \; mod \; p = (a \; mod \; p)^n \; mod \; p$

12. L'inverse modulo p de b est le nombre entier b-1 tel que $b \cdot b^{-1} \; mod \; p = 1$. On peut le calculer avec l'algorithme d'Euclide étendu. [09]

II-3-2-6-2 L'algorithme d'Euclide étendu :

L'algorithme d'Euclide étendu permet de calculer l'inverse de b modulo n s'il existe. Rappelons que l'inverse modulo p de b est le nombre entier b-1

tel que $b \cdot b^{-1} \; (mod \; p) = 1$. Par exemple 7 est l'inverse modulo 9 de 4,

car $4 \cdot 7 \; (mod \; 9) = 28 \; (mod \; 9) = 1$.

L'algorithme
$\mathbf{n_o := n}$;
$\mathbf{b_o := b}$;
$\mathbf{t_o := 0}$;
$\mathbf{t := 1}$;
q := nombre entier immédiatement inférieur ou égal à n_o / b_o
$\mathbf{r := n_o - q \cdot b_o}$;
Tant que r > 0 **faire**
Début
$\mathbf{temp := t_o - q \cdot t}$;
Si temp >= 0 **alors** $\mathbf{temp := temp \; mod \; n}$,
Sinon $\mathbf{temp := n - ((-temp) \; mod \; n)}$
$\mathbf{t_o := t}$;
$\mathbf{t := temp}$;
$\mathbf{n_o := b_o}$;
$\mathbf{b_o := r}$;
q := nombre entier immédiatement inférieur ou égal à n_o / b_o
$\mathbf{r := n_o - q \cdot b_o}$;
Fin Si
$b_o = 1$ **Alors** b n'a pas d'inverse modulo n, **sinon** $\mathbf{b^{-1} \; mod \; n = t}$;

II-3-2-7 Définition:

Soit E une courbe elliptique définie sur un corps K.

Soit n un nombre entier positif. On pose :

$E[n] := \{P \in E(\overline{K}) \backslash nP = O\}$, ou $\overline{K}$ est une clôture algébrique de K.

II-3-2-8 Théorème:

Si la caractéristique de K est nulle ou ne divise pas n, alors

$E[n] \cong Z/nZ \oplus Z/nZ.$

Si la caractéristique de K est $p > 0$ et$p|n$, écrivons n = prn0 avec p - n0. Alors

$E[n] \cong Z/n'Z \oplus Z/n'Z$ ou $E[n] \cong Z/nZ \oplus Z/n'Z.$

En particulier, $E[p] \cong Z/pZ$ ou $E[p] = \{O\}$.

II-3-2-9 Définition:

Soit une courbe elliptique E définie sur un corps K de caractéristique p. On dit que E est une courbe elliptique super singulière si

$E[p] = \{O\}.$

II-4 L'accouplement de Weil

II-4-1 Définition:

Soit un corps K et soit n un nombre entier qui n'est pas divisible par la caractéristique de K. On pose :

$\mu_n(\overline{K}) := \{x \in \overline{K} \backslash x^n = 1\}$,

le groupe des racines $n^{éme}$ de l'unité dans $\overline{K}$. Puisque la caractéristique de K ne divise pas n, l'équation $x^n = 1$ n'a pas de racines multiples. Ainsi μ_n est cyclique d'ordre n. Un générateur $\zeta\ de\ \mu_n$ est appelé une racine primitive $n^{éme}$ de l'unité. [07]

II-4-2 Théorème:

Soit E une courbe elliptique définie sur un corps K et soit n un entier positif tel que la caractéristique de K ne divise pas n. Alors il existe une application

$e_n : E[n] \times E[n] \to \mu_n,$

appelé l'accouplement de Weil, qui satisfait les propriétés suivantes :

1. e_n est bilinéaire, c'est-à-dire

$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$ et

$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$

pour tous $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

2. $e_n(T, T) = 1$ pour tout $T \in E[n]$.

3. $e_n(S, T) = e_n(T, S) - 1$ pour tout $S, T \in E[n]$, i.e en est antisymétrique.

4. e_n est non dégénéré, c'est-à-dire que si $e_n(S, T) = 1$ pour tout $T \in E[n]$ alors $S = 0$ et si $e_n(S, T) = 1$ pour tout $S \in E[n]$ alors $T = O$.

II-4-3 Corollaire:

Soit $\{T_1, T_2\}$ une base de $E[n]$. Alors $e_n(T_1, T_2)$ est une racine primitive $n^{éme}$ de l'unité.

Preuve. Posons $\zeta = e_n(T_1, T_2)$ avec $\zeta^d = 1$. Alors $e_n(T_1, dT_2) = 1$ par la linéarité de La deuxième composante. De plus, $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$ par la **propriété 3 du théorème 1.8.**

Soit $S \in E[n]$, alors $S = aT_1 + bT_2$ ou a, b sont des entiers. Ainsi

$$e_n(S, dT_2) = e_n(T_1, T_2)^a e_n(T_2, T_2)^b = 1.$$

Puisque ceci est vrai pour tout $S \in E[n]$, alors $dT_2 = O$. Puisque $dT_2 = O$ si et seulement si $n|d$ (car T_2 est d'ordre n), ceci implique que ζ est une racine primitive $n^{éme}$ De l'unité.

II-4-4 Corollaire:

Si $E[n] \subset E(K)$, alors $\mu_n \subset K$.

II-5 Courbes elliptiques sur un corps fini :

En cryptographie on s'intéresse surtout aux courbes elliptiques sur des corps finis. En particulier, il est crucial de savoir calculer $\#E(\mathbb{F}_q)$ pour E une courbe elliptique définie sur $\mathbb{F}_q$. Dans ce paragraphe nous rappelons le théorème de Hasse une méthode algorithmique pour calculer $\#E(\mathbb{F}_q)$.

Dans tout ce paragraphe nous considérons E une courbe elliptique sur un corps fini $\mathbb{F}_q$, avec $q = p^r$ pour un nombre premier p. On fixe une clôture algébrique $\overline{\mathbb{F}}_q$ de F_q.

II-6 : Compter les points d'une courbe elliptique sur un corps fini :

Nous avons vu qu'il est très important de connaître $\#E(Fq)$ pour les methodes de cryptages utilisant les courbes elliptiques.

Dans cette partie nous allons montrer qu'il est facile de calculer l'ordre d'une courbe $E(F_{q^n})$ si nous connaissons son ordre pour $E(Fq)$.

Ensuite nous allons donner un algorithme qui nous permet de calculer

$\#E(Fp)$ Pour un p premier. [06]

II-7-1Théorème : Soit $\#E(Fq) = q + 1 - a$.

Posons $X^2 - aX + q = (X - \alpha)(X - \beta)$, ou $\alpha\ \beta \in Fq$.

Alors

$$\#E(Fqn) = q^n + 1 - (\alpha^n + \beta^n)$$

pour tout $n \geq 1$.

Preuve : Commençons par montrer que $\alpha^n + \beta^n$ est un nombre entier.

Posons $s_n = \alpha^n + \beta^n$, alors $s_0 = 2$ et $s_1 = a$. Montrons que $s_{n+1} = as_n - qs_n - 1$ pour tout $n \geq 1$.

En effet, en multipliant la relation $\alpha^2 - a\alpha + q = 0$ par α^{n-1}, nous obtenons $\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}$.

Nous faisons de même pour β et nous trouvons

$$\beta^{n+1} = a\beta^n - q\beta^{n-1.}$$

En additionnant ces deux égalités ensembles nous avons bien

$s_{n+1} = as_n - qs_{n-1}$.

Posons

$$f(X) = (Xn - \alpha n)(Xn - \beta n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n.$$

Alors $X^2 - aX + q = (X - \alpha)(X - \beta)$ divise $f(X)$ car α et β sont des racines de f.

Ainsi, il existe un polynôme $Q \in Z[X]$ tel que

$$f(X) = Q(X)(X^2 - aX + q).$$

Et donc,

$(\emptyset_q^n)^2 - (\alpha^n + \beta^n)\emptyset_q^n + q^n = f(\emptyset_q) = Q(\emptyset_q)(\emptyset_q^2 - a\emptyset_q + q) = O$,

Comme endomorphisme de E. De plus, remarquons que

$$\emptyset_q^n = \emptyset_{q^n}.$$

, il n'y a qu'un unique nombre entier k qui satisfait

$$\emptyset_{q^n}^2 - k\emptyset_{q^n} + q^n = O$$

et ce k est donne par $k = q^n + 1 - \#E(Fq^n)$. Ainsi,

$$\alpha^n + \beta^n = q^n + 1 - \#E(Fq^n).$$

Donnons un exemple de calcul.

Exemple. Considérons la courbe elliptique $E : y^2 = x^3 + 2$ définie sur F_7,

E(F7) = $\{O, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}$.

Ainsi $\#E(F_7) = 9$ et $a = 7 + 1 - 9 = -1$ et nous avons le polynôme suivant

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

Nous pouvons donc calculer la cardinalité de tout groupe $E(F_{7^n})$.

Par exemple :

$$((-1 + \sqrt{(-27)})/2)^{60} + \left(\left(-1 - \sqrt{(-27)}\right)/2\right)^{60} = 1804985852611988480600649 8$$

Et donc

$$\#E(F_{7^{60}}) = 760 + 1 - 1804985852611988480600649 8$$

$$= 508021860739623365322188179602357975652549718829504.$$

Grace à ce théorème nous pouvons très vite calculer la cardinalité d'un groupe $E(Fq^n)$ du moment que nous connaissons $\#E(Fq)$. [22]

II-7 Test de primalité :

Pour des nombres de tailles raisonnables, il est assez aisé de déterminer si ces nombres sont composes ou premiers avec certitude. Par contre, pour un nombre de Plusieurs centaines de chiffres, il devient plus difficile de dire si celui-ci est premier de manière déterministe. Il existe des tests probabilistes qui nous permettent de dire Si un nombre est premier avec une certaine probabilité.

Mais, pour qu'un système de type RSA soit sur, il nous faut être certain que les nombres que nous employons soient premiers.[25]

Nous allons, ici, présenter un test de primalité déterministe basé sur les courbes elliptiques. Ce test s'appelle le test de primalité de Goldwasser-Kilian .

Ce test n'est utilisé que pour des nombres n qui ont passé un grand nombre de tests de pseudo-primalité avant. Nous pouvons donc travailler avec n comme s'il était premier. Ainsi, nous pouvons supposer que tous les nombres différents de zéro modulo n sont inversibles modulo n. Dans le cas malheureux ou un nombre $l \neq 0 (mod\ n)$ n'est pas inversible, nous saurons non seulement que n n'est pas premier mais nous aurons aussi trouve un facteur de n qui est $PGDC(n, l)$.

Considérons maintenant une courbe elliptique E définie sur Z $/n\ Z$.

Nous additionnons des points sur cette courbe comme si n était premier. Puisque la loi de groupe de E n'utilise que des additions et multiplications/divisions dans $\mathrm{Z}/n\,Z$,

La seule chose qui peut se passer si n n'est pas premier est qu'une division soit

Impossible et nous aurons donc trouve un facteur de n.

Nous supposerons pour la suite que toutes les opérations que nous ferons ne posent pas de problèmes.

Proposition Soit n un entier, $n > 1, PGDC(n,6) = 1$ et E une courbe elliptique modulo n. Supposons que nous connaissions un nombre entier m et un point $P \in E(Z/n\,Z)$ satisfaisant les conditions suivantes :

1. Il existe un nombre premier q divisant m tel que

$$q > \left(\sqrt[4]{n} + 1\right)^2$$

2. $mP = O = (0 : 1 : 0)$.

3. $(m/q)P = (x : y : t)$ avec $t \in (Z/n\,Z)^*$.

Alors n est premier.

Preuve Soit p un facteur premier de n. En réduisant modulo p, nous savons que

dans le groupe $E(Z/p\,Z)$, l'image de P a un ordre divisant m, mais ne divisant pas

m/q puisque $t \in (Z/n\,Z)^*$. Puisque q est premier, alors q divise l'ordre de l'image de P dans $E(Z/p\,Z)$ et donc $q \leq \#E(Z/p\,Z)$. Par le théorème de Hasse (4-5), nous avons que $q \leq (\sqrt{p} + 1)^2$.

Supposons que n ne soit pas premier. Nous pouvons alors choisir un nombre premier p diviseur de n tel que $p \leq \sqrt{n}$. Nous aurions donc $q \leq \left(\sqrt[4]{n} + 1\right)^2$,ce qui est absurde. Le nombre n est donc premier.

La proposition que nous venons d'énoncer ne nous permet pas de trouver un tel m. Il nous dit juste que si nous en avons un qui satisfait les hypothèses, alors n est premier.[03]

La proposition 4.2 affirme que si nous déterminons un entier m satisfaisant les hypothèses 1,2,3, alors n est premier, mais ne donne pas de méthode pour trouver un tel m. Cependant il est assez naturel de prendre $m = \#E(Z/n\,Z)$. Ainsi, l'hypothèse 2 sera automatiquement satisfaite. En fait on a la proposition suivante.

Proposition Soient n un nombre premier tel que $PGDC(n,6) = 1$, E une courbe elliptique définie sur $Z/n\,Z$ et soit

$$m = \#E(Z/nZ).$$

S'il existe un nombre premier q avec $q \mid m$ tel que

$$q > \left(\sqrt[4]{n}+1\right)^2$$

alors il existe un point $P \in E(Z/nZ)$ tel que $mP = O$ et $(m/q)P = (x : y : t)$ avec $t \in (Z/nZ)^*$.

Preuve : Posons $G = E(Z/nZ)$. Remarquons tout d'abord que pour tout $P \in G$ nous avons $mP = O$.

De plus, puisque n est premier, $t \in (Z/nZ)^*$ veut dire que $t \neq 0$ et donc que $(m/q)P \neq O$ pour la condition 2.

Supposons que pour tout $P \in G$ nous avons $(m/q)P = O$.

Alors l'ordre de G divise m/q.

Par le théorème, nous avons $G \cong Z\frac{}{d_1Z} + Z/d_2Z$ avec $d2 \mid d1$.

Ainsi l'ordre de G est d_1, puisque $\#G = d_1d_2 \leq d_1^2$

Nous avons donc $m = \#G \leq d_1^2 \leq \left(\frac{m}{q}\right)^2$ ce qui veut dire que $q^2 \leq m$

Utilisant notre hypothèse sur la taille de q et le théorème de Hasse (4-5), nous avons

$$(\sqrt[4]{(n\ )}+1)^2 < \sqrt{n}+1$$

ce qui est absurde.

Résumons finalement l'algorithme de Goldwasser-Kilian.

Algorithme de Goldwasser-Kilian :

Soit n un entier positif différent de 1 et premier avec 6. Si n n'est pas premier, l'algorithme le détectera ou tournera indéfiniment. C'est pourquoi il faut absolument utiliser le test de Rabin-Miller avant d'utiliser cet algorithme.

1. Posons $i = 0$ et $ni = n$.

2. Si $n < 2^{30}$, diviser par tous les premiers jusqu'a 2^{15} . Si ni n'est pas premier aller a l'´etape 9.

3.Choisir a et b dans Z/niZ et vérifier que $4a^3 + 27b^2 \in (Z/niZ)^*$.

Poser $E : y^2 = x^3 + ax + b$.

4. Avec l'algorithme de Schoof (voir l'annexe) , calculer $m = \#E(Z/niZ)$. Si l'algorithme de Schoof bloque, aller a l'´etape 9.

5. Diviser m par des petits nombres premiers dont on note m' le produit. On suppose $m = m'q$ avec $q > (4\sqrt{n} + 1)^2$ ayant passe le test de Rabin-Miller. Si ce n'est pas le cas, aller a l'étape 3.

6. Choisir un $x \in Z/niZ$ tel que le symbole de Legendre $(\frac{x^3+ax+b}{ni}) = 0$ ou 1.

Utiliser l'algorithme de Tonelli-Shanks (voir l'annexe) pour trouver $y \in Z/niZ$ tel que $y^2 = x^3 + ax + b$. Si l'algorithme bloque, aller a l'étape 9.

7. Calculer $P_1 = mP$ et $P_2 = (m/q)P$. Si pendant les calculs une division était impossible, aller a l'´etape 9. Sinon vérifier si $P_1 = O$, i.e. $P_1 = (0 : 1 : 0)$.

Si $P_1 \neq O$, aller ` a l'´etape 9. Si $P_2 = O$, aller a l'étape 6.

8. Poser $i = i + 1$ et $ni = q$ et aller a l'étape 2.

9. Si $i = 0$, n est compose, on arrête. Sinon, poser $i = i - 1$ et aller a l'étape 3.

Ce test a été utilisé pour prouver la primalité de nombres de l'ordre de 10^{1000} .

II-8 Génération de paramètres :

Nous avons également étudie la sécurité des courbes qui en général ne sont pas dans les standards, mais qui présenteraient de nombreux avantages.

Pour une utilisation des Courbes elliptiques en environnement contraint, il est extrêmement tentant de choisir un corps de base intermédiaire", c'est- a- dire une extension de degré moyen d'un corps premier lui-même de taille moyenne,

Adaptée à l'architecture visée. Fabriquer de bonnes courbes pour ces corps est un problème peu étudie, car les paramètres se situent a la limite de validité de divers algorithmes.

- Etape 1 : choix d'une courbe elliptique. On choisit a et b tel que $4a^3 + 27b^2$ soit premier avec n. Si en les prenant au hasard ce n'est pas le cas, c'est encore mieux car $pgcd(4a^3 + 27b^2, n)$ donne un diviseur strict de n.

  Remarquons que, puisque $4a^3 + 27b^2$est premier avec n, il est premier avec p et est inversible dans Z/pZ. L'équation $y^2 = x^3 + ax + b$ définit une courbe elliptique sur Z/pZ, que nous noterons $E(a, b, p)$ (signalons que, puisqu'on ne connait pas p, on ne connait pas cette courbe elliptique).

- Etape 2 : choix d'un point sur la courbe elliptique. On trouve deux entiers x et y tels que $y^2 = x^3 + ax + b$. En particulier, P(x,y) est un point de la courbe elliptique $E(a, b, p)$.

- Etape 3 : choix d'un entier auxiliaire. On choisit K un entier pas très grand, mais qui est produit de petits facteurs premiers à des exposants déjà élevés. Par exemple, $K = 210385674..$
- Etape 4 : calcul sur les courbes elliptiques. On calcule les coordonnées du point KP, en utilisant les formules classiques, les calculs s'effectuant modulo n. Ces calculs font intervenir des divisions, et ceci n'est pas toujours possible $modulo\ n$: il faut que le dénominateur d soit premier avec n. Mais ce qu'on espère, c'est que ce n'est pas le cas! En effet, si d n'est pas premier avec n, $pgcd(d, n)$ donne un diviseur premier de n. Si on a pu mener les calculs jusqu'au bout, on recommence à l'étape 1, en changeant de courbe elliptique.

II.9 Comparaison des tailles des clés

C'est là le gros avantage des courbes elliptiques par rapport à RSA puisque pour un niveau de sécurité équivalent, RSA nécessite l'utilisation de clé de plus de 1024 bits. De plus, le rapport de taille devient de plus en plus important à mesure que le niveau de sécurité augmente. Ainsi une clé ECC de 256 bits est aussi robuste qu'une clé RSA de 3072 bits. Pis encore, avoir le niveau de sécurité d'une clé ECC de 512 bits requiert l'utilisation de clés RSA de 15360 bits. Dans le tableau 1.4 nous donnons différentes tailles de clé ayant des niveaux de sécurité équivalente sur différents algorithmes (Table II.2) [21].[25]

Sécurité (en bits)	RSA ou Diffie-Hellman	courbes elliptiques
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table II-3 : Comparaison de tailles de clé à niveau de sécurité équivalent

II-10 Conclusion :

Les crypto systèmes basés sur les courbes elliptiques se posent en alternative efficace face à l'incontournable RSA. En effet, ils exploitent un problème mathématique différent, qui est réputé pour sa solidité égale à RSA pour des clés de longueur bien inférieure. Cela les rend parfaitement adaptés aux utilisations embarquées, comme les cartes à puce par exemple, où la mémoire et la puissance des processeurs ne sont pas suffisants pour réaliser en un temps convenable les calculs exigés par RSA. De nos jours la cryptographie est en perpétuelle évolution afin de pouvoir répondre aux besoins de sécurisation des données qui ne cessent d'augmenter. En effet, les crypto systèmes se doivent d'être performants face à des attaques de plus en plus nombreuses. C'est pourquoi nous ne pouvons pas prédire combien de temps les crypto systèmes basés sur les courbes elliptiques seront les plus efficaces au niveau sécurité.

Chapitre III

Algorithme de cryptage

Par

Les courbes elliptiques

III-1 introduction :

Depuis la nuit des temps des empires cherchent à cacher des informations à leurs ennemis. Ils ont pour cela développé des méthodes pour encoder et décoder leurs donnés. Aujourd'hui avec l'ère de l'informatique et la puissance de calcul qui en découle, la cryptologie est une science primordiale pour les services secrets, mais également pour le secteur bancaire et plus généralement les entreprises.

Dans ce chapitre nous expliquerons les fondements théoriques du protocole de Diffie-Hellman. Pour cela nous démontrerons les résultats d'algèbre nécessaires à son fonctionnement.

Nous parlerons également de Plusieurs problème liés à la cryptographie et utilisant les courbes elliptiques Plus précisément, nous parlerons du problème du logarithme discret.

III-2 Généralités sur les protocoles :

Les modes communication ont connu de grands changements (téléphone, courrier électronique, etc...) qui sont difficiles à maîtriser du point de vu de la sécurité.

Les nouveaux systèmes de communication sont beaucoup plus rapides que l'intervention humaine et moins contraignants mais n'offrent pas les propriétés de sécurité nécessaires à toute communication importante.

C'est ainsi que les protocoles de communication ont été développés pour combler ces déficits de sécurité, donc d'empêcher la possibilité pour un participant de la Communication ou une personne extérieure d'obtenir une information qu'il ne devrait pas connaître, ou de se faire passer pour quelqu'un d'autre..

III-2-1 Protocoles cryptographiques :

III-2-1-1 Protocoles de communication :

a) Échange de messages :

La communication est l'échange d'information entre deux ou plusieurs personnes via un canal qui peut être public (les médias, tels la presse ou la radio) ou privé ; chaque personne étant appelée participant ou agent. Ces participants communiquent grâce à des envois de messages (concrètement, chaque message envoyé n'est qu'une suite de bits).[14]

Un protocole de communication permet l'échange de messages entre différents participants via un canal de communication. La forme, le contenu des messages, les différents participants à la communication et l'ordre dans lequel les messages sont échangés via un canal de communication spécifient un protocole de communication.[02]

b) Session :

L'étude des instances d'un protocole cryptographique introduit la notion de session de protocole qui est un ensemble d'échanges de messages entre plusieurs participants formant un ensemble cohérent et pouvant être répété. Pour différencier deux sessions différentes, on introduit généralement dans le protocole des nombres aléatoires générés par les participants de la communication, appelés nonces. Une nonce est une donnée de grande taille, choisie au hasard par un participant et utilisée une seule fois.

c) Les participants :

Chaque participant peut établir, simultanément, avec différents participants, plusieurs sessions du protocole. Les participants sont de deux types : honnêtes ou intrus.

Participants honnêtes :

Dans la description d'un protocole, les participants sont supposés être honnêtes, c'est-à-dire des participants qui ne collaborent pas avec les attaquants et qui effectuent correctement les échanges dans l'ordre défini par le protocole.

Pour réaliser correctement un protocole, il faut des participants honnêtes pour respecter les spécifications du protocole.

Intrus :

Un intrus ou attaquant est un participant qui ne suit pas exactement le déroulement du protocole. Il espionne les communications qui circulent sur les canaux publics, joue plusieurs sessions de protocoles avec des participants, en se faisant passer pour un agent honnête et ainsi effectue des

actions non prévues par la spécification du protocole, afin de découvrir des informations supposées rester secrètes.

III-2-1-2 Vérification de protocoles cryptographiques :

Actuellement, de plus en plus de protocoles cryptographiques sont vérifiés avant leurs commercialisations. L'analyse de ces protocoles est un problème de vérification en présence de canaux de communications non sécurisés.

Pour attaquer un protocole cryptographique, il existe deux approches possibles :

A. La première consiste à essayer de déchiffrer les messages chiffrés échangés. Ce type d'attaques développées par les cryptographes porte sur l'algorithme cryptographique employé.
B. La seconde approche suppose que la méthode de chiffrement est inviolable, grâce à un raisonnement logique, cherche à obtenir de l'information.

Nous énonçons ici les principales propriétés concernant les protocoles cryptographiques.

Propriétés à vérifier :

Il existe de nombreuses propriétés de sécurité, nous présentons en quelques mots les plus usuelles.

1. Secret : La notion de secret s est utilisée par la plupart des auteurs. Un secret s est une donnée confidentielle ne devant pas être découverte par une tierce personne qui n'est pas censée la connaître. Un protocole vérifie la propriété de secret pour un secret s, si une personne malhonnête (l'intrus) en fonction de ses capacités ne peut jamais obtenir une partie de s échangé entre plusieurs participants honnêtes.

2. Accord non répudiable : Un protocole doit établir un accord non répudiable entre deux agents c'est à dire chaque agent peut fournir la preuve que l'autre a accepté les termes de l'accord.

3. Authentification : La propriété d'authentification garantit à un interlocuteur qu'il communique avec le "vrai" participant. Ceci est fort utile pour sécuriser les transactions bancaires sur internet par exemple.

4. Équité : Un protocole d'accord non répudiable entre deux agents A et B doit être équitable c'est à dire aucun agent ne peut obtenir d'avantage sur l'autre : A n'obtient pas la preuve de l'accord de B avant que B n'ait une preuve de l'accord de A (et vice-versa).[13]

III-3 le protocole de Diffie-Hellmann :

Les algorithmes de chiffrement asymétriques reposent sur l'utilisation de 2clés différents, mais mathématiquement liées , pour le chiffrement et le déchiffrement ,les données chiffrées en utilisant une clé ne peuvent être déchiffrées qu'avec l'autre qui complète la paire . les deux clés sont :

- La clé publique : comme son nom l'indique, cette clé peut être largement diffusée, pour permettre à quiconque le souhaite de communiquer de façons sécuriser avec le détenteur de la clé privée associée.

- La clé privée : elle est gardée précieusement et permet de déchiffrer les messages chiffrés avec la clé publique correspondante. [22]

III-3-1 : A quoi sert le protocole ?

La cryptologie est une science qui englobe d'une part la cryptographie, c'est à dire l'écriture secrète des données, et la cryptanalyse qui est l'analyse de cette dernière.
En règle générale les méthodes de cryptage font appellent à des clés de cryptage. Une clé de cryptage est un ensemble de valeurs qui permet d'encoder et de décoder des données.
Des algorithmes tels que le RSA utilisent plusieurs nombres premiers qui doivent être tenus secrets. Or la difficulté est de pouvoir communiquer la clé de cryptage d'un émetteur A à un destinataire B sans qu'une tiers personne ne puisse l'intercepter c'est là que le protocole Diffie-Hellman intervient.
Il propose à A et B de pouvoir définir une clé secrète même si E écoute leur communication[09]

III-3-2 Procédure :

Nous allons présenter la procédure étape par étape. Elle permet d'échanger des clés de manière sécurisée. Considérons deux individus, A et B, qui souhaitent s'envoyer un message crypte. Les données et les échanges sont les suivants :
– Tout d'abord A et B se mettent d'accord sur un nombre premier p.
Puis ils conviennent d'une racine primitive g
– A choisi un nombre secret $0 \leq a \leq p - 1$.
– A envoie la valeur $g^a \bmod p$ a B.
– B choisi un nombre secret $0 \leq b \leq p - 1$.
– B envoie la valeur $g^b \bmod p$ a A.
– A peut désormais calculer la clé secrète Key = $(g^b \bmod p)^a \bmod p$.
– B procède de manière analogue et obtient la même clé que A : key =$(g^a \bmod p)^b \bmod p$.
A et B sont alors en possession chacun de la même clé secrète (Key) et peuvent ainsi utiliser un simple algorithme de clé privée.[22]

III-3-2 Pourquoi cette méthode est sécurisée :

Supposons qu'une troisième personne, disons E écoute les transmissions de A et B.

Dans ce cas E n'a accès qu'à p, g, ga mod p et gb mod p.

Dans ce cas, on peut se demander pourquoi il n'est pas possible a E de calculer a ou b afin d'obtenir la clé secrète. Il peut, en apparence, paraˆtre simple de calculer a = $\log_g$ (ga) ou b = $\log_g$(gb). Mais ce n'est pas le cas car on travaille ici en mod p. Ce qui implique de calculer un logarithme discret. Or d'après la littérature, il n'existe pas `a ce jour de solution rapide pour le calculer.

E est donc dans l'impossibilité de déterminer (ga mod p)b mod p.

Notons tout de même qu'il faut que p soit suffisamment grand pour éviter que E tente une recherche exhaustive1. Actuellement, en utilisant un nombre premier p de l'ordre de 500 `a 1024 chiffres et a et b de l'ordre de 100 chiffres, il est impossible de déterminer la clé secrète, même avec les meilleures algorithmes de résolution de logarithme discret.

Cependant comme de nombreux algorithmes utilisent le protocole de Diffie-Hellman, si une solution pratique pour résoudre un logarithme discret était découverte, elle rendrait ceux-ci inutiles. Sachant que ce protocole est notamment utilise pour les connections sécurisées Internet, on laisse au lecteur le soin d'imaginer les problèmes qui en résulteraient.[07]

III-3-1 Protocole d'échange de clés de Diffie-Hellmann :

A et B veulent avoir une clé en commun pour s'échanger des données en toute sécurité.

Supposons que leur seul moyen de communication soit public. Un des moyens de sécuriser leurs données est qu'ils établissent une clé privée entre eux. La méthode de Diffie-Hellmann permet justement de faire cela (en général on utilise cette méthode avec des groupes F_q^* , mais nous présentons cette méthode adaptée pour les courbes elliptiques).[21]

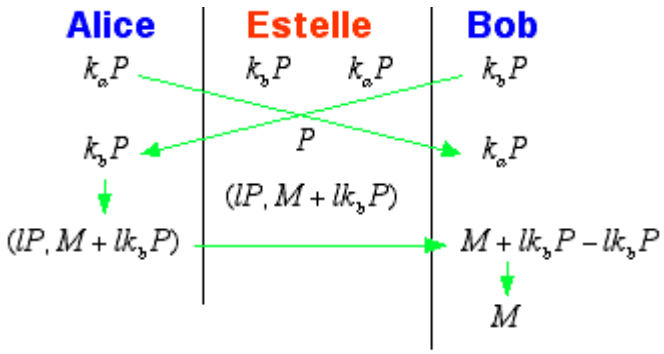


Figure III-1 : protocole d'échange de clé

1. A et B choisissent une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$ tel que le logarithme discret soit difficile à résoudre.

Ils choisissent aussi un point $P \in E(\mathbb{F}_q)$ tel que le sous-groupe généré par P ait un ordre de grande taille. (En général, la courbe E et le point P sont choisis de manière à Ce que l'ordre soit un grand nombre premier.)

2. A choisit un nombre entier secret a, calcule $\mathbf{P_a = aP}$ et envoie $\mathbf{P_a}$ à B.

3. B choisit un nombre entier secret b, calcule $\mathbf{P_b = bP}$ et envoie $\mathbf{P_b}$ à A

4. A calcule $\mathbf{P_b = abP}$.

5. B calcule $\mathbf{P_a = baP}$.

6. A et B utilisent une méthode quelconque connue pour extraire une clé secrète de .

Par exemple, ils peuvent utiliser les derniers 256 bits de la première coordonnée de **abP** comme clé, ou ils peuvent hacher une des coordonnées de **abP** avec une fonction de hachage pour laquelle ils se sont mis d'accord.

Les seules informations qu'un espion peut connaître sont la courbe E, le corps $\mathbb{F}_q$ et les points $\mathbf{P}, \mathbf{aP}, \mathbf{bP}$.

Ainsi s'il veut pouvoir connaitre la clé secrète, l'espion doit résoudre le problème suivant :

III-3-2 Problème de Diffie-Hellmann :

Connaissant $\mathbf{P}, \mathbf{aP}, \mathbf{bP}$ des points de $E(\mathbb{F}_q)$, peut-on trouver **abP** ?

Si l'espion peut résoudre le problème du logarithme discret sur $E(\mathbb{F}_q)$, alors il peut résoudre le problème de Diffie-Hellmann. Actuellement, on ne connait pas de moyen de trouver **abP** sans d'abord résoudre le problème du logarithme discret.

Une autre question est la suivante :

III-3-3 Problème de décision de Diffie-Hellmann :

Connaissant $\mathbf{P}, \mathbf{aP}, \mathbf{bP}$ des points de $E(\mathbb{F}_q)$ et un point $Q \in \mathbb{F}_q$, peut-on déterminer

Si $\mathbf{Q = abP}$?

Autrement dit, si quelqu'un fournit à l'espion un point Q en lui affirmant qu'il est égal à , l'espion a-t-il un moyen de vérifier si l'information est correcte ?

Le problème de Diffie-Hellmann et le problème de décision de Diffie-Hellmann peuvent être posés pour des groupes arbitraires. Pour les courbes elliptiques, l'accouplement de Weil peut être

utilisé pour résoudre le problème de décision de Diffie-Hellmann dans certains cas. Voyons ceci.[13]

III-4 protocole de Diffie-Hellmann:

A veut envoyer un message secret à B. Tout d'abord, B fabrique une clé publique de la manière suivante. Il choisit une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$, de telle manière que le problème du logarithme discret soit plus difficile à résoudre sur $E(\mathbb{F}_q)$, que sur $\mathbb{F}_q$,. Il choisit aussi un point P sur E tel que l'ordre de P soit un grand nombre premier. Il choisit un nombre entier secret s et calcule $\mathbf{H = sP}$.

La courbe E, le corps fini $\mathbb{F}_q$ et les points P et H sont la clé publique de B.

La clé secrète de B est s. Pour envoyer le message, A fait comme suit :

1.A télécharge la clé publique de B.

2. A transforme son message en M.

3. A choisit un nombre entier secret k et calcule $M_1 = kP$.

4. A calcule $M_2 = M + kH$.

5. A envoie M_1 et M_2 à B.

B déchiffre le message en calculant $M = M_2 - sM_1$.

Nous avons cette égalité parce que

$M_2 - sM_1 = (M + kH) - s(kP) = M + k(sP) - skP = M$.

Un espion qui connaît la clé publique et les points M1 et M2. Si l'espion savait résoudre le problème du logarithme discret, il pourrait utiliser P et H pour trouver s et ainsi calculer $M_2 - sM_1$. L'espion pourrait aussi utiliser P et M_1 pour trouver k et calculer $M = M_2 - kH$. Actuellement, on ne connaît pas de moyen plus rapide pour retrouver le message initial en ne sachant que ce qui est rendu public du système de cryptage. Donc, apriori, la fiabilité de ce genre de cryptosystèmes dépend fortement des progrès fait en matière de résolution du logarithme discret.

Remarque : Il est important qu'A utilise, à chaque fois qu'il envoie un message crypté à B avec la même clé, un k différent. En effet, si il utilise le même k pour deux messages différents M et M', alors $M_1 = M'_1$. Un espion ayant intercepté les deux messages codés s'en apercevra et pourra calculer $M'_2 - M_2 = M' - kH - (M - kH) = M' - M$.

Supposons que pour une raison quelconque le message M soit rendu public dès que L'information n'est plus d'actualité, alors l'espion calculera sans peine M' qui vaut $M - M_2 + M'_2$.[09]

Exemple :

Echange de clé entre Ali et Ahmed :

a) Ahmed choisi une courbe E(-15,20,9719) , point P (1541,9201) Tel que P ∈ E, une clé secrète S=179 et calculer SP=(2110,4838)
b) Ahmed envoie a Ali la clé publique (E, P, SP)
c) Ali choisi une clé secrète R=97, calculer RP=(2507,1868), calcule RSP=(3584,6581), crypter le message(M) par la clé (3584)
d) Ali envoie à Ahmed un message crypté(M') et RP
e) Ahmed calcule SRP=(3584,6581) et décrypte le message (M') par la clé(3584).

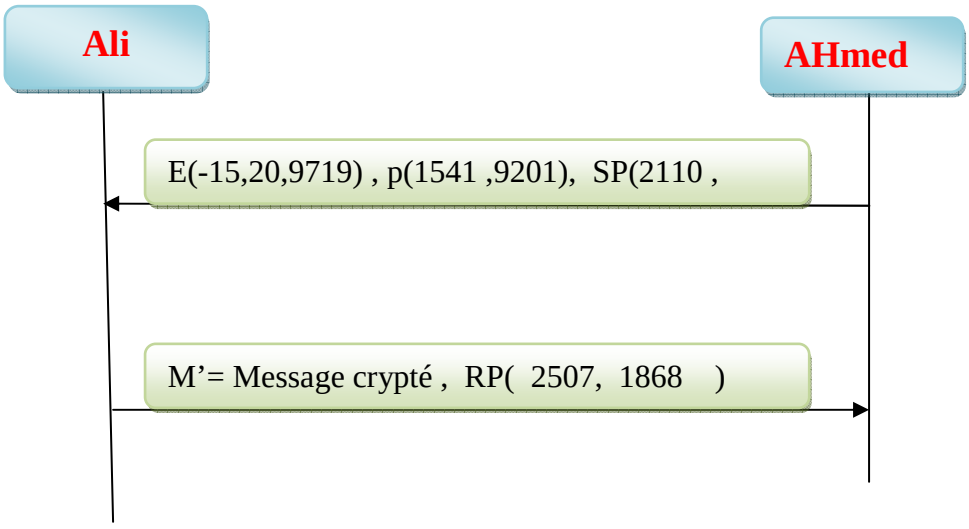


Figure III-2 : protocole d'échange de clé

III-5 Problème du logarithme discret:

Commençons par définir le problème du logarithme discret dans un groupe G quelconque.[21]

III-5-1 Définition:

Soient G un groupe et g ∈ G.

Le problème du logarithme discret dans G en base g est, pour y ∈ G donné, de trouver un entier x tel que :

$g^x = y$ (xg = y si G est noté additivement).

Dans le cas ou G = E est une courbe elliptique, le problème

du logarithme discret en base P ∈ E est de trouver, étant donné Q ∈ E, un entier x tel que :

Q = xP Si un tel x existe.

Nous parlerons plus spécialement du problème du logarithme discret.

III-5-2 Définition:

On peut définir également des courbes elliptiques sur des corps finis, et les munir d'une addition analogue à la précédente. Ce sont de telles courbes qui sont utilisées en cryptographie. Il est facile de calculer, à partir de la donnée du point P et de l'entier d, le point Q tel que Q = d. P ; le problème inverse, consistant à trouver d en supposant P et Q connus (problème dit du logarithme discret sur les courbes elliptiques) est par contre très difficile à résoudre lorsque la courbe elliptique est définie sur un corps fini, même avec des ressources considérables.[02]

- C'est cette difficulté qui constitue le fondement de la sécurité des ECC. Nous allons traiter du problème du logarithme discret.
- Nous présenterons plusieurs méthodes qui permettent, dans certains cas, de résoudre ce problème.

Remarque :

Une méthode pour trouver k serait de calculer tout les multiples de P , jusqu'a aboutir à Q.

L'applet suivant montre le temps nécessaire pour aboutir à k Sur mon ordinateur, il faut 1.42s pour k = 220, 5.66s pour k = 222,22.3s pour k = 224. On peut donc en déduire que l'algorithme est de complexité linéaire

(car 22.3 = 4 * 5.66 = 16 * 1.42) , de plus, on peut calculer qu'il faut envieront (1.42 - 22.3) / (220 - 224) = 1.27*10-6 s pour effectuer une itération. Avec k faisant 192 bits, il faudrait environ 7.66*1051 s, c'est à dire 2.53*1044 ans (à comparer avec l'âge de l'univers: 15*109 ans).

Même en utilisant toute la puissance de calcul de tous les ordinateurs de la planète pendant des années, c'est absolument impensable.[07]

III-6 Comparaison entre la méthode de diffie-hellmann et la méthode d'elgamel :[22]

La clé secrète	Temps ms/ elgamel	Temps ms diffie_hellmann
25371	10	10
97213	60	30
297321	190	110
3421567	2150	770
147245691	92080	31410

Tableau III -1 : tableau récapitulatif des temps de calcul.

Comme le tableau indique par la méthode de deffie-hellmann on gagne le temps Pour le même clé utiliser par la méthode d'elgamel

Malgré que les deux méthodes utilisent la même proche des courbes elliptiques mais la méthode deffie-hellmann plus compliqué car elle baser sur les calcules exponentiel par contre la méthode d'elgamel un peu simples car elle baser sur les calcules multiplicatifs

III-7 CONCLUSION :

Pour la cryptographie à clé secrète, l'échange de clé peut être assuré par des protocoles qui utilisent l'idée du protocole Diffie-Hellman et ce dernier repose sur le logarithme discret.

La cryptographie à clé publique joue un rôle fondamental pour la sécurité car elle offre des services que n'offre pas la cryptographie à clé secrète telle que la non répudiation entre autre. En cryptographie à clé publique, beaucoup de schémas utilisent le problème du logarithme discret dont le meilleur cadre d'utilisation actuel est le domaine des courbes elliptiques issues de la théorie des nombres.[14]

Chapitre IV

Implémentation

du logiciel

IV-1 INTRODUCTION :

Dans ce chapitre on a deux parties

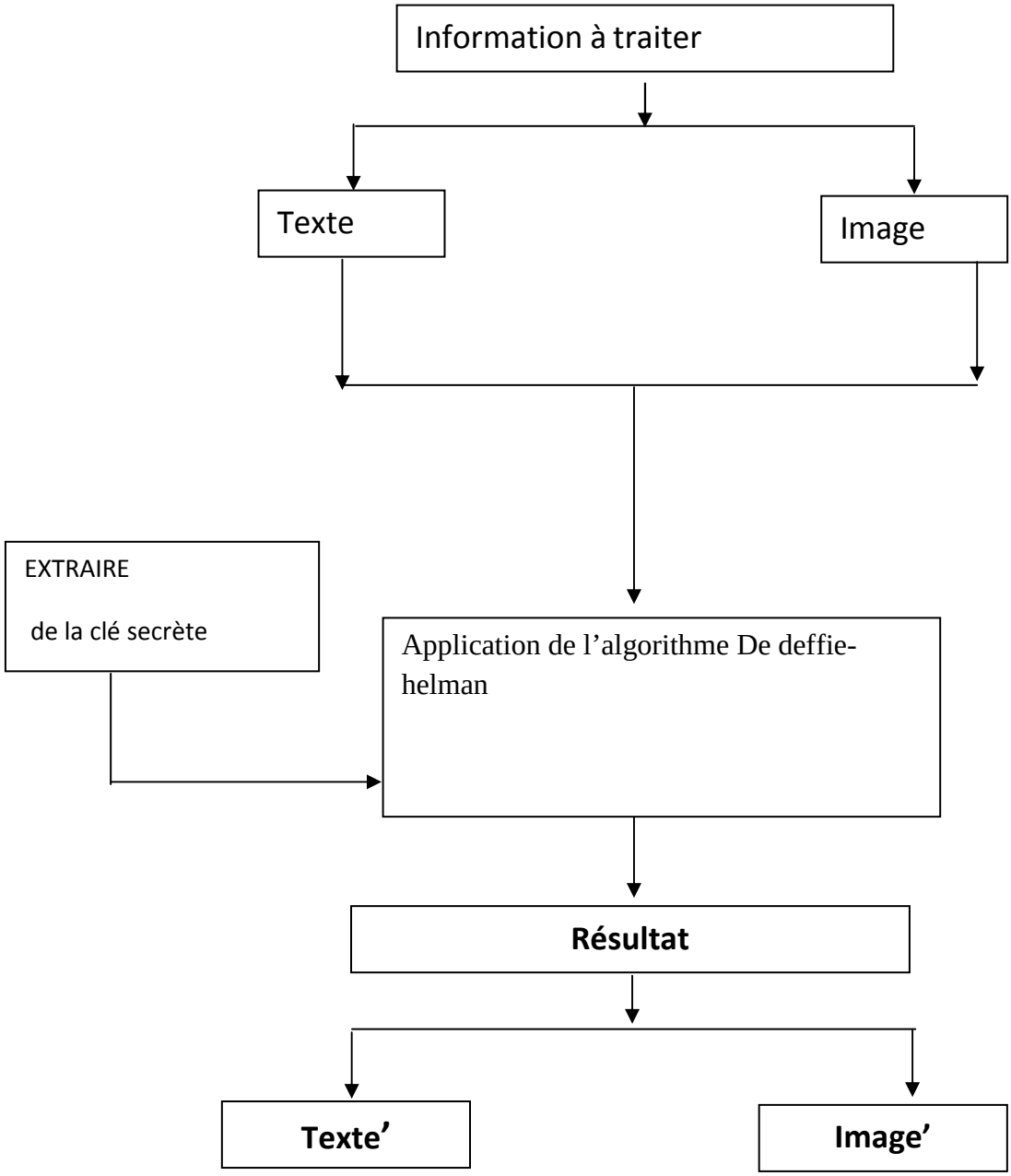
La première partie est consacrée à la représentation et a la description de notre logiciel

La deuxième est consacrée aux résultats de la simulation.

IV-1-1 environnement de programmation :

Notre logiciel est implémenté sous un langage de programmation orienté objet, évolué, conçu par la firme BORLAND, il s'agit de C++ BUILDER version 6.0.+java (transfert des données) Qui est un nouveau produit de développement rapide d'application Windows. Il regroupe toute la puissance du langage C++ avec plus de facilité et de rapidité qu'auparavant, vous pouvez créer instantanément l'interface utilisateur d'un programme.

IV-1-2 L'organigramme du logiciel :



IV-2 L'interface du logiciel :

Elle joue un rôle très important qui s'éclaircie dans la facilité d'utilisation de l'application.

Il est à noter que l'interface que nous avons choisit pour notre logiciel paraît très simple, et cela pour donner à l'application un espace libre supplémentaire pour pouvoir travailler dans les meilleures conditions.

Surtout quand on sait la complexité de l'algorithme ECC

IV-2-1 Interface principale :

Figure IV-1: Interface principale

IV-2-2 Le menu cryptage

Figure IV-2 : menu cryptage

Le menu cryptage contient les fenêtres suivantes :

1. Calcule de clé
2. Cryptage du texte
3. Cryptage d'image
4. Quitter

IV-2-3 Le menu outils:

Figure IV-3 **: menu outils**

Le menu outils contient les fenêtres suivantes :

1. Paint
2. Bloc Note
3. Active/désactive mot de passe
4. Transfert des fichiers par réseau

IV-2-4 Le menu aide:

Figure IV-4 **: menu aide**

Le menu aide contient les fenêtres suivantes :

- Changement de mot de passe
- Aide
- A propos

IV-3 Le développement du logiciel :

IV-3-1 pour une clé:

Pour calculer la clé on utilise les paramètres suivant :

la courbe E(A,B,Q) $y^2 = x^3 + Ax + B$ dans un corps fini Z/QZ

1. le point P appartient a ce courbe E
2. une clé secret S et calculer sp
3. L'algorithme de «deffie-hellmann »

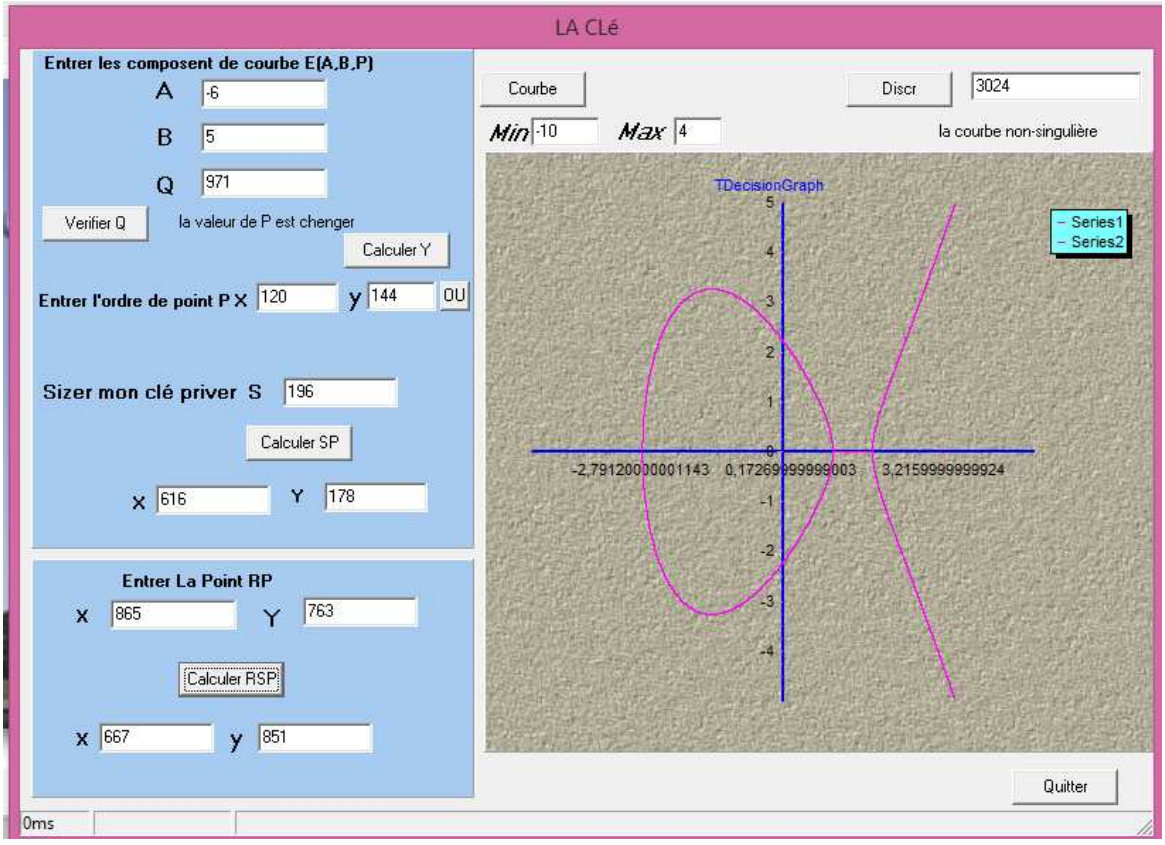


Figure IV-5**:** fenetre de la clé

IV-3-2 pour un texte :

Lecture d'un texte :

Consiste à lire le contenu d'un fichier texte (*.Txt), puis le stocker dans une chaine de Caractère.

Conversion texte :

Convertir les caractères du texte en binaire en utilisent le code **ASCII**

Sauvegarder un texte :

Stocker le texte après le chiffrement dans un autre Chaine de caractère, ensuite créer un fichier résultat qui va le contenir.

Affichage du texte :

Pour afficher ou créer un nouveau fichier texte

Dans l'interface principale cliquer sur le bouton texte une nouvelle fenêtre s'affiche (figure 7)

Figure IV-6: la fenêtre Cryptage de texte.

- Pour saisir un nouveau texte cliquer sur le bouton ***nouveau.***

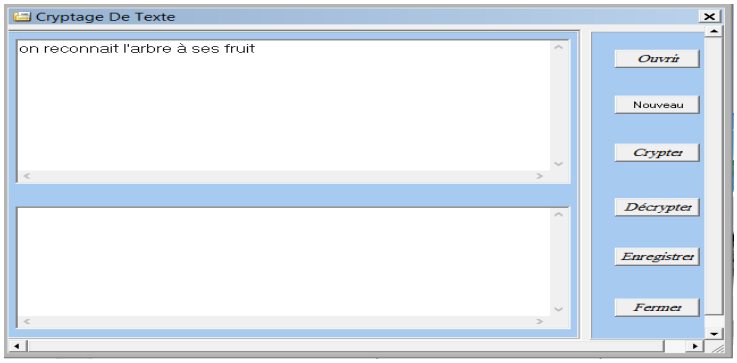


Figure IV-7: la fenêtre saisir le texte.

- Pour crypter un texte cliquer sur le bouton crypter.
- Pour Décrypter un texte cliquer sur le bouton Décrypter
- Si vous intéressez par l'enregistrement du texte chiffré appuyé sur ***bouton enregistrer***, la fenêtre d'enregistrement s'affiche.

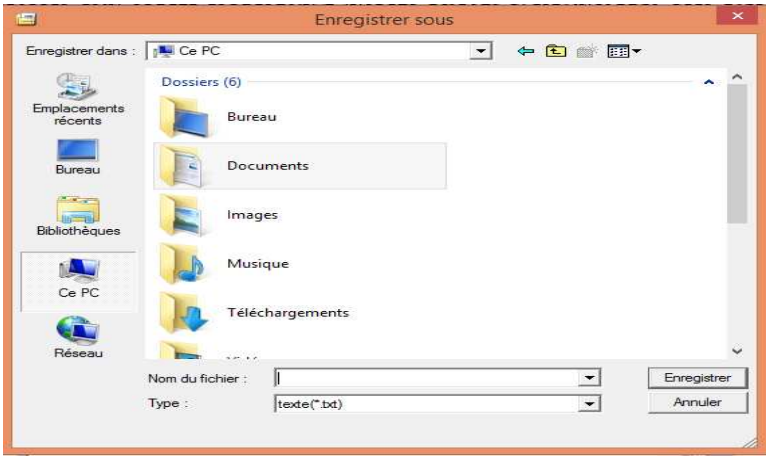


Figure IV-8: enregistrement du texte.

- Nommez le fichier à enregistrer et valider en cliquant sur le bouton ***enregistrer***.

❖ Pour ouvrir un texte existant (d'extension .Txt) cliquer sur le ***bouton ouvrir.*** Une fenêtre de sélection s'affiche.

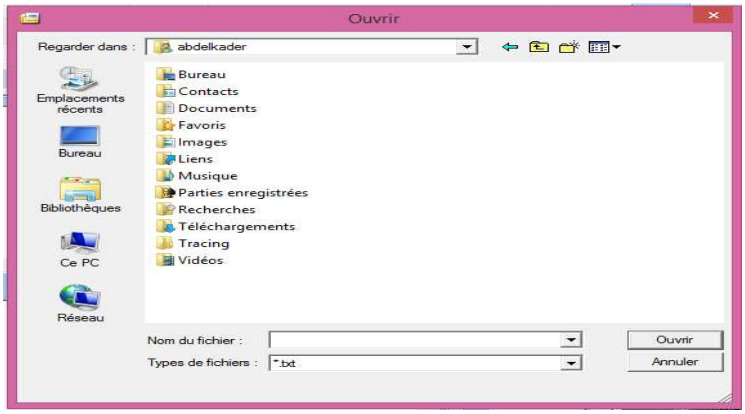


Figure IV-9: ouvrir du texte.

Exemple :

Cryptage de texte « Etude et implémentation d'un système de chiffrement asymétrique basé sur les courbes elliptiques» avec les paramètres suivants :

avec la courbe **E(-7,12,1597)** point **p(137,321)** clé secret de L'émetteur **S=371** point **Sp(259,1517)** clé secret de récepteurs **R=923**
point **RP(354,1169)** point **RSP(32 ,340)**

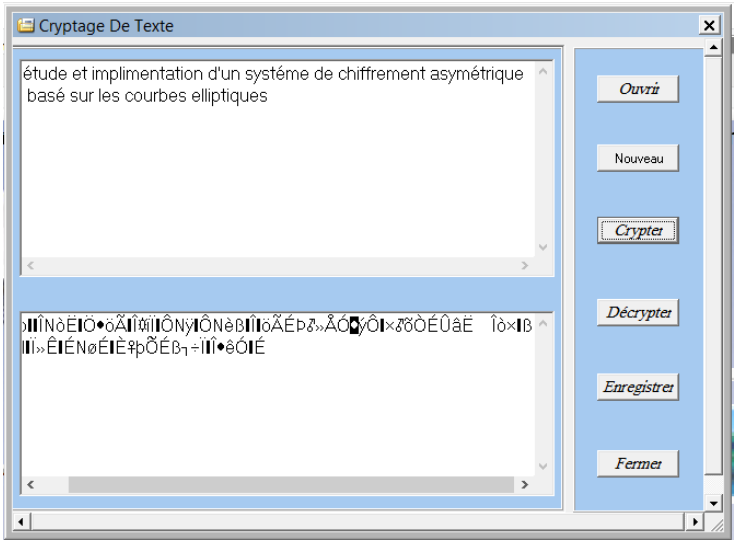


Figure IV-10: Cryptage de texte

IV-3-3 pour une image :

Chargement d'une image :

consiste à lire le contenu d'un fichier image (*.bmp).

Stockage d'une image :

stocker l'image dans un fichier résultat (*.bmp) .

Affichage d'image :

Permet d'afficher toutes les images (*.bmp).

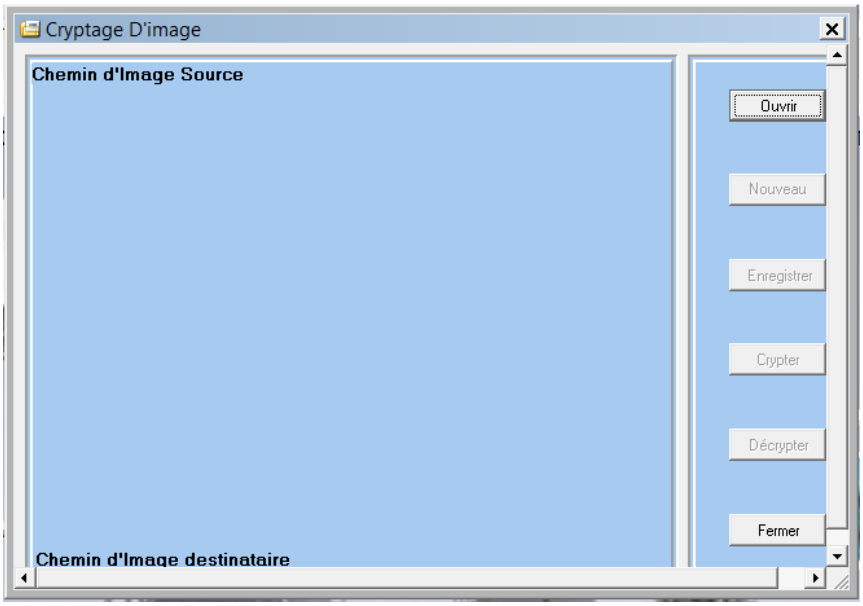


Figure IV-11: Fenêtre Cryptage d'image

1. Pour ouvrir une image (d'extension .BMP) cliquer sur le ***bouton ouvrir.*** Une fenêtre de sélection s'affiche.

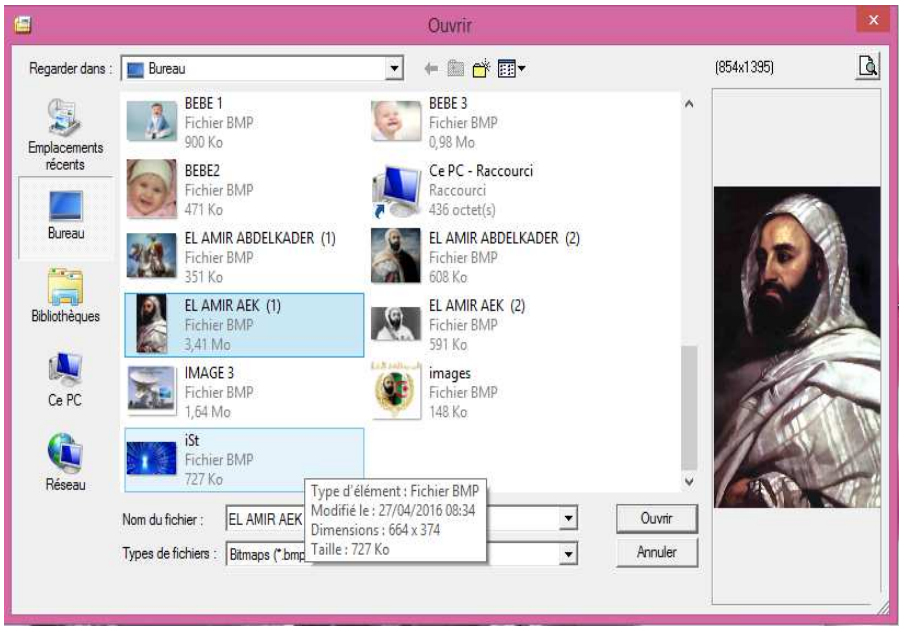


Figure IV-12: boite de sélection image

2. Lorsque vous cliquer sur le bouton ouvrir la fenêtre ‘’cryptage de l’image’’ s’affiche charger par limage choisi et son chemin **.**

Figure IV-13: fenêtre chargée par limage choisi et son chemin.

1. Pour crypter une image cliquer sur le bouton crypter.

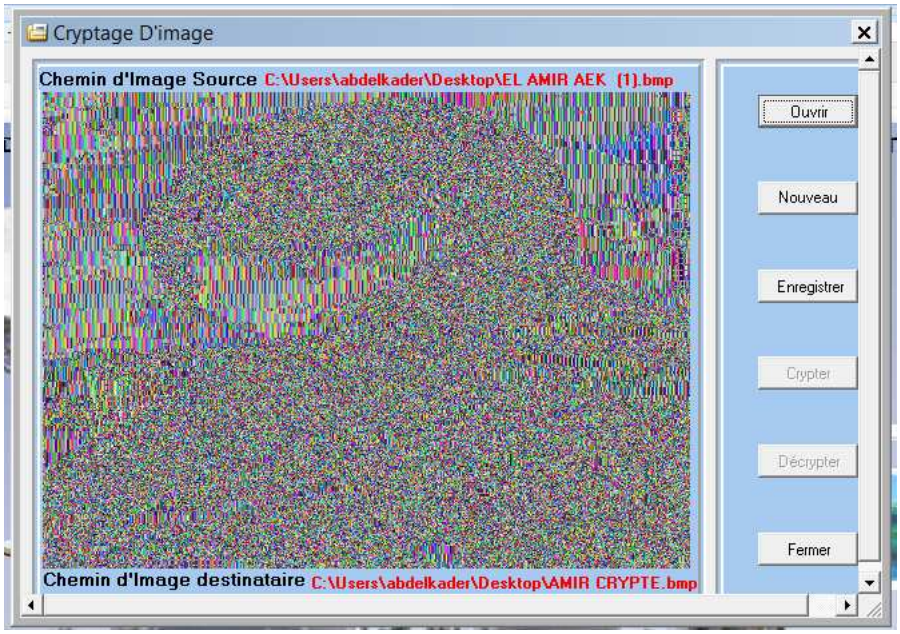


Figure IV-14: L'image crypte.

2. Pour Décrypter une image suivi les mêmes étapes de cryptage

1. Pour quitter l'application cliquer sur le bouton **Fermer**

IV-4 les résultats expérimentaux :

A)-clé

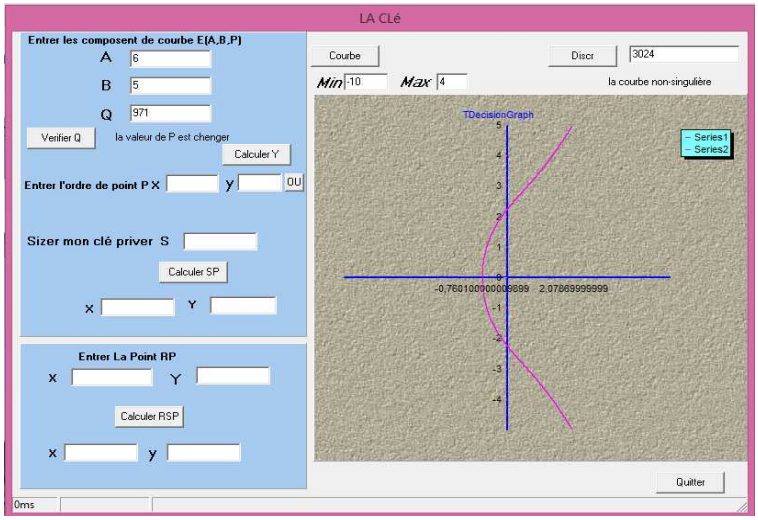


Figure IV-15: fenêtre de clé charger

le bouton (Vérifier Q) :pour vérifié Q est un nombre premier
si Q est un nombre non premier il affiche un nombre premier supérieur et plus proche de Q et affiche un message « le nombre est changer »

1. le bouton (calculer y) : Pour calculer y
2. le bouton (ou) : Pour choisir la 2eme valeur de y
3. le bouton (courbe) : Pour tracer le courbe
4. le bouton (discr) : Pour calculer le discriminant et afficher un message pour définir le type de courbe
5. le bouton « calculer SP » : pour remplir les champs de X ,Y
6. le bouton « calculer RSP » : pour remplir les champs de X ,Y
7. le bouton « quitter » : pour fermer cette fenêtre
8. au bas de la fenêtre de la cote gauche un timer pour calculer le temps de calcule de l'application

Calcul du Temps :
On a : E (-7,12,1597) ; un point p(120,394)

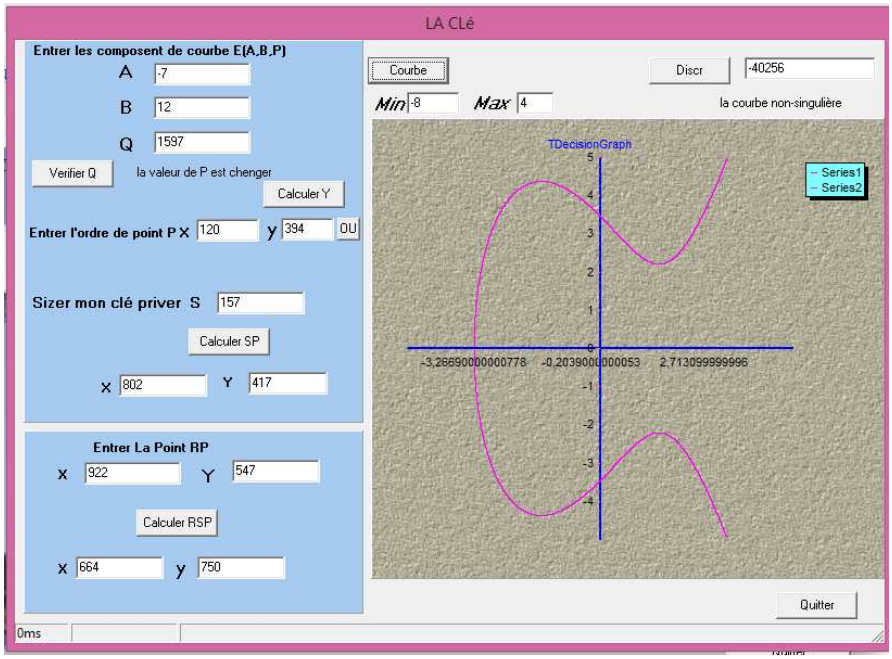


Figure IV-16: fenêtre de clé

La clé secrète	Temps ms ECC/diffie_hellmann
25371	10
97213	30
297321	110
3421567	770
147245691	31410

Table IV-1 : Tableau récapitulatif des temps de calcul.

Remarque :

9. il ya une relation entre les clés secrets(s, r) d et le temps de calcule quand on agrandit les clés secrets le temps s'accroit
10. Le temps de calcule des petits clés secrets tend vers zéro

B)-Texte:

Chiffrement de texte **«Depuis une quarantaine d'années, la cryptologie s'est enrichie de plus en plus vers une structure mathématique. Notamment d'une part l'algèbre linéaire»**

1-avec la courbe **E(-7,12,1597)** point **p(137,321)** clé secret de L'émetteur **S=371** point **Sp(259,1517)** clé secret de récepteurs **R=923**

point **RP(354,1169)** point **RSP(32 ,340)**

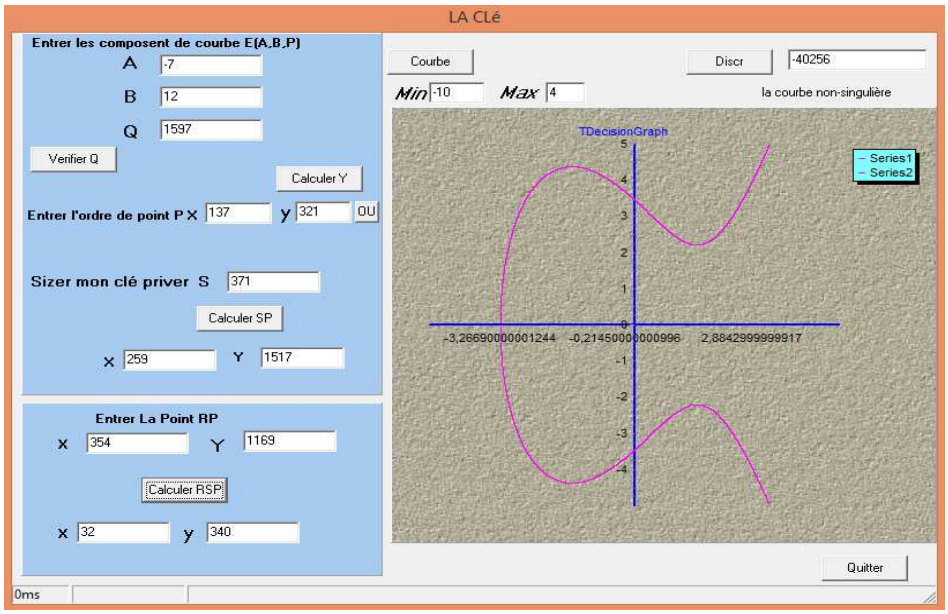


Figure IV-17: fenêtre de clé charger **E(-7,12,1597) p(137,321) S=371 R=923**

Résultat :

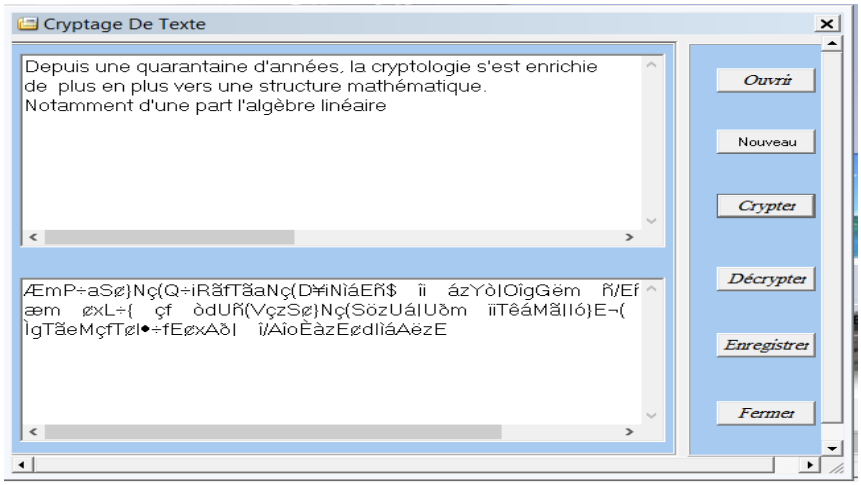


Figure IV-18: CRYPTAGE D'UN TEXTE

IV-B-1 Changement d'un caractère :

Chiffrement :

Chiffrement de **«Etude et implémentation d'un cryptage par courbes elliptiques sous le protocole Diffie Hellman»**

avec la courbe **E(-7,12,1597)** point **p(137,321)** clé secret de L'émetteur **S=371** point **Sp (259,1517)** clé secret de récepteurs **R=923**

point **RP(354,1169)** point **RSP(32 ,340) (Figure 15)**

Résultat de chiffrement:

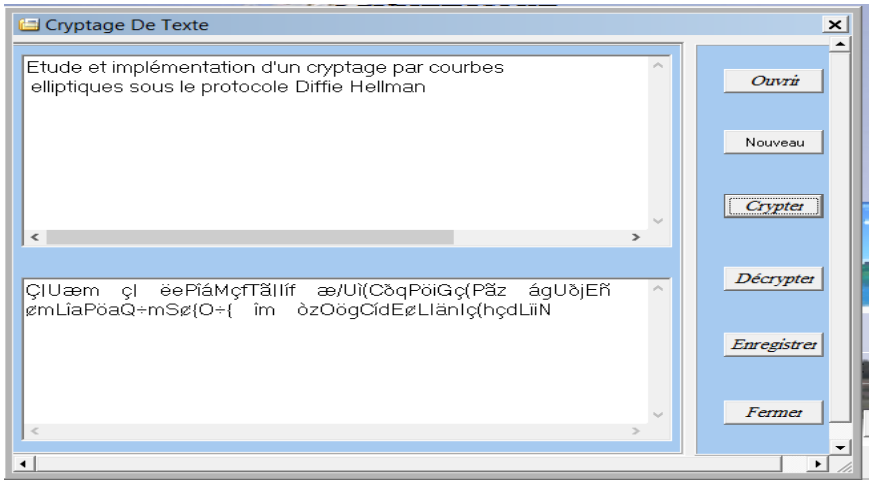


Figure IV-19: texte crypté

Changement du caractère 'm' du mot 'inverse' par un 'p'.

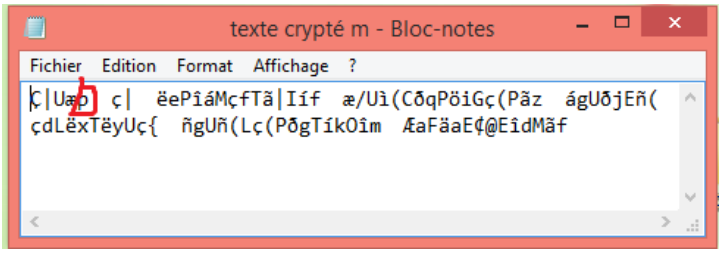


Figure IV-20:texte crypté modifié

Résultat de déchiffrement

Avec les mêmes paramètres et la même clé

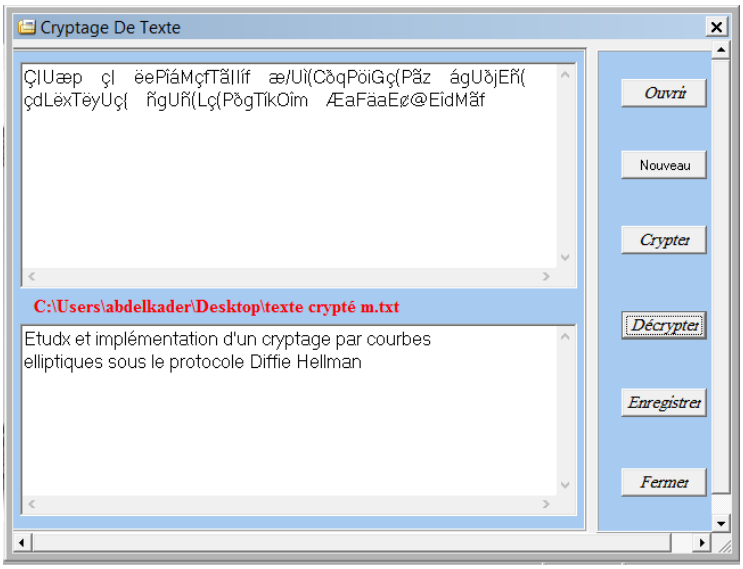


Figure IV-21: : texte décrypté

Remarque :

Si on change un caractère alors ce caractère sera changé dans le nouveau chiffrement ou déchiffrement.

IV-4-B-2 Enlèvement d'un caractère :

Chiffrement :
Suppression du 'm' du Texte chiffre.

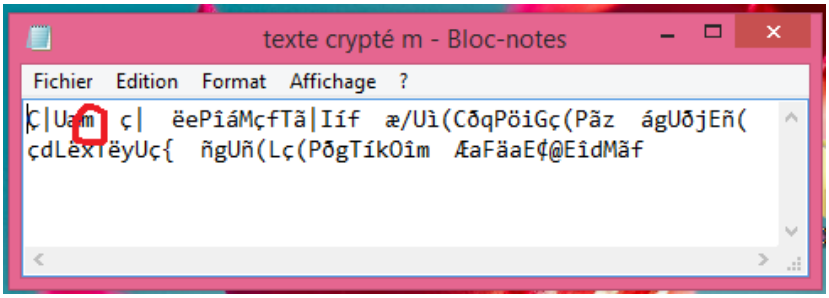


Figure IV-22: :texte crypté modifié par suppression

Résultat de Déchiffrement :
Avec les mêmes paramètres et la même clé

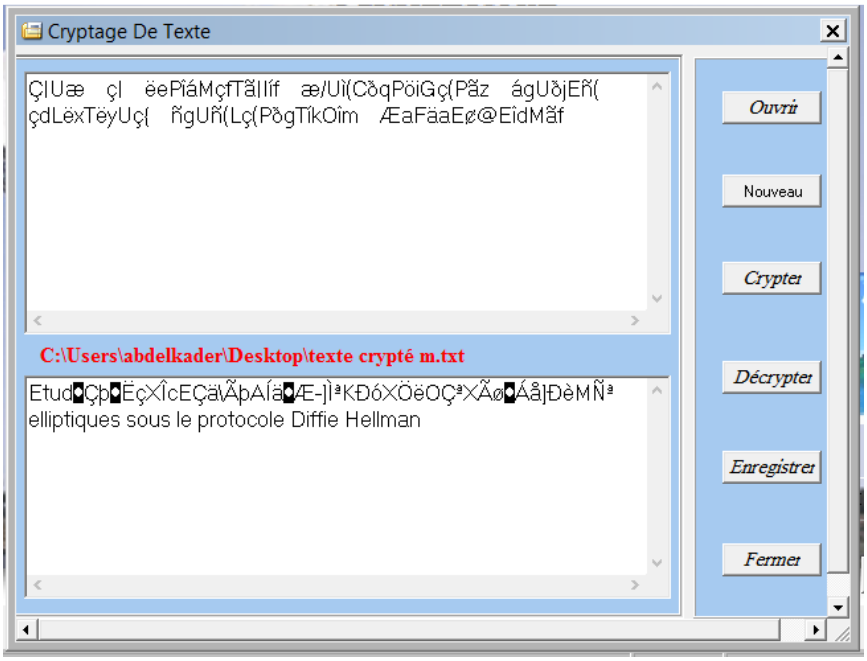


Figure IV-23 : décryptage d'un texte crypté modifié par suppression

Remarque :

si on enlève un caractère alors tous se qui suit ce caractère sera modifier dans le chiffrement ou déchiffrement ; c.-à-d. le caractère et tous ce qui suit dans la même ligne.

IV-4-B-2 Insertion d'un caractère :

Insertion d'un caractère **'Z'** dans le texte chiffre.

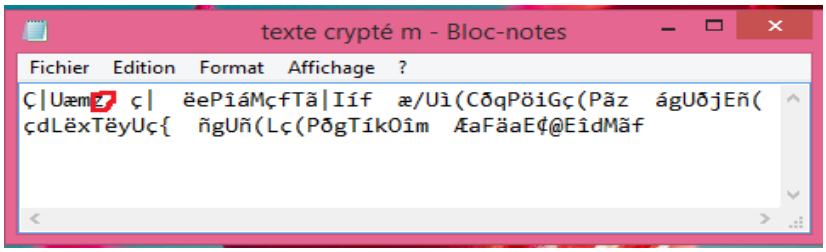


Figure IV-24: texte crypté modifié par insertion

Résultat de Déchiffrement :

Avec les mêmes paramètres et la même clé

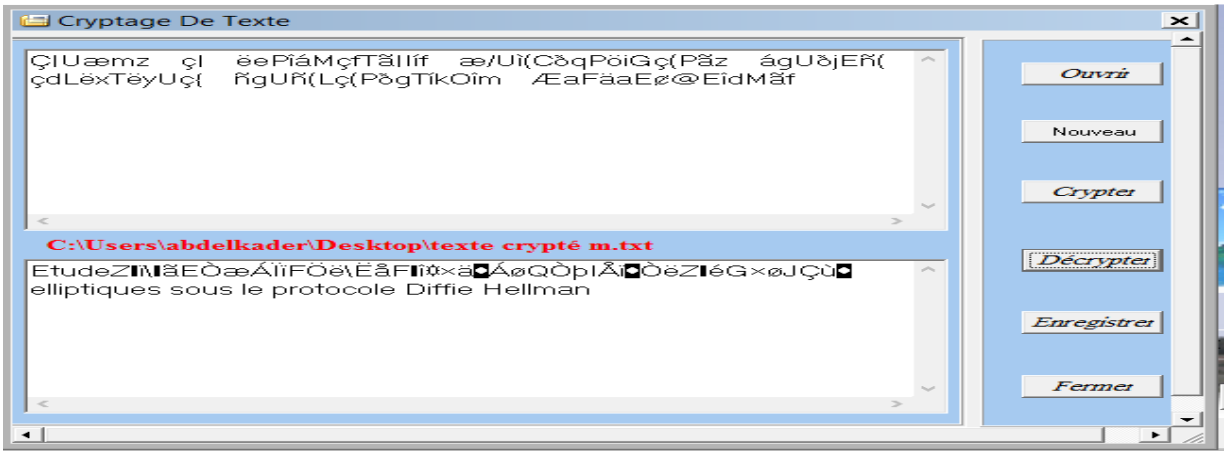


Figure IV-25: décryptage d'un texte crypté modifié par insertion

Remarque :
si on ajoute un caractère alors tous se qui suit ce caractère sera modifier dans le chiffrement ou déchiffrement ; c a d le caractère et tous ce qui suit dans la même ligne.

IV-4-B-3 Remarques et explications :

1. la taille d'un texte après le chiffrement reste inchangée.
2. le résultat du chiffrement du même texte se diffère d'une clé à une autre.
3. si on a chiffré un texte avec une clé et qu'on veut le déchiffrer avec une autre alors on aura comme résultat un texte autre que l'original.
4. le chiffrement de deux caractères identiques successifs ne donne pas deux caractères identiques, et cela à cause de la différence dans la position entre les deux.
5. si on veut modifier le texte chiffré ou déchiffré alors on aura deux cas :
    1. si on change un caractère alors ce caractère sera changé dans le nouveau chiffrement ou déchiffrement.
    2. si on enlève ou en ajoute un caractère alors tous se qui suit ce caractère sera modifier dans le chiffrement ou déchiffrement ; c a d le caractère et tous ce qui suit dans la même ligne.

C)-IMAGE :

1) Cryptage dune image noir et blanc

avec les paramètres suivants :

avec la courbe **E(-6,7, 15971)** point **p(123,793)** clé secret de L'émetteur **S=137**
point **Sp(259,1517)** clé secret de récepteurs **R=923**
point **RP(765,1169)** point **RSP(1138 ,1574)**

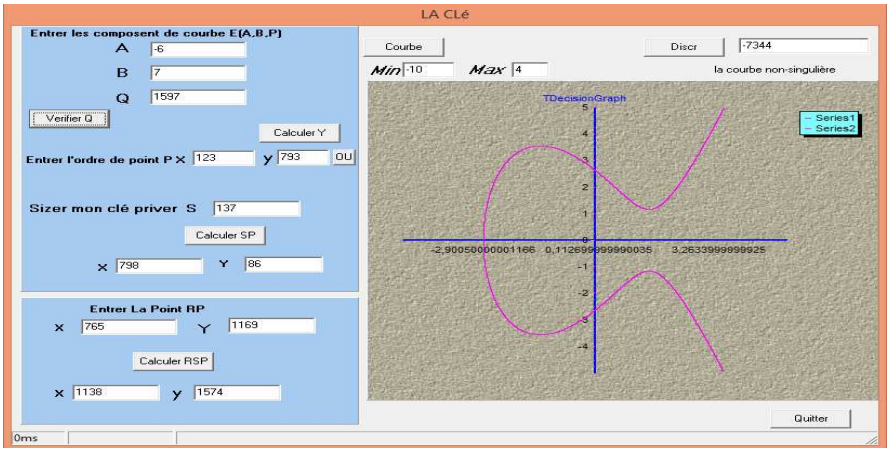


Figure IV-26: calcule de la clé

Chargement et cryptage d'image noir et blanc

chargement d'image noir et blanc **cryptage d'image noir et blanc**

Figure IV-27: cryptage d'une image noir et blanc par la clé 1138

2) **Cryptage dune image on couleur**

avec les paramètres suivants :

avec la courbe **E(-6,7, 15971)** point **p(123,793)** clé secret de L'émetteur **S=137**
point **Sp(259,1517)** clé secret de récepteurs **R=923**
point **RP(765,1169)** point **RSP(1138 ,1574) (figure23)**

Chargement et cryptage d'image on couleur :

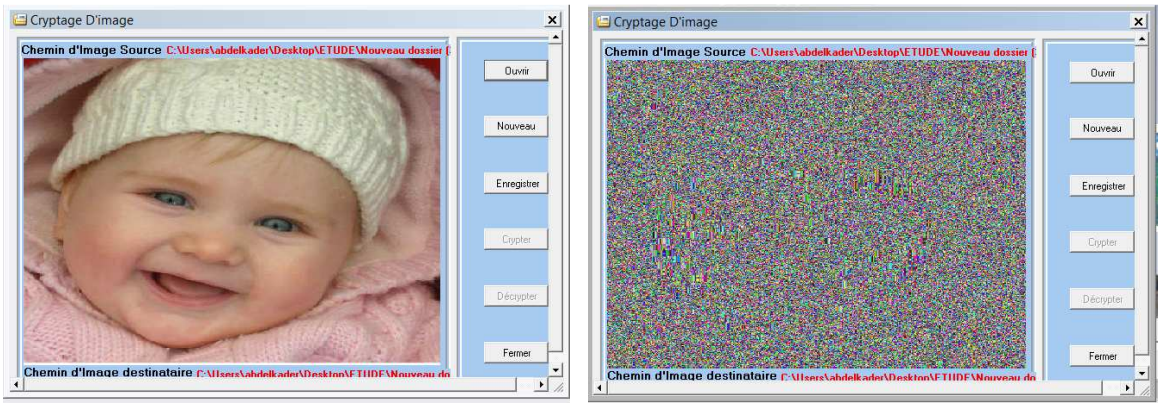


Image original **Image on couleur crypté**

Figure IV-28: cryptage dune image on couleur

Remarque :

L'image crypté sauvegardé les caractéristiques d'image originale (La taille, l'extension,…….)

Autres résultats

avec les paramètres suivants«la clé A » :

avec la courbe **E(-11,5, 17903)** point **p(43,6437)** clé secret de L'émetteur **S=** 3791
point **Sp(8062, 1357)** clé secret de récepteurs **R=757**
point **RP(10259,15823)** point **RSP(2794 , 7370)**

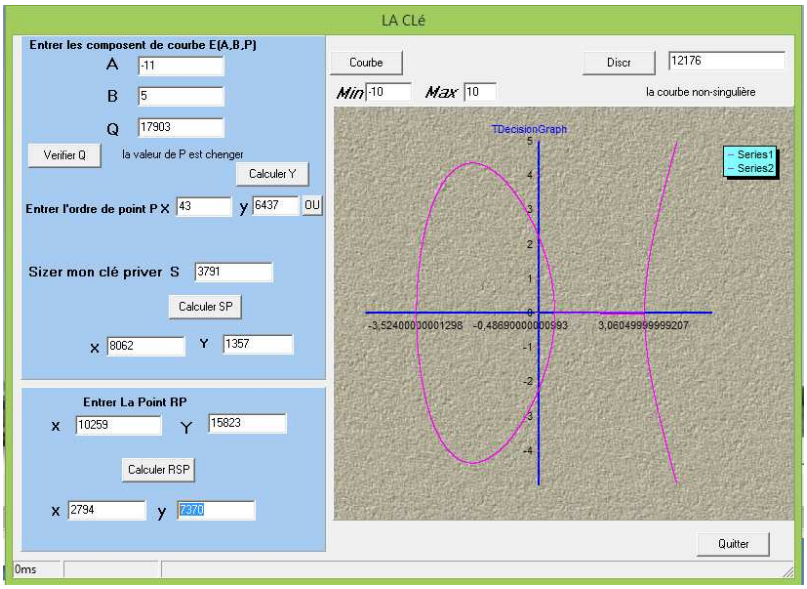


Figure IV-29: calcule de la clé A

avec les paramètres suivants «la clé B » :

avec la courbe **E(-5,7, 821)** point **p(75,158)** clé secret de L'émetteur **S=** 183
point **Sp(698, 503)** clé secret de récepteurs **R=71**
point **RP(10259,15823)** point **RSP(626 , 673)**

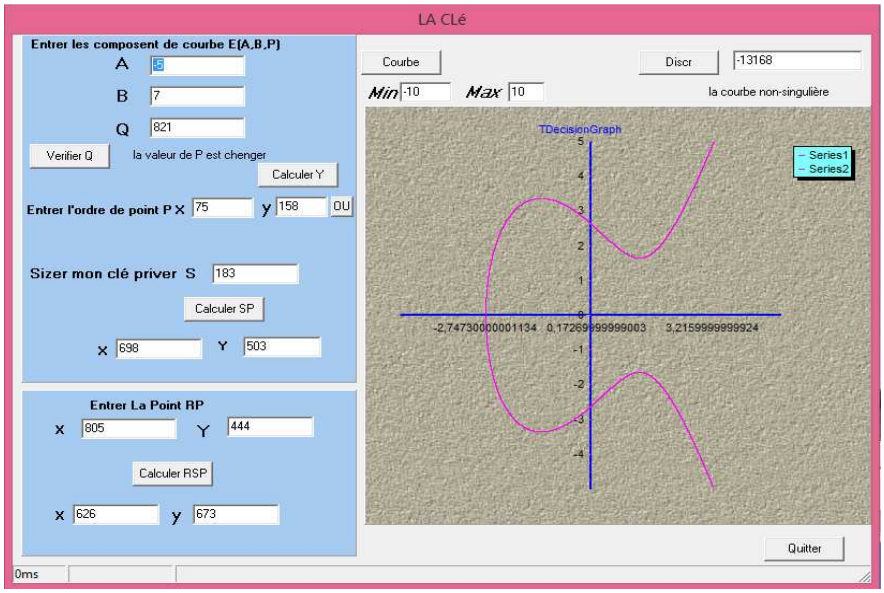


Figure IV-30: calcule de la clé B

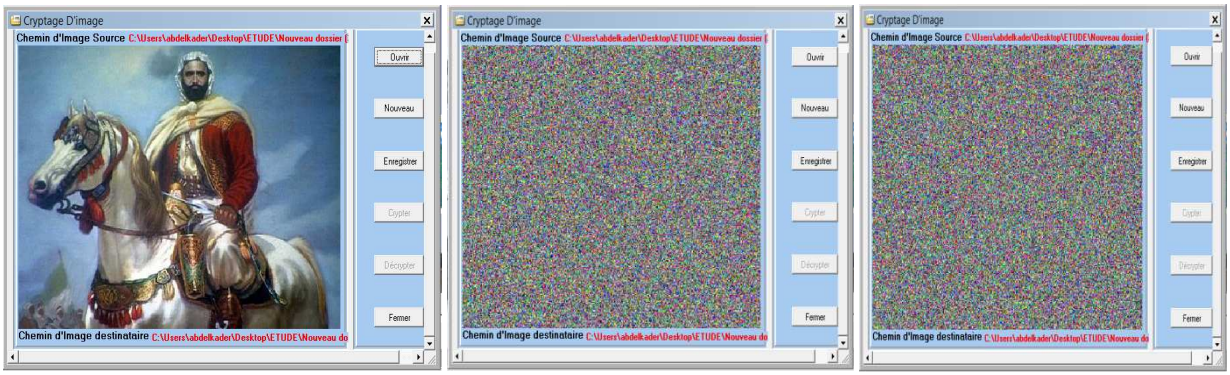


Image d'origine **image crypté par la clé A** **image crypté par la clé B**

Figure IV-31: résultat d'un cryptage d'image crypté par deux clés déférentes

REMARQUE :

Le résultat de cryptage se diffère d'une clé à une autre.

Autre resultat : avec les paramètres suivants :

avec la courbe **E(-6,7, 15971)** point **p(123,793)** clé secret de L'émetteur **S=793**
point **Sp(1471,55)** clé secret de récepteurs **R=719**
point **RP(765,1169)** point **RSP(5737 ,13130)**

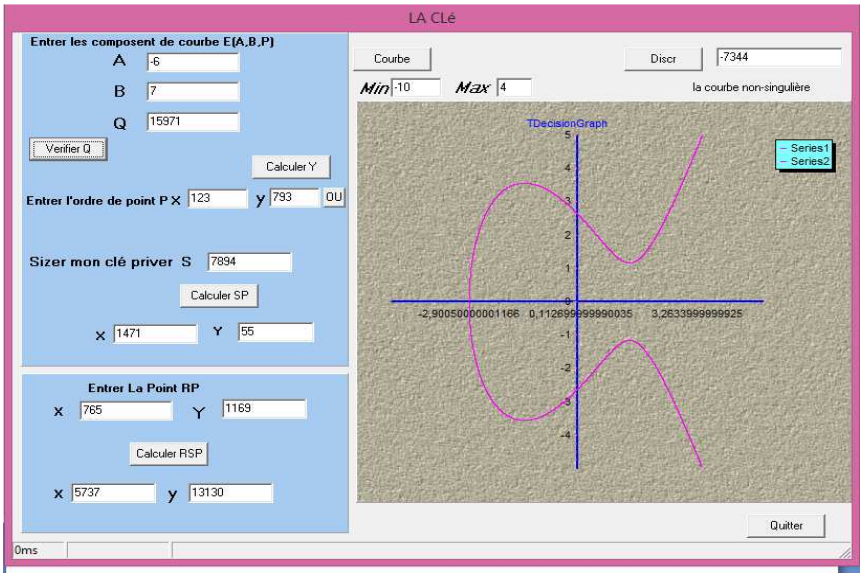


Figure IV-32: fenetre de calcule de la clé 5737

avec les paramètres suivants :

avec la courbe **E(-6,7, 15971)** point **p(123,793)** clé secret de L'émetteur **S=12345**
point **Sp(7941,12989)** clé secret de récepteurs **R=923**
point **RP(765,1169)** point **RSP(12043 ,5089)**

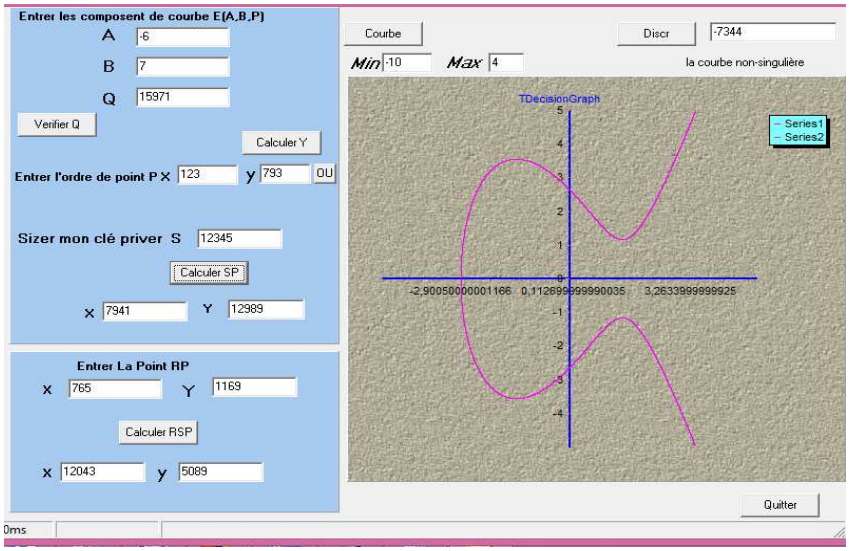


Figure IV-33: fenetre de calcule de la clé 12043

Image originale

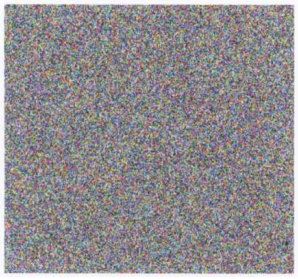


Image Crypte par la clé 5737

Image décrypté par la Clé 12043

Figure IV-34: résultat de décrypte d'une image par une clé différente a la clé de cryptage

Remarque :

Une image crypte par une clé ne peut pas être décrypte correctement si on change la clé

Décryptage d'image modifiée :

avec les paramètres suivants :

avec la courbe **E(-9,5, 15971)** point **p(43,76)** clé secret de L'émetteur **S=1177** point **Sp(1369,1781)** clé secret de récepteurs **R=523**
point **RP(276,1733)** point **RSP(725 ,713)**

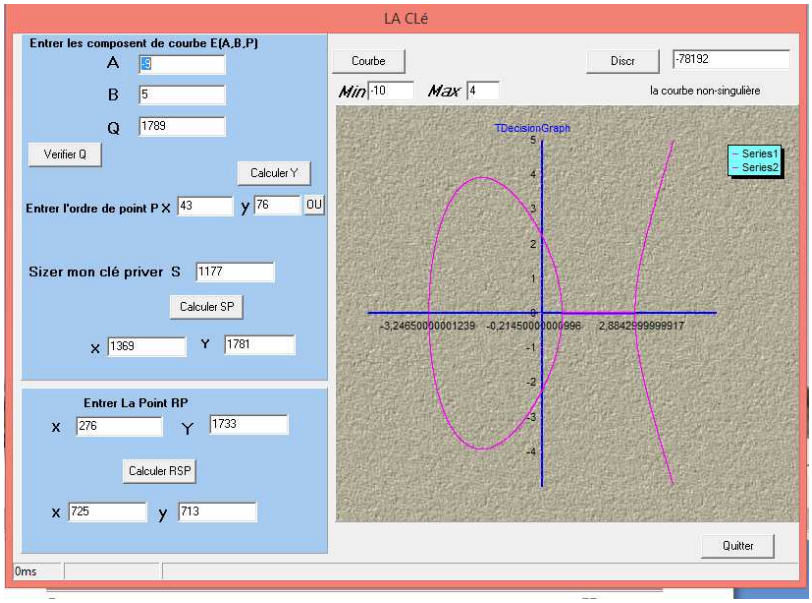


Figure IV-35: fenetre de calcule de la clé

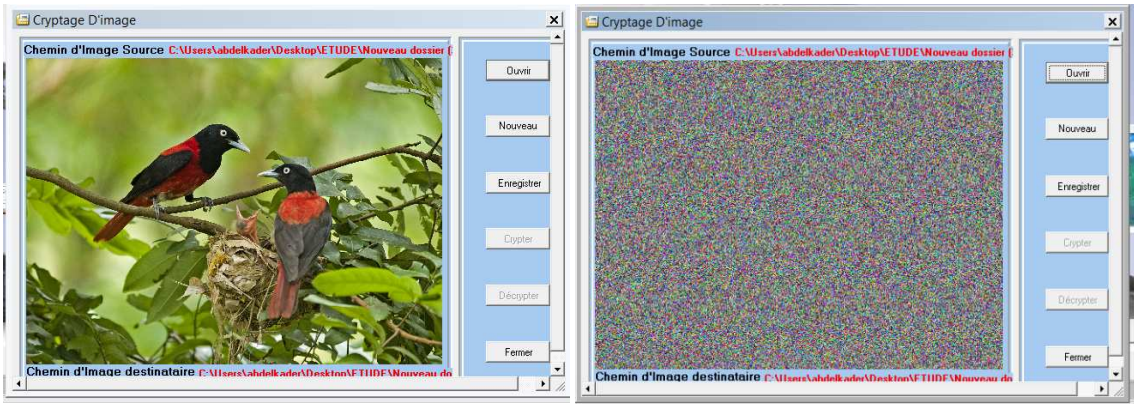


Image original **image crypter**

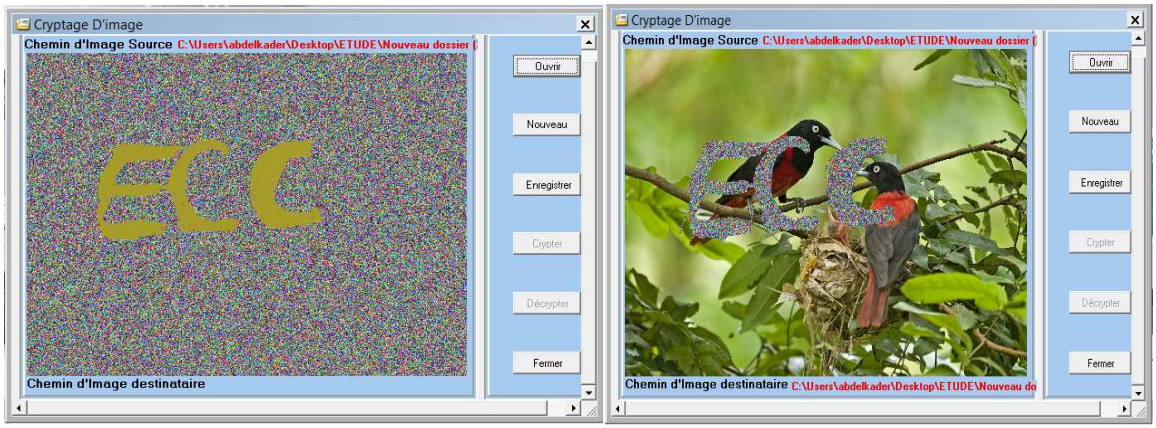


Image crypter modifier **Décryptage de l'image crypte modifier avec la même clé de cryptage**

Figure IV-36: Décryptage d'une image « crypte et modifier » avec la même clé

Remarque :

Le décryptage d'une image crypte modifiée ne donne pas l'image original (seul les pixels qui sont modifiés seraient mal décryptes).

Observations :

1. l'image crypte sauvegardé les caractéristiques d'image originale

   (La taille, l'extension,…….)

2. Le résultat de cryptage se diffère d'une clé à une autre.

3. Une image crypte par une clé ne peut pas être décrypte correctement si on change la clé.

4. Le décryptage d'une image crypte modifiée ne donne pas l'image original (seul les pixels qui sont modifiés seraient mal décryptes).

IV- 5 Comparaison du Crypto Système basé sur les courbes Elliptiques avec RSA

Pour conclure, nous donnons une comparaison de la cryptographie basée sur les Courbes elliptiques avec RSA. RSA est actuellement le système de cryptographie A clé publique le plus utilisé. Néanmoins, nous avons déjà vu que les courbes elliptiques Présentaient un certain nombre d'avantages et nous allons les expliciter Plus précisément ici.

Tous ces avantages sont base sur la différence de complexité pour résoudre Les problèmes mathématiques sous-jacents. D'un cote la factorisation (et donc RSA) peut être effectuée a l'aide d'algorithmes sous-exponentiels tandis que de L'autre seul des algorithmes exponentiels permettent de résoudre le problème du Logarithme discret sur une courbe elliptique. Cela a pour première conséquence Que les clés sont plus courtes avec ECC qu'avec RSA. Typiquement, actuellement Une clé inviolable doit avoir 1024 bits pour RSA contre 170 pour ECC. Mais le Phénomène le plus remarquable est que cette différence de taille de clé va aller en s'amplifiant avec le temps du fait de la différence de complexité. Par exemple, Pour une sécurité requise de 115 bits (c'est _a dire qu'on considère que le système est sûr si il faut plus de 2115 opérations pour le *casser),* les clés ECC seront de 230 bits tandis que les clés RSA seront de 2048 bits. On passe (entre 85 et 115 bits de sécurité) d'un rapport 6 entre les tailles de clé à un rapport 9. Cette

différence de taille de clé induit de nombreux avantages (qui vont donc aller en S'amplifiant quand on augmente le niveau de sécurité requis). En particulier, Les calculs sont à priori plus rapides et requièrent moins de mémoire.[19];[22]

Ainsi les premières applications des courbes elliptiques ont été pour les environnements Restreints (PDA, téléphones mobiles, cartes _a puces,...) qui ont peu de puissance de calcul (par exemple, traiter du 1024 bits avec un processeur 8 Bits demande une multi précision lourde) et surtout peu de mémoire disponible. En fait on s'est depuis rendu compte que même sur des machines puissantes, ECC _était intéressante. Ainsi un serveur SSL peut il traiter de 20 à 30 % de Requêtes supplémentaires avec un *ECC* 170 qu'avec RSA 1024 et 200 % avec *ECC* 230 plutôt que RSA 1024. Et encore, l'implémentation de RSA dans SSL est certainement beaucoup mieux optimise que l'adaptation à *ECC* qui en a été faite pour ce test.[26]

Plus précisément on ne peut pas vraiment dire que *ECC* soit toujours plus efficace que RSA. En e et, dans la pratique courante, on observe que *ECC* est Beaucoup plus rapide que RSA pour déchirer ou signer un message (facteur 4 à 20) c'est à dire pour les opérations privées alors que pour chiffrer ou vérifier une signature (opérations publiques), RSA est beaucoup plus rapide. En fait *ECC* met à peu prées le même temps pour tout alors que RSA est beaucoup plus déséquilibré.[19]

Le choix peut donc dépendre de l'utilisation qui doit être faite (puissance de Calcul des acteurs, exigence en terme d'efficacité pour les différentes opérations). Ainsi, si le chiffrement (opération publique) est effectue par une carte à puce et le déchiffrement par un gros serveur, RSA sera très bien adapte. Il en sera de même si le temps de déchiffrement n'a pas d'importance mais que le chiffrement doit être le plus rapide possible (en fait dés qu'il y a un déséquilibre entre l'opération publique et l'opération privée). Cela est du au fait qu'avec RSA les gens choisissent en générale comme exposant public (bien que ce soit reconnu que c'est une faille majeure de RSA) et il n'y a donc essentiellement rien a faire pour les Opérations publiques. Par contre les opérations privées

sont beaucoup plus longues car elles utilisent cette fois comme exposant l'inverse de **e** modulo (p - 1) (q - 1) qui lui pèse bien ses 1024 bits. En choisissant un autre exposant public que 3 (65535 par exemple)

RSA est encore plus rapide que ECC pour les Opérations publiques (et toujours aussi lent pour les Opérations privée bien sur) mais dans des proportions bien Plus raisonnables (facteur 2 ou 3) que c'est beaucoup plus faible qu'avec 3 car ca reste très petit. Enfin il y a fort à parier qu'avec une implémentation avec un exposant public aléatoire les Opérations publiques deviendraient aussi catastrophique que les Opérations privées sans pour autant que celles ci ne deviennent plus rapides.

Pour finir, même si c'est une opération à priori rare, il est intéressant de noter que la génération de clé (trouver deux nombres premier pour RSA, trouver un point sur la courbe pour ECC) est beaucoup plus rapide pour ECC.[19]

IV- 5-1 Comparaison des niveaux de sécurité

Le tableau suivant, élaboré par RSA Laboratoires, donne une estimation des ressources nécessaires Pour *casser les* trois systèmes ECC, RSA pour différentes tailles de clé.[25]

Année MIPS	*RSA* Taille des Clés	ECC Taille des Clés	Rapport des Tailles des Clés
104	**512**	**106**	**5 :1**
108	**768**	**132**	**6 :1**
10"	**1024**	**160**	**7 :1**
1020	**2048**	**210**	**10 :1**
1078	**21000**	**600**	**35 :1**

Table IV-2 : Estimation des ressources *nécessaires* Pour *cosser* les trois systèmes ECC. RSA et DSA

Comme la puissance de calcul des machines augmente très rapidement, les tailles des clés doivent augmenter si on veut garder le même niveau de sécurité. Mais le tableau précédent

prouve que ceci est irréalisable avec RSA pour des applications disposant de ressources limitées,

c'est pourquoi un ECC semble être idéal dans ces cas.

IV-6 Avantages et inconvénients des courbes elliptiques

Nous dressons ci-dessous les principaux avantages et inconvénients d'un point de vue ryptographique des courbes elliptiques par rapport aux systèmes plus anciens, notamment RSA.

Inconvénients

- La sécurité du système ne repose pas sur une démonstration, ni même sur la preuve que vé d'équivalence avec un problème NP-complet, mais sur l'inexistence actuelle d'une méthode sous-exponentielle pour calculer le logarithme discret dans le groupe d'une courbe elliptique.

- La vérification d'une signature électronique est un ordre de grandeur plus lent avec ECDSA qu'avec RSA (avec des tailles de clefs offrant une sécurité comparable).
- La taille d'un message chiffré par ECC est multipliée par quatre par rapport à la taille du message d'origine.

- Certaines courbes elliptiques n'offrent pas une bonne sécurité.

Avantages

- *À* sécurité équivalente, les clefs peuvent être plus petites dans les systèmes fondés sur les courbes elliptiques que dans RSA. Ainsi, un chiffrement ECC à 224 bits est équivalent à un chiffrement RSA à 2048 bits. En outre, l'écart s'accroît à mesure que la sécurité augmente.

- Des standards fondés sur les courbes elliptiques ont été proposés par l'ANSI, ITEEE, ITETF et le NIST[3]. Les courbes elliptiques peuvent d'ores et déjà être utilisées dans les protocoles SSL et IPsec.

- Beaucoup de courbes elliptiques sont a priori intéressantes d'un point de vue cryptographique. En effet, le théorème de Hasse (1933) *assure* que les courbes elliptiques sur le corps Fp ont beaucoup de solutions : si l'on note Np leur nombre, on a $|Np - p| < 2/p$.

- Des méthodes existent pour choisir de bonnes courbes elliptiques. Ainsi, le NIST a pu proposer quinze courbes dont il garantit la robustesse.

Les courbes elliptiques commencent donc à s'implanter dans l'industrie et à devenir une alternative crédible aux yeux des acteurs économiques. Si leur sécurité n'est pas démontrée de

manière théorique, on sait choisir en pratique des paramètres offrant une sécurité de bonne qualité.

IV-7 CONCLUSION :

Les systèmes cryptographiques basés sur les courbes elliptiques permettent d'obtenir un gain en efficacité dans la gestion de clés. En effet, de tels crypto systèmes nécessitent des clés de taille beaucoup plus modeste, par exemple, une clé ECC de 160 bits réalise le même niveau de sécurité qu'une clé RSA 1024 bits, ce qui représente un avantage pour les systèmes utilisant les cartes à puces dont l'espace mémoire est très limité. De plus, les algorithmes de calculs liés aux courbes elliptiques sont plus rapides, et ont donc un débit de générations et d'échanges de clé beaucoup plus important

Conclusion Générale

Conclusion générale

L'application la plus évidente de la cryptographie est la protection de la confidentialité d'une information, qu'elle soit stockée localement sur une machine ou transmise sur un réseau.
Le besoin de la confidentialité n'est pas l'apanage du militaire ou de certains gros industriels. tous les individus, toutes les organisations, ont à des degrés divers, un tel besoins. Pour cella nous avons étudiées un système de chiffrement ECC qui a les avantages suivantes :

- Facile à construire.
- Beaucoup de sécurité.
- Evolution très rapide.

Le système de chiffrement étudie est basé sur les courbes elliptiques et le protocole de deffie-hellmann qui sont très utile dans la télécommunication.
Nous souhaitons que notre travail consiste un pas appréciable et sera une orientation dans le futur pour améliorer d'autre méthodes comme :

- l'utilisation de la méthode de cahotique
- Réalisation d'autres logiciels et l'utilisation des différents format d'extension d'image.
- Application de ce protocole sur les fichier vidéo et son(avi, wav, mpg, etc…).

Bibliographie

Bibliographie

LIVRES ET MEMOIRES :

1) ***« Cryptography for the Internet » de Philip R. Zimmermann. Scientific American, octobre 1998.***

2) ***« Courbes elliptiques, Cryptographie à clés publiques et Protocolesd'échange de clés » de Demba SOW Université Cheikh Anta DIOP de Dakar 2013 .***

3) ***« cryptoghraghie basée sur les courbes elliptiques » de oudjdi damarji nazim université des sciences et de la technologie d'oran ustomb juin 2016.***

4) ***« Outils algébriques et cryptosystémes » de ADOUI Salah Université de MENTOURIE Constantine 2011 .***

5) ***« Opérateurs Arithmétiques pour la Cryptographie Basée sur les Courbes Elliptiques » de Christophe NEGRE UNIVERSITE MONTPELLIER II, 2004***

6) ***« Implémentation de benchmark d'opérations crypto baséesECC pour l'étude et comparaison de courbes elliptiques F_P et F_{2^N} » de Mahammedi Nadjiba et Mahdadi Houda UNIVERSITE KASDI MERBAH OUARGLA ,2013***

7) ***« Privacy on the Line » de Whitfield Diffie et Susan Eva Landau. MIT Press ; ISBN : 0262041677.***

8) ***« The Codebreakers » de David Kahn. Scribner ; ISBN : 0684831309.***

9) ***« Network Security : Private Communication in a Public World » de Charlie Kaufman, Radia Perlman et Mike Spencer Prentice Hall ; ISBN :0-13-061466-1.***

10) ***« Applied Cryptography : Protocols, Algorithms, and Source Code in C » de Bruce Schneier, John Wiley & Sons ; ISBN : 0-471-12845-7.***

11) ***B.Rungaldier : « Algèbre Linière Bien Tempérée » (France 1993 Code 04-03-191)***

12) ***« Handbook of Applied Cryptography » d'Alfred J. Menezes, Paul C. van Oorschot et Scott Vanstone. CRC Press ; ISBN : 0-8493-8523-7.***

13) *« Internet Cryptography » de Richard E. Smith. Addison-Wesley Pub Co ; ISBN : 0201924803.*

14) *« Firewalls and Internet Security : Repelling the Wily Hacker » de William R. Cheswick et Steven M. Bellovin. Addison-Wesley Pub Co ; ISBN : 0201633574.*

15) *« A Course in Number Theory and Cryptography » de Neal Koblitz. Sprin- ger-Verlag ; ISBN : 0-387-94293-9.*

16) *« Differential Cryptanalysis of the Data Encryption Standard » de Eli Biham et Adi Shamir. Springer-Verlag ; ISBN : 0-387-97930-1.*

17) *« algèbre linéaire » de R.Cairoli Press polytechniques romandes code 04-03-142*

18) *DRIBAT Hadja & BERMILI Rachida : Etude et implémentation d'une méthode de chiffrement en continu usto 2004*

19) *Sabeur & Tenah Mohamed : étude et implémentation d'un logiciel cryptographique à clé public : RSA (usto 2000)*

20) *Hafid mohamed amine & Daham samir : étude et implémentation d'un système cryptographique à clé secrète AES (usto 2005).*

21) *Hàgler Michael :" Courbes Elliptiques et Cryptographie" Eva Bayer Fluckiger (2006).*

22) *Marc Jove : "introduction élémentaire à la théorie des courbes elliptiques "(université catholique de louvain 1995)*

23) *J. Daemen and V. Rijmen, "AES Proposal: Rijndael," AES Algorithm Submission,3rd September 1999.*

24) *R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, "The RC6TM BlockCipher", M. I. T laboratory for Computer Science, USA, 20 August 1998.*

25) *R. F. Sewell, "Bulk Encryption Algorithm for Use with RSA," Electronics Letters,Vol. 29, No. 25, pp. 2183-2185, 9th December 1993.*

26) *D. Stinson, "Cryptography: Theory and Practice", 2nd edition, Chapman & Hall CRC Boc Raton, USA, 2002.*

27) ***"New directions in cryptography" W. Diffie and M. E. Hellman. IEEE Transactions on Information Theory (IT), Vol. 22, No. 6, pp.644–654, November 1976.***

28) ***"Asymmetrical Encryption Based Automated Trust Negotiation Mode" H Jin, Z. Liao, D. Zou, and C. Li, , The 2nd IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp. 363- 368, Feb. 2008.***

29) ***R. Kusters and M Tuengerthal, "Universally Composable Symmetric Encryption", The 2nd IEEE Computer Security Foundations Symposium (CSF), pp. 293- 307, July 2009.***

30) ***D E Newton, "Encyclopedia of Cryptology, ABC-CLIO Inc , California", USA, 1997.***

31) ***S. Lian, "Multimedia content encryption: techniques and applications", CRC Press LLC, 2009.***

ANNEXE

Annexe

1 L'algorithme RSA
1-1 Cryptographie des Données par RSA:
1-1-1 Le Protocole d'Encryption :

RSA est basé sur la difficulté de factoriser un nombre qui est le produit de deux grands nombres premiers. On sait que, si A est un entier quelconque, alors : Acd = A (mod n).

C'est cette identité qui va tout faire fonctionner. Création des clefs. Destinataire :

Construit un quadruplet de nombres (p, q, e, d)

L'utilisateur choisit deux grands nombres p et q premiers et les multiplié pour obtenir n = p * q.

Il choisit un nombre grand e et premier avec (p - l)*(q - 1).

On calcul d inverse de e, tel que : ed - 1 est un multiple de (p - l)(q - 1)

C'est-à-dire tel que :Ced = 1 mod (p-l)(q-l)

Celle-ci peut être résolue grâce à une version étendue de l'algorithme d'Euclide.

Publication la clef publique :.

Destinataire rend publics (n, e), qui constituent la clef publique. Il la publie dans un annuaire ou la communique à Emetteur, qui la lui demande. Il ne communique surtout pas p, q ou d.

Les nombres p et q peuvent être oubliés, car ils ne serviront plus à personne. Le nombre (n, d) constitue la clef secrète de Destinataire

Transmission d'information.

Emetteur, qui veut transmettre une information secrète à Destinataire, transforme son information en un nombre entier A, inférieur à n (ou en plusieurs si nécessaire), en utilisant des conventions connues de tous comme par exemple le code ASCII.

Une personne voulant envoyer le message A au propriétaire des paramètres

(n, e) va décomposer A en blocs a,- de longueur strictement inférieure à la taille (en nombre de chiffres) de n. ;Chiffrage de l'information.

Emetteur calcule, grâce à la méthode d'exponentiation rapide : o Calculer pour tout i :

b = a* Mod n o Former le message B en regroupant les blocs b,-.

o B = Ae (mod n), envoie B à Destinataire par un canal qui n'a pas besoin d'être protégé (par exemple, le courrier électronique).

Déchiffrage de l'information.

Destinataire, pour décoder B, calcule Bd (mod n), ce qui lui redonne A, car, d'après le théorème du RSA, on a :Bd = Aed =A (mod n).

Exemple de Cryptage

Si p = 47 et q = 71 alors N= p.q = 3337

La clef de chiffrement e ne doit pas avoir de facteurs communs avec :(p-1). (q-1) = 46.70 = 3220

On choisi e (aléatoirement) égal à 79. Dans ce cas :d = 79 1 mod 3220 = 1019

Ce nombre a été calculer on utilisant l'algorithme d'Euclide étendu. On publie e et on garde d secret. On jette p et q.

Pour chiffrer le message : m = 6882326879666683

Divisant le en petit blocs. Des blocs de trois chiffres conviendront dans ce cas ci. Le message est divisé en six blocs mi tels que :mi = 688 ; m2 = 232 ; m3 = 687 m4 = 966 ; m5 = 668 ; m6 = 3

Le premier bloc est chiffré par : 688 79 mod 3337 = 1570 = Ci

En effectuant la même opération pour tous les blocs, on obtient le message chiffré :

C = 1570 2756 2091 2276 2423 158

Pour déchiffrer le message, il faut effectuer les mêmes exponentiation mais en utilisant la clef de déchiffrement 1019 Donc :1570 1019 mod 3337 = 688 = mi

Le reste du message est obtenu de la même manière.

1-1-2 Résultats et Interprétations

Annexe

Afin d'illustrer le système de cryptage à clé publique RSA appliqué aux stockage et à la transmission des données sous forme images et / où textes nous tenons compte de :Génération des clés.
Cryptage de textes.
Pour la génération des clefs on choisi p = 19 et q = 101 alors n = p.q = 1919;
(p -1) (q - 1) =1800 ; e premier On trouve alors:

N°	p	9	N=p.q	e	d
1	101	19	1919	401	1001
2	211	59	12449	8999	10859
3	181	109	19729	9599	19199
4	419	59	24721	6999	18099
5	151	101	15251	2999	11999
6	307	113	34691	3499	30883
7	503	53	26659	2799	10007
8	109	307	33463	7399	30511
9	601	97	58297	7699	28699
10	419	113	47347	7299	19659

Tableau Génération de quelques clés de cryptage

d = 151 1 mod 1800 = 751
Lire un texte (d'extension *. TXT) caractère par caractère et le convertir en nombre, on se servant de la table d'ASCII, par exemple nous allons crypter le texte clair «Qui veut aller loin ménage sa monture » avec différents clefs:

texte en clair	«Qui veut aller loin ménage sa monture»
conversion en nombre.	81 117 105 118 101 116 117 97 108 108 101 114 108 111 105 110 109 233 110 97 103 101 115 97 109 111 116 117 101
Texte crypté avec la clé (N=1919 ; E=151)	00586 00420 00509 00000 01431 01111 00420 00793 00000 00299 00599 00599 01111 00114 00000 00599 01404 00509 00716 00000 00497 01111 00716 00299 00806 01111 00000 00115 00299 00000 00497 01404 00716 00793 00420 00114 01111 .
Texte crypté avec la clé (N= 64507, E= 5079)	13510 55093 30365 00000 46016 36989 55093 04955 00000 40301 10412 10412 36989 42467 00000 10412 25711 30365 20372 00000 08633 36989 20372 40301 29855 36989 00000 02598 40301 00000 08633 25711 20372 04955 55093 42467 36989

Nous remarquons que le changement des clefs donne des résultats différents. La taille ne change pas avec le changement des clefs, car les caractères sont lus un par un, convertis en nombre (Code ASCII), on ajoute à chaque nombre des zéros non significatifs pour former des blocs de cinq chiffres et coder bloc par bloc.

Annexe

Prenons maintenant une seul lettre, par exemple la lettre a et essayons de la cryptée avec les clefs (N=1919 et E=151)

texte en clair	LA
conversion en nombre.	97
Texte crypté avec la clé *N=1919 et E=151'	00299

La taille du texte crypté est plus grande que la taille du texte clair.

Blowfish [Al]:

A été conçu par Bruce Schneier en 1993 comme étant une alternative aux algorithmes existants, en étant rapide et gratuit. Blowf ish est sensiblement plus rapide que le DES. Il est un chiffrement Feistel, utilisant itérativement une fonction de chiffrement 16fois. La grandeur des blocs est de 64 bits.

Il peut prendre une longueur de clé variant entre 32 bits et 448 bits.

Depuis sa conception il a été grandement analysé et est aujourd'hui considéré comme étant un algorithme de chiffrement robuste. Il n'est pas breveté et ainsi son utilisation est libre et gratuite.

Cet algorithme peut être optimisé dans les applications matérielles (puces), mais il est surtout utilisé dans des logiciels.

Il y a deux parties dans l'algorithme : une première partie qui manipule l'expansion de la clé et une deuxième partie qui manipule le chiffrement des données.

L'algorithme DES [A2]:

Data Encryption Standard, a été créé dans les laboratoires de la firme IBM Corp. Il est devenu le standard du NIST en 1976 et a été adopté par le gouvernement en 1977. C'est un chiffrement qui transforme des blocs de **64 bits** avec une clé secrète de **56 bits** au moyen de permutations et de substitutions. Le DES est considéré comme étant raisonnablement sécuritaire.

Le DES est officiellement défini dans la publication FIPS 46-3 et il est public.

La clé est en fait constituée de 64 bits, dont 56 bits sont générés aléatoirement et utilisés dans l'algorithme. Les huit autres bits peuvent être utilisés pour la détection d'erreurs (dans une transmission par exemple). Chacun des huit bits est utilisé comme bit de parité des sept groupes de 8 bits.

Comme blowfish, le DES est un chiffrement Feistel. Il utilise les transformations de substitution et de transposition (chiffrement par produit). Il est aussi appelé Data Encryption Algorithm (DEA).

IDEA [A3] :

Développé à Zurich en Suisse par Xuejia Lai et James tAassey en 1992, le chiffrement par blocs IDEA (International Data Encryption Algorithm) utilise des blocs de **64 bits** et est contrôlé par une clé de **128 bits.** Malgré le fait que IDEA n'est pas un chiffrement Feistel, le déchiffrement est effectué avec la même fonction que celle utilisée dans le chiffrement. L'algorithme a innové dans son domaine en utilisant des opérations de trois groupes algébriques différents. Le processus de chiffrement est le même que pour le déchiffrement, à moins d'une utilisation de différentes sous-clés, ce qui est rare. En gros, le processus se résume à huit étapes de chiffrement identiques, les rounds, suivies d|une transformation au bloc de sortie. Contrairement au DES et à Blowfish, IDEA n'utilise aucune 5-Box.L'algorithme peut être utilisé avec les modes d'opération ECB, CBC, CFB et OFB. Sa vitesse est environ la même que le DES.

4- RC2, RC5 et RC6 [A4] :

Sont des algorithmes créés par Ronald Rivest pour la RSA Security. L'acronyme "RC" signifie "Ron's Codé1 ou xxRivest's ûpher*\

Annexe

RC2 :
Le RC2 a été conçu en 1989. Il avait été programmé pour être efficace avec les processeurs de 16 bits comme remplacement au DES. Il s'opère sur des blocs de **64 bits.** La grandeur de la clé est variable, de 1 octet (8 bits) à 128 octets (1024 bits). Habituellement, l'algorithme s'applique avec une clé de **64 bits.**
Le procédé nouveau qu'a apporté cet algorithme a été d'offrir aux utilisateurs la possibilité de choisir la grandeur de la clé. Cette propriété est maintenant offerte dans plusieurs chiffrements par blocs, étant primordiale dans les applications commerciales.

RC5 :
Le RC5 a été conçu en 1995. Il a l'avantage d'avoir une longueur de bloc de données variable, un nombre de rounds variable et une clé de longueur variable. Ainsi, l'utilisateur a le contrôle sur le rapport entre la vitesse d'exécution et la sécurité de son chiffrement. En général, une longue clé et un nombre élevé de rounds assurent une plus grande sécurité. La taille des blocs de données pour sa part accommode différentes architectures de systèmes.
La simplicité de l'algorithme du RC5 rend son implémentation facile et, le plus important, rend son analyse plus aisée. De plus, la forte utilisation des décalages de bits (appelés rotations) dans le chiffrement prévient I'usage de la cryptanalyse linéaire et différentielle. En plus du mode EBC (Electronic Code Book), le RC5 est aussi utilisé avec le mode CBC (Cipher-Block Chai ni ng).
RC6 :
Le RC6 a été créé en 1998. Il propose des améliorations au RC5 et, comme celui-ci, est fortement dépendant de la transformation de décalage de bits (rotation). Comme le RC5, il a l'avantage d'avoir une longueur de bloc de données variable, un nombre de rounds variable et une clé de longueur variable.
Toutefois, il utilise la multiplication, ce qui augmente la diffusion dans chacun des rounds, donc la sécurité, et il a dû se conformer à des spécifications : opérer des blocs de 128 bits divisés en quatre dans le traitement et être hautement sécuritaire par rapport à sa complexité. RC6 a été soumis au NIST pour devenir le nouveau standard de la cryptographie avancée (Advanced Encryption Standard - AES).
Rijndael [A5] :

Rijndael a été conçu par Joan Daemen et Vincent Rijmen, deux chercheurs de la Belgique, dans le but de devenir un candidat à I ' Advanced Encryption Standard (AES) du NIST. Après avoir réussi à se classer dans les six premiers, Rijndael a été choisi le standard en 2000, prenant la place du premier véritable standard de la cryptographie : le DES. Le chiffrement a une longueur de bloc variable, une longueur de clé variable et un nombre de rounds variables. Par contre, Rijndael version "AES" est restreint à des longueurs de clé de **128, 192** et **256 bits** avec une longueur de bloc fixée à **128 bits.**
Trois critères principaux ont été respectés dans sa conception :
Résistance face à toutes les attaques connues;
rapidité du code sur la plus grande variété de plates-formes possible
simplicité dans la conception.
Rijndael (1998) a été fortement influencé par son prédécesseur, l'algorithme Square (1997). Les algorithmes Crypton et Twofish utilisent aussi des opérations de Square.
AES [A6]:
(Advanced Encryption Standard) qui remplace DES. Choix de Rijndael parmi 15 puis 5 algorithmes, d'evelopp'e en Belgique par **I"** équipe de Bart Preneel (Joan Daemen et Vincent Rijmen)% a Louvain.
7- L'algorithme de Schoof [A7]:

Annexe

Nous allons maintenant présenter un algorithme du a René Schoof qui permet de calculer #F(Fp) pour un grand nombre premier **p.** Sa complexité est O Ainsi nous pourrons calculer #E(Fpn) grâce au théorème
Soit E : **y2 = v3** +.-H **+ S** une courbe elliptique définie sur Fp avec P un nombre Premier et soit Q = p + l - PE(Fp). L'idée de cet algorithme est de déterminer U **mod;** Pour de petits nombres premiers:. Par le théorème de Hasse nous avons p + **1 -** 2jp < #E(Fp) < p **+ 1 +** 2jp, i.e. |U| **s 2V p.** Il nous suffit donc de prendre tous les k premiers nombres
premiers //de manières a avoir pour pouvoir déterminer #E(Fp) de manière unique grâce au théorème chinois.
Notons **5** l'ensemble de ces premiers. On remarque que puisque p est grand, les premiers U sont petits par rapport a p et U **- p.** Nous allons maintenant voir comment déterminer a?jwdi: pour les différents **II e 5.**
Cas : **= 2** : Si **E(Fp) = 0 (mod2)** 3ca veut dire que l'ordre du groupe est pair, sinon son ordre est impair. Nous savons que les seuls éléments d'ordre 2 de E(Fp) sont de la forme **<>,0)** avec e e Fp, i.e. <?est une racine de **x3 *** Ax **+ 5** et donc p **+ 1 - a = 0(.mod2)** ce qui veut dire que
a = 0 (mod 2).
Si **x3 + Av + 5** n'a pas de racine dar\sFp, alors **#E**(Fp) = **1 (mod 2)** et donc **a s 1 (mod 2).**
Pour d'eterminer si ***3 +** **+ S** possède des racines dansF^-, il suffit de se rappeler que les éléments defp sont exactement les racines de x* - x. Ainsi **v1** + Ax + S a une racine dans Fp si et seulement s'il a une racine en
commun avec xp - x, i.e si et Seulement si
PGDCÇx3 + Ax **+ 5, v~ - v) «t 1.**
Pour faire ce calcul, nous utilisons l'algorithme d'Euclide applique aux polynômes.
Si **p** est grand, le polynôme xp est de degré grand. Il est donc préférable de calculer
[x] = xp **(mod** x3+Ax**+b)**
Et d'utiliser le résultat suivant :
PGDC([x] - x,xl + Ax **+ 5) =** PGDC(x* - x,x2 **+ Ai + 5).** Ceci termine le cas **1 = 2.**
Cas f * 2: D'après le théorème 1.15, pour déterminer **a (mod**Je), il suffit d" examiner quelle relation du type o£ -kop+p Peut avoir lieu sur £[.':] On aura alors k s a:mod
8-Baby Step, Siant Step [A8] :
Cette méthode, développée par D. Shanks, fait environ **NTï** pas et stocke environ **N7ï** données.
C'est pourquoi elle ne fonctionne bien que pour des N de taille modérée. Par commodité, dans ce paragraphe, nous exposons la méthode du Baby Step, 6iant Step pour un groupe de la forme E(Fq) avec E une courbe elliptique sur Fq mais elle est valable pour un groupe quelconque. Nous supposerons qu'il existe un nombre entier k tel que Q = kF avec

Et que **.V,** l'ordre de E, est connu. L'algorithme se déroule comme suit :
Choisir un entier m **>** \~**Y** et calculer mP.
Calculer et stocker dans une liste les tP pour o < t < m.
Calculer les points Q - jmP pour / = **0,1** m - l jusqu'xa ce qu'un
de ces éléments correspondent a un iP de la liste précédente.
Si iP - Q - jmP, nous avons Q = kF avec fe **s** t **4** jm (mod **.Y).**
Nous allons maintenant regarder pourquoi cet algorithme fonctionne. Puisque **m2** > N, nous avons **0** < k < m2. Ecrivons k = kQ - mktt ainsi k = kO {mod m).
avec 0 <kc < m et kl = (k - fkj _0)/m et donc 0 < kl < m.
Posons i = **H**0et / = klt
nous obtenons donc
Q - ktmP - kP - lcxmP = k0P
est la relation voulue.

Annexe

Le point iP est calculé en ajoutant P ("baby step") a (i - i)P. Le point Q - fmP est trouvé en ajoutant - mP ("giant step") a
Q - U -
Remarquons que nous ne devons pas connaître l'ordre exact de E(Fq). Nous devons juste connaître une borne supérieure de N. Ainsi pour une courbe elliptique définie sur un corps fini Fq, nous pouvons prendre un m tel que m2 > q **- i - 2** ~q Par le théorème de Hasse.

9-L'algorithme MOV se déroulé ainsi [A9] :
Choisir un point T **e** E(Fqm)
Calculer M, l'ordre de 7.
Soit d = PGDC(M,N). Posons r, = (M/d)T. l'ordre de 7\ est d. Celui-ci divise .V, ainsi r, 6 f[.v].
Calculer = ^'(P.r^et **ç>; =** eXiQS^. Donc ^ et <*>: sont dans **ud e |iN e F^m.** En effet,
1 = eS(P.O) = eMP.dT^) = eN(P,TJ}4 = <pf idem pour <p:.
Résoudre le problème du logarithme discret pour dans/7;-). Nous trouvons k {modd).
Recommencer avec des points T choisis au hasard jusqu'xa ce que nous ayons PGDC(\l.\r) = **.Y.** Cec\ détermine **K** (modX).
Remarque. A priori, on pourrait penser que le cas d = 1 apparaisse très fréquemment.
En réalité, il se passe le contraire. Voyons pourquoi. Rappelons que
E(Fqm) = Z/n^Z- Z/n:Z
pour des entiers nlt nz tels que **>z_ih_2.** Ainsi X\n:, puisque n: est l'ordre le plus grand possible pour un élément du groupe E(Fq^.). Soient **51.52** des points d'ordres nl.nl respectivement tels qu'ils engendrent E(Fqm) Nous pouvons donc écrire
T = alBl - a2B2.
Soit Ie\Xavec / premier. Donc lf \n2 avec f > e. Si î **# Q2,** alors /' l'ordre de r. En effet,

Puisque B1,B2 engendrent **£(F-m),** cela implique Que **A/ftjBj = Afa2£: =** o et donc que **wJAfa^,** de plus l *** a:** et **Z* j?z>,** donc /' **|M.** Ainsi l*| cf# avecd = PGDC(M,X).
La probabilité que **Z * a,** est de l - l/l, et donc la probabilité que d **# 1** est au moins **1 - i/J.** Ainsi, âpres avoir choisi plusieurs T différents nous devrions trouver un d *** 1,** et après quelques itérations de l'algorithme trouver k.
Montrons maintenant que dans le cas d'une courbe elliptique super singulière
Nous pouvons, en général, prendre m = 2.
Soit E une courbe elliptique définie sur Fq ou q est la puissance d'un nombre
premier p.
Alors *£(fq) = q - i - **a, Entête du fichier**
La signature (sur 2 octets), indiquant qu'il s'agit d'un fichier BMP à l'aide des deux caractères
La taille totale du fichier en octets (codée sur 4 octets) Un champ réservé (sur 4 octets) L'offset de l'image (sur 4 octets), **Entête de l'image**
La taille de l'entête de l'image en octets (codée sur 4 octets). Les valeurs hexadécimales suivantes sont possibles suivant le type de format BMP : La largeur de l'image (sur 4 octets), c'est-à-dire le nombre de pixels horizontalement (en anglais width)
La hauteur de l'image (sur 4 octets), c'est-à-dire le nombre de pixels verticalement (en anglais height)
Le nombre de plans (sur 2 octets). Cette valeur vaut toujours 1 La profondeur de codage de la couleur (sur 2 octets), c'est-à-dire le nombre de bits utilisés pour coder la couleur. Cette valeur peut-être égale à 1,4, 8,16,24 ou 32
La méthode de compression (sur 4 octets). Cette valeur vaut 0 lorsque l'image n'est pas compressée, ou bien 1, 2 ou 3 suivant le type de compression utilisé :
La taille totale de l'image en octets (sur 4 octets).

Annexe

La résolution horizontale (sur 4 octets), c'est-à-dire le nombre de pixels par mètre horizontalement
La résolution verticale (sur 4 octets), c'est-à-dire le nombre de pixels par mètre verticalement
Le nombre de couleurs de la palette (sur 4 octets)
Le nombre de couleurs importantes de la palette (sur 4 octets). Ce champ peut être égal à 0 lorsque chaque couleur a son importance

الملخص: تم مؤخرا إحياء نظرية المنحنيات الإهليلجية بظهور التشفير .بدأ كل شيء عندما اكتشف لينسترا خوارزمية عاملية متعددة الحدود على هذه الهياكل، ثم في عام 1985، اقترح كوبليتز وميلر بشكل مستقل للتكيف مع بروتوكولات التشفير الموجودة على المنحنيات الإهليلجية.
في هذه المذكرة ندرس المنحنيات الإهليلجية ومجموعة طوبوغرافية من هذه المنحنيات .وسيظهر أيضا أن منحنى بيضاوي الشكل يمكن أن يكتب في شكل معين يسمى "معادلات ويرستراس" وأخيرا مخطط التشفير من ديفي-هلمان التي سيتم تكييفها لاستخدامها على المنحنيات الإهليلجية.

Abstract: The theory of elliptic curves has recently been revived by the emergence of cryptography. It all began when Lenstra discovered a polynomial factorization algorithm on these structures. Then, in 1985, Koblitz and Miller independently proposed to adapt the existing cryptographic protocols on the elliptic curves.
In this memory, we study the elliptic curves and the topological group of such curves. It will also be shown that an elliptic curve can be written in a particular form called "Weierstrass equations" and finally the cryptographic scheme of Diffie-Helman which will be adapted to be used on elliptic curves.

Résumé: La théorie des courbes elliptiques a connu un récent regain d'intérêt grâce à l'émergence de la cryptographie. Tout a commence lorsque Lenstra a découvert un algorithme de factorisation polynomial sur ces structures Ensuite, en 1985, Koblitz et Miller ont proposé indépendamment d'adapter les protocoles cryptographiques existant sur les courbes elliptiques.

Dans cette mémoire on étudier les courbes elliptiques et le groupe topologique d'une telles courbes. Il sera également montré qu'une courbe elliptique peut s'écrire sous une forme particulière appelée « équations de Weierstrass » et enfin le schéma cryptographique de Diffie-Helman qui sera adapté pour pouvoir être utilisés sur les courbes elliptiques.