Implémentation et réalisation

Introduction

Dans ce chapitre, nous avant essayer d'implémentation de quelque algorithmes de cryptage d'image,tels que : RSA, EL Gamal et les courbes elliptiques .Ensuite on présente les résultats de l'implémentation de ces algorithmes qui sont appliqués sur différents types d'images médicales.
Une interprétation des résultats est faite moyennant comme critères d'évaluation de la qualité du chiffrement : l'histogramme, la corrélation et l'entropie.

Présentation des algorithmes

Algorithme RSA

RSA est un système cryptographique, ou crypto-système, pour le chiffre- ment à clé publique.

Il est souvent utilisé pour la sécurisation des données confidentielles, en particulier lorsqu'elles sont transmises sur un réseau peu sûr comme Internet.

Principe de fonctionnement : Génération des clés :

Pour générer le pair de clés RSA on suit les étapes suivantes :

1. Générer deux grands nombres premiers p et q.
2. Calculer n : n= p*q.
3. Calculer $\varphi(n)$: $\varphi(n)$= (p-1)(q-1)
4. Sélectionner un entier e $s]$ 1, $\varphi(n)$(n) [tels que : pgcd ($\varphi(n)$, e)=1 (e est premier avec $\varphi(n)$)
5. Calculer d= e_1 dans Z$\varphi(n)$ c.à.d : d*e =1 mod $\varphi(n)$ ou e*d mod ($\varphi(n)$)=1

- clé publique = (e,n).
- clé privé = (d,n).

Chiffrement et Déchiffrement d'un message

Soit m le message en clair (non crypté) et c le message encrypté.

1.Pour encrypter le message : c = m^e mod n 2.Pour décrypter le message : m = c^d mod n

Soit Alice la personne qui désire recevoir un message chiffré, et Bob la personne qui envoie le message.

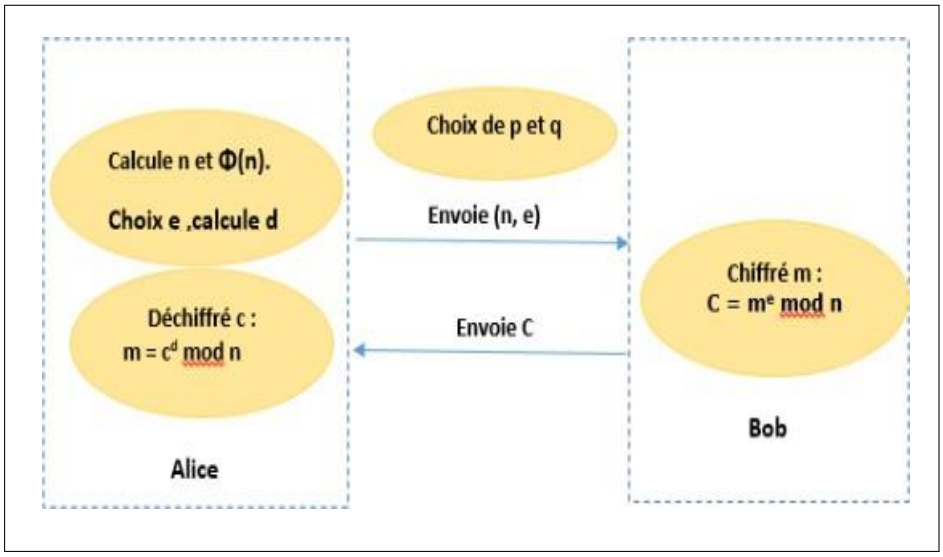


FIGURE 4.1 – principe de l'algorithme RSA

.

Comme illustre la figure ci-dessus, Alice choisit p et q et fait leur produit n = p.q. Puis elle choisit un entier e premier avec $\varphi(n)$. Enfin, elle publie dans un annuaire, par exemple sur le web, sa clef publique : (n, e).
Bob veut donc envoyer un message à Alice. Il cherche dans l'annuaire la clef de chiffrement qu'elle a publiée.
Le message m est chiffré par la formule c= m^e mod n, où c est le message chiffré que Bob enverra à Alice.
Alice calcule àpartir de p et q, qu'elle a gardés secrets, la clef d de déchiffrage (c'est sa clef privée). Le message chiffré C sera déchiffré par la formule m
= cd mod n.

Exemple

Supposons qu'on veuille envoyer le message sécurité en se servant du tableau de l'alphabet pour transformer les lettres en nombres :

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	18	19	20	21	22	23	24

TABLE 4.1 – lettre de l'alphabet

On choisit :
- Les deux entiers : p=17 et q=19.
- La clé publique : n=p*q = 17*19 = 323.
- $\varphi(n)$ =(p-1)*(q-1)=288.
- e= 5 (clé publique).

Le message est donné par la position de l'alphabet

S	é	C	U	R	I	T	E
19	5	3	21	18	9	20	5

TABLE 4.2 – ordre de l'alphabet correspondant au mot sécurité

Chiffrement du message m :
En appliquant la formule : c =m^e mod(n) sur chaque caractère on obtient le message chiffré : C= 304 218 243 89 18 263 39 21

S	E	C	U	R	I	T	é
304	2018	243	89	18	263	39	218

TABLE 4.3 – chiffrement du mot sécurité

Déchiffrement du message c :
On déchiffre chaque nombre du message par : m=c^d mod(n) Tel que d= $e_1$mod ($\varphi(n)$) (clé secrète)
Pour obtenir d on calcule l'inverse d=5_1 mod(288) en utilisant l'algorithme d'Euclide étendu.

288= 5*57+3 3=288-5*57

5 = 3*1+2 2=5-3*1

3 = 2*1+ 1 1= 3-2*1

2 = 1*2+0

1= 3-2*1

= 3-(5-3)= 3-1*5+1*3

= -3*3+2*5
= -3*(288-5*57)+2*5
= -3*288+3*5*57+10
1 = -3*288+173*5 donc : d = 173

La position des lettres dans l'ordre alphabétique est représenté dans le ta- bleau suivant :

304	218	243	89	18	263	39	218
19	5	3	21	18	9	20	5

TABLE 4.4 – déchiffrement du mot chiffré.

Le message déchiffré correspondant à cet ordre est : sécurité.

ELGamel

L'algorithme EL Gamal est une suite logique de l'échange de clés déffie-hellman.
On peut résumer le fonctionnement de cet algorithme comme suit : [60]

Principe de fonctionnement

1. **Génération des clés**

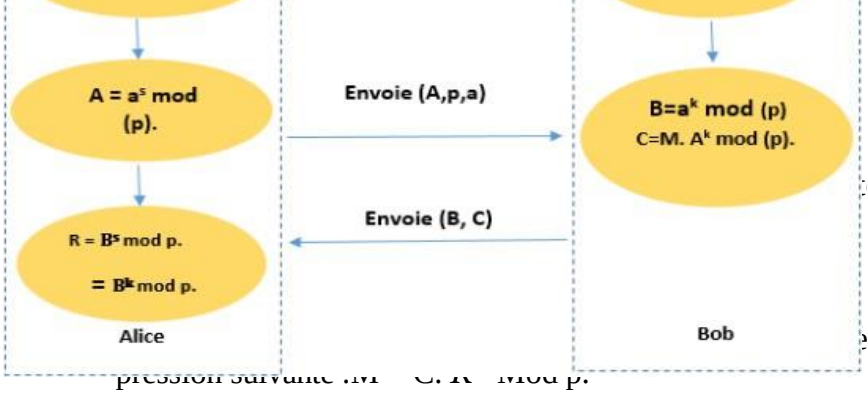
—Détermination de p et a : On choisit deux entiers p et a.

—Détermination de s : On choisit la clé secrète s tel que s $<$ p

—Détermination de A : On calcul la clé publique A = a^s mod(p).

2. **Chiffrement d'un message**
Pour chiffrer un message M, on choisit un nombre aléatoire k qui est connu par l'émetteur. On notera que la valeur de k 'est utilisée qu'une seule fois, c'est-à-dire le chiffrement d'un seul message. La haute sécurisation de ce chiffrement d'ELGAMEL vient du fait qu'un clair pourra avoir plusieurs chiffrés. Pour chaque k choisie, on calcule alors :
B=a_k mod (p)
C=M. A^k mod (p).

On obtient alors le message chiffré qui est représenté par le couple = (B,C).



e 's', on calcule

e par l'ex-

pression suivante :M = C. R^-1 Mod p.

FIGURE 4.2 – principe de l'algorithme ALGamel .

Exemple

On veut chiffrer le mot " Médical "en utilisant le protocole EL Gamal, pour cela on choisit : p=661, a=23 et une clé secrète s=7.

Chiffrement du message M

On commence par convertir ce message en chiffres. On assigne un nombre à deux chiffres à chaque caractère en se référant au tableau ci-dessous.

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	18	19	20	21	22	23	24

TABLE 4.5 – lettre de l'alphabet 2 .

Le message chiffré Médical est : M=13050409030112
Ce message est découpé en blocs de même longueur de telle façon que la valeur numérique de chacun de ces blocs devant être inférieure à p=661.

On peut donc, pour ce cas, former des blocs de taille de 3 chiffres.
M=130504090301120

À noter qu'il faut compléter par des zéros le dernier bloc afin d'aboutir à la taille exigée.

Calcul de A : $A=a^s$ mod(p) = 23^7 mod 661 =566
La clé publique est donc : (661, 23,566). On choisit aléatoirement l'entier k=13
Chiffrement du premier bloc M_1=130
B=a^kmod (p) =23^{13} mod (661) =105
C=M_1. A^k mod (p) =130 * 56613 mod (661) =429
M_1'= (105,429)

Blocs clair Mi	130	504	090	134	120
Blocs chiffrés M_i'	(105,429)	(105,209)	(105,297)	(105,134)	(105,396)

TABLE 4.6 – chiffrement du message M

Le message chiffré est : M'=429 209 297 134 396
Déchiffrement du message M'
Pour tous les couples B, on a la même valeur de R. R
=B^s mod (p) =105^7 mod (661)
$R^{(-1)}$ = y mod (p) Tel
qu' y= R mod (p)
Pour calculer y, on calcule le reste de la division euclidienne de d=466-1 mod(661)
Donc : y= -200
$R^{(-1)}$ = y mod(p) =-200 mod(661) =-200+661 =461

Déchiffrement du premier bloc M_1' =(105,429)
M_1=C. $R^{(-1)}$ mod(p)=429 * 461 mod(661) =130

Blocs chiffrés M'i	(105,429)	(105,209)	(105,297)	(105,134)	(105,396)
Blocs déchiffrés Mi	130	504	90	301	120

TABLE 4.7 – Déchiffrement du message M'

On obtient alors une suite de nombres : M=130504090301120 qu'on décompose en une suite de deux nombres : M=13 05 04 09 03 01 12 et par correspondance au tableau d'alphabets, on obtient le message déchiffré identique au message en clair : " Médical "

Les courbes elliptiques

Les courbes elliptiques sont un sujet très à la mode en mathématiques. Elles sont à la base de la démonstration du grand théorème de Fermat par Andrew Wiles. Elles sont aussi à l'origine de nouveaux algorithmes de cryptographie très sûrs, et on entrevoit les prémices de leur utilisation pour la factorisation de grands nombres entiers [60].

Définition

Un courbes elliptiques est un cas particulier d'une courbe algébrique munie d'une loi de groupe, pas n'importe quelle loi de groupe, évidement, sinon ce serait facile et ça n'aurait aucun intérêt, lais loi tels que les coordonnées de la somme s'expriment en fonction de celles des point de départ suivant l'équation Weierstrass :

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a^4x + a_6$

—Les coefficients a_1, a_2 , a_3, a_4 et a_6 sont des éléments du corps K sur lequel est définie la courbe. Ces éléments formés de deux opérations : l'addition et manipulation.

—Une courbe elliptique E est définie sur K à laquelle on a rajouté un point à l'infini, noté $\circ$.

$E = \{(x,y) \in K^2 \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a^4x + a_6 \cup \{\circ\}\}$

—La condition $\delta = -16(4a^3 + 27b^2)f = 0$ s'assure que la courbe elliptique est ¡lisse¿, c'est-à-d, qu'elle ne possède ni point double, ni point de rebroussement (il n'y aucun point auquel la courbe possède deux ou plusieurs tangents distinctes

Équations de Weierstrass

Pour leur usage en cryptographie, a_1, a_2 et a_3 doivent être égaux à 0. Comme les cryptographes ont l'habitude de renommer a_4 = a et a_6 = b, on obtient :

Un exemple typique de courbe elliptique est donné sur la figure ci-dessous. Son équation est :

$y^2 = x^3 - x$

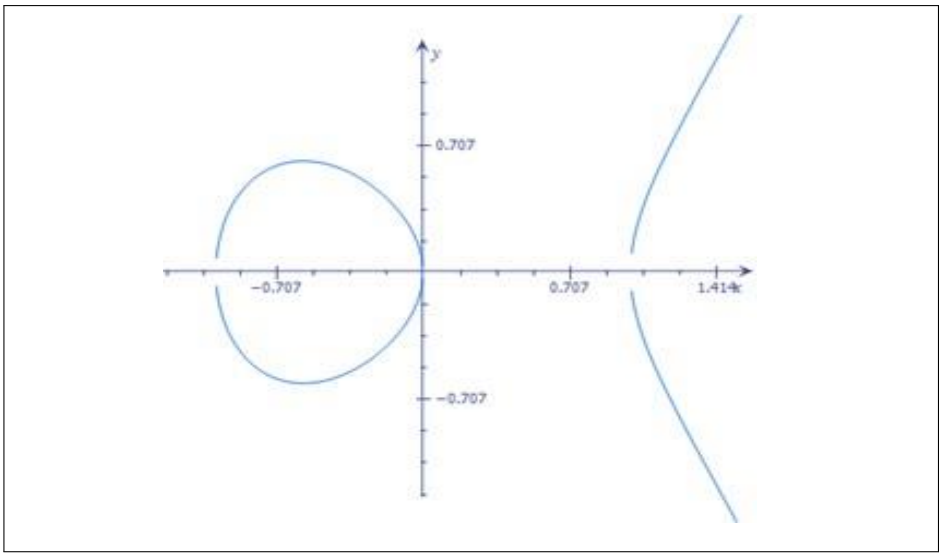


FIGURE 4.3 – exemple d'une courbe elliptique.

Opérations sur les courbes elliptique

On va définir les forme qui permettent de calculer les coordonné du point 'R' résultant d'une addition ou multiplication ou soustraction de deux point p et q.

Addition des points : Soient E une courbe elliptique définie sur un corps K, et deux points P, Q $\in$ E(K), (L) la droite reliant P à Q (la tangente à E si P = Q) et R le troisième point d'intersection de (L) avec E. Soit (L')la droite verticale passant par R. On définit $P + Q \in$ E(K) comme étant le deuxième point d'intersection de (L') avec E. le groupe muni de cette loi de composition $(E(K)+)$ est un groupe abélien dont l'élément neutre est le point à l'infini O.

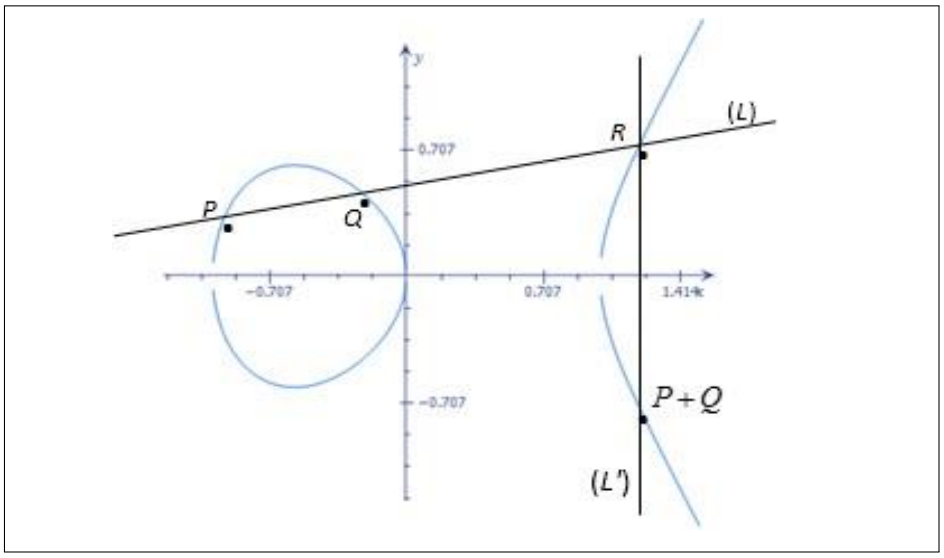


FIGURE 4.4 – Représentation graphique de l'addition de deux .

Algorithme d'addition de deux points

Soient deux points sur la courbe elliptique E, avec : $P_1=(x_1=y_1)$ et $P_2=(x_2=y_2)$ = ! 0

On a : $P_1+P_2 =P_3 =(x_3=y_3)$

si x_1 = ! x_2 , alors : $x_3 = m^2 - (x_1 + x_2)$ y_3 = m(x_1 - x_3)- y_1

où : m= y_2 - y_1 x_2 - x_1

si $x_1 = x_2$ et y_1 = ! y_2, alors : P_3 =0 si P_1

= P_2 et y_1 =!0 , alors :

$x_3 = m^2 - 2\ x_1$

y_3 = m(x_1 - x_3)- y_1

où : m= 3 x_1 + a $_2y_1$ –

si $P_1 = P_2$ et y_1 =0 , alors : P_3 =0

Pourquoi le point à l'infini est égal à O (élément neutre pour l'addition) ?

Soit P0 ce point à l'infini. Pour trouver P + P0, on doit, selon la méthode décrite, tracer la droite passante par le point P et le point P0 (figure II.3), c'est la verticale passant par P. Elle recoupe justement la courbe elliptique au point P', symétrique de P par rapport à la droite des abscisses ; le point P + P0 cherché, par définition de l'addition, est le symétrique de ce point P', donc c'est P lui-même. On a bien trouvé que P + P0 = P ce qui correspond bien à ce qu'on attend d'un " zéro " pour l'addition.

Soustraction de deux points dans Ep(a,b) : Soient E une courbe elliptique définie sur un corps K, et deux points P, Q E(K).On définit par R le point résultant de la soustraction de P et Q.

R= P-Q = P+(-Q).

Donc pour soustraire Q de P, on commence par la négation de Q. On considère Q=(x_q, y_q), et on veut calculer Q_n=-Q = (x_r, y_r).

On choisit deux points S=(x_s, y_s) et T=(x_t, y_t) symétriques par rapport à la droite y=moy.

moy= (y_s + y_t)/2

- y_r=y_q+ 2(moy- y_q)
- x_r=x_q

Enfin, R est calculé en utilisant l'algorithme d'addition décrit précédemment.

Doublement successif :

P est un point sur une courbe elliptique et k est un nombre entier positif,

alors kP peut être calculé par :

KP= P+P+. ..... +P K¿0

-P-P-.....-P K¡0

Quand l'entier k est très grand, il est pratique d'utiliser le doublement successif, Soit par exemple 38P.

2P+= P + P

4P+= 2P + 2P

8P+= 4P + 4P

16P+=8P + 8P

32P+=16P + 16P

Donc : 38P+=32P + 4P+ 2P

Pour chaque entier n on doit le binariser, c'est-à-dire on lui écrit sous forme d'une somme de 2^n , avec n= 0,1,2...

Chiffrement à l'aide des courbes elliptiques

Échange de clés par courbes elliptiques : Il s'agit d'un échange de clés à la manière de Diffie et Hellman, c'est-à-dire sans se les communiquer directement. Alice et Bob se mettent d'accord ensemble et publiquement sur une courbe elliptique E (a,b,K), c'est-à-dire qu'ils choisissent un corps fini K (ex : Z/pZ), et une courbe elliptique $y_2=x^3$+ax+b. Ils se mettent aussi d'accord sur un point P situé sur la courbe.

Secrètement, Alice choisit un entier kA, et Bob un entier kB. Alice envoie à Bob le point kaP, et Bob envoie à Alice kBP. Chacun de leur côté, ils sont capables de calculer $k_A(k_B\text{P})=k_B(k_A\text{P})=(k_A\ k_B)\text{P}$, qui est un point de la courbe, et constitue leur clé secrète.

Transmission de messages : On suppose qu'Alice et Bob ont suivi le protocole d'échange de clés expliqué ci-dessus. Alice veut envoyer à Bob un message : ils se sont mis d'accord sur la façon de transformer un texte en suite de points de la courbe elliptique. Alice doit donc transmettre, de façon secrète, un point M de la courbe E (a,b,K). Elle choisit (secrètement) un nombre k_A, et envoie à Bob le couple (k_AP,M+$k_A\ k_B$P). Bob, lui, multiplie k_AP par k_B (sa clé secrète), puis retranche $k_A\ k_B$P à M+$k_A\ k_B$P : il retrouve M. Si quelqu'un espionne les échanges, il lui faut absolument connaitre k_B pour retrouver M : c'est encore une fois le problème du logarithme discret à résoudre.

Donc le principe des courbes elliptiques est comme suit :

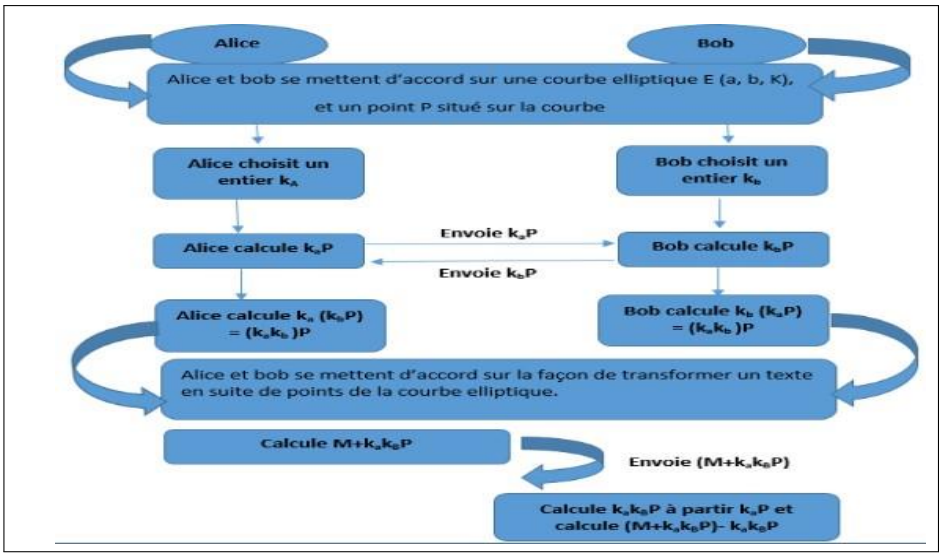


FIGURE 4.5 – exemple d'une courbe elliptique.

Exemple

ALICE veut envoyer un message à BOB avec le système de cryptage basé sur les courbes elliptiques. Elle récupère la clef publique (E_p (a,b),P,B) =($E_1$01(8,1),(11,39),(26,89)) de BOB et chiffre

1.M=(74,91) $\in E_1$0

2.K =128 $\Rightarrow C_1$ = K . P =128 . (11,39) = (85,76).

3. C_2 = M+ KB = (74,91) +128 . (26,98) = (76,72)

1. Ensuite envoie le couple (C_1,C_2) à BOB.

5.Enfin, BOB calcule C_2 - sC_1 = (76,72) - 96 . (85,76)= (74,91) = M .

Avantage

C Ce qui fait la sûreté de l'algorithme à base de courbes elliptiques par rapport au RSA est que, pour le vaincre, il faut résoudre le logarithme discret sur le groupe de la courbe elliptique, et non plus sur (Z/pZ)*. Mais ces groupes sont beaucoup moins bien connus que ce dernier, et ils diffèrent d'une courbe à l'autre. Les algorithmes dont on dispose pour résoudre le logarithme dis- cret sur les courbes elliptiques sont donc moins efficaces. Ce qui fait la sûreté de l'algorithme à base de courbes elliptiques par rapport au RSA est que, pour le vaincre, il faut résoudre le logarithme discret sur le groupe de la courbe elliptique, et non plus sur (Z/pZ)*. Mais ces groupes sont beaucoup moins bien connus que ce dernier, et ils diffèrent d'une courbe à l'autre. Les algorithmes dont on dispose pour résoudre le logarithme discret sur les courbes elliptiques sont donc moins efficaces.

Inconvénient

- La théorie des fonctions elliptiques est complexe, et encore relativement récente. Il n'est pas exclu que des trappes permettent de contourner le problème du logarithme discret.
- La technologie de cryptographie par courbe elliptique a fait l'objet du dépôt de nombreux brevets à travers le monde. Cela peut rendre son utilisation très coûteuse!

Réalisation

Environnement de développement

Dans cette partie nous allons citer l'environnement logiciel (Software) et matériel (Hardware) utilisés.

Environnement logiciel :

Langage de programmation

Nous avons choisi le logiciel de Matlab pour développer notre système,la version 2013.

Environnement matériel :

L'application a été créer sur un PC TOSHIBA SATELLITE C660 ayant les caractéristiques suivantes :.

Mémoire : 8192 MB RAM.

Processeur : Intel ® CoreTM i5-2410M CPU @ 2.30 GHZ (4 CPUs).

Système d'exploitation : Windows 8.1 Pro 64 bits.

Carte Graphique : NVIDIA GeForce 315M.

- **Cryptage d'image médicale par l'algorithme RSA**

Dans cet exemple, on va appliquer l'algorithme RSA pour chiffrer et déchiffrer une image médicale.

. Les clefs utilisées sont les suivantes :

- La clef publique : 11,135
- La clef secrète :(11-1,135), (la clef de chiffrement, chez l'expéditeu)

Les résultats sont donnés dans la figure suivante, avec l'histogramme de chaque image.

FIGURE 4.6 – cryptage d'image par RSA (a)Image originale (b) image crypté (c) image décrypté.

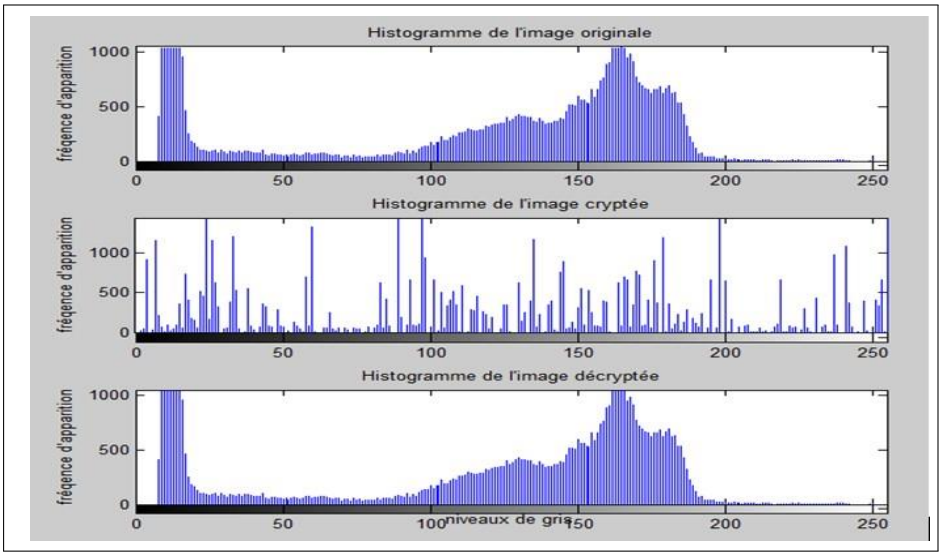


FIGURE 4.7 – l'histogramme de cryptage d'image (a)Image originale (b) image crypté (c) image décrypté.

÷ **Cryptage d'image médicale par l'algorithme El Gamal**

Dans cet exemple, on va appliquer l'algorithme ALGAMAL pour chiffrer et déchiffrer une image.

- Les clefs utilisées sont les suivantes :
- La clef publique : (p,a,P)=(449,31,377)
- La clef secrète : (la clef de déchiffrement, chez le récepteur)
- La clef secrète : k=5 (la clef de chiffrement, chez l'expéditeur)

Les résultats sont donnés dans la figure suivante, avec l'histogramme de chaque image.

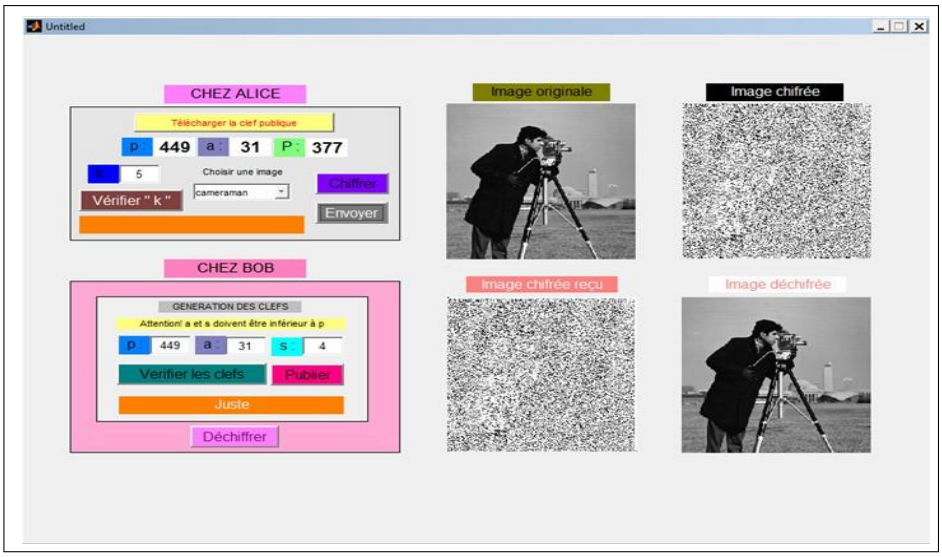


FIGURE 4.8 – cryptage d'image par El Gamal (a)Image originale (b) image crypté (c) image décrypté

Dans l'histogrammede chacune des images précédentes, on remarque que l'image chiffrée est répartie sur toute la gamme (0,255), la distribution des fréquences d'apparition est assez uniforme et complètement différente à celle de l'image originale.

÷ **Cryptage d'image médicale par l'algorithme des courbes elliptiques** Dans cet exemple, on va appliquer l'algorithme des courbes elliptiques pour chiffrer et déchiffrer une image.

Les clefs utilisées sont les suivantes :

- La clef publique : (Ep (a,b),P,B)= Ep(8,1),(71,42),(115,108)).
- La clef secrète k = 60 du chiffrement.
- La clef secrète s= 97 du déchiffrement.
- Les résultats sont donnés dans la figure suivante, avec l'histogramme de chaque image.

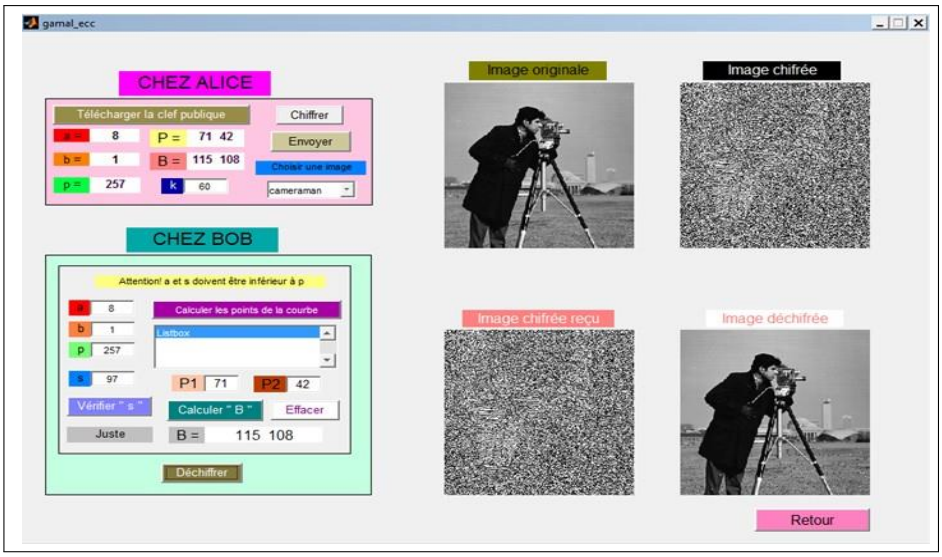


FIGURE 4.9 – cryptage d'image par les courbe elliptique (a)Image originale (b) image crypté (c) image décrypté

Si on compare les résultats du chiffrement de RSA, El Gamal et les courbe elliptique.On déduit que l'utilisation des courbes elliptiques améliore la qualité du chiffrement.

Cependant, les algorithmes RSA et ELGamel sont moins performance par rapport a les courbes elliptiques.

Conclusion

Dans ce chapitre nous avons chiffré/Déchiffré les images avec quelques algorithmes de la cryptographie à clef publique. Le critère de validation de ces algorithmes est l'histogramme.

Conclusion générale

De nos jours, l'image médicale acquise dans un hôpital ou dans un centre d'imagerie peut être partagée entre plusieurs professionnels de santé afin de faciliter la prise en charge des patients et permettre l'amélioration de la gestion de l'information médicale. Ce partage est souvent effectué sur des réseaux peu (ou pas) sûrs, exposant l'image médicale à plusieurs menaces de sécurité, qui peuvent être exprimées en termes de pertes de données, de falsification, d'erreurs, et/ou d'attaques d'où un besoin accru en termes de sécurité (confidentialité, disponibilité, et fiabilité qui regroupent l'intégrité et l'authenticité).

La cryptographie existe depuis plus de 3 000 ans et pourtant, elle a toujours sa propre place dans le domaine de la sécurité, car les êtres humains ont toujours essayé de cacher leurs informations en temps de paix et de guerre.

La plupart des mécanismes de sécurité existants comme les techniques cryptographiques et le contrôle d'accès offrent une protection permettent d'empêcher les utilisateurs non autorisés d'accéder au contenu des données ,des images pour ce qui nous concerne.

Dans ce mémoire, Nous avons commencé par expliquer Les concepts fondamen- taux de la cryptographie ainsi que les objectifs, les type de la cryptographie moderne et ont parlé sur les algorithmes de cryptage asymétrique (cryptographie moderne) : Deffie-Hellman, RSA, el Gamal et les courbe elliptique. Après cela, nous avons Nous avons fourni un bref aperçu sur la cryptographie utilisée dans le futur qui appelé la cryptographie quantique. Ensuite, Nous avons expliqué l'image numérique en général et l'image médicale en particulier où nous avons mentionné les différents types d'images numériques et leurs couleurs. Puis nous avons abordé l'image médicale, Nous avons expliqué leurs types, leurs spécificités et leurs manipulations et attaques, enfin Nous avons expliqué les méthodes de cryptage d'images (spatial et fréquentiel).

Dans le troisième chapitre, nous avons présenté les travaux de cryptage d'images médicales et leurs résultats tel que le cryptage d'image médicales qui est basé sur : les cartes de bord, l'arrangement des pixels et la permutation

aléatoire, la séquence d'ADN,la détection par compression et l'approche de permutation basée sur l'échange de pixels et sur les cartes chaotique à l'aide de la cryptographie symétrique.
Dans le dernier chapitre, nous avons choisi les trois algorithmes de chiffrements asymétriques : RSA, El Gamal et les courbe elliptique est en expliquant leurs prin- cipes de fonctionnement. Après, nous avons implémenté ces algorithmes à l'aide du langage de programmation MATLAB pour obtenir les résultats de cryptage des images et leurs histogrammes.

Bibliographie

[1] Assia Beloucif. *Contribution à l'étude des mécanismes cryptographiques*. PhD thesis, Université de Batna 2, 2016.

[2] Renaud Dumont. Cryptographie et sécurité informatique. *Eyrolles*, 2010, 2009.

[3] https ://fr.wikipedia.org/wiki/Cryptosyst

[4] Ghislaine Labouret. Introduction à la cryptographie. *Supports de cours, Cabinet Hervé Schauer Consultants-HSC*, 9, 2001.

[5] Behrouz A Forouzan. *Cryptography & network security*. McGraw-Hill, Inc., 2007.

[6] principe de base de la cryptographie. http://dspace.univ-tlemcen.dz/bitstream/112/1046/8/chapitre2.pdf.

[7] Confusion et diffusion. https://fr.wikipedia.org/wiki/Confusionetdiffusion.

[8] principe de base de la cryptographie. http://dspace.univ-tlemcen.dz/bitstream/112/1046/8/chapitre2.pdf.

[9] https ://www.quora.com/What-are-the-objectives-of-cryptography-1. [10]AHMED BELHADJ et al. *Etude comparative entre la cryptographie à clé*

secrète et à clé publique appliquée aux textes arabes. PhD thesis.

[11]Bruce Schneier. *Applied cryptography : protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[12]https ://medium.com/@antoine.ansel/l-algorithme-d-

[13]https ://www.tutorialspoint.com/cryptography with python/cryptography withpython [14]http ://mathweb.free.fr/crypto/moderne/rsa.php3.

[15]https ://fr.wikipedia.org/wiki/Cryptosyst

[16]https ://fr.wikipedia.org/wiki/Cryptographie _quantique : :text=Un

[17]Anders Ballestad and Gerwin Damberg. Local definition of global image transformations, December 9 2014. US Patent 8,907,971.

[18]Faiçal HADJI. *Conception et réalisation d'un système de cryptage pour les images médicales*. PhD thesis, UNIVERSITE MOHAMED BOUDIAF- M ?SILA FACULTE DES MATHEMATIQUES ET DE L ?, 2018.

[19]Numeriksciences. http://numeriksciences.fr,consult¥unhbox¥voidb@x¥bgroup¥let¥unhbox¥voidb@x¥setbox¥@tempboxa¥hbox{e¥global¥mathchardef¥accent@spacefactor¥spacefactor}¥accent19e¥egroup¥spacefactor¥accent@spacefactorle18-04-2018.

[20]Qu'est-ce qu'une image numérique. université rennes 2. https://www.sites.univrennes2.fr/.

[21]André Roy. *Dictionnaire général du cinéma : Du cinématographe à internet : art, technique, industrie*. Les Editions Fides, 2007.

[22]Khouildat Hadjer and Djebaili Karima. Méthode de cryptage d?image basée sur la permutation et la matrice de householder.

[23]https ://tecfa.unige.ch/tecfa/teaching/staf13/fiches-mm/bitmapvectoriel.htm.

[24]Image file formats. wikipedia. Https://en.wikipedia.org/wiki/Image_file_formats.

[25]http ://edutechwiki.unige.ch/fr/Image _matricielle.

[26]https ://www.imedias.pro/cours-en-ligne/graphisme-design/definition-resolution-taille-image/les-images-vectorielles-matricielles/.

[27]FOUAD KARAM. *Transfert sécurisé des données visuelles (images) dans un réseau intranet selon l?architecture client/serveur*. PhD thesis.

[28][28] http ://sciences-du-numerique.fr/connaissances-pour-la-specialite-isn/representation-numerique-des-images/13.

[29]Bernard Mazoyer. Guy Frija, Clara Delpas. Imagerie médicale .fondation pour la recherche médicale. *www.frm.orgClara Delpas*, 2002.

[30]https ://fr.wikipedia.org/wiki/Imagerie _m

[31]https ://www.doctissimo.fr/html/sante/imagerie/imagerie _sommaire.htm.

[32]Nour El-Houda GOLEA. *RGB color image digital watermarking*. PhD thesis, Thése de Magistére, University Elhadj Lakhder-Batna, 2010.

[33]J.A. Seibert. *Medical Image Data Characteristics-Society for Imaging Informatics in Medicine*.

[34]A Naït-Ali and Christine Cavaro-Ménard. Compression des images et des signaux médicaux, 2007.

[35]Jerrold T Bushberg, J Anthony Seibert, Edwin M Leidholdt Jr, John M Boone, and Edward J Goldschmidt Jr. The essential physics of medical imaging. *Medical Physics*, 30(7) :1936–1936, 2003.

[36]Elizabeth Krupinski. *Digital Mammography : 9th International Workshop, IWDM 2008 Tucson, AZ, USA, July 20-23, 2008 Proceedings*, volume5116. Springer, 2008.

[37]M. GONTIES Michael. L'apport de l'internet dans la pratique quoti- dienne du médecin généraliste. *Université Paris VAL-DE-MARNE Faculté de médecine de Creteil*, 2003.

[38]https ://searchhealthit.techtarget.com/definition/DICOM-Digital-Imaging- and-Communications-in-Medicine.

[39] _https ://fr.wikipedia.org/wiki/Digital imaging and communications in medicine. [40]Liliane Dusserre, Henry Ducrot, and François-André Allaërt. *L'information médicale, l'ordinateur et la loi*. Editions médicales internationales, 1996.

[41]Wei Pan, Gouenou Coatrieux, Nora Cuppens-Boulahia, Frederic Cuppens, and Christian Roux. Watermarking to enforce medical image access and usage control policy. In *2010 Sixth International Conference on Signal-Image Technology and Internet Based Systems*, pages 251–260. IEEE, 2010.

[42]C. Roger-France, F. Michel. Le défi de sécurité dans les réseaux informa- tiques de santé. *dans Collection Informatique et santé : Santé et Réseaux Informatiques*, 10 :185–191, 1998.

[43]R. Anderson. Séuritédans les systémes médicaux informatisés. computer laboratory, university of cambridge. *Medical Physics*, page 30, 1996.

[44]William Puech, José Rodrigues, and Jean-Eric Develay-Morice. Transfert sécurisé d'images médicales par codage conjoint : cryptage sélectif par aes en mode par flot et compression jpeg. *traitement du signal*, 23(3), 2006.

[45]Yicong Zhou, Karen Panetta, and Sos Agaian. A lossless encryption me- thod for medical images using edge maps. In *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 3707–3710. IEEE, 2009.

[46]Don Coppersmith, Prabhakar Raghavan, and Thomas G Zimmerman. Sys- tem and method for near-field human-body coupling for encrypted commu- nication with identification cards, August 18 1998. US Patent 5,796,827.

[47]Koredianto Usman, Hiroshi Juzoji, Isao Nakajima, Soegijardjo Soegidjoko, Mohamad Ramdhani, Toshihiro Hori, and Seiji Igi. Medical image encryp- tion based on pixel arrangement and random permutation for transmission security. In *2007 9th International Conference on e-Health Networking, Ap- plication and Services*, pages 244–247. IEEE, 2007.

[48]Jan Sher Khan, Jawad Ahmad, Saadullah Farooq Abbasi, Sema Koc Kayhan, et al. Dna sequence based medical image encryption scheme. In *2018 10th Computer Science and Electronic Engineering(CEEC)*, pages 24–29. IEEE, 2018.

[49]Meghdad Ashtiyani, Parmida Moradi Birgani, and Hesam M Hosseini. Chaos-based medical image encryption using symmetric cryptography. In *2008 3rd International Conference on Information and Communication Technologies : From Theory to Applications*, pages 1–5. IEEE, 2008.

[50]Medien Zeghid, Mohsen Machhout, Lazhar Khriji, Adel Baganne, Rached Tourki, et al. A modified aes based algorithm for image encryption. *International Journal of Computer Science and Engineering*, 1(1) :70–75,2007.

[51]Jun-xin Chen, Zhi-liang Zhu, Chong Fu, Li-bo Zhang, and Yushu Zhang. An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach. *Communications in Nonlinear Science and Numerical Simulation*, 23(1-3) :294–310, 2015.

[52]Sareh Mortajez, Marziyeh Tahmasbi, Javad Zarei, and Amir Jamshidnezhad. A novel chaotic encryption scheme based on efficient secret keys andconfu- sion technique for confidential of dicom images. *Informatics in Medicine Unlocked*, 20 :100396, 2020.

[53]Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. Applied cryptography. *CRC, Boca Raton*,1996.

[54]https ://www.google.com/search?q=Histogramme+d.

[55]Nodar MOMTSELIDZE. Programming part for robot painter using image processing algorithms written in java. *Journal of Technical Science and Technologies*, pages 41–46, 2013.

[56] https://fr.wikipedia.org/wiki/Histogramme#:~:text=En%20statistique%2C%20un%20histogramme%20est,repr%C3%A9sentant%20avec%20des%20colonnes%20verticales.

[57] Akram Aimeur. *Conception et implémentation d'un système hybride pour la sécurité de données : application aux images numériques FACULTE : MATHEMATIQUES ET DE L INFORMATIQUE DEPARTEMENT : D INFORMATIQUE N° . DOMAINE : Mathématiques et Informatique FILIERE : Informatique OPTION : Réseaux.* PhD thesis, FACULTE : MATHEMATIQUES ET DE L ?INFORMATIQUE- UNIVERSITE MOHAMED BOUDIAF-M ?SILA,2017.

[58]Claude Elwood Shannon. A mathematical theory of communication. *ACM SIGMOBILE mobile computing and communications review*, 5(1) :3–55, 2001.

[59]wikipedia. entropie de shannon. https://fr.wikipedia.org/wiki/Entropie_de_Shannon.

[60]http ://entrop-x.com/index.php/fr/cryptography-and-crypto-currencies- fr/108-chiffrement-elgamal.