***REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE***
***MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE***

***Université de Jijel***

***Faculté des Sciences et de la Technologie***

***Département d'Electronique***

***Projet de fin d'études pour l'obtention du diplôme de Master en Télécommunications***

*Option*

***Systèmes de télécommunications***

***Thème***

# Sécurisation des images médicales sur courbes elliptiques

**Présenté par :**

- Mlle Amina Khaoula AMZERT
- Mlle Omayma BELMERABET

**Encadré par :**

- Dr. Samira DIB

*Année universitaire : 2019-2020*

# *Remerciements*

*À l'issue de ce travail, nous tenons à remercier dans un premier temps **ALLAH** de nous avoir accordé la santé et la volonté dans la réalisation de ce projet.*

*Nous tenons à remercier particulièrement et chaleureusement notre encadreur, Mme DIB Samira, Docteur à l'université de Jijel, pour son encadrement, sa patience, ses conseils très judicieux, ses encouragements et sa disponibilité tout au long de notre projet.*

*Nous remercions également notre second encadreur Mr GRIMES Mourad, docteur à l'université de Jijel pour nous avoir proposé ce thème qui nous a apporté de nouvelles connaissances dans ce large domaine.*

*Nos remerciements vont aussi à Mme BOUATMANE Sabrina, Docteur à l'université de Jijel, pour nous avoir facilité la compréhension des images médicales.*

*Nous exprimons toute notre gratitude aux membres du jury pour avoir accepté de juger notre travail, ainsi que tous les enseignants du département d'électronique.*

# *Dédicaces*

*À la prunelle de mes yeux, ma Maman,*

*À mon pilier dans la vie, mon Papa,*

*À mon unique sœur Bouchra,*

*À tous ceux qui me sont cher et proches,*

*À tous ceux qui ont semé en moi une graine de soutien et d'encouragement,*

*Merci !*

*Khaoula*

# *Dédicaces*

*C'est avec une très grande émotion et un immense plaisir que je dédie ce modeste travail :*

*À ma chéré Mère*

*A mon Père Saleh Dont le mérite, les sacrifices et les qualités humaines m'ont permis de vivre ce jour,*

*À ma chère Grand-Mère,*

*À mes Frères et Sœurs,*

*À l'homme de ma vie, Abdelali,*

*À tous ceux qui me sont cher et proches,*

*À tous ceux qui ont semé en moi une graine de soutien et d'encouragement,*

*Merci !*

*Omayma*

# Table des matières



# Chapitre 1
## Généralités sur l'imagerie médicale

# Chapitre 2

## Cryptographie sur courbes elliptiques

# Chapitre 3
## Algorithme proposé



# Chapitre 4
## Résultats et discussion

# Liste des Figures

# Liste des tableaux

# Abréviations

| | |
|---|---|
| **ANSI** | American National Standards Institute |
| **ARDS** | Acute Respiratory Distress Syndrome |
| **BB84** | Bennett and Brassard 1984, premier mécanisme d'échange de clé quantique |
| **C.M.Y.K** | Cyan, Magenta, Yellow, Black |
| **DCM** | DICOM File Format (file extension; medical imaging) |
| **DICOM** | Digital Imaging and Communications In Medicine |
| **DPI** | Dots Per Inche |
| **DSA** | Digital Signature Algorithm |
| **DSS** | Digital Signature Service |
| **ECC** | Elliptic Curve Cryptography |
| **ECC avec G** | Elliptic Curve Cryptography avec Groupement |
| **ECC sans G** | Elliptic Curve Cryptography sans Groupement |
| **ECDH** | Elliptic-Curve Diffie–Hellman |
| **ECDSA** | Elliptic Curve Digital Signature Algorithm |
| **ECMQV** | Elliptic Curve Menezes-Qu-Vanstone |
| **EM** | Electro-Magnétique |
| **FIPS** | Federal Information Processing Standard |
| **HTTPS** | HyperText Transfer Protocol Secure |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IP** | Internet Protocol |
| **IRM** | Imagerie par Résonance Magnétique |
| **JPG** | Joint Photographic Experts Group |
| **LUT** | Look Up Table |
| **MERS** | Middle East respiratory syndrome |
| **NIST** | National Institute of Standards and Technology |
| **PACS** | Picture Archiving and Communication System |
| **Pixel** | Picture Element |
| **PKCS** | Public Key Cryptographic Standards |
| **PPI** | Point Per Inch |
| **PPP** | Point Par Pouce |
| **PSNR** | Peak Signal to Noise Ratio |
| **RMN** | Résonance Magnétique Nucléaire |
| **R.V.B** | Rouge, Vert, Bleu |
| **RX** | Rayon X |

| | |
|---|---|
| **SEP** | Sclérose En Plaques |
| **SRAS** | Syndrome Respiratoire Aigu Sévère |
| **SSH** | Secure SHell |
| **SSIM** | Structural SIMilarity |
| **TDM** | Tomodensitométrie |
| **TLS** | Transport Layer Security |
| **T.V** | télévision |
| **US** | ultrasound |
| **Voxel** | Volume Element |
| **VPN** | Virtual Private Network |
| **1D** | Unidimensionnelle |
| **2D** | Bidimensionnelle |
| **3D** | Tridimensionnel |

# Introduction générale

Avant le début de l'ère de l'imagerie médicale jusqu'en 1895, aucun moyen n'existait pour sonder ou explorer in vivo le monde intérieur caché du corps humain. Les médecins ont appris à ausculter les patients en ayant recours à leurs sens : l'observation, l'odorat et la palpation. La découverte des rayons X pénétrant, par Wilhelm Röntgen, a donné le coup d'envoi vers une révolution de l'imagerie médicale et a commencé une réunification de la science médicale avec les sciences exactes.

Les images planes bidimensionnelles (2D) ont fait place à l'imagerie tridimensionnelle (3D) à l'imagerie quadridimensionnelle c'est-à-dire l'imagerie tridimensionnelle en temps réel, à l'imagerie fonctionnelle, à l'imagerie moléculaire. En 1958, Ian Donald a utilisé pour la première fois les ultrasons en gynécologie (échographie). En 1967, Godfrey Hounsfield a inventé le premier tomodensitomètre assisté par ordinateur (scanner à rayon X). C'est l'une des innovations les plus importantes de l'histoire de l'humanité : les images affichent les tissus du corps humain avec des détails anatomiques ce qui permet une précision du diagnostic sans précédent. Par la suite la découverte de l'imagerie par résonnance magnétique (IRM) en 1973 a été le fruit de nombreuses contributions des domaines cliniques, scientifiques et techniques [1].

La réussite de l'imagerie médicale au cours des dernières décennies est dû aux progrès du numérique. Les radiologues peuvent interpréter à distance des images en temps réel ou longtemps après que le patient ait quitté le point de soin.

L'industrie des systèmes d'archivages et de communication d'images (PACS) s'est développée parallèlement aux besoins de l'imagerie médicale pour gérer et stocker les données numériques via le système d'information hospitalier. Par conséquent, les médecins peuvent accéder aux antécédents médicaux et renseignements complets des patients. En revanche, de nombreux cabinets de médecins et centres d'imagerie ne respectent pas les règles élémentaires de sécurité et connectent leur PACS directement à internet sans mot de passe ni VPN où on y trouve principalement des images de radiographies, d'IRM et d'échographies qui proviennent de 52 pays. Les Etats-Unis arrivent en tête avec 13.7 millions d'ensembles de données et 45.8 millions d'images librement accessibles. En Europe, cinq serveurs allemands seraient concernés et 5000 images au Royaume-Uni [2].

Ces données mal protégées exposent non seulement les images médicales de nombreux patients mais également leur nom, prénom, date de naissance, diagnostic, numéro de sécurité social, etc. Des informations extrêmement sensibles dont l'utilisation frauduleuse pourrait être exploitée à des fins d'usurpations d'identité et de fraudes à l'assurance.

Il se pose donc un réel problème quant à la sécurité lors de la transmission de données. Pour des raisons éthiques, le transfert des images médicales ne peut se faire avec un tel risque et doit donc se protéger. La protection la plus adaptée pour ce type de communication réside dans la cryptographie.
Beaucoup de techniques de chiffrement de texte ont été développées. Depuis l'antiquité, les hommes ont toujours essayé de coder des messages secrets pour se prévenir des oreilles malveillantes. Dans les premières esquisses de cette science du secret, la sécurité résidait dans la confidentialité de l'algorithme qui permettait le chiffrement et le déchiffrement. C'est au fil du temps qu'est apparue progressivement la notion de clé. Aujourd'hui, les systèmes de chiffrement reposent sur des algorithmes mis à disposition de tous et c'est la clé, code secret particulier, qui est confidentielle et qui permet de chiffrer ou de déchiffrer le message [3].

De ce fait et dans le but de contribuer à la sécurité des images médicales, nous avons réalisé ce modeste travail qui s'articule sur quatre chapitres :

- Le premier chapitre aborde des généralités sur le traitement d'images ainsi que les différentes modalités d'imagerie médicales.
- Le deuxième chapitre résume les différentes classes et techniques de cryptographie en se focalisant sur la cryptographie sur courbes elliptiques.
- Le troisième chapitre comporte la description et l'implémentation de l'algorithme de chiffrement d'un texte sur courbes elliptiques.
- Le quatrième chapitre est consacré aux résultats obtenus en appliquant deux techniques de cryptographie moderne notamment : RSA et ElGamel ainsi que la technique de cryptographie sur courbes elliptiques de plusieurs images dont : une image ultrason, une image radiographique, une image d'un scanner et une image IRM.

Chapitre 1

# *Généralités sur l'imagerie médicale*

# 1. Introduction

Le récent développement des appareillages et outils médicaux a fait que l'imagerie médicale devienne une pratique primordiale pour un diagnostic fiable et précis. Celle-ci est souvent transmise entre les centres d'acquisition d'images et les médecins pour faciliter la prise en charge du patient, néanmoins et d'après un récent article : plus d'un milliard d'imageries médicales aurait été exposées librement à travers internet dans de simples navigateurs classiques [4]. Cette faille aurait interpelé l'attention des spécialistes en sécurité et des grands organismes de règlementation, car une divulgation d'une information privée pourrait entrainer à sa falsification.

Plusieurs solutions ont été mises en œuvre dans le but de remédier à ce problème, la première serait de sécuriser les équipements qui stockent l'information dont : les serveurs, la seconde se résume aux différentes techniques de chiffrement.

Il existe plusieurs modes de chiffrement généralement classifiés en deux types : le chiffrement symétrique basé sur une même clé pour chiffrer et déchiffrer, et le chiffrement asymétrique utilisant des clés différentes [5].

Dans ce chapitre, nous abordons les notions de traitement basées sur les images et les caractéristiques qui distinguent les images médicales en particulier.

# 2. Notions de base sur le traitement d'images

Le traitement d'images représente l'ensemble des techniques permettant de modifier une image numérique afin de l'améliorer ou d'extraire les informations qu'elle contient. Les étapes citées ci-dessous représentent le processus de traitement d'une image numérique.

## 2.1. Formation d'une image

Nous commençons tout d'abord par nous intéresser à la toute première étape qui est la formation de l'image qui résulte d'une scène réelle captée. Le capteur émet, reflète ou réfracte une onde électromagnétique EM, tout dépend si ce dernier représente une source ou une destination.

Il est important de savoir que la longueur d'onde EM englobe le visible [400µm-800µm] ainsi que l'infra-rouge et l'ultra-violet car l'imagerie infrarouge est aussi utilisée pour détecter des zones émettant de la chaleur spécialement dans la télésanté comme la thermographie (détection précise de tumeur).

Il existe différents capteurs, on cite en particulier :

- Système biologique comme l'œil humain.
- Capteur thermique servant à convertir les ondes infrarouges en une image représentant la température, exemple : caméra thermique qui contrôle la température corporelle de l'humain.
- Capteur photoélectrique (photodiode), exemple : radiographies standards.

Le signal obtenu sera traité en fonction de sa dimension et de sa nature : un signal de dimension 1 (1D) correspond à une image linéique ayant une seule ligne ou une seule colonne exemple (signal d'oscilloscope). Un signal de dimension 2 (2D) correspond à une image plane ayant une matrice exemple : une photographie d'une pièce d'identité. Un signal de dimension 3 (3D) correspond à une image volumique avec 3 dimensions spatiales c.-à-d. que l'image a une certaine épaisseur où chaque unité du volume corporel appelé voxel stocke une information physique (couleur, densité, intensité..) sur un maillage régulier, exemple : IRM. Une image 3D peut également être une vidéo, dans ce cas on parle de 2 dimensions spatiales et 1 dimension temporelle.

## 2.2. Traitement d'image

Le traitement d'image est une discipline de l'informatique et des mathématiques appliquées qui étudie les images numériques et leurs transformations, dans le but d'extraire les informations les plus pertinentes ou d'améliorer leur qualité ou tout simplement pour fournir une image plus perceptible à l' œil humain.

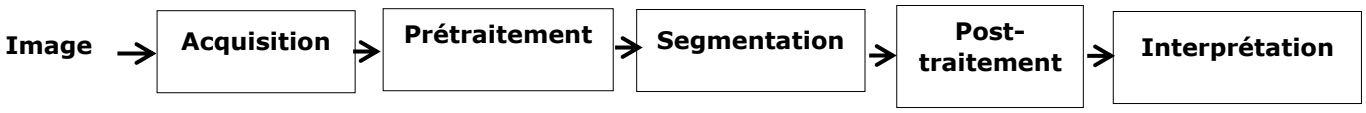



**Figure 1.1** : Schéma d'un système de traitement d'images.

### 2.2.1. Acquisition d'une image

L'acquisition d'images constitue un des maillons essentiels de toute chaîne de conception et de production d'images. Pour pouvoir manipuler une image sur un système informatique, il est nécessaire de lui faire subir une transformation qui la rendra lisible et manipulable par ce système. Le passage de cet objet externe (l'image d'origine) à sa représentation interne (dans l'unité de traitement) se fait grâce à une procédure de

numérisation. Ces systèmes de saisie, dénommés optiques, peuvent être classés en deux catégories principales [6]:

- Caméras numériques.
- Scanners.

A ce niveau, notons que le principe utilisé par le scanner est de plus en plus adapté aux domaines professionnels utilisant le traitement de l'image comme la télédétection, les arts graphiques, la médecine, etc.

Ce processus est effectué par cartes d'acquisition, qui reçoit les images de la camera, de la T.V. ou du scanner afin de les convertir en informations binaires qui seront stockées dans un fichier.

### 2.2.2. Prétraitement d'images

Cette phase a lieu juste après l'acquisition des images, et a pour objectif d'améliorer la qualité de l'image acquise en vue de sa segmentation.

### 2.2.3. Segmentation en régions

La segmentation est un processus qui consiste à découper une image en régions présentant une homogénéité selon un certain critère, comme par exemple la couleur. L'union de ces régions doit redonner l'image initiale. On regroupe généralement les algorithmes de segmentation en trois grandes classes :

- Segmentation basée sur les pixels.
- Segmentation basée sur les régions.
- Segmentation basée sur les contours.

### 2.2.4. Post-traitement

Il comprend toutes les opérations effectuées pour améliorer le rendu de l'image, et permet de corriger les défauts de prise de vue, le rendu des couleurs, leur saturation, le contraste, etc.

### 2.2.5. Interprétation

Elle consiste en la visualisation et la transmission des résultats qui sont faites soit subjectivement par un interprète humain soit objectivement par une analyse numérique (ordinateur) basée sur une maitrise de la manipulation des nombres, soit par la combinaison des deux.

## 2.3. Caractéristiques d'une image numérique

Une image numérique est une surface divisée en un ensemble fini de valeurs entières dont chacune est caractérisée par des paramètres, à savoir :

### 2.3.1. Pixel

C'est l'abréviation de « Picture élément » c'est-à-dire élément d'image qui représente le plus petit point de l'image pouvant être manipulé par les outils d'affichage et de traitement résultant d'une discrétisation. Il est quantifiable et se situe sur une grille régulière où chaque pixel de la grille est associé à une nuance de gris ou une couleur.

***a.*** **Image en niveau de gris** : Dans une image numérique, un pixel ne peut prendre qu'un nombre fini de valeurs appartenant à l'intervalle entre 0 et N-1 communément appelé dans le domaine de traitement d'image « niveau de gris ». Les 0 sont attribués au noir et le N-1 au blanc. Dans ce cas chaque pixel est codé sur un octet. Une image qui ne contient que deux niveau de gris le 0 pour le noir et le 1 pour le blanc est appelée image binaire.

**b. Image en couleurs** : C'est le résultat d'un couplage entre un système de codage de couleur et la représentation des niveaux de luminosité. Il existe de nombreux systèmes de codage de la couleur, on citera :

- (R.V.B) : un pixel est représenté par une combinaison de trois octets, un octet pour chacune des couleurs R (Rouge), V (Vert), B (Bleu).
- CMYK ou (CMJN) : un pixel est représenté par un mélange de trois octets C (Cyan), M (Magenta), J (Jaune), N (noir), etc.

### 2.3.2. Dimension

Une image numérique est représentée sous forme d'une matrice. Le nombre de lignes multipliées par le nombre de colonnes donne le nombre total des pixels dans une image.

### 2.3.3. Résolution

Elle détermine la précision de la représentation des détails de l'image et correspond au nombre de pixels par unité de longueur dans cette image, mesurée en « pixels par pouce » (ppp) équivalent à « dots per inch » (dpi), (1pouce = 2.54cm). Plus le nombre de pixels représentés est élevé plus la résolution est élevée et Meilleure est la représentation des détails.

### 2.3.4. Contours, textures, bruit, luminance et contraste

Les contours représentent les limites entre les différents objets d'une image. La texture décrit la structure de ces objets. L'identification des contours consiste à extraire les points qui séparent les différentes textures.
Le bruit est la dégradation que subit une image et qui est à l'origine une variation de l'intensité d'un pixel par rapport à ses voisins. Les sources du bruit peuvent être d'origine physique liées à l'instant d'acquisition de l'image, ou liées à son traitement.
La luminance est le degré de luminosité des points de l'image, définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface.
Le contraste est l'opposition marquée entre les régions sombres et les régions claires d'une image. Il est défini en fonction des luminances de deux zones d'images.

## 2.4. Techniques d'analyse d'une image numérique

### 2.4.1. Histogramme

Un histogramme est un graphique statistique permettant de représenter la distribution des intensités des pixels d'une image, c'est-à-dire le nombre de pixels pour chaque intensité lumineuse. Par convention un histogramme représente le niveau d'intensité en abscisse en allant du plus foncé (à gauche) au plus clair (à droite) [7].
Ainsi, l'histogramme d'une image en 256 niveaux de gris sera représenté par un graphique possédant 256 valeurs en abscisses, et le nombre de pixels de l'image en ordonnées :

- Un histogramme équilibré proche d'une fonction plate donne en général une image visuellement plaisante.
- Un histogramme tassé sur la gauche donne une image trop sombre.
- Un histogramme tassé au centre donne une image grisâtre.
- Un histogramme tassé à droite donne une image trop claire.
- Un histogramme trop creusé au centre (les noirs sont trop noirs, les blancs sont trop blancs) donne une image saturée.

### 2.4.2. Modification de l'histogramme

Au-delà du fait que l'histogramme permet d'étudier la répartition des valeurs des pixels d'une image, il permet également de corriger le contraste des couleurs pour des images surexposées ou sous-exposées.
En outre, sa modification n'altère pas les informations contenues dans l'image mais les rend plus ou moins visibles. Ces transformations apparaissent dans presque tous les

processus de traitement et d'analyse d'images : en prétraitement pour normaliser l'image, ou en post-traitement pour améliorer la visualisation.
La modification d'un histogramme est généralement représentée sur une courbe (appelée courbe tonale) indiquant la modification globale des composantes de l'image avec en abscisse les valeurs initiales et en ordonnées les valeurs après modification.
La courbe tonale correspond à une fonction de transfert définie par une table de transcodage appelé **look up table**, notée **LUT**.

### 2.4.3. Égalisation de l'histogramme

L'égalisation d'histogramme a pour but d'harmoniser la répartition des niveaux de luminosité de l'image, de telle manière à tendre vers un même nombre de pixel pour chacun des niveaux de l'histogramme. Cette opération vise à augmenter les nuances dans l'image.

### 2.4.4. Étirement de l'histogramme

Il consiste à répartir les fréquences d'apparition des pixels sur la largeur de l'histogramme c'est-à-dire répartir au mieux les intensités sur l'échelle des valeurs disponibles. Ceci revient à étendre l'histogramme afin que la valeur d'intensité la plus faible soit à zéro et que la plus haute soit à la valeur maximale. De cette façon, si les valeurs de l'histogramme sont très proches les unes des autres, l'étirement va permettre de fournir une meilleure répartition afin de rendre les pixels clairs encore plus clairs et les pixels foncés proches du noir.

### 2.4.5. Seuillage

Il consiste à mettre à zéro tous les pixels ayant un niveau de gris inférieur à un certain seuil, et à la valeur maximale les pixels ayant une valeur supérieure. Ainsi le résultat du seuillage est une image binaire contenant des pixels noirs et blancs, c'est la raison pour laquelle le terme de binarisation est parfois employé. Le seuillage permet de mettre en évidence des formes ou des objets dans une image. Toutefois la difficulté réside dans le choix du seuil à adopter.

### 2.4.6. Inversion

Elle consiste à inverser les extrêmes noir et blanc car parfois, on distingue mieux certains détails en blanc sur fond noir qu'en noir sur fond blanc.

# 3. Imagerie médicale

L'imagerie médicale est née il y a à peine cent ans à partir de grandes découvertes de la physique au XXème siècle et du progrès de la chimie, mathématiques appliquées et informatique dont le but était de diagnostiquer les maladies, mais aussi de suivre leur évolution, comprendre leur fonctionnement et de les soigner le plus efficacement possible.

Le principe de base est de repousser les limites du visible par l'absorption des rayons X, la résonance magnétique nucléaire, la réflexion d'ondes ultrasonores ou la radioactivité.
L'imagerie médicale traite deux types d'informations : celles liées à l'anatomie des organes (taille, volume, localisation, …) et celles liées à leurs fonctionnement (physiologie, métabolisme, …) qu'on appellera respectivement l'imagerie anatomique et l'imagerie fonctionnelle.

## 3.1. Principales modalités d'imagerie médicale

Un service d'imagerie de nos jours est constitué d'une multitude de modalités que nous citerons ci-dessous.

### 3.1.1. Radiographie

La radiographie par rayons X est la plus ancienne technique d'imagerie médicale en radiologie basée sur l'utilisation de rayons X pour visualiser un objet non uniformément composé, c'est-à-dire de densité et composition variables.

Lors de l'acquisition, un faisceau hétérogène de rayons X est produit par un générateur de rayons X et est projeté sur un objet. La densité et la composition de chaque zone de l'objet détermine la quantité de rayon absorbé. Les rayons X traversent l'objet et sont capturés par un capteur, positionné derrière l'objet, qui donne une représentation 2D de toutes les structures superposées les unes aux autres. L'image produite permet de mettre en évidence la structure et la forme des différentes parties du corps. Les systèmes d'acquisition modernes utilisent des outils informatiques avancés facilitant considérablement la capture numérique des images [8].

Actuellement, la radiographie, utilisée dans un sens plus large d'imagerie médicale, est notamment utilisée en orthopédie, orthodontie, pneumologie (radio de poumons) aussi pour la mammographie, etc.

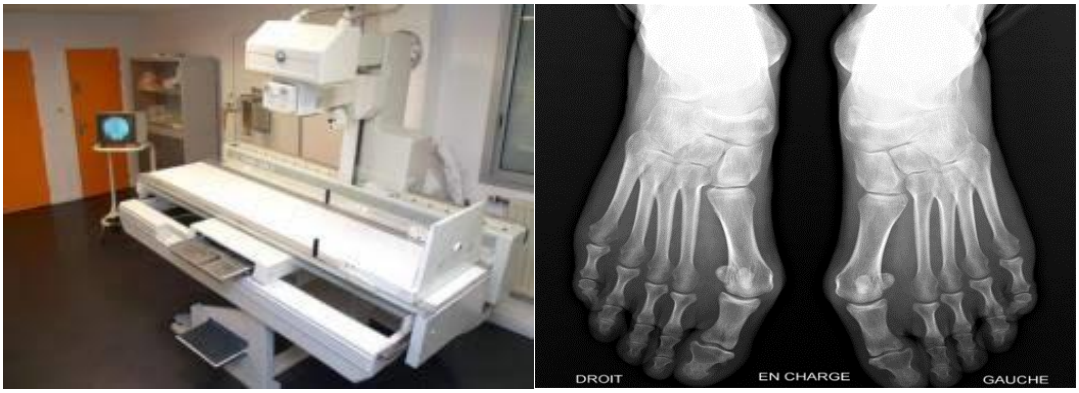



**Figure 1.2** : Schéma d'un système de radiographie (à gauche) [9] et un échantillon d'images radiographiques (à droite) [10].

### 3.1.2. Tomodensitométrie (TDM)

Tomodensitométrie (TDM) appelée aussi le scanner est une technique d'imagerie médicale qui permet de visualiser des modifications de volume ainsi que des anomalies de structure au niveau des tissus ou des organes.

Cette technique permet de mesurer l'absorption des rayons x par les tissus du patient, et reconstituer des images 2D et 3D des structures anatomiques, des images en coupe du corps humain à partir des différentes projections transversales obtenues par le système constituant l'appareillage [8].

Cette technique est utilisée pour la cancérologie, chimiothérapie, chirurgie, traumatologie, etc.

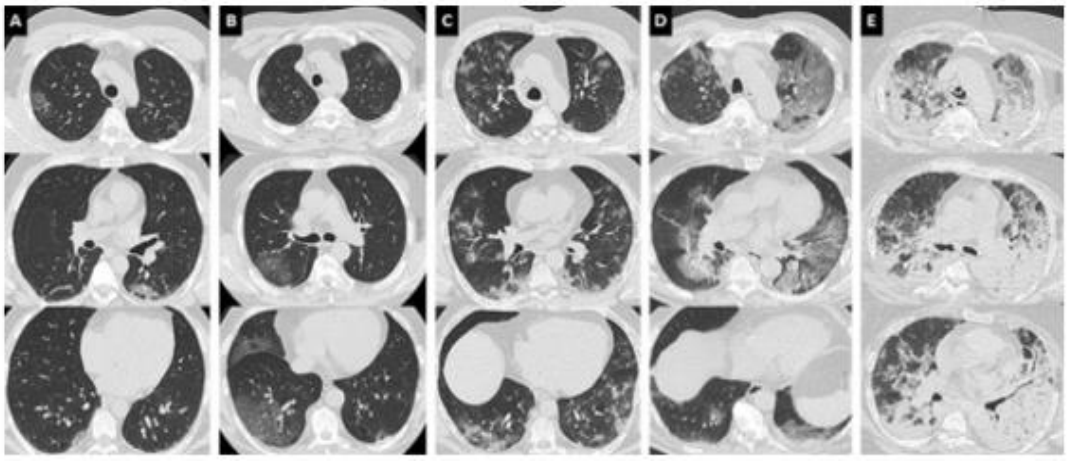



**Figure 1.3** : Schéma d'un scanner [10] (en haut) et un échantillon d'images (en bas) :

Différents degrés d'atteinte de pneumonie COVID-19. L'atteinte pulmonaire, évaluée visuellement comme le ratio du poumon pathologique sur le poumon sain, peut être classée comme minime < 10 % (A), modérée 10-25 % (B), étendue 25-50 % (C), sévère 50- 75 % (D) ou critique > 75 % (E). Une atteinte diffuse et des condensations déclives font évoquer un syndrome de détresse respiratoire aigu (E) [11].

### 3.1.3. Imagerie par Résonance Magnétique (IRM)

L'IRM est une technique d'imagerie médicale non invasive largement répandue dans les milieux hospitaliers. Elle donne accès à des images en deux ou trois dimensions de l'intérieur du corps avec de bonnes résolutions spatiale et temporelle.

Cette technique est basée sur le phénomène physique de Résonance Magnétique Nucléaire (RMN) du proton des atomes dihydrogène contenus dans les tissues et soumis d'une part à un champ magnétique produit par un aimant et d'autre part à une impulsion

radiofréquences. Lors de l'excitation du proton par l'onde radiofréquence, il accumule de l'énergie qu'il restitue à l'arrêt de l'impulsion sous forme d'un signal. C'est ce dernier qui est converti en image à l'aide d'un champ magnétique, d'ondes radio et d'ordinateurs qui génèrent des images des tissus internes [12].

La résonance magnétique est utilisée en particulier dans le diagnostic du système nerveux central, mais aussi dans des examens de la tête et de la colonne vertébrale, etc.

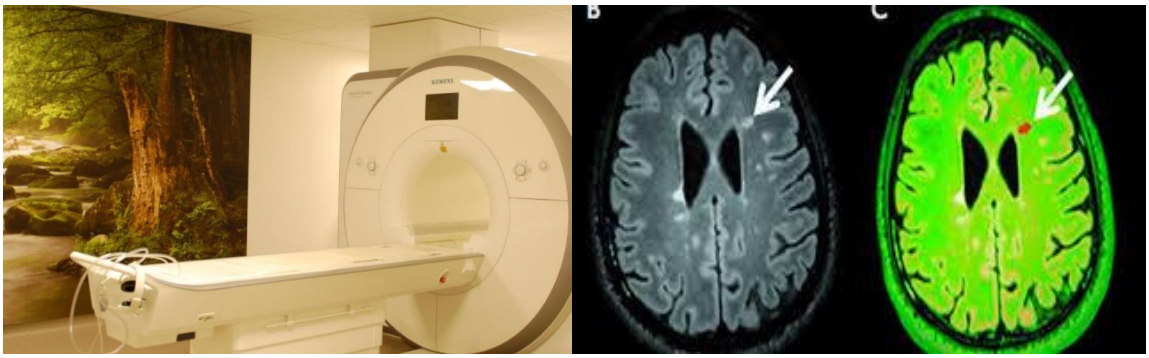


**Figure 1.4** : Schéma d'un système d'IRM [10] (à gauche) et un échantillon d'image (à droite) indiquant les formes progressives de sclérose en plaques (SEP) [13].

### 3.1.4. Imagerie nucléaire

La méthode d'examen d'imagerie nucléaire se base sur l'administration du radionucléide au patient. Il suffit de boire le produit contenant des isotopes sous la forme d'une solution ou injecté par voie intraveineuse. Après l'administration du produit, une caméra gamma est déplacée au-dessus du corps du patient. Cette caméra suit et enregistre le chemin parcouru par l'isotope dans le corps, en particulier les emplacements où il est accumulé, indiquant ainsi la voie pour atteindre les organes [14].

Il existe plusieurs techniques notamment : scintigraphie cérébrale, cardiaque et thyroïdienne, etc.

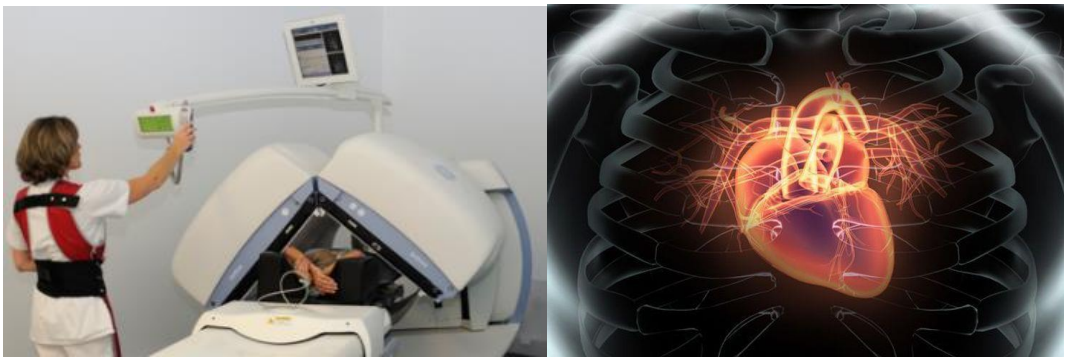


**Figure 1.5** : Schéma d'une machine nucléaire [15] (à gauche) et un échantillon d'image (à droite) issue de scintigraphie cardiaque [16].

### 3.1.5. Imagerie par Ultrasons ou Echographie

L'échographe est un appareil qui se compose d'une sonde émettant des ondes vers les tissus et recevant celles qu'ils renvoient. Selon leur densité, les tissus traversés font écho différemment : plus le tissu est dense, plus l'écho est important. Les ondes reçues sont analysées pour fournir une image [17].

Cette technique est utilisée pour étudier les organes pleins de l'abdomen, le cœur et tous les organes non masqués par lui.

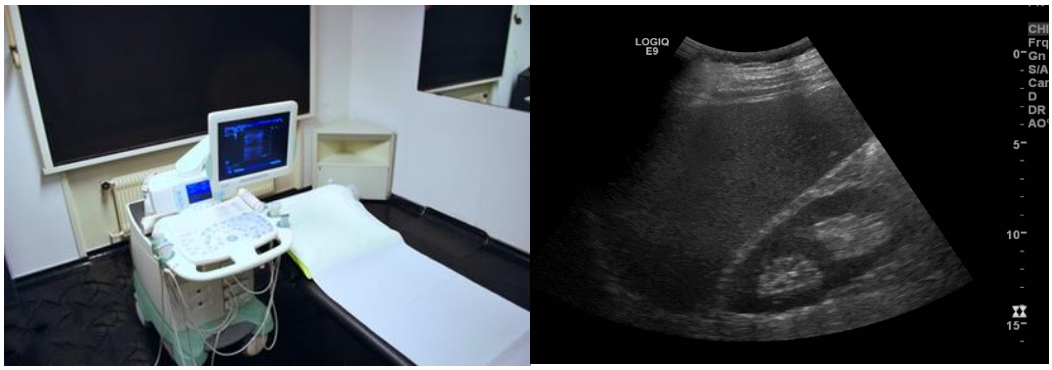



**Figure 1.6** : Schéma d'un système d'échographie [18] (à gauche) et un échantillon d'images (à droite) [10].

## 3.2. Spécificité des images médicales

- **Des pixels aux voxels**

Comparé à l'imagerie numérique bidimensionnelle où le processus d'échantillonnage se base sur les composantes élémentaires « pixel », l'échantillonnage volumique ajoute une troisième dimension « voxel ». Le mécanisme d'imagerie médicale reconstitue des images volumiques modélisées sous forme d'une fonction discrète de [1…X] × [1…Y] × [1…Z] où à chaque position s'associe une information.

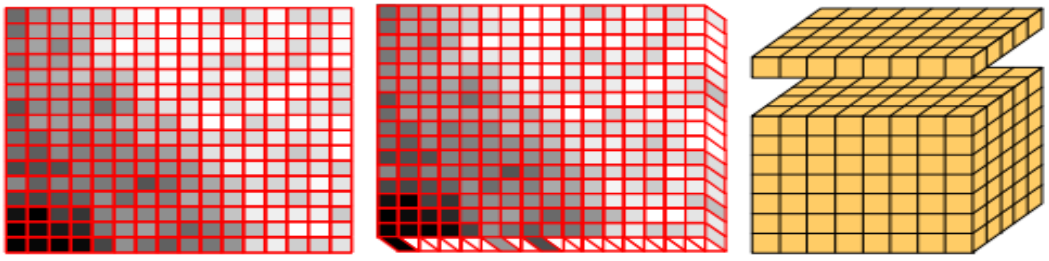


**Figure 1.7 :** Échantillonnage 2D-3D [17].

- **Taille des images**

La taille d'une image médicale dépend du capteur responsable de l'acquisition de la région anatomique à imager. Généralement en tomodensitométrie (technique d'analyse par coupe), les images font du 512 × 512 × 12 bits. En IRM, les formats d'images varient plus que n'importe quelle autre modalité avec des formats matriciels carrés et non carrés (par exemple 64 x 64, 64 x 128, 128 x 128, 128 x 192, 256 x 512, 512 x 512, 512 x 1024, ...) [19].

- **Résolution spatiale et temporelle**

La résolution spatiale est la capacité de voir des structures fines dans une image, au sens strict c'est de pouvoir distinguer deux objets petits et très rapprochés. Chaque modalité d'imagerie a une résolution propre à elle en fonction de plusieurs facteurs pouvant la limiter comme les propriétés des capteurs.
D'autres modalités d'imagerie médicale possèdent une résolution temporelle qui représente le nombre d'images acquises par seconde [20].

- **Bruit**

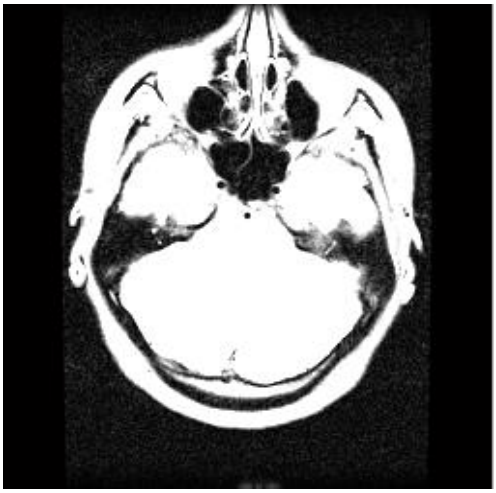
Par définition, un bruit est un phénomène aléatoire indésirable qui s'ajoute à l'image idéale dont l'impact dans une image médicale limite la détection d'anomalie. Cela est dû soit à l'anatomie corporelle où des variations de nature anatomiques non désirées au sein de l'image rendent la reconnaissance difficile d'organes nécessaire au diagnostic ou pour des raisons liées aux éléments physiques de la chaine d'acquisition de l'image comme : la source d'énergie, le matériel d'acquisition confondu et/ou un réglage de l'appareil.

- **Contraste**

Dans une image médicale, un diagnostic est généralement fait en discernant le signal anormal d'une lésion au sein d'un organe normal. C'est donc le contraste entre les deux qui permet le diagnostic.

## 3.3. Formats des images médicales

Les images médicales sont enregistrées sous un format de Stockage et d'échange appelé Digital Imaging Communication in Médicine (DICOM) qui contient, outre l'image elle-même, des métadonnées la caractérisant (identité du patient, date et heure d'acquisition, type d'appareil, paramètres d'acquisition détaillés, etc.). Dans les établissements de santé, les images sont désormais archivées dans un système en réseau appelé Picture Archiving and Communication System (PACS), habituellement consultable également par les correspondants [21].



FileModDate: '20-nov.-2002 16:02:48'
Format: 'DICOM'
ColorType: 'grayscale'
FileMetaInformationVersion: [2x1 uint8]
Modality: 'MR'
StudyDescription: 'BRAIN'
SeriesDescription: 'FSE PD AXIAL OBL'
PatientID: '123565'
PatientSex: 'F'
PatientAge: '028Y'
PatientWeight: 61.2350

**Figure 1.8 :** Exemple d'une image IRM du cerveau lue sur Matlab [22].

## 3.4. Sécurité des images et données médicales

Le récent développement de la télémédecine a attiré un grand public vers la consultation et le diagnostic à distance en envoyant via internet des dossiers médicaux contenant des rapports et des images médicales. Cependant une étude en 2013 de l'institut Ponemon a révélé que 15% des victimes d'usurpation d'identité médicale ont été mal diagnostiquées, 14% ont connu un retard pour obtenir un traitement, 13% ont reçu le mauvais traitement et 11% ont reçu les mauvais médicaments en raison d'erreurs qui se sont inscrites dans leur dossier. Vous pouvez également échouer à un examen d'emploi physique parce qu'une condition médicale que vous n'avez pas se retrouve dans votre dossier médical. Si vos informations médicales sont volées, cela vous expose à un plus grand risque de discrimination, en particulier au travail. En 2015, 45% des personnes interrogées ont déclaré que la divulgation non autorisée de leurs informations de santé avait affecté leur réputation [23].

Ces statistiques ont fait que les chercheurs et les spécialistes accordent plus d'attention à la sécurité des données médicales dans le but de préserver la confidentialité de la vie privée des patients et assurer une interprétation précise et efficace.

## 4. Conclusion

Dans ce chapitre, nous avons abordé des généralités qui décrivent une image numérique en allant de sa formation jusqu'à son traitement. Nous avons également expliqué ce qu'est une image médicale ainsi que le principe de fonctionnement des différentes modalités d'imagerie médicale et leurs utilisations. Nous avons décrit le format DICOM propre à l'image médicale. Toutefois, l'avancée de l'imagerie médicale actuellement nécessite un haut niveau de sécurité pour assurer la confidentialité de la vie privée des patients.

Dans le chapitre suivant, nous présenterons les différentes techniques de chiffrement en nous focalisant sur les algorithmes de chiffrement asymétrique.

Chapitre 2

# *Cryptographie sur courbes Elliptiques*

1. Introduction
2. Définitions
3. Classes de cryptographie
4. Cryptographie sur Courbes Elliptiques
5. Algorithmes de cryptographie basés sur les courbes elliptiques
6. Application de la cryptographie
7. Conclusion

## 1. Introduction

L'histoire de la cryptographie remonte à 1900 ans avant Jésus-Christ. Son utilisation concrète date du 5ème siècle avant J-C en Grèce antique établie dans un contexte de guerre utilisant un dispositif connu sous le nom du bâton de Scytale ainsi que le fameux chiffrement de Jules César qui date de la même époque. L'apparition des premiers ordinateurs durant la seconde guerre mondiale (1944) a permis aux américains de développer les organismes nationaux puissants chargés des écoutes. Vers 1976, l'usage de la cryptographie passe majoritairement des applications militaires aux applications civiles et de nombreux chercheurs du domaine s'y consacrent.

La cryptographie a toujours eu une grande importance dans l'histoire. Actuellement les réseaux informatiques exigent son utilisation pour assurer la confidentialité des données transmises notamment dans la téléphonie mobile, le paiement bancaire, les pièces d'identité, la télésanté, etc.

## 2. Définitions

- **Cryptologie :** mot composé de deux termes d'origine grec, kruptos «caché» et Logos «discours». C'est une combinaison des sciences mathématiques et informatiques qui étudie les communications secrètes composée de deux branches complémentaires à savoir : la **cryptographie** et la **cryptanalyse.**
  La première est basée sur la transformation des données d'une manière confidentielle pour rendre l'information incompréhensible afin de garantir son intégrité et sa confidentialité. La seconde étudie les faiblesses d'un système chiffré afin de révéler l'information en clair sans connaitre la clé de chiffrement.

- **Clé :** paramètre secret utilisé dans l'algorithme de cryptographie pour chiffrer l'information en clair en information chiffrée et vice versa. Elle se présente sous forme d'un nombre binaire (bits) dont la taille est proportionnelle au degré de sécurité de la donnée. Il est impératif que la clé ne soit dévoilée que pour le propriétaire légitime de l'information.

- **Chiffrement :** C'est la méthode ou l'algorithme qui rend la donnée incompréhensible pour une personne autre que l'émetteur et le destinataire.

- **Déchiffrement :** C'est la fonction qui permet de retrouver la donnée claire à partir de la donnée chiffrée à condition de connaitre la clé.
- **Texte chiffré :** ou cryptogramme c'est le résultat de l'application d'un chiffrement sur une donnée claire [24].

- **Texte clair :** c'est une donnée lisible et compréhensible par opposition au texte chiffré.

- **Crypto-Système :** ensemble de clés possibles (espace de clés), données claires et chiffrées et protocoles associés à un algorithme, nécessaires pour réaliser le processus de chiffrement/déchiffrement. La robustesse d'un système cryptographique se base sur deux critères : la résistance de l'algorithme de cryptographie et la confidentialité de la clé.

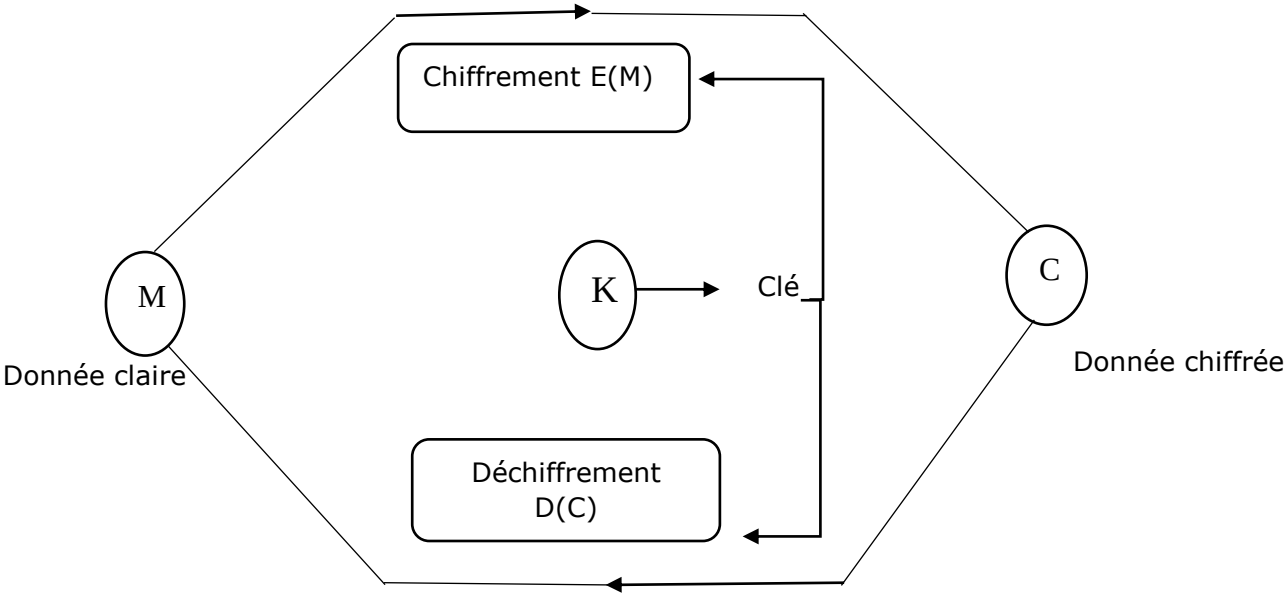



**Figure 2.1 :** Schéma d'un crypto-système.

Ce système est en réalité composé de trois algorithmes : un premier génère les clés K, un deuxième pour chiffrer M et un troisième pour déchiffrer C.

Le but d'un crypto système est de transformer un message intelligible (**texte clair**) en un **texte chiffré** (cryptogramme). Le destinataire légitime doit pouvoir **déchiffrer** le cryptogramme et obtenir le texte clair. Cependant, un **espion** (cryptanalyste) ne doit pas être en mesure de **déchiffrer** (cryptanalyse) le texte chiffré. Il ne faut donc pas confondre entre le **déchiffrement** qui est une opération effectuée par le destinataire légitime et le **décryptement** que l'*espion* tente d'effectuer.

- **Fonctions de la cryptographie :** On attend souvent de la cryptographie d'accomplir plusieurs fonctions pour garantir la sécurité de communication, ces fonctions sont : confidentialité, authentification, intégrité et non–reniement.

  - **La confidentialité** : permet de garantir que les données transmises vers un destinataire ne seraient déchiffrées que par ce destinataire, et par aucun autre. Ceci nécessite une identification précise du destinataire, et une méthodologie permettant de rendre inutilisable l'information à tout autre qu'à ce destinataire.
  - **La disponibilité** : a pour but de s'assurer qu'un système ou une donnée soit accessible et permanente durant le temps d'utilisation prévu.
  - **L'authentification** : permet de s'assurer de l'origine d'un message, ainsi que de l'identité du destinataire. Par les mécanismes d'authentification d'un protocole, on doit donc pouvoir garantir l'identité des deux partenaires d'une communication.
  - **L'intégrité :** est la méthode permettant de s'assurer que l'information n'a pas été altérée pendant son passage ou son stockage sur le réseau.
  - **Le non–reniement :** est la méthode pour s'assurer que l'information ne peut pas être désavouée. Une fois que le procédé de non–reniement est en place, l'expéditeur ne peut pas nier être le créateur des données.

## 3. Classes de la cryptographie

De nombreux systèmes de cryptographie ont été imaginés depuis plusieurs siècles, on peut les regrouper en trois grandes classes illustrées dans la figure ci-dessous :

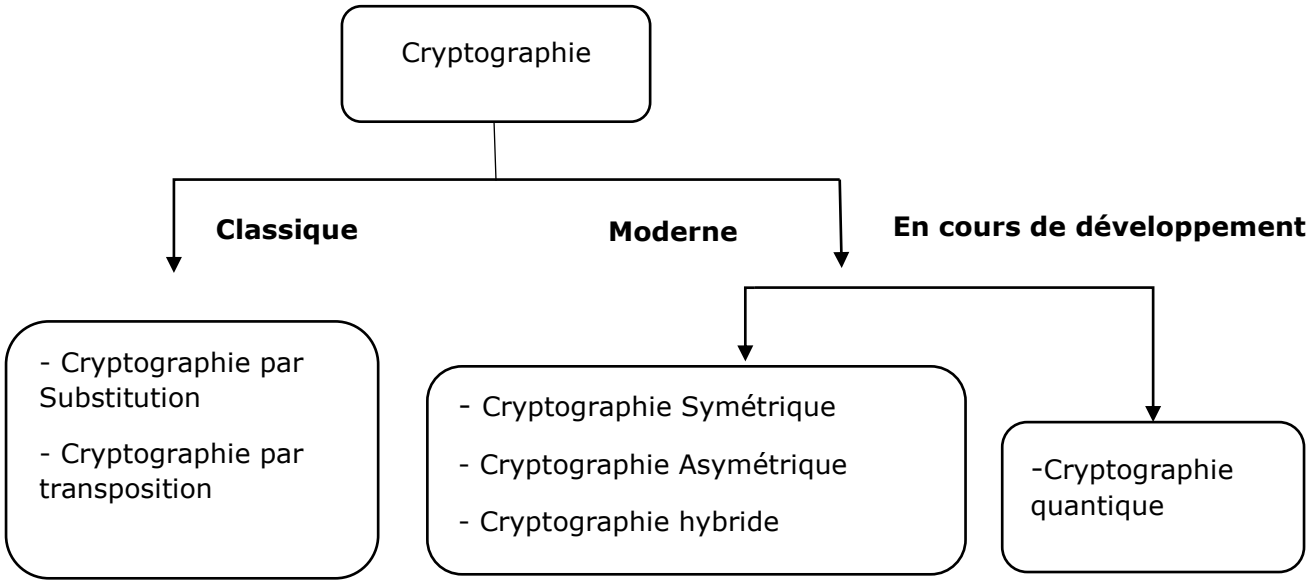



**Figure 2.2** : Schéma résumant les différentes classes de la cryptographie.

## 3.1. Cryptographie classique

Elle décrit la période avant le développement de l'informatique vers le Vème siècle avant J-C, et consiste à remplacer des caractères par d'autres et changer leur ordre tout en maintenant cette procédure secrète.

### 3.1.1. Cryptographie par substitution

**a. Substitution mono-alphabétique :** consiste à remplacer chaque lettre du message par une autre lettre ou un autre symbole. On citera à titre d'exemple le chiffrement de César qui est basé sur un simple décalage de lettres. Le principe de cet algorithme permet de chiffrer un message avec 26 façons seulement. De plus, il ne cache pas les fréquences d'apparition des lettres, ce qui facilite sa cryptanalyse.
On peut aussi citer : le chiffrement affine, les alphabets désordonnés, etc.

**b. Substitution poly-alphabétique** ou à alphabets multiples consiste à remplacer chaque lettre du message par plus d'une lettre ou symbole pris aléatoirement. On citera l'exemple le plus courant qui est le chiffrement de Vigenère qui représente une amélioration du chiffrement de César où une même lettre sera chiffrée de différentes manières en utilisant le carré de Vigenère.

### 3.1.2. Cryptographie par transposition

**a. Transposition simple par colonne :** On écrit le message horizontalement dans une matrice prédéfinie, et pour retrouver le texte chiffré, on lit la grille verticalement [25]. Le procédé inverse représente le procédé de déchiffrement.
**b. Transposition complexe par colonne :** La différence ici est qu'on utilise une clé de caractères différents pour constituer une séquence de chiffres qui représentent l'ordre d'apparition croissant des lettres alphabétiques. On écrit par la suite le texte clair par ligne dans une matrice et on lit le texte chiffré par colonne suivant l'ordre croissant de la séquence de chiffres.

## 3.2. Cryptographie Moderne

La cryptographie moderne a été développée après la seconde guerre mondiale dont le principe est d'utiliser des algorithmes ayant une clé pour chiffrer et déchiffrer des informations. À partir de 1949, Claude E. Shannon a travaillé sur le développement de la cryptographie moderne, et a influencé plusieurs chercheurs notamment M.E. Hellman et W. Diffie.

### 3.2.1. Cryptographie symétrique (à clé secrète)

L'algorithme de chiffrement dépend de l'utilisation de la même clé par l'émetteur et le destinataire, c'est à dire que la clé de chiffrement et celle de déchiffrement sont identiques. La figure 2.3 illustre le principe du chiffrement à clé secrète.

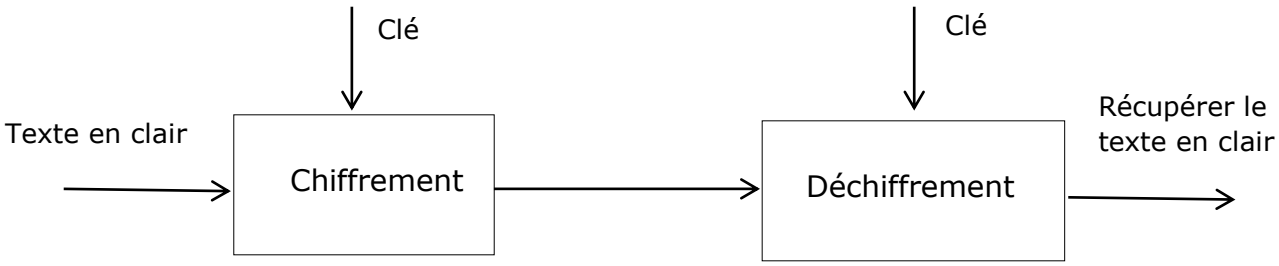



**Figure 2.3**: Cryptographie symétrique.

**Chiffrement de Vernam :** Un tel chiffrement parfait existe : Gilbert Vernam, ingénieur au laboratoire de recherche de la compagnie "American Telephone & Telegraph" l'a inventé et publié en 1926. Il peut être décrit simplement comme un chiffre de Vigenère, mais la clé répond aux trois impératifs suivants :

- Il faut que la clé soit de la même longueur que le message en clair.
- Elle est parfaitement aléatoire.
- Elle n'est utilisée que pour chiffrer un seul message.

De façon moderne, le chiffrement de Vernam (on parle aussi de masque jetable, pour souligner le fait que la clé doit être à usage unique), est implémenté de la façon suivante:

- Le message est converti informatiquement en suites de bits (0 et 1).
- On prend une clé (complètement aléatoire) composée elle aussi d'une suite de 0 et de 1, aussi longue que le message à chiffrer.
- On applique, ensuite, entre chaque bit du message clair et de la clé un ou exclusif (XOR) notée $\oplus$.

Le chiffrement de Vernam est parfait mais théorique. Les chiffrements actuels ne sont pas parfaits car [26]:

- Ils utilisent des clés plus courtes que le message à chiffrer.
- Ils réutilisent la clé plusieurs fois.

Pour cela, les méthodes actuelles de cryptographie symétrique se divisent en deux catégories:

a. Chiffrement par bloc (Block ciphers).
b. Chiffrement par flux ou bien chiffrement en continu (Stream ciphers).

### 3.2.2. Cryptographie asymétrique

La cryptographie asymétrique est un procédé qui intègre deux clés de chiffrement : une clé *publique* et une clé *privée*. Par convention, la clé de chiffrement du message est appelée clé publique (et peut-être communiquée sans aucune restriction), et la clé de déchiffrement du message est appelée clé privée [27]. Cette dernière ne doit être communiquée sous aucun prétexte. Avec une clé publique, l'expéditeur code dans un algorithme de chiffrement un message (ou une énigme) qui ne pourra être, au final, décodé ou résolu que par le destinataire détenteur d'une clé privée donnée en entrée d'un algorithme de déchiffrement.


**Figure 2.4 :** Chiffrement asymétrique.

Les algorithmes de chiffrement asymétrique les plus célèbres sont : RSA et ElGamel.

#### a. Algorithme RSA

Il a été décrit, pour la première fois, en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman du MIT. Dans le chiffrement RSA, tant la clé publique que la clé privée peuvent servir à chiffrer un message [28]. Dans ce cas, c'est la clé opposée à celle ayant servi au chiffrement qui est utilisée pour le déchiffrement. C'est notamment grâce à cette caractéristique que RSA est devenu l'algorithme asymétrique le plus répandu. Il offre, en effet, une méthode permettant d'assurer la confidentialité, l'intégrité, l'authenticité et la non-répudiabilité des communications électroniques et du stockage de données.

On peut résumer le fonctionnement de l'algorithme RSA comme suit [29]:

***Fonction de chiffrement E (publique) :*** la clé publique $k$ utilisée pour le chiffrement comporte deux entiers $K(e,n)$. L'opération de chiffrement se fait au moyen de l'élévation à la puissance e modulo n : $E_K(M) = M^e \ mod(n)$.

***Fonction de déchiffrement D (privée) :*** la clé secrète $k'$ utilisée pour le déchiffrement est aussi un couple d'entiers $k'(d,n)$. Le déchiffrement se fait au moyen de l'élévation à la puissance d modulo $n$ : $D_{k'}(M) = M^d \ mod(n)$.

***Détermination des clés***

- *Détermination de* $n$ *:* on doit initialement choisir deux entiers premiers $p$ et $q$ très grands et leurs valeurs sont secrètes et ne sont connues que par l'utilisateur.
- *Détermination de* $e$ *:* on calcule premièrement un entier w tel que : $w = (p-1)\cdot(q-1)$ Puis tout simplement choisir un entier e premier avec w.
- *Détermination de* $d$ *:* Calculer d tel que $e \cdot d \ mod(w) = 1$.

***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 |

**Tableau 2.1 :** Lettres de l'alphabet.

On choisit :

- Les deux entiers : $p = 17 \ et \ q = 19.$
- La clé publique : $n = p \times q = 17 \times 19 = 323.$
- L'indicateur d'Euler : $w = (p-1) \times (q-1) = 288.$
- $e = 5$ (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 |

**Tableau 2.2 :** Ordre de l'alphabet correspondant au mot « sécurité ».

**Chiffrement du message** $M$

En appliquant la formule : $E_K(M) = M^e \ mod(n)$ sur chaque caractère on obtient le message chiffré : $M' = 304\ 218\ 243\ 89\ 18\ 263\ 39\ 21$

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

**Tableau 2.3 :** Chiffrement du mot « sécurité ».

**Déchiffrement du message** $M'$

On déchiffre chaque nombre du message par : $D_{k'}(M) = M^d \ mod(n)$

Tel que $d = e^{-1} \ mod(w)$ (clé secrète)

Pour obtenir « d » on calcule l'inverse $d = 5^{-1} \ mod(288)$ en utilisant l'algorithme d'Euclide étendu.

$288 = 5 \times 57 + 3$ $\qquad$ $3 = 288 - 5 \times 57$
$5 = 3 \times 1 + 2$ $\qquad$ $2 = 5 - 3 \times 1$
$3 = 3 \times 1 + 2$ $\qquad$ $1 = 3 - 2 \times 1$
$2 = 1 \times 2 + 0$

$1 = 3 - 2 \times 1$
$= 3 - (5 - 3)$
$= -3 \times 3 + 2 \times 5$
$= -3 \times (288 - 5 \times 57)$
$= -3 \times 288 + 3 \times 5 \times 57 + 10$
$1 = -3 \times 288 + 173 \times 5$ $\qquad$ $donc : d = 173$

La position des lettres dans l'ordre alphabétique est représenté dans le tableau suivant :

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

**Tableau 2.4 :** Déchiffrement du mot chiffré.

Le message déchiffré correspondant à cet ordre est: **sécurité.**

### b. Algorithme ElGamel

Cet algorithme de chiffrement à clés publiques a été inventé par Tahar ElGamel en 1985, et il est lié au problème du logarithme discret utilisé pour le chiffrement asymétrique. On peut résumer le fonctionnement d'ElGamel par [30] :

***Détermination des clés***

- *Détermination de p et a :* On choisit deux entiers $p$ et $a$ tel que $p$ premier, $p$ et a sont premiers entre eux.
- *Détermination de s : On choisit* la clé secrète $s$ tel que $s < p$ .
- *Détermination de B :* On calcul la clé publique $B = a^s \ mod(p)$.

***Chiffrement***

– Soit un message $M < P$ on choisit un entier k qui n'est connu que par l'émetteur.

– Le message chiffré $C = (c_1, c_2)$ tel que $c_1 = a^k \ mod(p)$ et $c_2 = M \cdot b^k \ mod(p).$

***Déchiffrement***

**-** Calcul de $R_1 = c_1^s \ mod(p)$.

- Le message clair est donné par: $M = c_2 \cdot R_1^{-1} \ mod(p)$.

***Exemple***

On veut chiffrer le mot **« Médical »** en utilisant le protocole ElGamel, 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 |

**Tableau 2.5 :** Lettres d'alphabets 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.

$$M = 13050409030112$$

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

*Calcul de B :*

$$B = a^s \, mod(p) = 23^7 \, mod\, 661 = 566$$

La clé publique est donc : $(661, 23, 566)$. On choisit aléatoirement l'entier $k = 13$

*Chiffrement du premier bloc* $M_1 = 130$

$$c_1 = a^k \, mod(p) = 23^{13} \, mod(661) = 105$$
$$c_2 = M_1 \cdot B^K \, mod(p) = 130 \times 566^{13} \, mod(661) = 429$$
$$M'_1 = (105, 429)$$

| Blocs claires $M_i$ | 130 | 504 | 090 | 134 | 120 |
|---|---|---|---|---|---|
| Blocs chiffrés $M_i'$ | (105,429) | (105,209) | (105,297) | (105,134) | (105,396) |

**Tableau 2.6:** chiffrement du message M.

Le message chiffré est : $M' = 429\,209\,297\,134\,396$

**Déchiffrement du message** $M'$

Pour tous les couples $c_1 = 105$, on a la même valeur de $R_1$

$$R_1 = c_1^s \, mod(p) = 105^7 \, mod(661)$$
$$R_1^{(-1)} = y \, mod(p)$$

Tel que $y = R_1^{(-1)} \, mod(p)$

Pour calculer y, on calcule le reste de la division euclidienne de $d = 466^{-1} \, mod(661)$

Donc : $y = -200$

$$R_1^{(-1)} = y \, mod(p) = -200 \, mod(661) = -200 + 661 = 461$$

*Déchiffrement du premier bloc* $M'_1 = (105, 429)$

- $M_1 = c_2 \cdot R_1^{(-1)} \, mod(p) = 429 \times 461 \, mod(661) = 130$

| Blocs chiffrés $M_i$' | (105,429) | (105,209) | (105,297) | (105,134) | (105,396) |
|---|---|---|---|---|---|
| Bloc déchiffré $M_i$ | 130 | 504 | 90 | 301 | 120 |

**Tableau 2.7 :** 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 ».**

## 3.3. Cryptographie quantique

Elle est aussi appelée cryptographie à clé inviolable et permet de garantir un secret absolu sur des communications chiffrées. Fondée sur une idée originale de S. Wiesner, refusée en 1969 par une revue scientifique, la cryptographie quantique abrégée par BB84 s'est développée à partir de la publication de C.H. Bennett et G. Brassard, en 1984 [31].

Plusieurs versions du protocole BB84 ont vu le jour mais dans la plus simple on polarise les photons avec des valeurs binaires '0' et '1' dont l'état de polarisation est orthogonal pour encoder des données suivant deux bases :

- Base horizontale/verticale : les valeurs '0' et '1' correspondent aux photons ayant respectivement des polarisations de 0° et 90°.
- Base diagonale/anti-diagonale les valeurs '0' et '1' correspondent aux photons ayant respectivement des polarisations de 45° et 135°.

En considérant deux points communiquant 'Alice' et 'Bob', le protocole de cryptographie quantique suivra 6 étapes :

**Étape 1 :** Alice sélectionne aléatoirement une des bases cité ci-dessus et encode une suite de photons et l'envoie à Bob via un canal quantique.

**Étape 2 :** Bob reçoit les photons et mesure leurs polarisations en choisissant aléatoirement une base d'analyse.

**Étape 3 :** Alice communique à Bob, via un canal publique, ses choix de bases pour qu'il mesure la polarisation de chacun des photons.

**Étape 4 :** Bob compare ses choix avec ceux d'Alice et lui communique par la suite, via le canal publique, les positions des bits correspondants au cas où le choix de bases est similaire, les bits sont rejetés dans le cas contraire.

**Étape 5 :** Bob envoie aléatoirement à Alice, via le canal publique, un sous ensemble de données résultantes de l'étape 4, pour qu'elle procède à une analyse d'erreurs en effectuant une comparaison avec sa propre séquence. Cette étape détermine s'ils ont été espionnés.

**Étape 6 :** Si le taux d'erreurs 'QBER' est supérieur à 11%, Alice et Bob rejettent les données échangées et recommencent le protocole à l'étape 1. Sinon (QBER<11%) Alice déduit qu'il n'y a pas eu d'espionnage, Alice et Bob conservent les bits restants de l'étape 5 pour former la clé secrète qui n'est connue que par eux.

## 4. Cryptographie sur Courbes Elliptiques

La cryptographie sur courbes elliptiques (ou elliptic curve cryptography (ECC) en Anglais) est proposée indépendamment par Koblitz [32] et Miller [33] dans les années 80. Elle comprend un ensemble de techniques qui permettent de sécuriser des données en consommant moins de ressources. L'avantage le plus important de l'ECC par rapport aux autres algorithmes de cryptographie asymétrique, par exemple RSA [34], est que l'on peut avoir un bon niveau de sécurité en utilisant une clé beaucoup plus courte. Pour expliquer le fonctionnement de l'ECC, ce chapitre est consacré à la définition d'une courbe elliptique et les concepts mathématiques fondamentaux qui la caractérisent, ainsi qu'aux opérations les plus importantes et les protocoles cryptographiques qui sont basés sur les courbes elliptiques.

## 4.1. Courbe elliptique

Une courbe elliptique est un cas particulier d'une courbe algébrique munie d'une loi de groupe. Pas n'importe quelle loi de groupe, évidemment, sinon ce serait facile et ça n'aurait aucun intérêt, mais une loi telle que les coordonnées de la somme s'expriment en fonction de celles des points de départ suivant l'équation de *Weierstrass*:

$$E : y^2 + a_1xy + a_3y = x_3 + a_2x_2 + a_4x + a \qquad (2.1)$$

- Les coefficients $a_1, a_2, a_3, a_4, a_6$ représentent un ensemble d'éléments formés de deux opérations : l'addition et la multiplication. On suppose que la courbe est définie dans un corps et les paramètres $a_1, a_2, a_3, a_4, a_6 \in k$
- Une courbe elliptique E est définie sur K à laquelle on a rajouté un point à l'infini (l'élément zéro de l'addition) :

$$E = \left\{(x, y) \in \bar{k}^2 \,\middle|\, y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\} \cup \{O\} \qquad (2.2)$$

La condition $\Delta = -16(4a^3 + 27b^2) \neq 0$ s'assure que la courbe elliptique est « lisse », c.-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 tangentes distinctes).

## 4.2. Forme réduite de l'équation de Weierstrass

Pour son usage en cryptographie, on considère k un nombre fini et $a_1, a_2$ *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 la forme réduite de l'équation *Weierstrass* :

$$y^2 = x^3 + aX + b \qquad (2.3)$$

Cette équation est utilisée pour former un groupe où A et B sont deux éléments réels de k vérifiant : $4a^3 + 27b^2 \neq 0$. Dans ce cas, la courbe est lisse (elle possède une tangente en tout point de sa courbe représentative) [35].

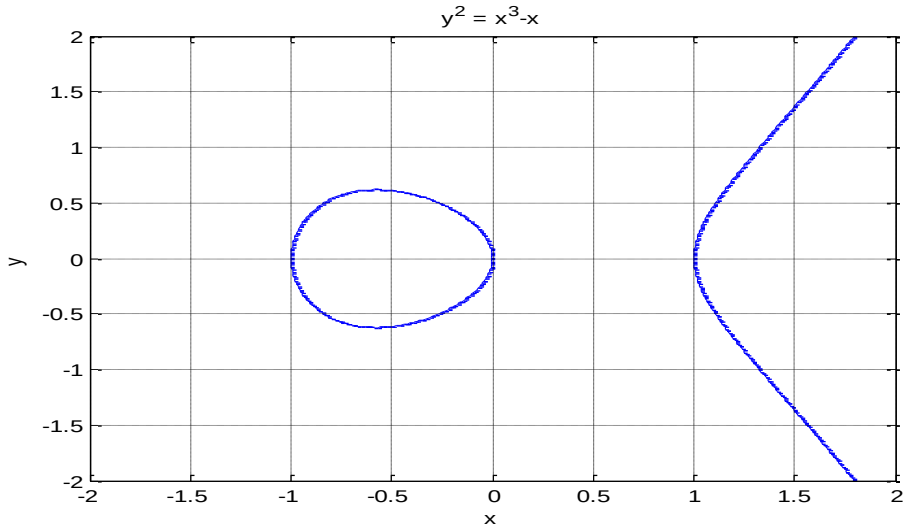



**Figure 2.5** : Exemple d'une courbe elliptique d'équation : $y^2 = x^3 - x$

## 4.3. Champ de points sur une courbe elliptique

Soit *E* une courbe elliptique sur $z_p$ Les variables de l'équation cubique obtenue peuvent prendre l'ensemble des entiers $E_P(a,b)$ : $\{0,1,\ldots,p-1\}$ vérifiant l'équation :

$$y^2 \equiv x^3 + ax + b \, mod(p) \qquad (2.4)$$

***Exemple :***

L'ensemble $E_{11}(1,7)$ est l'ensemble des nombres entiers $(x, y)$ vérifiant :

$$y^2 \equiv x^3 + x + 7 \, mod(11)$$

Pour trouver tous les points dans $E_{11}(1,7)$, on commence par déterminer tous les cas possibles que peut prendre l'équation (2.4) et on détermine par la suite les valeurs de $y^2$.

Dans cet exemple, *x* et *y* varient entre 0 et 10. Donc on obtient les résultats suivants :

$x = 0 \Rightarrow y^2 = 7$

$x = 1 \Rightarrow y^2 = 9$

$x = 2 \Rightarrow y^2 = 17 \equiv 6$

$x = 3 \Rightarrow y^2 = 37 \equiv 4$

$x = 4 \Rightarrow y^2 = 75 \equiv 9$

$x = 5 \Rightarrow y^2 = 137 \equiv 5$

$x = 6 \Rightarrow y^2 = 229 \equiv 9$

$x = 7 \Rightarrow y^2 = 357 \equiv 5$

$x = 8 \Rightarrow y^2 = 527 \equiv 10$

$x = 9 \Rightarrow y^2 = 745 \equiv 8$

$x = 10 \Rightarrow y^2 = 1017 \equiv 5$

| | | |
|---|---|---|
| $y = 0$ | $y^2 = 0$ | Aucun point |
| $y = 1$ | $y^2 = 1$ | Aucun point |
| $y = 2$ | $y^2 = 4$ | $x = 3$ |
| $y = 3$ | $y^2 = 9$ | $x = 1, 4, 6$ |
| $y = 4$ | $y^2 = 16 \equiv 5$ | $x = 5, 7, 10$ |
| $y = 5$ | $y^2 = 25 \equiv 3$ | Aucun point |
| $y = 6$ | $y^2 = 36 \equiv 3$ | Aucun point |
| $y = 7$ | $y^2 = 49 \equiv 5$ | $x = 5, 7, 10$ |
| $y = 8$ | $y^2 = 64 \equiv 9$ | $x = 1, 4, 6$ |
| $y = 9$ | $y^2 = 81 \equiv 4$ | $x = 3$ |
| $y = 10$ | $y^2 = 100 \equiv 1$ | Aucun point |

**Tableau 2.8 :** Recherche du champ de points de $E_{11}(1,7)$.

Ainsi, il y a 15 points possibles dans $E_{11}(1,7)$ (les 14 points au-dessus + le 15ème qui se trouve à l'infini).

$E_{11}(1,7) = \{(1,3),(1,8),(3,2),(3,9),(4,3),(4,8),(5,4),(5,7),(6,3),(6,8),(7,4),(7,7)$
$(10,4),(10,7),\infty\}$

La figure suivante donne le champ de points $E_{11}(1,7)$ possible sur la courbe de (2.5).

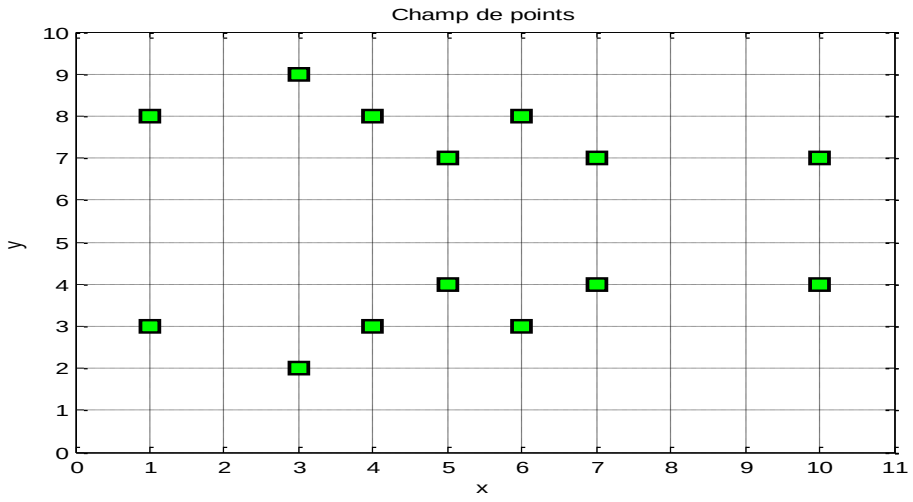



**Figure 2.6** : Champ de point de $E_{11}(1,7)$

## 4.4. Opérations sur les courbes elliptiques

On va définir les formules qui permettent de calculer les coordonnées du point « R » résultant d'une addition ou multiplication ou soustraction de deux points P et Q.

### 4.4.1. Addition de 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*. Muni de cette loi de composition $(E(K),+)$ est un groupe abélien dont l'élément neutre est le point à l'infini (*O*).

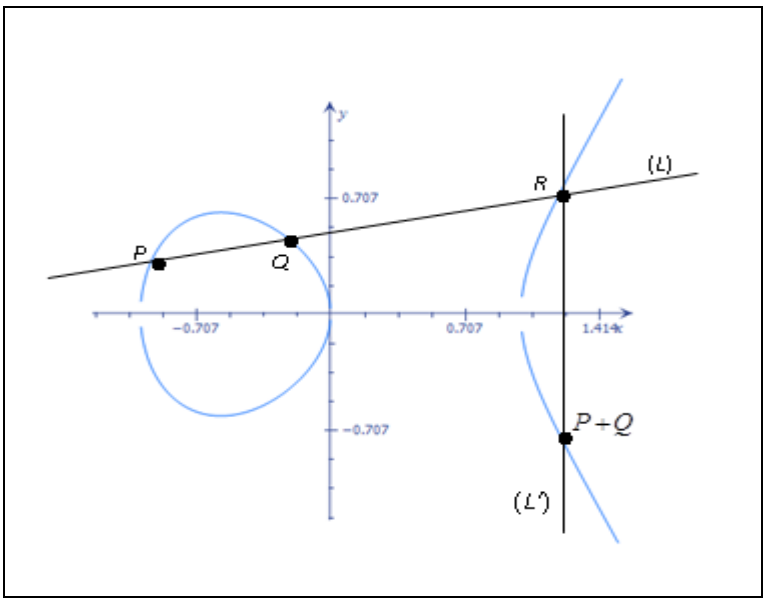



**Figure 2.7 :** Addition de deux points sur une courbe elliptique [36]

**Algorithme d'addition de deux points dans $E_p(a,b)$** [37]

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

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

- Si $x_1 \neq x_2$, alors

$$\begin{cases} x_3=\left(m^2-(x_1+x_2)\right)\bmod(p) \\ y_3=\left(m(x_1-x_3)-y_1\right)\bmod(p) \end{cases} \quad où \ : m=\frac{y_2-y_1}{x_2-x_1}=\frac{c}{d}=\left(c\cdot inv(d)\right)\bmod(p). \qquad (2.5)$$

- Si $x_1=x_2$ et $y_1 \neq y_2$, alors : $P_3=O$.
- Si $P_1=P_2$ et $y_1 \neq O$, alors :

$$\begin{cases} x_3=\left(m^2-2x_1\right)mod(p) \\ y_3=\left(m(x_1-x_3)-y_1\right)mod(p) \end{cases} \quad où : m=\frac{3x_1^2+a}{2y_1}=\frac{c}{d}=\left(c\cdot inv(d)\right)mod(p). \qquad (2.6)$$

- Si $P_1=P_2$ et $y_1=O$, alors : $P_3=O$.

**Pourquoi le point à l'infini est égal à *O* (élément neutre pour l'addition) ? [37]**

Soit $P_0$ ce point à l'infini. Pour trouver $P + P_0$, on doit, selon la méthode décrite, tracer la droite passant par le point $P$ et le point $P_0$ (figure 2.8 ), 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 $P + P_0$ cherché, par définition de l'addition, est le symétrique de ce point *P*', donc c'est *P* lui-même : on a bien trouvé que $P + P_0 = P$ ce qui correspond bien à ce qu'on attend d'un " zéro " pour l'addition.

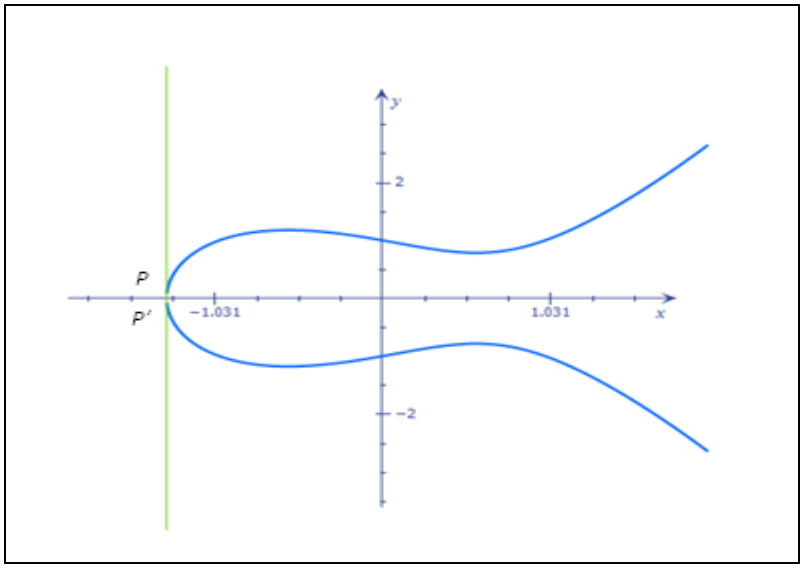



**Figure 2.8 :** Représentation de l'équation dans $E : y^2 = x^3 - x + 1$

### 4.4.2. Soustraction de deux points

Soient E une courbe elliptique définie sur un corps K, et deux points P, Q de E(K). Donc pour soustraire Q de P, on fait la négation de Q puis l'addition. La négation se fait comme suit [31] :

On considère $Q = (x_q, y_q)$, et on veut calculer $R = -Q = (x_r, y_r)$.

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

$$y = moy = \frac{y_s + y_t}{2} \quad \rightarrow \begin{cases} y_r = y_q + 2(moy - y_q) \\ x_r = x_q \end{cases} \qquad (2.7)$$

Enfin, $P + (-Q)$ est calculé en utilisant l'algorithme d'addition décrit précédemment.

### 4.4.3. Doublement successif [38]

On considère un point sur une courbe elliptique, P, et n un nombre entier positif, alors $nP$ peut être calculé par :

$$nP = \begin{cases} P + P + \ldots\ldots\ldots\ldots + P & n > 0 \\ -P - P - \ldots\ldots\ldots\ldots - P & n < 0 \end{cases} \qquad (2.8)$$

Quand l'entier $n$ est très grand, il est pratique d'utiliser le doublement consécutif.

Soit à calculer, par exemple, $36P$ .

$2P = P + P$

$4P = 2P + 2P$

$8P = 4P + 4P \quad \Rightarrow \quad Donc : 36P = 32P + 4P$

$16P = 8P + 8P$

$32P = 16P + 16P$

Pour chaque entier $m$ on doit le binariser, c'est-à-dire on l'écrit sous forme d'une somme de $2^m$ , avec $m = 0, 1, 2, \ldots$

***Exemple :***

On calcule dans $E_{17}(2,2)$ : $18 \cdot P$ avec $P = (5,1) \in E_{17}(2,2)$

On commence par la binarisation de 18 : $18 = 2^4 + 2 = 16 + 2 \Rightarrow 18P = 16P + 2P$

Avec l'algorithme d'addition décrit précédemment, on procède comme suit :

$4P = 2P + 2P = (6,3) - (6-3) = (3,1)$

$8P = 4P + 4P = (3,1) + (3,1) = (13,7)$

$16P = 8P + 8P = (13,7) = (10,11) \qquad Donc : 16P + 2P = (10,11) + (6,3) = (5,16)$

# 5. Algorithmes de cryptographie basés sur les courbes elliptiques

## 5.1. Diffie-Hellmann elliptique

L'un des usages les plus courants des courbes elliptiques est la génération d'un secret partagé entre Alice et Bob en utilisant le mécanisme de Diffie-Hellman dans le groupe d'une courbe elliptique défini sur un corps fini K (ex : Z\PZ).

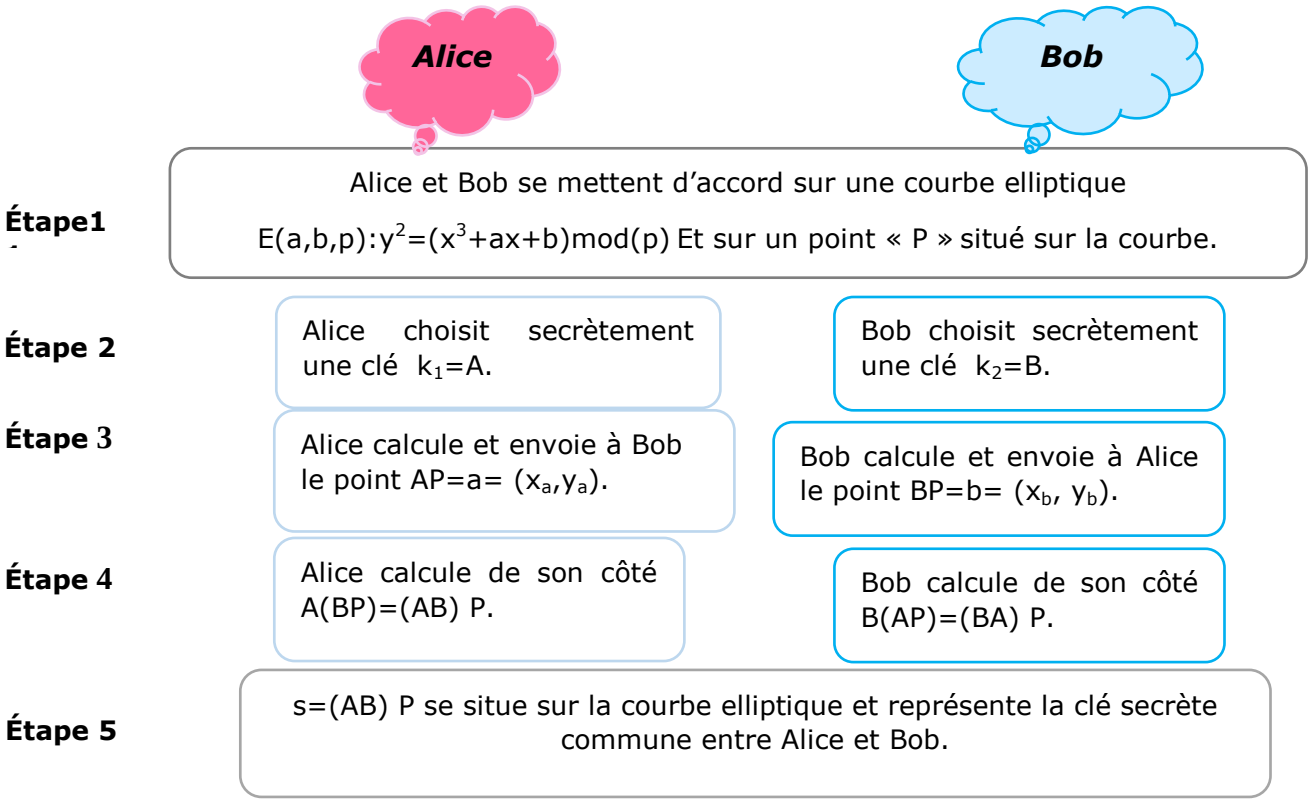



**Figure 2.9 :** Schéma du protocole Diffie-Hellmann elliptique.

**Remarque :**

- Dans le cas où Ève espionne leurs échanges, elle est au courant de $E(a,b,p), p, AP, BP$
- Pour déchiffrer la clé secrète, il faut calculer $A$ connaissant $P$ et $AP$. C'est ce qu'on appele « Résolution du logarithme discret »

***Exemple***

**Étape 1** : Alice et Bob choisissent une courbe elliptique définie sur un corps fini :

$E : y^2 = x^3 - 4 \, mod(211)$ Et un point de la courbe : $P = (2,2) \in E$

**Étape2 :** Alice et Bob choisissent respectivement deux clés secrètes (entiers) :

$k_1 = A = 150$ et $k_2 = B = 170$

**Étape 3** : - Alice calcule et envoie à Bob : $AP = a = (150) \times (2,2) = (206,90)$

- Bob calcule et envoie à Alice : $BP = b = (170) \times (2,2) = (196,29)$

**Étape 4** : - Alice calcule de son côté $A \times (BP) = A \times b = 150 \times (196,29) = (83,87)$

- Bob calcule de son côté $B(A \times P) = B \times a = 170 \times (206,90) = (83,87)$

**Étape 5** : $s = (A \times B)P$ se situe sur la courbe elliptique et représente la clé secrète commune entre Alice et Bob.

## 5.2. ElGamel elliptique

On suppose cette fois-ci qu'Alice veuille envoyer à Bob un message en utilisant l'algorithme ElGamel elliptique.

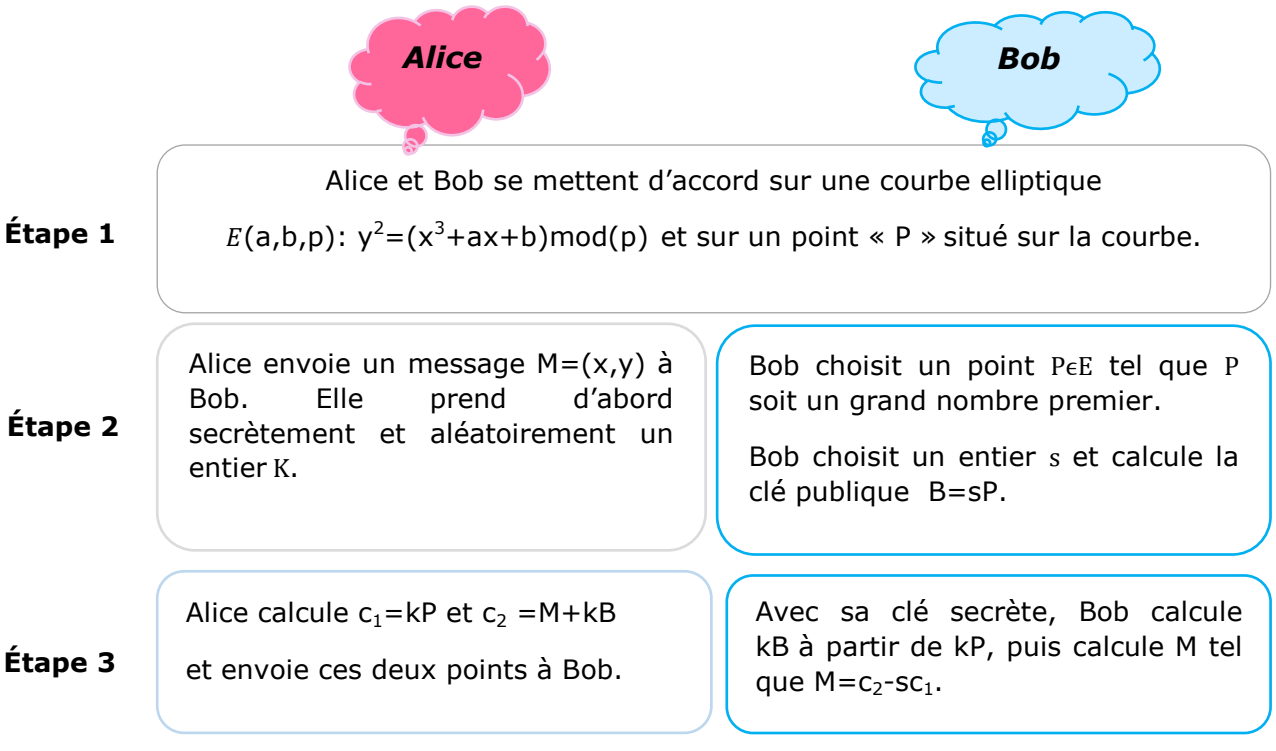



**Figure 2.10 :** Schéma du protocole ElGamel elliptique.

***Remarque :***

Pour échanger un texte, il faut pouvoir le transformer en une suite de points de la courbe elliptique. Car il n'est pas toujours facile de trouver des points sur une courbe elliptique. Si quelqu'un espionne les échanges, on ne connait pas de chemin plus facile que de calculer $\boldsymbol{s}$ pour retrouver $\boldsymbol{M}$ : c'est encore une fois le problème du logarithme discret à résoudre. Un espion connait la clé publique et les points $\boldsymbol{c_1}$ et $\boldsymbol{c_2}$, s'il savait résoudre le problème du logarithme discret, il pourrait utiliser $\boldsymbol{p}$ et $\boldsymbol{B}$ pour trouver $\boldsymbol{s}$ et ainsi calculer $\boldsymbol{c_2 - s\,c_1}$. L'espion pourrait aussi utiliser $\boldsymbol{p}$ et $\boldsymbol{c_1}$ pour trouver $\boldsymbol{k}$ et calculer $\boldsymbol{M = c_2 - kB}$.

***Exemple :***

**Étape 1**: Alice et Bob choisissent une courbe elliptique définie sur un corps fini :

$$E : y^2 = x^3 + 3x + 45 \; mod(8831)$$

**Étape 2**: Bob choisit un point de la courbe $p = (4,11)$ et un entier s=5 pour calculer B tel que $B = s \times p = 5 \times (4,11) = (3602,4699)$ Alice veut envoyer un message $M = (5,1743)$ et choisit secrètement et aléatoirement un entier $k = 10$

**Étape 3** :

- Alice envoie le couple $(c_1, c_2)$ à Bob :

$$c_1 = k \times p = 10 \times (4,11) = (6950,1113)$$

$$c_2 = M + kB = (5,1743) + 10 \times (3602,4699) = (4930,3343)$$

- Bob déchiffre le message :

$$M = c_2 - sc_1 = (4930,3343) - 5 \times (6950,1113)$$
$$= (4930,3343) + (1716 - 8253) = (5,1743) = M$$

## 6. Applications de la cryptographie sur les courbes elliptiques

De nos jours, le développement des systèmes informatiques et de cryptanalyse ont engendré des applications gourmandes en sécurité et ce dans plusieurs domaines tel que : les systèmes et cartes bancaires, les applications multimédias à temps réel comme la téléphonie IP, la télésanté, etc.

Les premières expérimentations pratiques mettant en œuvre la cryptographie à base de courbes elliptiques sont des résultats de laboratoire.

Ainsi, en 1989, Mullin et Vanstone présentent pour la première fois une carte électronique implantant des opérations sur des courbes elliptiques [39]. Cette carte était construite autour d'un processeur Motorola M68008. En 1992, la faisabilité de crypto systèmes construits à base de courbes elliptiques avec des clefs de l'ordre de 100 bits est étudiée dans la référence [40]. Des taux de 2 Kbits/s sont atteints sur station de travail. En 1993, Menezes et Vanstone [33] explorent la faisabilité d'implanter en hardware un processeur arithmétique pour effectuer des calculs sur des courbes elliptiques définies sur des corps finis. Enfin, en 1995, Schroeppel et al. [41] décrivent une implantation logicielle d'un échange de clef à la Diffie-Hellman à base de courbes elliptiques définies sur F2155 dont les performances sont, à niveau de sécurité équivalent, légèrement meilleures que celles du Diffie-Hellman usuel.
Depuis ces expérimentations, plusieurs normes déjà approuvées ou en cours d'approbation ont vu le jour. Nous rappelons les principales ci-dessous.

**ANSI:** "American National Standards Institute".

– ANSI X9.62 : "Elliptic Curve Digital Signature Algorithm " (ECDSA) est un standard de signature électronique.

– ANSI X9.63 : "Elliptic Curve Key Agreement and Key Management" normalise l'utilisation de courbes elliptiques à des fins de chiffrement.

**FIPS:** "Federal Information Processing Standard" du NIST (US government's "National Institute of Standards and Technology"). Il s'agit d'une RÉFÉRENCES 7 extension du standard de signature électronique (DSS) pour inclure l'algorithme ECDSA (ANSI X9.62).

**IEEE :** La norme IEEE 1363-2000 couvre la cryptographie asymétrique à base de logarithmes discrets (corps finis ou courbes elliptiques) ainsi que celle à base de RSA. Elle spécifie les mécanismes ECDSA, ECDH et ECMQV.

**PKCS :** émis par la société RSA inc. Cette norme adresse de nombreux aspects : la génération des clés et des paramètres, la signature électronique, le chiffrement asymétrique, etc.

**TLS** et serveurs **HTTPS :** Les clés de sessions sont échangées avec ECDH (depuis 2006) et les signatures effectuées avec ECDSA (sur certains serveurs).

**SSH :** Utilise les courbes elliptiques depuis 2009 avec ECDH et ECDSA.

**Bitcoin :** un Bitcoin est en fait une chaîne de transactions chiffrées et signées. Les adresses sont déduites des clés publiques et les transactions sont authentifiées en utilisant ECDSA.

## 7. Conclusion

On a vu dans ce chapitre des généralités sur les différentes classes de cryptographie notamment la cryptographie moderne qui comprend les deux algorithmes les plus utilisés actuellement dont : RSA et ElGamel. Aussi, on a introduit les notions de base sur les courbes elliptiques et leurs applications spécialement en cryptographie. Le chapitre suivant sera consacré à l'implémentation d'un algorithme de cryptographie basé sur les courbes elliptiques pour chiffrer un texte proposé par Sagheer et amélioré par W.K. Kadir. L'algorithme est sélectionné afin de l'appliquer pour la cryptographie des images médicales.

# Chapitre 3

# *Algorithme proposé*

1. Introduction.
2. Revue de la littérature.
3. Simulation de chiffrement/déchiffrement d'un texte sur une courbe Elliptique prédéfinie.
4. Performances des algorithmes RSA, ElGamel et ECC.
5. Conclusion.

## 1. Introduction

Les technologies de l'information et de la communication sont désormais présentes dans toutes les couches de la société, et les informations sont communiquées et traitées automatiquement à grande échelle, telles que les services bancaires électroniques les multimédias, le commerce électronique, le gouvernement électronique, le système de santé et les vidéoconférences. Toutes ces applications ont besoin de protéger leurs informations afin d'assurer la confidentialité, prévenir la fraude et sauvegarder les intérêts économiques.

Depuis le début de la cryptographie à clé publique, il existe deux principaux systèmes de chiffrement : RSA et ElGamel, qui semblent vaincre toutes les attaques. Pour cette raison, ces deux crypto systèmes sont les plus respectés et les plus largement utilisés de nos jours. Cependant, au fil du développement de la technologie, la longueur de la clé en Bits de l'algorithme RSA augmentait pour assurer sa robustesse et sa sécurité, ce qui a alourdi le traitement basé sur des applications l'utilisant [3]. Cette charge présente des implications, en particulier pour les applications de commerce électronique qui effectuent un grand nombre de transmissions sécurisées. Cela a conduit à l'attrait pour la cryptographie à courbe elliptique (ECC).

ECC possède certains avantages notamment : efficacité de calcul, faible capacité de stockage et bande passante étroite par rapport à d'autres crypto systèmes à clé publique. Il inclut la distribution des clés, schémas de chiffrement/déchiffrement et algorithme signature numérique (DSA : Digital Signature algorithms) [42]. L'algorithme de distribution de clé est utilisé pour partager une clé secrète, l'algorithme de chiffrement/déchiffrement permet une communication confidentielle, et le DSA est utilisé pour authentifier le signataire et valider l'intégrité du message.

## 2. Revue de la littérature

En 1975 fut proposé le principe de la cryptographie à clé publique. Ce n'est qu'en 1977 que fut présenté le premier protocole effectif : RSA et le deuxième en 1985 : l'algorithme El Gamel. Principalement basé sur le problème de la factorisation des grands entiers, RSA est encore aujourd'hui la primitive la plus utilisée en cryptographie. Cependant les nombreux progrès effectués dans le domaine de la factorisation font que la taille des clés RSA augmente plus rapidement que ne le requiert l'augmentation de la puissance des ordinateurs. C'est l'une des raisons pour lesquelles la cryptographie basée sur les courbes elliptiques (ECC) a connu un tel intérêt depuis son introduction par Miller et

Koblitz en 1987. Reposant sur le problème du logarithme discret, ECC requiert un niveau de sécurité équivalent, des clés bien plus petites que RSA (une clé ECC de 160 bits est aussi robuste qu'une clé RSA de 1024 bits), celui-là étant donc plus adapté à des environnements à puissance réduite (tels que les cartes à puce) [43].

Depuis 1985, beaucoup d'attention a été portée aux courbes elliptiques pour les applications cryptographiques et un grand nombre de travaux de recherche a été présenté dans la littérature [42, 44, 47].

Le travail présenté dans ce manuscrit se base sur l'article de W.K. Kadir et al. [44] qui peut être considéré comme une généralisation des travaux de A. M. Sagheer [42]. En fait, le schéma est déduit de celui de Sagheer en deux étapes avec de nombreux modificateurs utilisant l'algorithme proposé par Teeriaho et al. [47]. De nombreux auteurs ont expliqué l'impact de l'ECC et ont proposé de nouvelles idées qui peuvent augmenter la sécurité du système. Miller a inventé les courbes elliptiques pour la cryptographie. Son algorithme était similaire à l'échange de clé Diffie Hellman mais 20% plus rapide [42].

Deux ans plus tard, Koblitz (1987) a expliqué en utilisant une courbe elliptique sur un champ fini dans la cryptographie à clé publique. Il a mentionné que le DLP sur un champ fini est plus difficile que le champ binaire. Koblitz et al. (2000) ont étudié le développement de la cryptographie sur courbes elliptiques depuis son invention. Ils ont fourni les facteurs qui peuvent être utilisés pour choisir une bonne courbe elliptique pour la cryptographie et ils ont également discuté les avantages de l'utilisation de la courbe elliptique dans les crypto systèmes à clé publique. En termes d'implémentation par Mathematica, Teeriaho (2011) a donné des exemples d'échange de clés à courbe elliptique, de chiffrement et de signature numérique. Alors que Kolhekar et Jadhav (2011) ont implémenté avec C++ le chiffrement de texte. Plusieurs algorithmes sont proposés dans la littérature notamment ceux de Kumar et al. (2012), Esfahani et al. (2013) qui convertissent le message en valeurs ASCII, puis mappent les valeurs ASCII en un point affin dans la courbe elliptique. Cependant, ces méthodes nécessitent le partage d'une table de correspondance [42].

L'avantage de l'algorithme étudié, dans ce mémoire, est que les auteurs éliminent la table partagée entre l'expéditeur et le destinataire et ils n'ont pas besoin de mapper la valeur ASCII à un point affin dans la courbe elliptique. La technique est conçue de manière à pouvoir être utilisée pour chiffrer et déchiffrer tout type de script avec une valeur ASCII définie. En effet, cet algorithme est basé sur le partage des codes ASCII de

n'importe quel message en blocs (groupes) afin de former des coordonnées (points) à courbures elliptiques. Cette méthode présente de nombreux avantages dont : réduction de la bande passante, adaptation aux messages à grand volume, rapidité du processus de chiffrement/déchiffrement, niveau de sécurité élevé avec une clé plus petite que les techniques de cryptographie modernes décrites précédemment.

## 2.1. Algorithme proposé

Dans cet algorithme, Alice et Bob s'accordent sur plusieurs paramètres publiquement :

- Une courbe elliptique dont les paramètres sont : A, B et p :

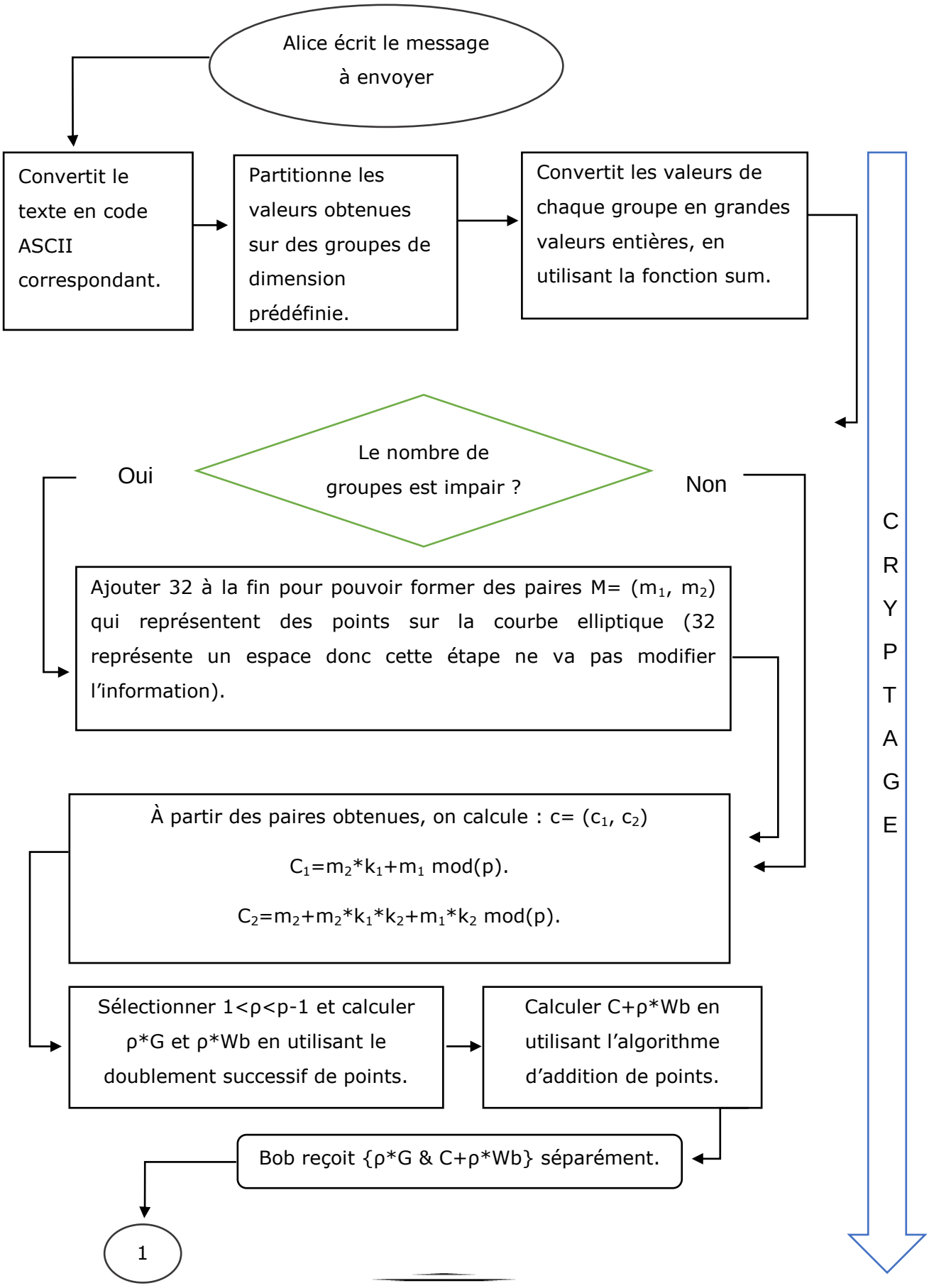
$$E : y^2 = x^3 + Ax + B \, mod(p).$$

- Un générateur de clés publiques qui représente un point de la courbe, $G \in E$
- Deux clés privées ka et kb pour calculer les deux clés publiques (* représente un doublement consécutif de points). :

$$Wa = Ka * G.$$
$$Wb = kb * G.$$

Secrètement, Alice forme la clé commune K= (k1, k2), en utilisant sa clé privée ka et la clé publique de Bob Wb : $K = ka * wa = (k_1, k_2) \, mod(p).$

Le schéma block, présenté ci-dessous, résume les différentes étapes de chiffrement et déchiffrement :


Alice écrit le message à envoyer
Convertit le texte en code ASCII correspondant.
Partitionne les valeurs obtenues sur des groupes de dimension prédéfinie.
Convertit les valeurs de chaque groupe en grandes valeurs entières, en utilisant la fonction sum.
Le nombre de groupes est impair ?
Oui
Non
Ajouter 32 à la fin pour pouvoir former des paires M= (m1, m2) qui représentent des points sur la courbe elliptique (32 représente un espace donc cette étape ne va pas modifier l'information).
À partir des paires obtenues, on calcule : c= (c1, c2)
C1=m2*k1+m1 mod(p).
C2=m2+m2*k1*k2+m1*k2 mod(p).
Sélectionner 1<ρ<p-1 et calculer ρ*G et ρ*Wb en utilisant le doublement successif de points.
Calculer C+ρ*Wb en utilisant l'algorithme d'addition de points.
Bob reçoit {ρ*G & C+ρ*Wb} séparément.
1
CRYPTAGE

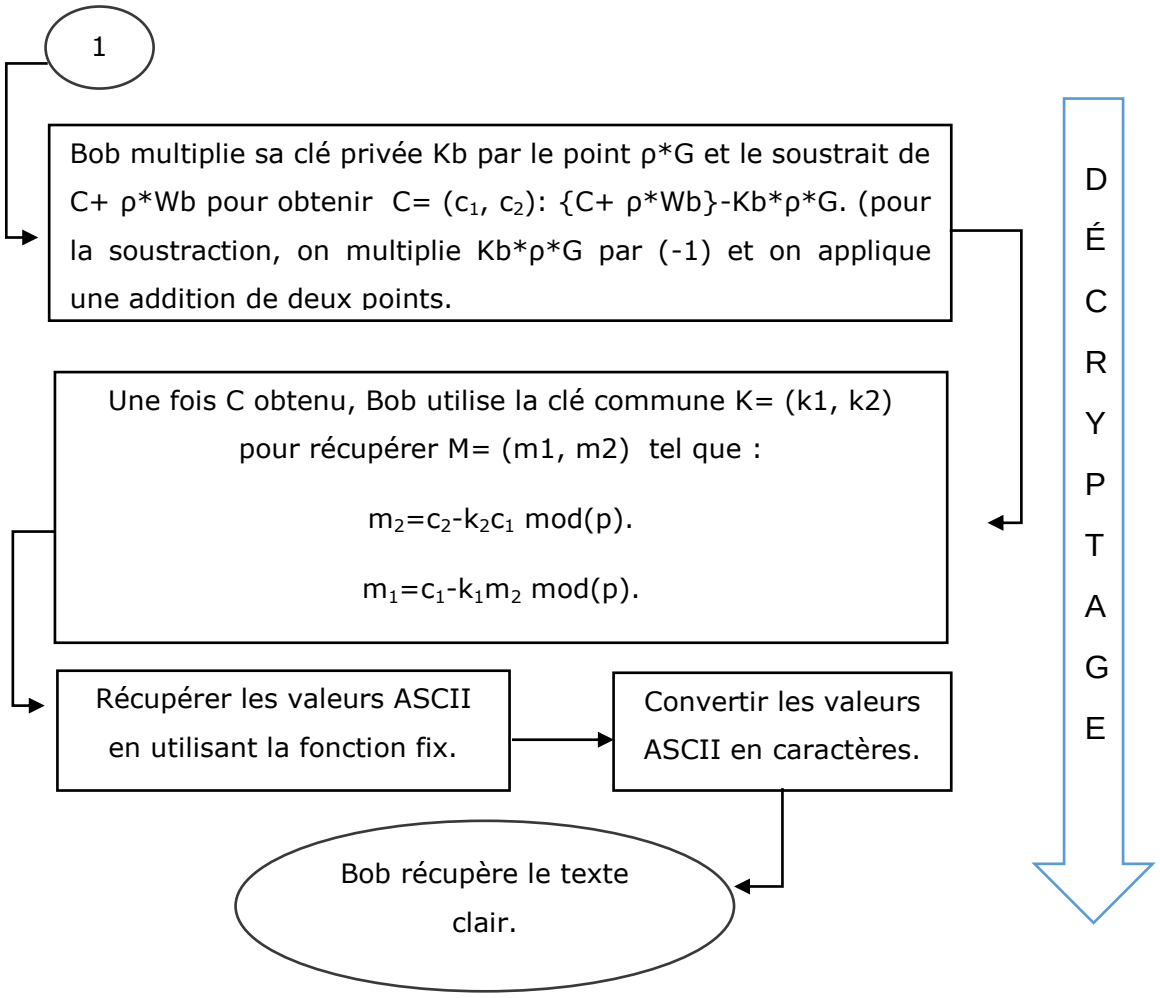



**Figure 3.1 :** Schéma bloc résumant chiffrement/déchiffrement de l'algorithme considéré.

## 3. Simulation de Chiffrement/déchiffrement d'un texte sur courbe elliptique prédéfinie

La simulation a été réalisée à l'aide de Matlab version 2009 sur un ordinateur portable Asus avec un processeur i5-7200U à 2.5 GHz et 4 Go de RAM.

*Exemple de simulation :*

Alice souhaite envoyer à Bob le message suivant : « ***Sécurisation des images médicales par courbes elliptiques.*** » en utilisant la courbe :

$$y^2 = x^3 + 5829x + 2079 \, mod(7829).$$

- Les clés privées d'Alice et Bob sont respectivement : $ka = 7487,\ kb = 6737$ .
- Le générateur de clés publiques : $G(2436,4951)$ .
- Les clés publiques d'Alice et Bob sont respectivement : $Wa = ka * G,\ Wb = kb * G$ .
- Alice utilise sa clé privée et la clé publique de Bob pour former une clé commune

$$k = ka * wb \, mod(7829) = (k_1, k_2) \, mod(p), \quad k = (3098,7235).$$

-

**a. Processus de chiffrement**

**Étape 1 :** Alice écrit le texte à chiffrer : ***Sécurisation des images médicales par courbes elliptiques.***

**Étape 2 :** Les codes ASCII correspondants aux caractères du texte sont :

*83,233,99,117,114,105,115,97,116,105,111,110,32,100,101,115,32,105,109*
*97,103,101,115,32,109,233,100,105,99,97,108,101,115,32,112,97,114,32*
*99,111,117,114,98,101,115,32,101,108,108,105,112,116,105,113,117,101*
*115,46.*

**Étape 3 :** Partition de la séquence obtenue en des groupes de dimensions 3 chacun :

$\{83,233,99\},\{117,114,105\},\{115,97,116\},\{105,111,110\},\{32,100,101\},\{115,32,105\}$
$\{109,97,103\},\{101,115,32\},\{109,233,100\},\{105,99,97\},\{108,101,115\},\{32,112,97\}$
$\{114,32,99\},\{111,117,114\},\{98,101,115\},\{32,101,108\},\{108,105,112\},\{116,105,113\}$
$\{117,101,115\},\{46\}.$

Le dernier groupe prend les valeurs restantes, ce n'est pas obligatoire d'avoir un groupe de dimension 3.

**Étape 4 :** Conversion des valeurs de chaque groupe en un grand nombre entier en utilisant la fonction « ***sum*** » et en prenant comme base « 256 » :

*5499235, 7697001, 7561588, 6909806, 2122 853, 7544937, 7168359, 6648608*
*7203172, 6906721, 7103859, 2125921, 7479 395, 7304562, 6448499, 123116*
*7104880, 7629169, 7693683, 46.*

**Étape 5 :** Le nombre de groupe est pair, on n'aura pas à ajouter 32 à la fin.

**Étape 6 :** A partir de l'étape précédente, on forme des paires $(m_1, m2)$ afin de calculer $(c_1, c_2)$ :

$$c_1 = m_2 \times k_1 + m_1 \, mod(p).$$
$$c_2 = m_2 + m_2 \times k_1 \times k_2 + m_1 \times k_2 \, mod(p).$$

***Exemple :*** Pour $m_1 = 5499235$ *et* $m_2 = 7697001$

$$c_1 = (7697001 \times 3098 + 5499235) \ mod(7829) = 2532.$$
$$c_2 = (7697001 + 7697001 \times 3098 \times 7235 + 5499235 \times 7235) \ mod \ (p) = 254.$$

Pour toute la séquence on aura :

$$(2532,254),\ (1419,7274),\ (594,5079),\ (5847,4745),\ (5016,4888),\ (6938,1144)$$
$$(7001,6539),\ (1685,2679),\ (5714,7393),\ (7191,3226).$$

**Étape 7 :** On choisit un entier $p = 5467$, et on calcule $p * G$ *et* $p * Wb$.

En utilisant le doublement consécutif de points, on aura :

$$\rho * G = (7257,3229).$$
$$\rho * Wb = (1063,829).$$

Si on prend ρ aléatoire, on aura un résultat différent à chaque exécution.

**Étape 8 :** En utilisant l'addition de points, on calcule $c + p * Wb$ où $c$ représente chaque paire $(c_1, c_2)$ de l'étape 6 qui représente un point sur la courbe

$$C + \rho * Wb = (1419,6697),\ (1202,3318),\ (4041,3004),\ (135,4539),\ (2320,4214)$$
$$(5794,130),\ (811,6562),\ (14,7653),\ (7778,1398),\ (2903,3766).$$

**Étape 9 :** Alice envoie à Bob le message chiffré $Pc = \{\rho * G,\ C + \rho * Wb\}$ :

$$pc = \{(7257,3229),\ (1419,6697),\ (1202,3318),\ (4041,3004),\ (135,4539),\ (2320,4214)$$
$$(5794,130),\ (811,6562),\ (14,7653),\ (7778,1398),\ (2903,3766)\}.$$

**b. Processus de déchiffrement**

**Étape 1 :** Bob reçoit le message chiffré $Pc = \{\rho * G,\ C + \rho * Wb\}$.

**Étape 2 :** On considère $\rho * G$ le premier point et $\rho * Wb$ le deuxième point.

**Étape 3 :** Bob multiplie sa clé privée Kb par le premier point $\rho * G$ et le soustrait du deuxième point pour obtenir C (valeurs de l'étape 6 de chiffrement) :

$\{C + \rho * Wb\} - Kb * \rho * G.$
$Kb * \rho * G = (1063, 829),\ Kb * \rho * G = (1063, -829).$
$(1419, 6697) + (1063, -829) = (2532, 254).$
$(1202, 3318) + (1063, -829) = (1419, 7274).$

Bob calcule de même pour toute la séquence chiffrée jusqu'à obtenir

$C = (c_1, c_2)$ : $(2532, 254)$, $(1419, 7274)$, $(594, 5079)$, $(5847, 4745)$, $(5016, 4888)$
$(6938, 1144)$, $(7001, 6539)$, $(1685, 2679)$, $(5714, 7393)$, $(7191, 3226)$.

**Étape 4 :** Bob utilise la clé commune $K = (k_1, k_2)$ pour calculer $M = (m_1, m_2)$ tel que :

$$m_2 = c_2 - k_2 \times c_1 \, mod\,(p).$$
$$m_1 = c_1 - k_1 \times m_2 \, mod\,(p).$$

$m_2 = 254 - 7235 \times 2532 = 1094 \equiv 7697001 \ mod\,(p).$
$m_1 = 2535 - 3098 \times 1094 = 3277 \equiv 5499235 \ mod\,(p).$

Bob calcule de même pour toute la séquence C jusqu'à obtenir $c = (c_1, c_2)$ :

$M = (m_1, m_2)$ : $(5499235,\ 7697001)$, $(7561588,\ 6909806)$, $(2122853,\ 7544937)$
$(7168359,\ 6648608)$, $(7203172,\ 6906721)$, $(7103859,\ 2125921)$
$(7479395,\ 7304562)$, $(6448499,\ 123116)$, $(7104880,\ 7629169)$
$(7693683,\ 46)$.

**Étape 5 :** Récupérer les valeurs ASCII en utilisant la fonction « ***fix*** » :

$\{83, 233, 99\}, \{117, 114, 105\}, \{115, 97, 116\}, \{105, 111, 110\}, \{32, 100, 101\}, \{115, 32, 105\}$
$\{109, 97, 103\}, \{101, 115, 32\}, \{109, 233, 100\}, \{105, 99, 97\}, \{108, 101, 115\}, \{32, 112, 97\}$
$\{114, 32, 99\}, \{111, 117, 114\}, \{98, 101, 115\}, \{32, 101, 108\}, \{108, 105, 112\}, \{116, 105, 113\}$
$\{117, 101, 115\}, \{46\}.$

**Étape 6 :** Convertir les valeurs ASCII en caractères et récupérer le message original :

***Sécurisation des images médicales par courbes elliptiques.***

## 4. Performances des algorithmes RSA, ElGamel et ECC

Tout d'abord, il faut choisir une bonne courbe elliptique adaptée aux applications cryptographiques. Les techniques proposées sont mises en œuvre et appliquées sur des messages de tailles différentes en allant de 1Kbits jusqu'à 5 KBits, où nous prenons le texte brut à chaque fois puis on applique le processus de chiffrement et de déchiffrement et on calcule le temps d'exécution de l'opération comme indiqué sur la figure 3.2 :

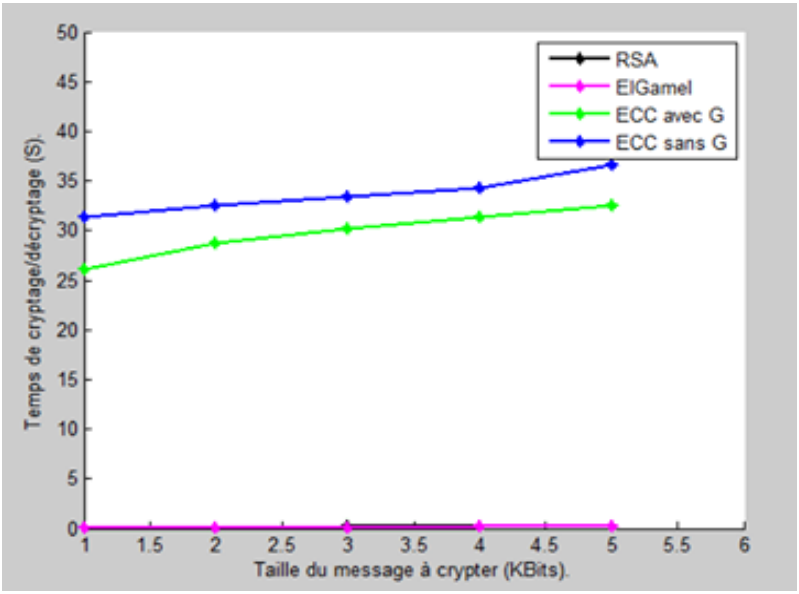



**Figure 3.2 :** Temps d'exécution du chiffrement et déchiffrement d'un texte en fonction de sa taille.

D'après les courbes obtenues des temps d'exécution des différents algorithmes RSA, ElGamel, ECC avec groupement et ECC sans groupement en fonction des tailles du message, on constate que l'ajout du groupement à l'algorithme ECC nous a fait gagner un temps considérable cependant ElGamel reste l'algorithme le plus rapide et cela est dû aux nombres d'opérations effectuées.

## 5. Conclusion

Dans ce chapitre, nous avons chiffré/déchiffré un texte en utilisant l'algorithme de cryptographie sur courbes elliptiques ainsi que RSA et ElGamel.

Ces trois algorithmes partagent la même propriété importante d'être des algorithmes asymétriques (une clé pour chiffrer et une clé pour déchiffrer). Cependant, RSA est plus rapide, mais ECC en termes de sécurité est plus fort. Il offre un même niveau de sécurité et puissance de chiffrement pour des clés beaucoup plus courtes, répondant ainsi aux besoins des utilisateurs tout en réduisant les besoins en calculs et espace de stockage.

Les clés plus courtes font de l'ECC une option très attrayante pour les nouvelles technologies dont la capacité de stockage ou la puissance de traitement est limitée, ce qui devient de plus en plus courant à l'ère de l'Internet des Objets.

Le chapitre qui suit sera consacré aux résultats d'implémentation de cet algorithme sur des images médicales.

# Chapitre 4

# *Résultats & discussion*

## 1. Introduction

Dans ce chapitre, on présente les résultats de l'implémentation de différents algorithmes, notamment RSA et ElGamel pour la cryptographie classique ainsi qu'un algorithme basé sur les courbes elliptiques. Ces algorithmes sont appliqués sur différents types d'images médicales issues d'échographie, radiologie, scanner et IRM.

Une interprétation des résultats est faite moyennant comme critères d'évaluation de la qualité du chiffrement : l'histogramme, le PSNR (Peak Signal to Noise Ratio) et le SSIM (Structural SIMilarity).

## 2. Quelques instructions Matlab pour traitement d'images

Une image est une matrice bidimensionnelle de valeurs entières ou réelles. Les principales fonctions de traitement d'images sous Matlab se trouvent dans la boîte à outils (toolbox images). Cette dernière contient de nombreuses fonctions qui permettent le développement facile et rapide d'algorithmes en fonction du problème à traiter. C'est un très bon outil pour la validation de méthodes de traitement d'images appliquées à un problème particulier.

Matlab est capable de lire et de décoder des fichiers images de différents formats sous forme d'une matrice. Les formats d'images médicales que nous avons implémentés sont : JPG, et DCM. On peut les lire et les afficher en utilisant les instructions suivantes :

- **Format JPG :** img=imread ('image.jpg'); imshow (img) ;
- **Format DCM :** img=dicomread ('image.dcm'); imshow (img) ;

Parfois, une image parait codée en niveaux de gris mais en réalité elle est en couleurs, en cherchant sa taille, on trouve 3 plans. La fonction qui permet de convertir une image couleur en niveau de gris est « rgb2gray ».

## 3. Description des images utilisées

- **Image par Ultrasons ou Échographie**

L'image de le figure 4.1 est collectée d'une base de données qui contient des images de l'artère carotide (en coupe longitudinale) de dix volontaires dont l'âge moyen est de (27,5 ± 3,5) ans. La résolution des images est d'environ 390x330px. Des sondes linéaires avec des fréquences de 10 MHz et 14 MHz ont été utilisées pendant le balayage.

Ces fréquences sont généralement adaptées à la capture d'organes de surface tels que l'artère carotide. Toutes les images ont été prises par un spécialiste avec cinq ans d'expérience.

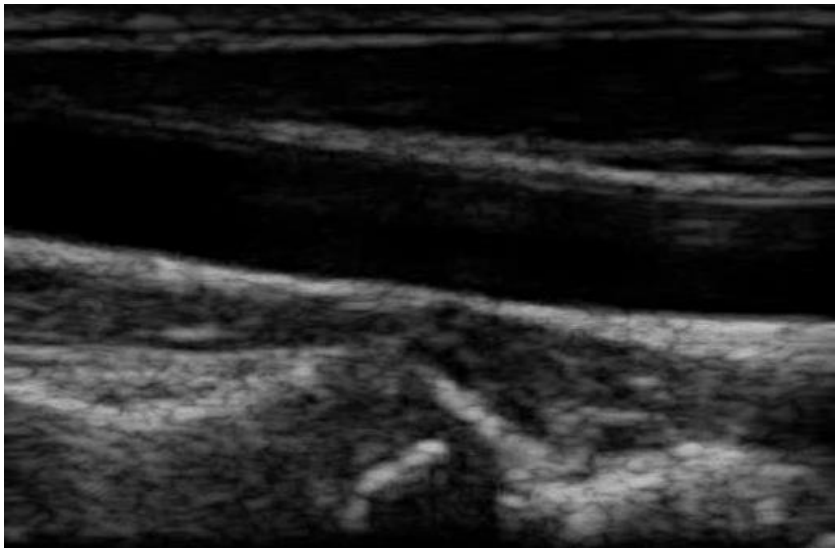


**Figure 4.1** : Image médicale par Ultrasons de taille 518x395 pixels [46].

- **Image de Radiographie ou RX**

L'image de la figure 4.2 est récupérée d'une base de données ouverte d'images de radiographie pulmonaire et de tomodensitométrie de patients positifs ou suspectés de COVID-19 ou d'autres pneumonies virales et bactériennes (MERS, SARS et ARDS). Les données sont collectées auprès de sources publiques ainsi que par collecte indirecte auprès des hôpitaux et des médecins.

**Figure 4.2** : Image médicale Rayon X de taille 384x384 pixels [47].

- **Image Scanner**

L'image de la figure 4.3 a été prise au service d'imagerie médicale, CHU de Rennes, France, la taille de cette image est 527x565 pixels.

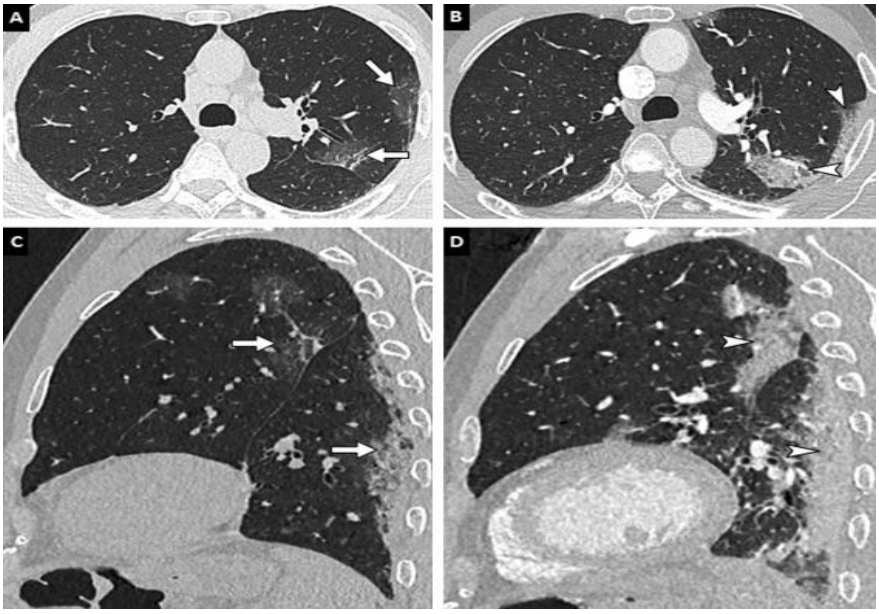



**Figure 4.3** : Présentation nodulaire de pneumonie COVID-19 chez une femme de 33 ans. Scanner thoracique sans injection en coupes axiales (A-D). Plusieurs formations nodulaires bilatérales du parenchyme pulmonaire, certaines présentant un verre dépoli central ou signe du halo inversé (flèche), d'autres un caractère sous-pleural arciforme (têtes de flèche), évocateurs d'un pattern de pneumonie organisée [16].

- **Image par Résonance Magnétique ou IRM**

L'image de la figure 4.4 est téléchargée du site GIMIAS qui est un environnement orienté flux de travail pour résoudre des problèmes avancés de calcul d'image biomédicale et de simulation individualisée. En outre, GIMIAS fournit un cadre open source pour le développement efficace de prototypes de logiciels de recherche et cliniques [2].

Cette image est présentée selon la norme DICOM.

L'instruction *dicominfo* permet de lister les informations concernant le patient et les caractéristiques de l'image.

L'instruction *imadjust* permet d'ajuster l'image.

FileModDate: '20-nov.-2002 16:02:48'
ColorType: 'grayscale'
Modality: 'MR'
StudyDescription: 'BRAIN'
SeriesDescription: 'FSE PD AXIAL OBL'
PatientID: '123565'
PatientSex: 'F'
PatientAge: '028Y'
PatientWeight: 61.2350
MRAcquisitionType: '2D'
ProtocolName: 'CLINICAL BRAIN'

**Figure 4.4** : Image médicale IRM, de taille 256x256 Pixels [2].

## 4. Critères d'évaluation

### 4.1. Histogramme

L'histogramme d'une image est une fonction discrète qui représente la distribution des intensités (ou des couleurs) de l'image.

Les images générées par un bon algorithme de chiffrement doivent avoir des histogrammes uniformes (toutes les couleurs ont la même probabilité de se produire), de manière à améliorer leur résistance à l'analyse statistique c.à.d. que l'histogramme de l'image chiffrée doit être très différent de celui l'image originale. Ainsi, l'attaquant ne peut pas extraire l'information à partir de l'histogramme de l'image chiffrée.

### 4.2. PSNR

PSNR est l'acronyme de Peak Signal to Noise Ratio ou rapport signal de crête à bruit. Il représente une mesure de distorsion et est largement utilisé dans le traitement du signal pour mesurer la qualité d'un signal en calculant le rapport entre le signal d'origine et le bruit. Il se mesure en décibels (dB) :

$$PSNR = 10 \times log_{10} \frac{(2^R - 1)^2}{MSE} \qquad (4.1)$$

Où R représente le nombre de bits désignés pour un pixel ; et MSE est l'erreur quadratique moyenne.

Si MSE est égale à zéro, cela signifie que l'image d'origine et celle après traitement sont identiques et la valeur du PSNR sera infinie. Plus ce rapport est grand, meilleure est la qualité de l'image.

Un PSNR élevé, indique que l'image modifiée est très proche de l'originale. Une valeur de plus de 20 dB est acceptable (varie dans différents cas selon le type de problème). Cependant, le PSNR fonctionne pour la comparaison d'intensité et ne fournit aucune information structurelle. Par conséquent, on peut également appliquer d'autres méthodes telles que SSIM.

### 4.3. SSIM

Aucune de ces mesures objectives citées n'est particulièrement efficace pour prédire la réponse visuelle humaine à la qualité d'image. Parfois, les PSNR varient énormément entre deux images presque impossibles à distinguer; de même, on peut avoir deux images avec le même PSNR où il y a une différence de qualité très évidente. La mesure de l'indice de similarité structurelle (SSIM) et certaines de ses variantes sont généralement considérées comme meilleures de ce point de vue, mais pas encore des modèles parfaits pour la perception humaine.

Le SSIM est une mesure de la similitude entre deux images. Ces valeurs sont comprises entre 0 et 1. Le 1 signifie que l'image de reconstruction correspond parfaitement à l'image d'origine ; alors que le 0 indique la différence totale.

Généralement, on retient les valeurs : 0.97, 0.98 et 0.99 pour de bonnes techniques de reconstruction de qualité.

## 5. Discussion des résultats

### 5.1. Implémentation de l'image par ultrasons

Les figures 4.5 – 4.8 représentent le chiffrement/déchiffrement de l'image US décrite précédemment avec les différents algorithmes utilisés. Les valeurs du PSNR et SSIM sont données dans le tableau 4.1.

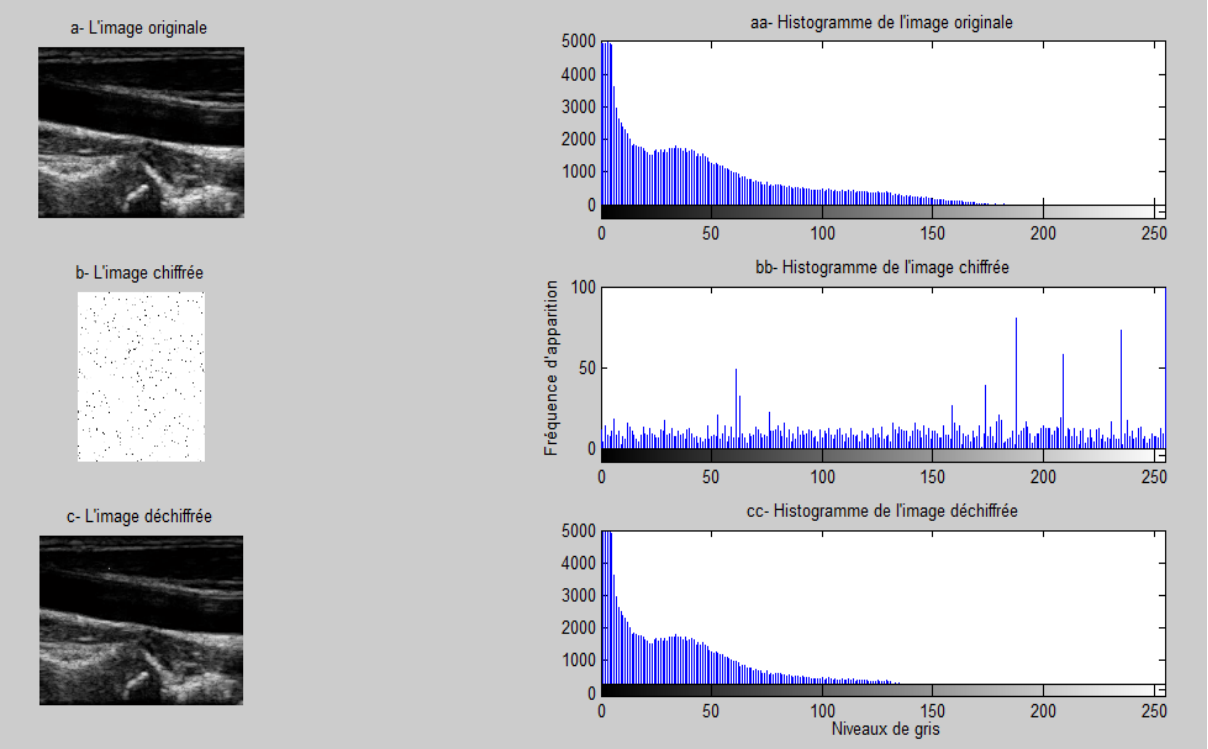



**Figure 4.5 :** Histogrammes des images : originale, chiffrée et déchiffrée (*US)* en utilisant l'algorithme *ECC avec groupement*.

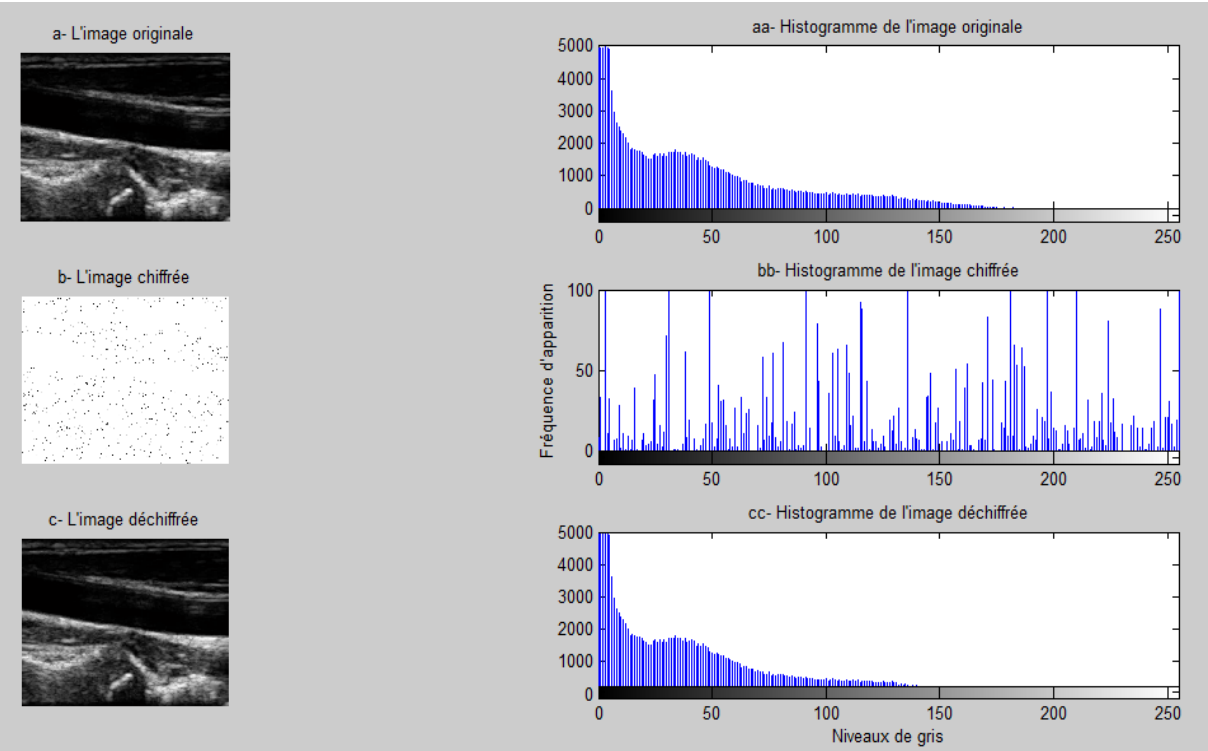



**Figure 4.6 :** Histogrammes des images : originale, chiffrée et déchiffrée (*US)* en utilisant l'algorithme *ECC sans groupement*.

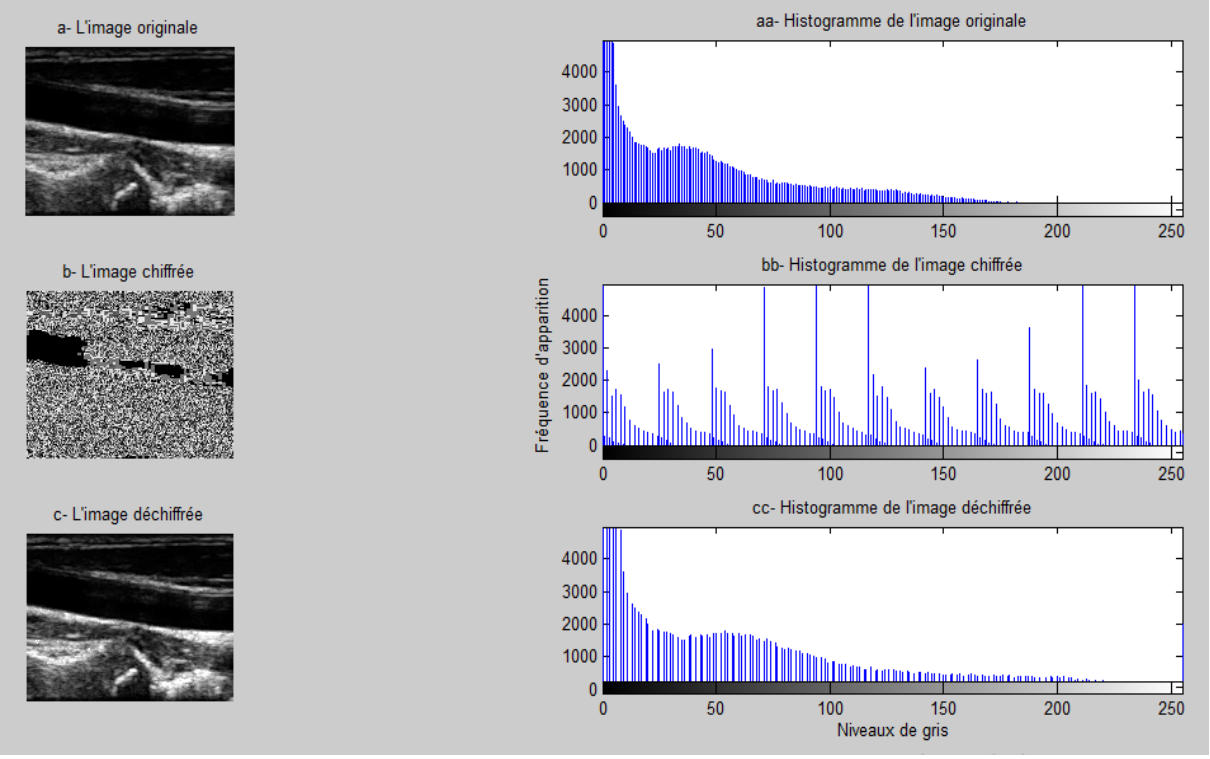



**Figure 4.7 :** Histogrammes des images : originale, chiffrée et déchiffrée (*US)* en utilisant l'algorithme *ElGamel*.

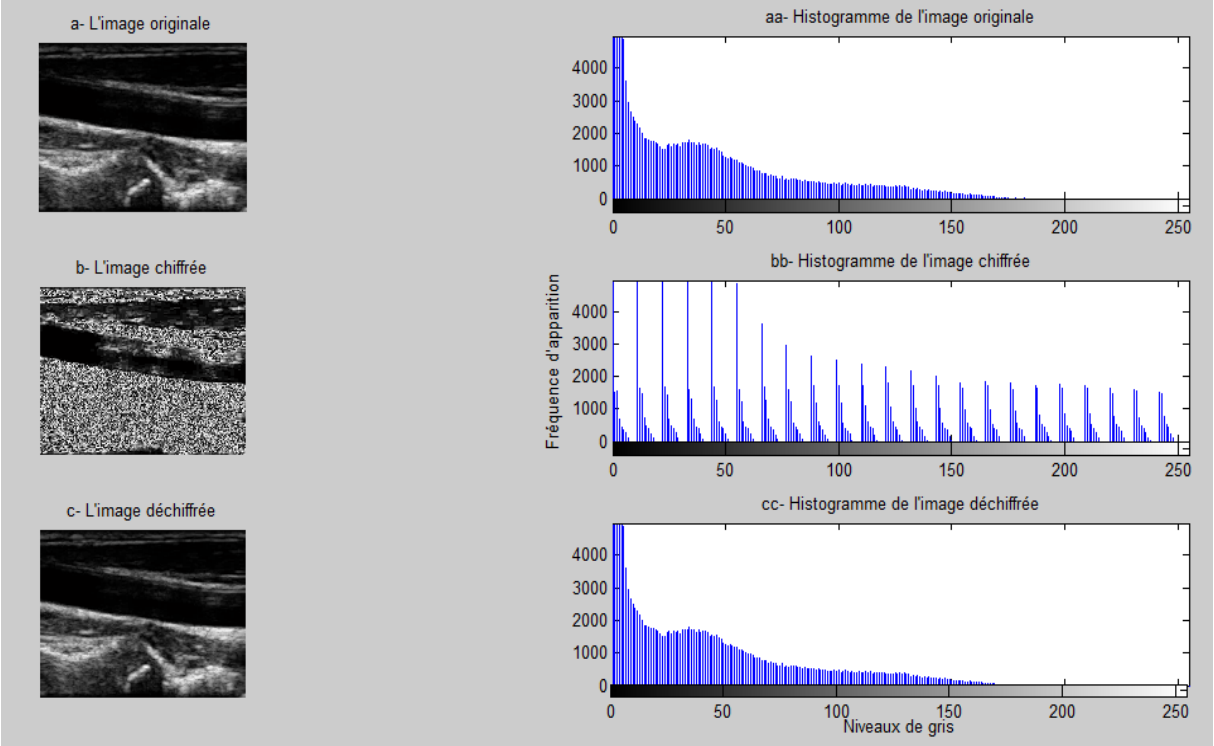



**Figure 4.8 :** Histogrammes des images : originale, chiffrée et déchiffrée (*US)* en utilisant l'algorithme *RSA*.

| Critère | ECC sans G | ECC avec G | ElGamel | RSA |
|---|---|---|---|---|
| PSNR (Originale et chiffrée) en dB | **01.35** | **01.35** | 06.84 | 09.30 |
| PSNR (Originale et déchiffrée) en dB | **∞** | 47.37 | 20.00 | **∞** |
| SSIM (Originale et chiffrée) | **00.04** | **00.05** | **00.06** | 00.11 |
| SSIM (Originale et déchiffrée) | **01.00** | **00.99** | 00.86 | **01.00** |

**Tableau 4.1 :** Mesures des performances des différents algorithmes pour l'image *US*.

***Interprétation***

Il ressort des figures 4.5 – 4.8 que les histogrammes des images chiffrées sont uniformément distribués (ECC) et aléatoires (RSA et ElGamel) par rapport aux histogrammes des images d'origine. Les algorithmes de chiffrement utilisés font en sorte que la dépendance des histogrammes des images chiffrées et celles d'origine soit quasi aléatoire. Ceci rend la cryptanalyse de plus en plus difficile car les images chiffrées ne fournissent aucun élément reposant sur l'exploitation de l'histogramme et permettant de concevoir une attaque statistique sur les procédés de chiffrement proposés. Cependant, cette dépendance est relativement la même pour les histogrammes des images déchiffrées et originale.

D'après le tableau 4.1, les valeurs du PSNR (Originale et chiffrée) sont très faibles et s'approchent du zéro pour ECC. Ce qui montre que l'image chiffrée est nettement dégradée pour tous les algorithmes appliqués. Alors que l'image chiffrée est parfaitement reconstruite avec l'algorithme RSA, ECC (PSNR tend vers l'infini). Elle reste relativement acceptable avec ElGamel (20 dB).

Les valeurs du SSIM confirment que, pour les quatre algorithmes, l'image chiffrée est dégradée $(SSIM \approx 0)$ (pas de similitude entre les deux images) et l'image déchiffrée est de très bonne qualité $(SSIM = 1)$.

## 5.2. Implémentation de l'image de radiographie ou RX

Les figures 4.9 – 4.12 représentent le chiffrement/déchiffrement de l'image RX avec les différents algorithmes utilisés. Les valeurs du PSNR et SSIM sont données dans le tableau 4.2.

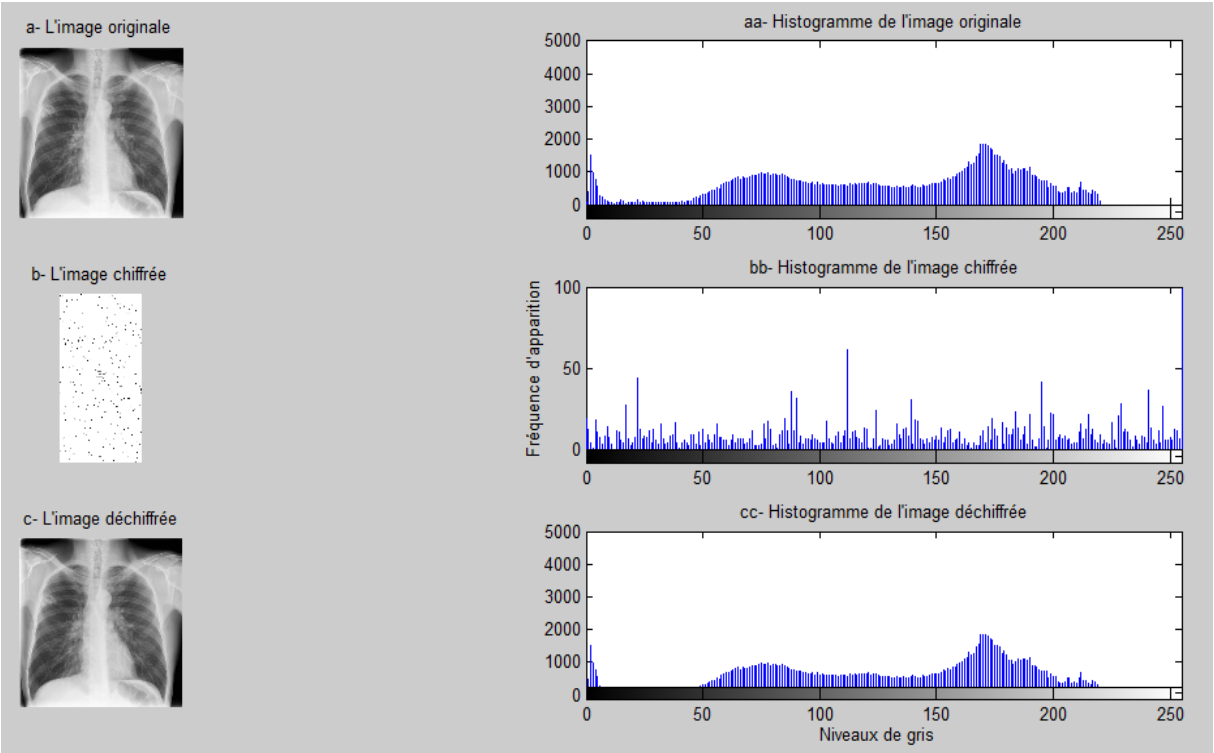



**Figure 4.9 :** Histogrammes des images : originale, chiffrée et déchiffrée (*RX)* en utilisant l'algorithme *ECC avec groupement*.

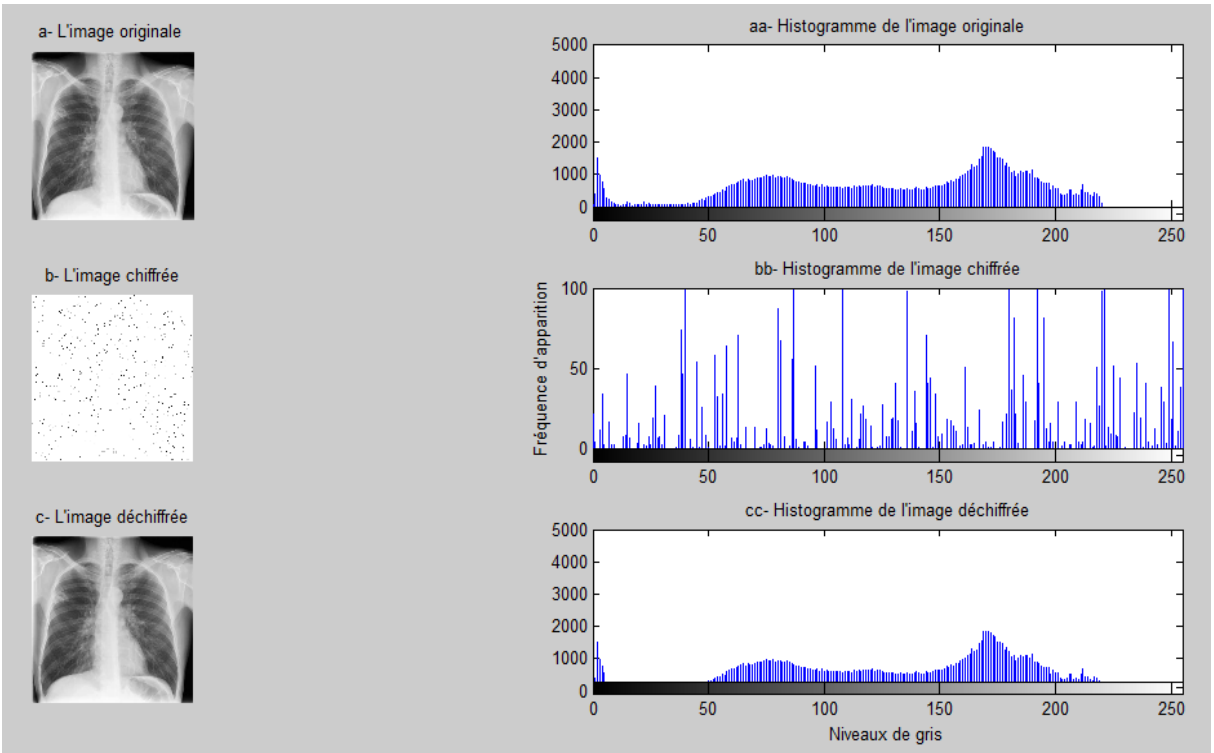



**Figure 4.10 :** Histogrammes des images : originale, chiffrée et déchiffrée (*RX)* en utilisant l'algorithme *ECC sans groupement*.

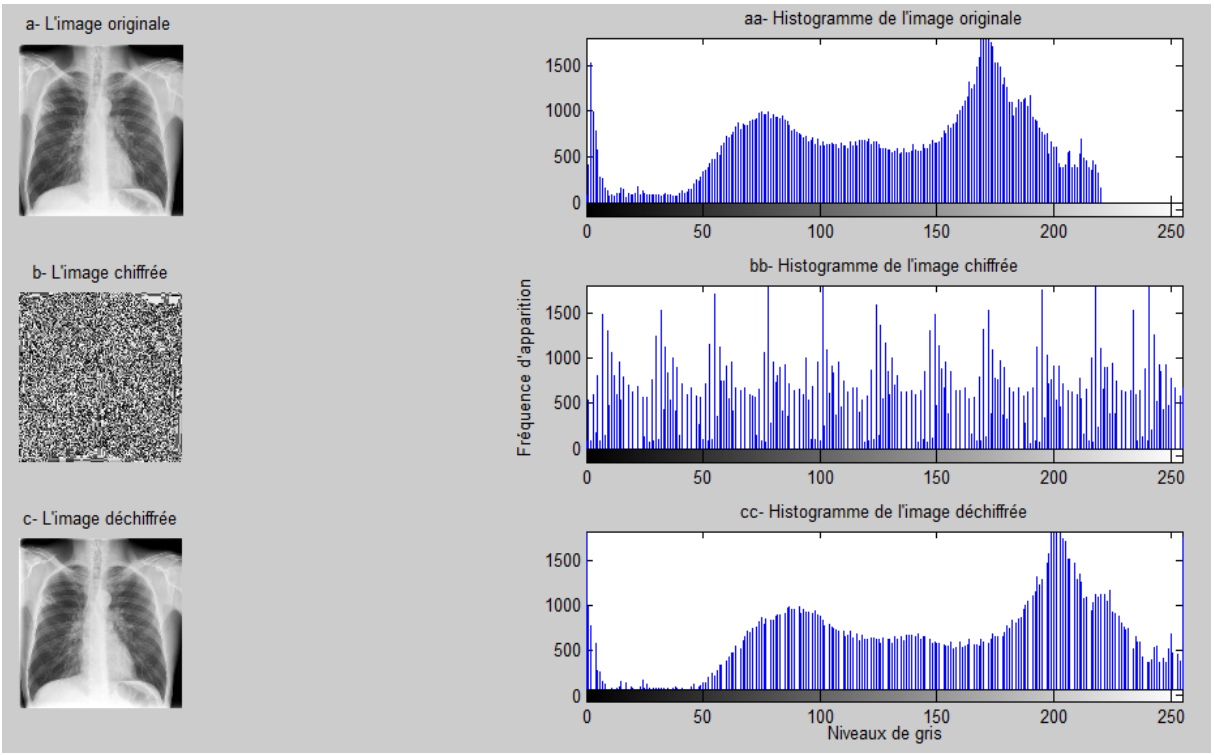



**Figure 4.11 :** Histogrammes des images originale, chiffrée et déchiffrée (*RX)* en utilisant l'algorithme *ElGamel*.

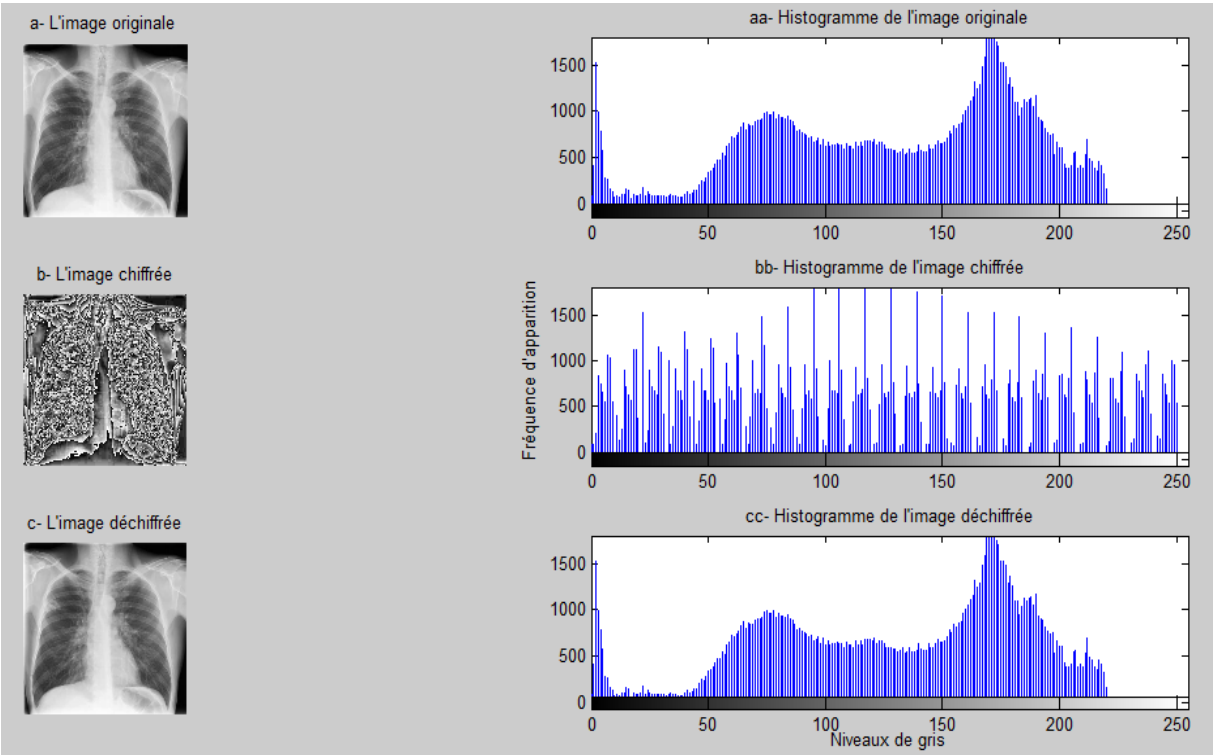



**Figure 4.12 :** Histogrammes des images : originale, chiffrée et déchiffrée (*RX)* en utilisant l'algorithme *RSA*.

| Critère | ECC sans G | ECC avec G | ElGamel | RSA |
|---|---|---|---|---|
| PSNR (Originale et chiffrée) en dB | **05.47** | **05.71** | 08.73 | 09.41 |
| PSNR (Originale et déchiffrée) en dB | **∞** | 50.46 | 20.34 | **∞** |
| SSIM (Originale et chiffrée) | 00.25 | 00.21 | **00.03** | **00.06** |
| SSIM (Originale et déchiffrée) | **01.00** | **01.00** | **00.98** | **01.00** |

**Tableau 4.2 :** Mesures des performances des différents algorithmes pour l'image *RX*.

### *Interprétation*

D'après les histogrammes représentés dans les figures 4.9 – 4.12, on constate que visuellement l'image originale est différente de l'image chiffrée mais similaire à l'image déchiffrée. D'après le tableau 4.2, on constate que les valeurs du PSNR (Originale et chiffrée) sont faibles. Ce qui montre que l'image chiffrée est nettement dégradée pour tous les algorithmes appliqués. Cependant elle est parfaitement reconstruite avec l'algorithme RSA, ECC (PSNR tend vers l'infini) et relativement acceptable avec ElGamel (20.34 dB).

Les valeurs du SSIM confirment que l'image chiffrée est dégradée pour les algorithmes ECC et elle l'est fortement pour ElGamel et RSA ; alors que l'image déchiffrée est de très bonne qualité pour les quatre algorithmes.

## 5.3. Implémentation de l'image d'un scanner

Les figures 4.13 – 4.16 représentent le chiffrement/déchiffrement de l'image d'un scanner. Les valeurs du PSNR et SSIM sont données dans le tableau 4.3.

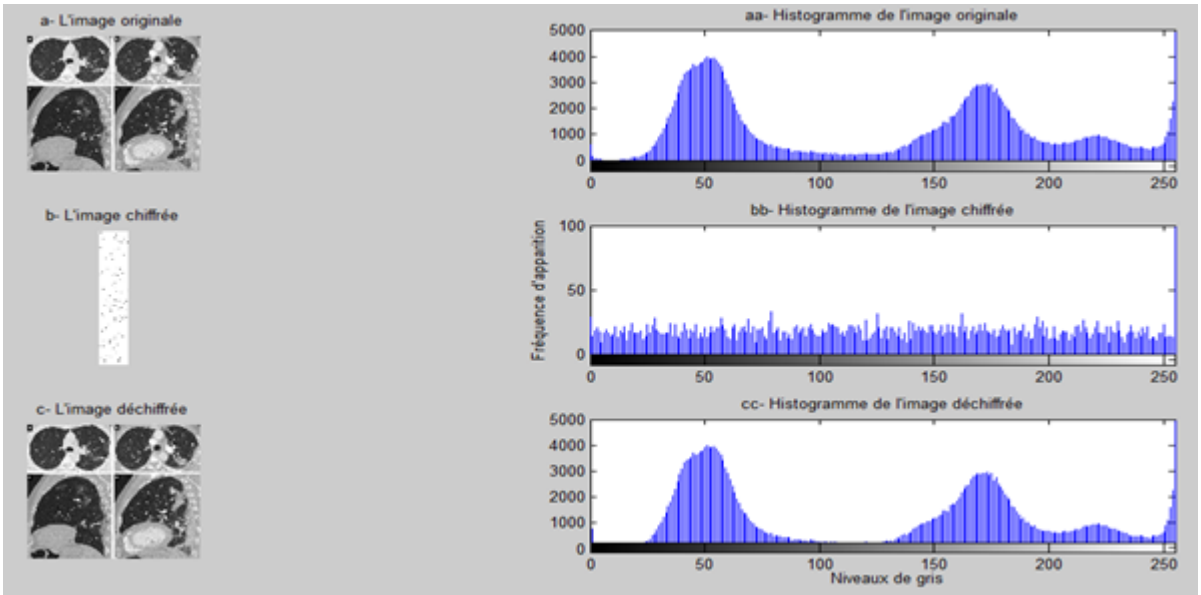



**Figure 4.13 :** Histogrammes des images : originale, chiffrée et déchiffrée (*scanner)* en utilisant l'algorithme *ECC avec groupement*.

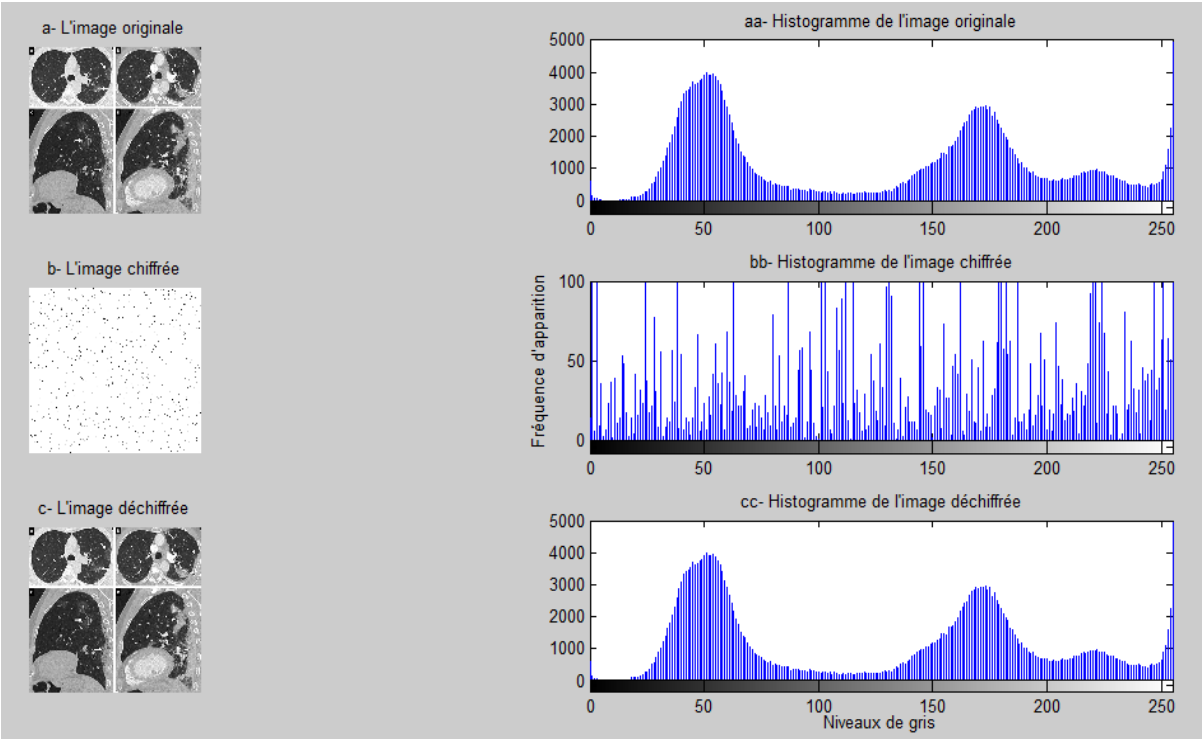



**Figure 4.14:** Histogrammes des images originale, chiffrée et déchiffrée (*scanner)* en utilisant l'algorithme *ECC sans groupement*.

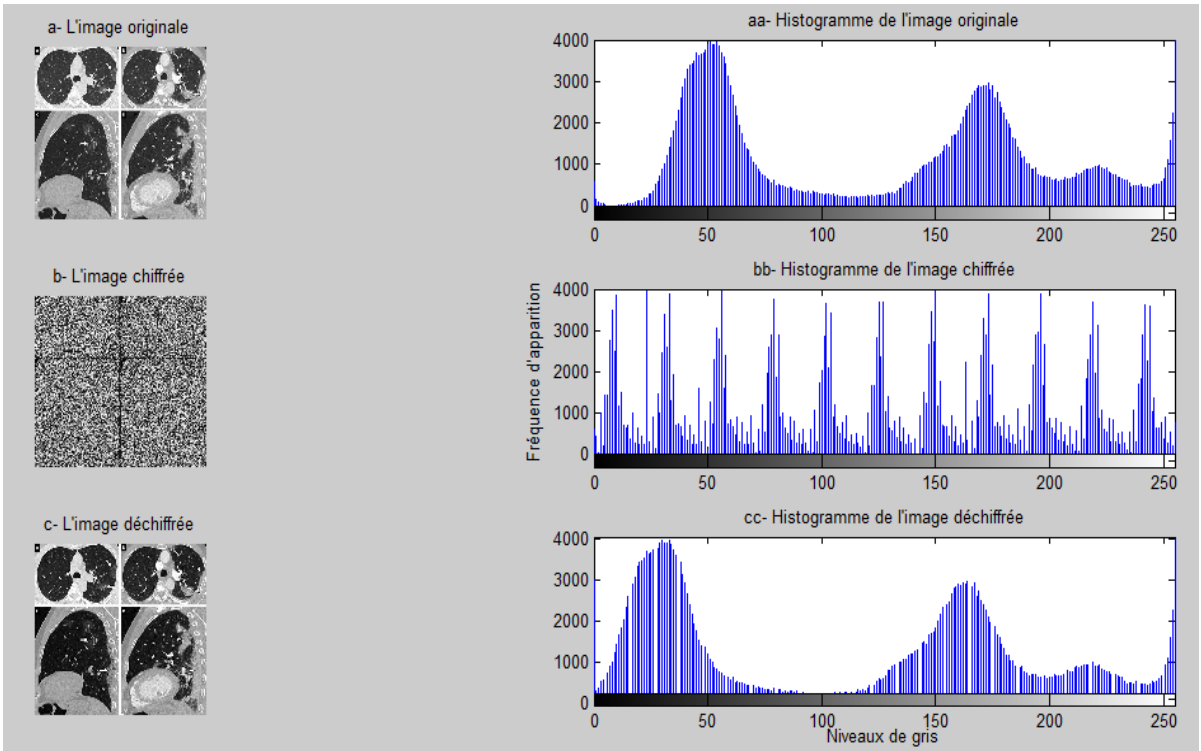



**Figure 4.15 :** Histogrammes des images : originale, chiffrée et déchiffrée (*scanner)* en utilisant l'algorithme *ElGamel*.

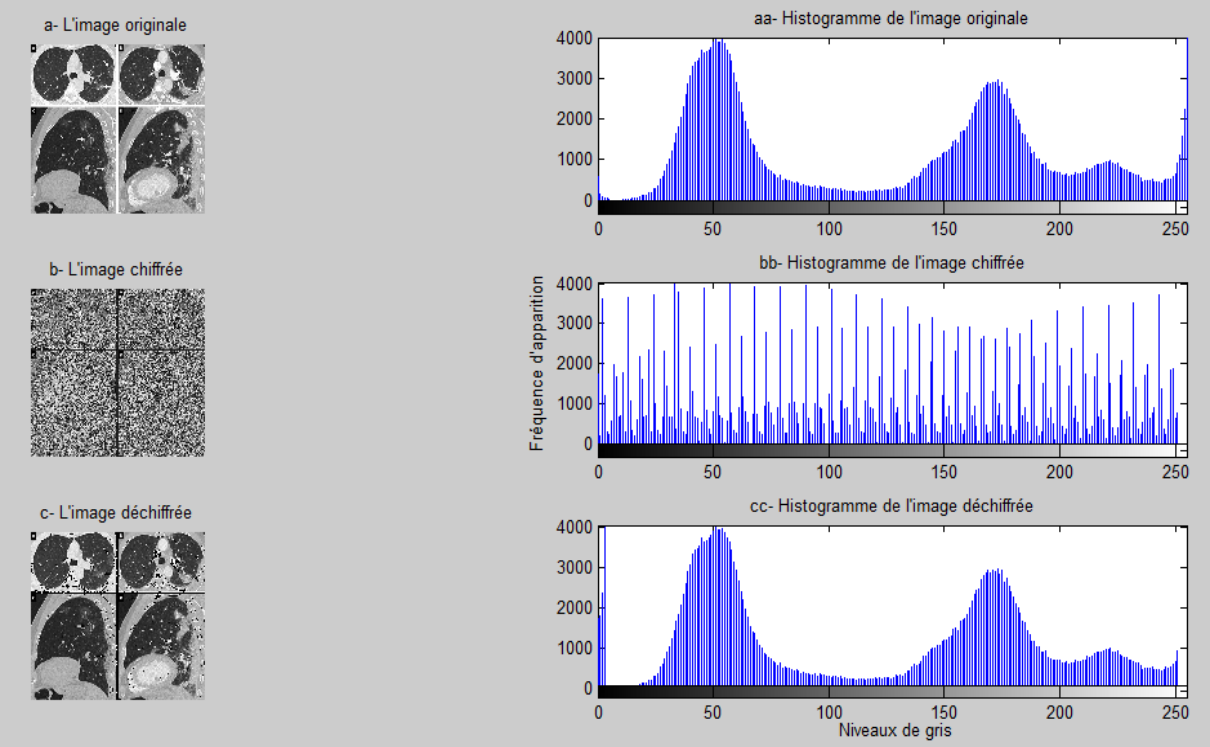



**Figure 4.16 :** Histogrammes des images : originale, chiffrée et déchiffrée (*scanner)* en utilisant l'algorithme *RSA*.

| Critère | ECC sans G | ECC avec G | ElGamel | RSA |
|---|---|---|---|---|
| PSNR (Originale et chiffrée) en dB | **04.82** | **04.37** | 07.70 | 07.77 |
| PSNR (Originale et déchiffrée) en dB | **59.22** | **49.19** | 24.49 | 14.00 |
| SSIM (Originale et chiffrée) | 00.09 | 00.10 | **00.01** | **00.01** |
| SSIM (Originale et déchiffrée) | **01.00** | **01.00** | **00.95** | 0.79 |

**Tableau 4.3 :** Mesures des performances des différents algorithmes pour l'image d'un *scanner*.

### *Interprétation*

D'après les histogrammes représentés dans les figures 4.13 – 4.16, on constate visuellement que l'image originale est différente de l'image chiffrée mais similaire à l'image déchiffrée.

Les valeurs du PSNR montrent que l'image originale est différente de l'image chiffrée cependant elle est parfaitement reconstruite avec l'algorithme ECC. Elle reste acceptable avec ElGamel (24.49 dB) mais moins bien reconstruite avec l'algorithme RSA (14 dB).

Les valeurs du SSIM confirment que pour les quatre algorithmes l'image chiffrée est dégradée et l'image reconstruite est de très bonne qualité avec l'algorithme ECC (égale à 1); cependant elle est acceptable avec ElGamel et moins bien déchiffrée avec RSA.

## 5.4. Implémentation des images IRM

Les figures 4.17 – 4.20 représentent le chiffrement/déchiffrement de l'image IRM décrite précédemment avec les différents algorithmes utilisés. Les valeurs du PSNR et SSIM sont données dans le tableau 4.4.

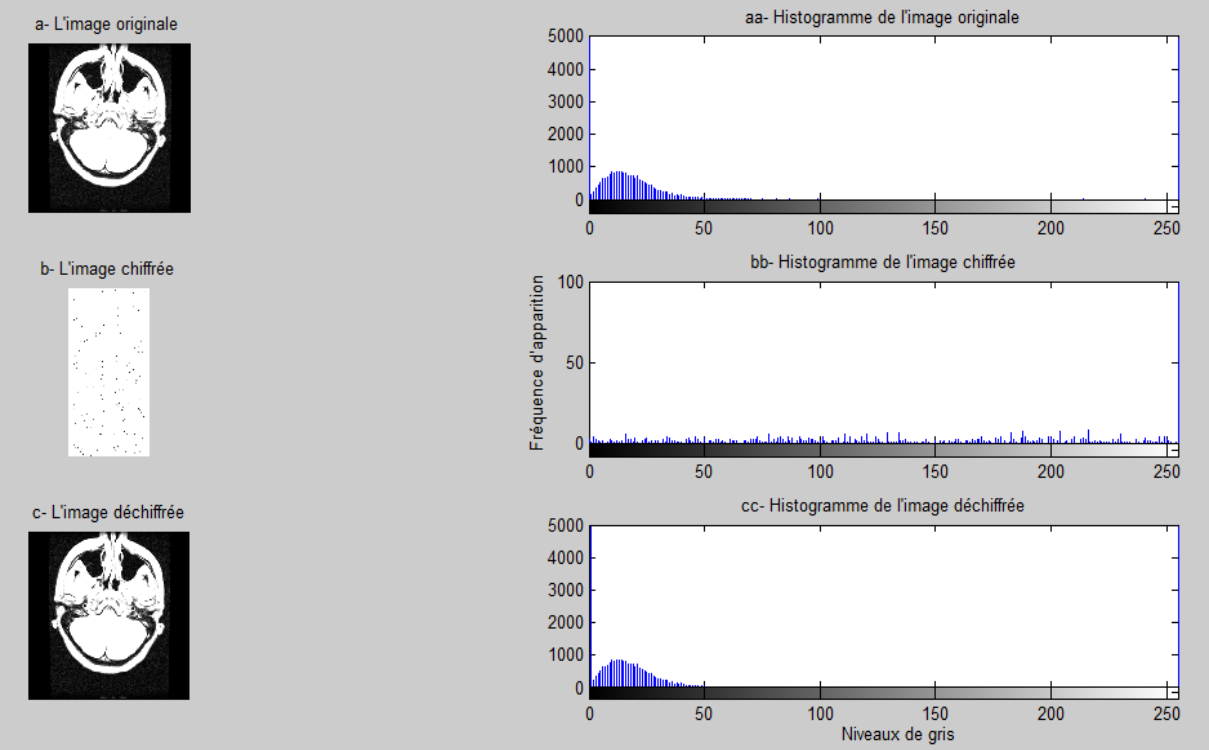



**Figure 4.17 :** Histogrammes des images : originale, chiffrée et déchiffrée (*IRM)* en utilisant l'algorithme *ECC avec groupement*.

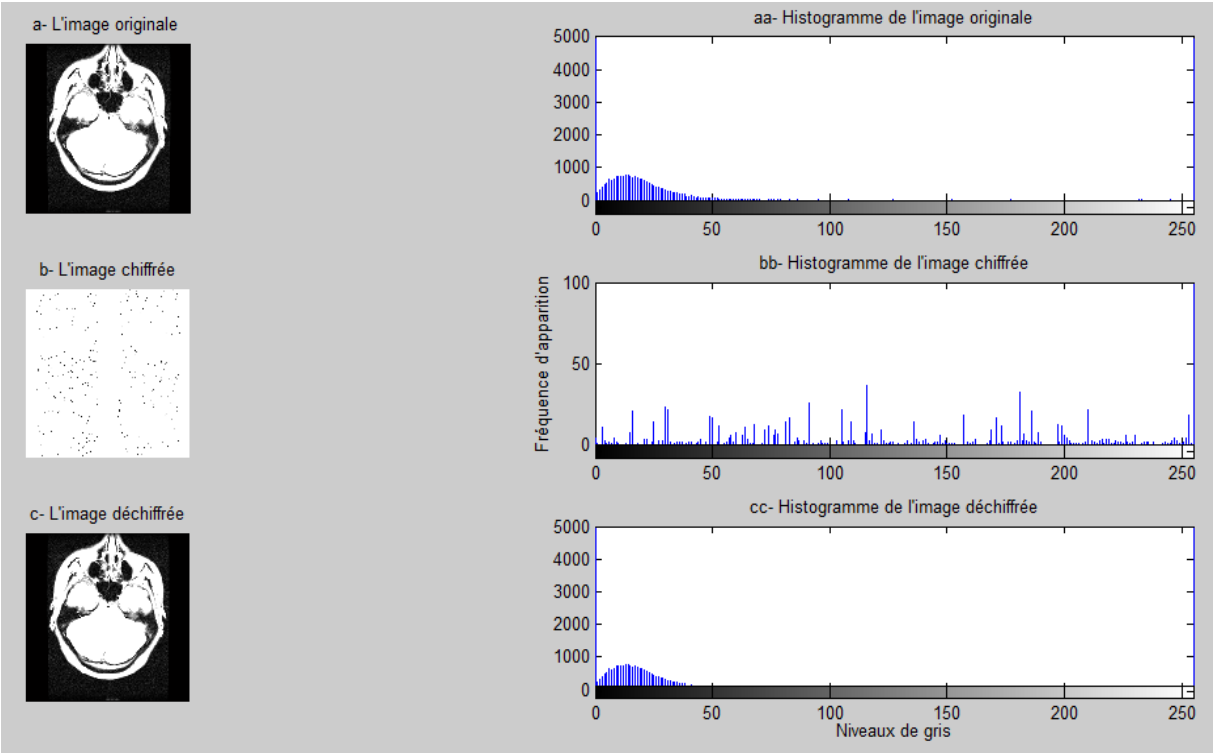



**Figure 4.18 :** Histogrammes des images : originale, chiffrée et déchiffrée (*IRM)* en utilisant l'algorithme *ECC sans groupement*.

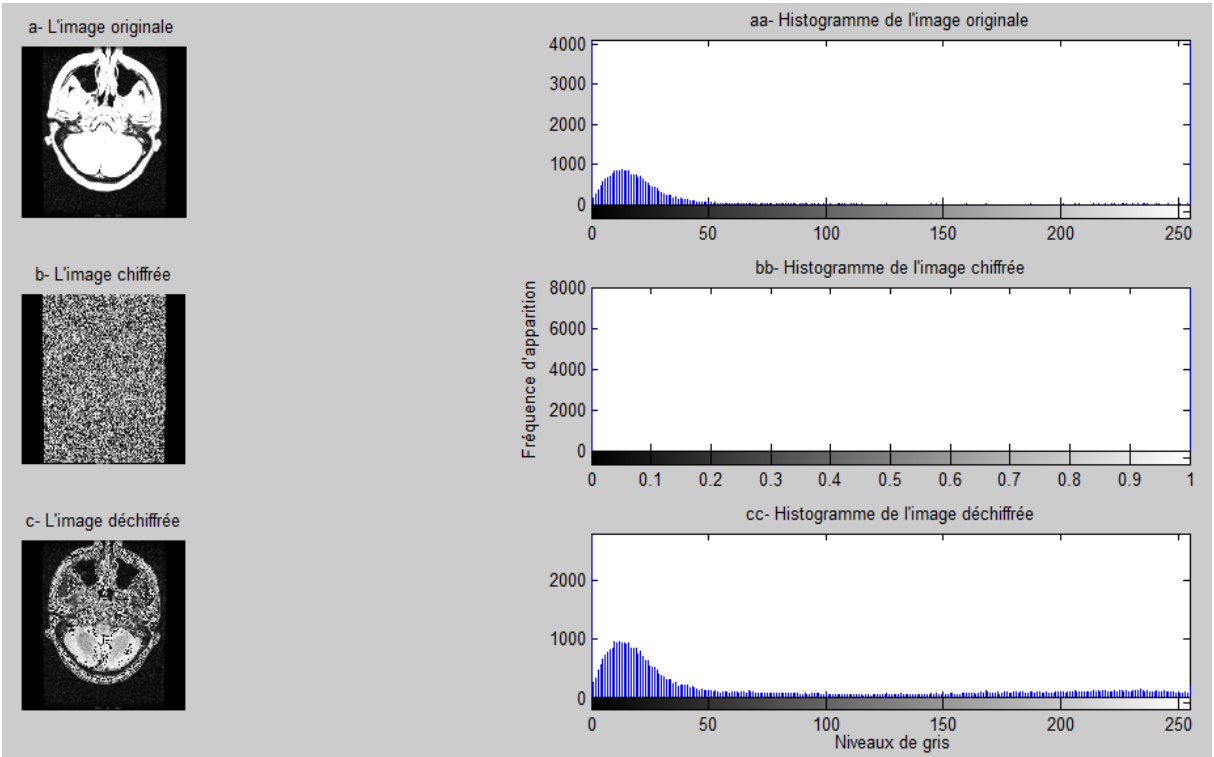



**Figure 4.19 :** Histogrammes des images : originale, chiffrée et déchiffrée *(IRM)* en utilisant l'algorithme *ElGamel*.

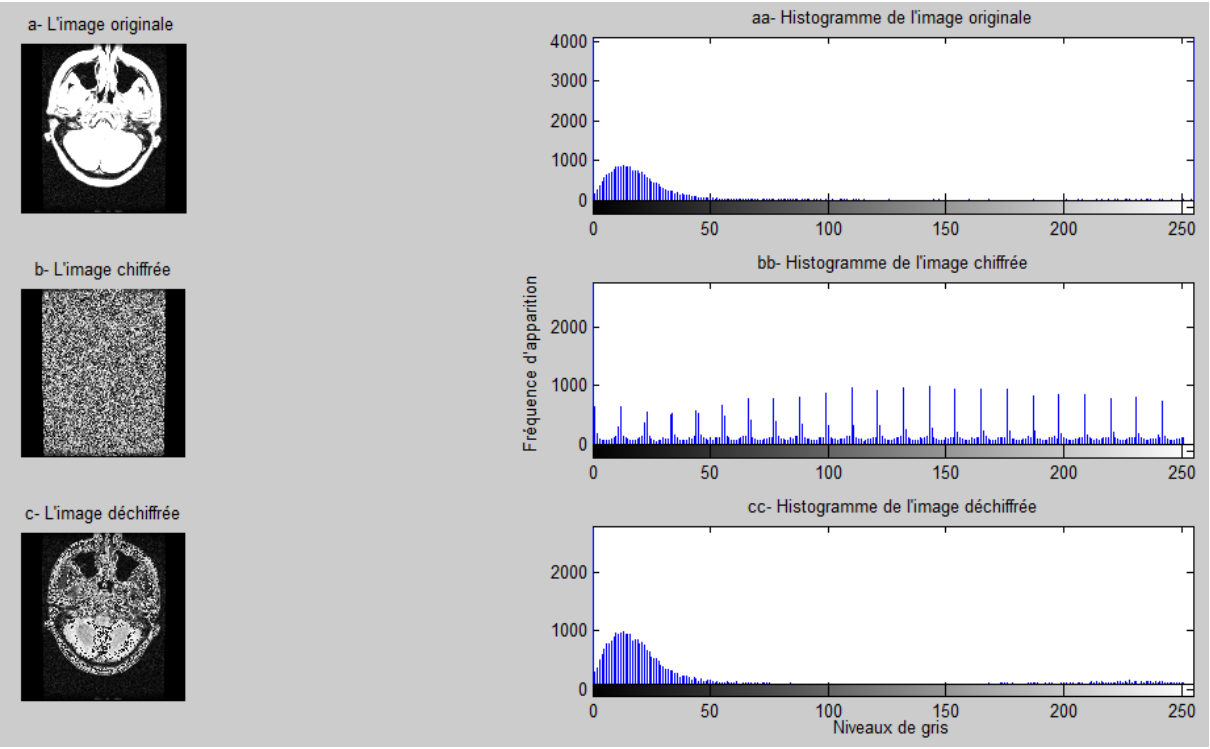



**Figure 4.20 :** Histogrammes des images : originale, chiffrée et déchiffrée de l'image (*IRM)* en utilisant l'algorithme *RSA*.

| Critère | ECC sans G | ECC avec G | ElGamel | RSA |
|---|---|---|---|---|
| PSNR (Originale et chiffrée) en db | **02.45** | **02.40** | 07.08 | 07.13 |
| PSNR (Originale et déchiffrée) en dB | **∞** | 46.35 | 10.37 | 09.93 |
| SSIM (Originale et chiffrée) | 00.13 | **00.11** | 00.21 | 00.21 |
| SSIM (Originale et déchiffrée) | **01.00** | **00.97** | 00.62 | 00.61 |

**Tableau 4.4 :** Mesures des performances des différents algorithmes pour l'image *IRM*.

### *Interprétation*

D'après les histogrammes représentés dans les figures 38, 41, 44 et 47, on remarque clairement que visuellement l'image originale est différente de l'image chiffrée mais similaire à l'image déchiffrée avec l'algorithme ECC. Elle ressemble moins à l'image originale pour l'algorithme RSA et ElGamel.

Les valeurs du PSNR montrent que l'image originale est différente de l'image chiffrée cependant l'image chiffrée est parfaitement reconstruite avec l'algorithme ECC. Par contre avec l'algorithme RSA (10.37 dB) et ElGamel (09.93 dB) elle est n'est pas bien

reconstruite. Les valeurs du SSIM confirment que pour les quatre algorithmes l'image chiffrée est dégradée et l'image déchiffrée est de très bonne qualité avec l'algorithme ECC (SSIM tend vers 1) cependant elle est moins bien déchiffrée avec ElGamel et RSA.

En vue d'une comparaison entre les deux types d'algorithmes ECC, on a calculé le temps d'exécution du chiffrement/déchiffrement des images considérées. D'après le tableau 4.5, on constate que l'algorithme ECC avec groupement est plus performant que celui sans groupement. En effet, il permet d'économiser le temps d'exécution surtout pour des images de grande taille.

| Image | Taille (Pixels) | Temps d'exécution (s) | |
|---|---|---|---|
| | | **ECC (sans G)** | **ECC (avec G)** |
| IRM | 256 × 256 | 14.909955 | 09.489136 |
| Radio | 384 × 384 | 70.657255 | 50.177655 |
| US | 518 × 395 | 199.341772 | 66.362140 |
| Scanner | **565 × 527** | **529.445193** | **169.454260** |

**Tableau 4.5 :** Temps d'exécution en fonction de la taille des images pour les deux ECC.

## 6. Conclusion

Dans ce chapitre, nous avons chiffré/déchiffré les images : US, Radiographique, Scanner et IRM avec différents algorithmes à savoir : RSA, ElGamel, ECC avec G et ECC sans G. Les critères de validation sur lesquels nous nous sommes basés sont : Histogramme, PSNR, SSIM et le temps d'exécution.

Les résultats obtenus montrent que l'algorithme ECC présente les meilleures performances en chiffrement en vue de la distribution uniforme ou aléatoire de l'histogramme de l'image chiffrée. On parle ici de dépendance des propriétés statistiques de l'image chiffrée et originale. Dans ce cas la probabilité qu'un cryptanalyse puisse

exploiter l'histogramme de l'image chiffrée pour tirer une information utile est quasi nulle. Cependant les algorithmes d'ElGamel et RSA sont moins performants surtout pour l'image IRM qui est traitée sous le format dcm.

Finalement et d'après le temps d'exécution, l'algorithme ECC avec groupement offre le meilleur compris entre la qualité et la rapidité de chiffrement/déchiffrement notamment pour les images de grande taille.

# Conclusion générale & perspectives

Le partage des images médicales est un moyen souvent incontournable chez les professionnels. Aujourd'hui, assurer la sécurité de ces données est devenu une obligation pour tout professionnel de santé comprenant ainsi la confidentialité, la disponibilité, et la fiabilité qui s'exprime en termes d'intégrité de l'information médicale.

Afin de contribuer à cette sécurisation de données médicales, nous avons proposé l'application d'un algorithme sur courbes elliptiques, initialement proposé pour le chiffrement de texte.

Nous avons introduit des généralités sur le traitement d'images et le fonctionnement des différentes modalités d'imagerie médicales.

Aussi nous avons présenté une vue globale sur la cryptographie en passant par les algorithmes de cryptographie moderne les plus utilisés actuellement, en donnant une explication plus ou moins détaillée sur la théorie des courbes elliptiques.

Nous avons implémenté, par la suite, l'algorithme de cryptographie sur courbes elliptiques en éliminant la table de partage entre l'expéditeur et le destinataire et en groupant les valeurs des pixels en paires pour former des points sur une courbe elliptique prédéfinie.

D'après les résultats de simulation, l'algorithme ECC avec groupement offre le meilleur compris entre la qualité et la rapidité de chiffrement/déchiffrement notamment pour les images de grande taille.

Finalement, nous avons comparé ECC à deux autres algorithmes de cryptographie moderne notamment ElGamel et RSA en terme de performance en utilisant trois critères de comparaison dont : l'histogramme, le PSNR et le SSIM. Les résultats obtenus ont montré que l'algorithme proposé offre de meilleures performances et son application, sur des images médicales, est prometteuse. De ce fait, il est possible d'effectuer un bon diagnostic.

Comme perspectives à ce travail, il serait souhaitable de :

- Tester notre méthode avec des algorithmes de cryptanalyse pour évaluer sa vraie résistance contre les piratages.
- Rendre la cryptanalyse plus difficile en ajoutant de l'aléatoire ou du chaos dans le code.
- Optimiser le temps d'exécution et l'espace de stockage en augmentant la taille des groupes.
- Envisager de réaliser une application pour l'exploiter dans les centres hospitaliers

# Annexe

Dans cette section, on présente les notions fondamentales sur lesquelles repose la cryptographie, à savoir : nombres premiers ; test de primalité, Décomposition en produit de facteurs premiers, Nombres premiers entre eux et Algorithme d'Euclide.

## 1. Rappel mathématique

### 1.1. Nombres premiers

On appelle un nombre premier, tout entier naturel $P \geq 2$ qui n'est divisible que par lui-même et par 1

- On considère que le nombre 1 n'est pas premier car il n'a qu'un seul diviseur : lui-même.
- Le nombre 0 est divisible par tous les entiers, donc il n'est pas premier.
- L'ensemble X des nombres premiers est infini, comme l'a démontré Euclide : on choisit un nombre premier P, multiplie tous les nombres premiers inférieurs à P entre eux et par P et on additionne 1 au résultat, on aura soit un nombre premier supérieur à x, soit un nombre divisible par un autre nombre premier, à partir de cette propriété on peut dire qu'il n'existe pas de plus grand nombre premier.

### 1.2. Test de primalité

C'est un algorithme qui indique si un nombre entier est premier ou pas en un temps raisonnable. Il existe plusieurs tests :

```
n>1
Pour k = 2,..., √n faire
{
r = reste de la division euclidienne de n par k
        Si r == 0 alors « n n'est pas premier »
}
« n est premier »
```

**Algorithme 1.1** : Algorithme de test de primalité [48].

### 1.3. Décomposition en produit de facteurs premiers

Cela consiste à écrire un nombre entier non nul sous forme d'un produit de nombres premiers ; exemple : $30 = 2 \times 3 \times 5$

Il faut savoir qu'un nombre premier ne peut pas être décomposé en produit de plusieurs nombres premiers.

### 1.4. Plus grand diviseur commun (PGCD)

On pose a et b deux entiers positifs, le PGCD de ces deux nombres est le plus grand nombre entier qui divise à la fois a et b

Exemple : PGCD(96,36)=12, 96/12=8, 36/12=3

- Propriétés :

- Si b divise a alors PGCD (a, b) = |b|
- Pour tout entier naturel k non nul, on a : PGCD (ka, kb) = k PGCD (a, b).

### 1.5. Nombres premiers entre eux

On dit que deux nombres sont premiers entre eux que s'ils ne partagent aucun diviseur commun sauf 1 et -1, c.-à-d. leurs PGCD=1 ;

D'après le théorème de Bézout, on peut savoir si a et b sont premiers entre eux si $ax + by = 1$ est vérifiée.

Exemple : PGCD (15, 8) = 1 donc 15 et 8 sont premiers entre eux.

- Propriétés :
  - Deux nombres premiers entre eux ne sont pas forcément premiers.
  - Deux nombres premiers distincts sont forcément premiers entre eux.

### 1.6. Algorithme d'Euclide

C'est une méthode qui permet d'identifier le PGCD de deux nombres sans avoir à faire leur décomposition en facteurs premiers.

**Théorème :** Si a et b sont deux entiers avec par exemple a>=b, si r est le reste de a par b, alors le pgcd de a et b vaut le pgcd de b et r [49].

Exemple : On calcule le PGCD (4539, 1958).

On effectue les divisions euclidiennes suivantes :

4539 = 1958 × 2 + 623

1958 = 623 × 3 + 89

623 = 89 × 7

Donc : PGCD (4 539, 1 958) = 89.

Variables d'entrés : a, b, q, r

Lire a, b

$E(a/b) \rightarrow q$

$a - bq \rightarrow r$

tant que $r \neq 0$ faire

$b \rightarrow a$

$r \rightarrow b$

$E(a/b) \rightarrow q$

$a - bq \rightarrow r$

**Algorithme 1.2** : Algorithme d'Euclide[49].

Cet algorithme permet aussi de calculer les coefficients de Bézout. Dans ce cas on l'appelle Algorithme d'Euclide étendu.

# Références


[1] F. Gaillard et al, Radiopaedia [en ligne]. (2005, mise à jours le 16/09/2020) Disponible sur : <https://images.radiopaedia.org/articles/godfrey-hounsfie ld?l an g =gb> (consulté le 14/09/2020).

[2] Infopro digital, L'usinenouvelle [en ligne]. (1998, mise à jours le 18/09/2020) Disponible sur : <https://www.usine-digitale.fr/article/a-cause-de-serveurs-mal-securises-plus-d-un-milliard-d-images-medicales-sont-exposees-sur-internet.N919194> (consulté le 14/09/2020).

[3] F. Karam et S. Imouloudene, "*Transfert sécurisé des données visuelles (images) dans un réseau intranet selon l'architecture client/serveur*". [en ligne], Mémoire de master en informatique, Université Abou Bakr Belkaid-Tlemcen, 2015,76p. Disponible sur : < http://dspace.univ-tlemcen.dz/bitstream/ 112/8160/1/ Transfert-des-securise-des-donnes-visuelles-images-dans-un-reseau-intranet-selon-larchitecteure-client-serveur.pdf > (consulté le 15 septembre 2020).

[4] J. Chabriais et P. Puech, "*Télétransmission des images médicales et des données associées. Aspects techniques*", fiche d'information et de recommandation du groupe SFR téléradiologie, octobre 2009. Disponible sur : <http://www.sfrnet.org/Data/upload/documents/sfr4i/Fiche%20Teleradiologie%20v1finale.pdf> (consulté en mars 2020).

[5] J. Wales et L. Sanger, *Encyclopédie*. Disponible sur : <www.wikipedia.org/wiki/Chiffrement> (Consulté le 27/8/2020).

[6] Y. Nedjar et I. Moussi, " *Application des méthodes numériques de traitement d'image sous Androïde*", mémoire de master, université Abou Bakr Belkaid-Tlemcen, 2018, Format PDF, Disponible sur :<http://dspace.univ-tlemcen. dz/bitstream/112/12907/1/Ms.Tel.MOUSSI%2BNEDJAR.pdf > (consulté en mars 2020).

[7] Techniques de traitement d'images [en ligne], Disponible sur :<http://www.pentes-tunnels.eu/didact/autres/Traitement%20d%20Image/Histogramme.html#:~:text=Un%20histogramme> (consulté le 19/8/2020).

[8] M. Karasad, "*Tatouages des images médicales partagées*" [en ligne], Thèse de doctorat, université de Bretagne occidentale-Brest(UBO), 25 juin 2018, Disponible sur : < https://tel.archives-ouvertes.fr/tel-02867836 > (consulté en juin 2020).

[9] J. Colard et F. Delpuech, "*Les rayons X une révolution dans l'avancé du diagnostic médical*" [en ligne]. (2011) Disponible sur :< http://tperayonsxjf.e-monsite.com/> (consulté le 25/8/2020).

[10] Coradix [en ligne], Disponible sur : <http://www.radiologieperpignan.fr/wp-content/uploads/photo_gallery/Photos%20Radiographie/?C=N;O=D> (consulté le 28/8/2020).

[11] B. Lodé et al, " Imagerie de la pneumonie COVID-19" [en ligne]. *Journal d'imagerie diagnostique* et Interventionnelle (2020) Disponible sur :<https://doi.org/10.1016/j.jidi.2020.04.011> (consulté en juillet 2020).

[12] A. Comment, *"Résonance Magnétique Nucléaire, Théorie et Manuel Pratique"* [en ligne], cours, section de physique, École Polytechnique Fédérale-Lausanne, 2013-2014 Disponible sur : https://www.epfl.ch/schools/sb/wp-content/uploads/2018/09/rmn.pdf(consulté en juillet 2020).

[13] J. Hodel, *"Formes progressives de sclérose en plaques : place actuelle de l'IRM pour le diagnostic positif et différentiel"* [en ligne], (mise à jour 1 décembre 2018), Disponible sur : https://neurologies.fr/formes-progressives-de-sclerose-en-plaques-irm-diagnostic-positif-et-differentiel/ (consulté en juillet 2020).

[14] H. Ghezali et O, Charif. *"Une étude comparative sur les différents types des images médicales"* [en ligne], mémoire Master, université Mohamed Boudiaf- M'silla 2018, Disponible sur : <http://dspace.univ-msila.dz:8080/xmlui/bitstream/handle/123456789/6602/620.pdf?sequence=1&isAllowed=y > (consulté en avril 2020).

[15] Medecine nucléaire de la doua [en ligne]. (2011, mise à jour le 4/6/2020) Disponible sur : < www.medecine-nucleaire.fr/scintigraphie-myocardique.html > (consulté le 30/8/2020).

[16] Doctissimo [enligne], Disponiblesur :<https://www.doctissimo.fr/sante/imagerie-medicale/scintigraphiecardiaque > (consulté le 25/8/2020).

[17] E. Durand et E, Blondiaux, "In *imagerie médicale*, Elsevier Masson SAS", 2017, 12p Disponible sur : <https://eu-ireland-custom-media-prod.s3-eu-west-1.amazonaws.com/France/Download/CERF475396/CERF475396.pdf> (consulté en mai 2020).

[18] Irimed, Institue de radiologie et d'imagerie médicale[en ligne]. (2007) Disponible sur : <www.irimed.ch/infos-medecins/prestations/ultrason--echographie.html> (consulté le 30/8/2020).

[19] J. Wales et L. Sanger, *Encyclopédie* [en ligne] Disponible sur : <https://webcache.googleusercontent.com/search?q=cache:oLuHUahC1_0J:https://fr.wikipedia.org/wiki/Tomodensitom%25C3%25A9trie+&cd=1&hl=fr&ct=clnk&gl=dz> (consulté le 10/8/2020).

[20] Résolution spatiale, espacement des pixels et échelle[en ligne] (mise à jour le 20/11/2015). Disponible sur :<https://www.rncan.gc.ca/cartes-outils-publications/imagerie-satellitaire-photos-aer/tutoriels-sur-la-teledetection/plates-formes-

capteurs/resolution-spatiale-espacement-des-pixels-et-echelle/9408 > (consulté le 25/08/2020).

[21] Orange Healthcare[en ligne] (mise à jour le 19/9/2020), Disponible sur:< https:// healthcare.orange.com/fr/nos-solutions/imagerie-medicale-partagee> (Consulté en juillet 2020).

[22] Gimias [en ligne], 2009, Disponible sur : <https://fr.osdn.net/projects/sfnetgimias/downloads/SampleData/digest_article.zip/> (consulté le 15/8/2020).

[23] the mighty [en ligne]. Disponible sur :<https://themighty.com/2020/01/unsecured-medical-image-data-threat-topatients/?fbclid=IwAR1TtBeaB1k1Pze3UV7h07k8FlYZV2jRl3pqri3778Oo4Rs1BSQeONaL0> (consulté le 29/8/2020).

[24] R. Dumong, *"cryptographie et sécurité informatique"* [en ligne], cours, université de liège, 2009-2010, 213p, Disponible sur : < https://docplayer.fr/2799061-Cry ptog r aphie-et-securite-informatique.html > (consulté en mars 2020).

[25] I. Souici, *"Cryptographie Nouvel Algorithme de Chiffrement Evolutionnaire basé Occurrences (ACEO)"* [en ligne], Mémoire de magister, Université de Guelma,2008, Disponible sur :<https://www.researchgate.net/publication/341575646NouvelAlgorithmede_Chiffrement_Evolutionniste_ACEO_Algorithme_de_Chiffrement_Evolutionniste_base_Occurences> (consulté en mars 2020).

[26] Cryptographie et codes secrets[en ligne] Disponible sur : <http:// www.bib math .net/crypto/index.php?action=affiche&quoi=moderne/vernam >www w.bibmat h.n e t/crypto/index.php?action=affiche&quoi=moderne/vernam >(consulté le 1 mars 2020).

[27] B. Preneel . selected areas in cryptography, Staffords Travares, Springer, Canada, Aout 2005, 104p Disponible sur : < https://link.springer.com /book/10.1007/978-1-4615-5489-9> (consulté en juin 2020).

[28] JDN [en ligne], (mise à jour le 11/2/2019) Disponible sur :www.journaldunet.fr/patrimoine/guide-des-financespersonnelles/1209336-cryptographie-asymetrique (consulté le 30/2/2020).

[29] M. Rouse, TechTarget [en ligne], (2007) Disponible sur : www.lemagit.fr/defini tion /RSA-algorithme (consulté le 30 février 2020).

[30] H. Attaf et H, Cherfa , *"Étude sur l'Applicabilité de la Cryptographie Asymétrique aux Réseaux de Capteurs sans Fi" l*[en ligne], mémoire de master, Université Abderrahmane Mira- Bejaia, juin 2012, 86p,Disponible sur :<https ://webcache .googleusercontent.com/search?q=cache%3A8FU9kA9othAJ%3Awww.univbejaia.dz%2Fjspui%2Fbitstream%2F123456789%2F9187%2F1%2FEtude%sur%Applicabilit%Cryptographie%2520Asym%25C3%25A9trique%%Capteurs%Fil.pdf >(consulté en juin 2020).

[31] F. Grosshans et P, Grancier, "La cryptographie quantique : l'incertitude quantique au service de la confidentialité" [en ligne], *optique quantique* vol.71, pp.34-39, 2014. Disponible sur : < https://www.photoniques.com/articles /photon /abs/ 2014 /03/photon201471p34/Photon201471p34.html > (consulté en mars 2020).

[32] N. Koblitz, "Elliptic curve cryptosystems" [en ligne], *Mathematics of computation* vol.48, pp:203–209,1987,. Disponible sur : <https://www.ams. org /journals /m c om/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf > (consulté en mars 2020).

[33] S. Victor et S. Miller, "Use of elliptic curves in cryptography" [en ligne]. *Advances in Cryptology*, pp 417–426, 1986, Format PDF, Disponible sur :<https ://link. Sprin ge r.com/chapter/10.1007%2F3-540-39799-X_31>(consulté en mars 2020).

[34] L. Ronald et S. Adi et L. Adlemen , "A method for obtaining digital signatures and public-key cryptosystems". [en ligne], *Communications of the* ACM, vol.21,pp 120–126, 1978. Disponible sur : < https://dl.acm.org/doi/ 10.11 45/359340.3593 42 > (consulté en mars 2020).

[35] I. Lotfi, " *Cryptographie à base de courbes elliptiques"* [en ligne], thèse de doctorat, Université de technologie- Nanyang, juin 2017,67p, Disponible sur : < https://www.researchgate.net/publication/323946296_Cryptographie_a_Base_de_c ourbes_elliptiques/link/5ab425ccaca272171003cb69/download > (consulté en mars 2020).

[36] B. Ayebie, " Courbes elliptiques : *formules d'addition et de doublement unifiées"* [en ligne]. Mémoire de master, université de Limoges, septembre 2012, 52p, Disponible sur : <https://www.researchgate.net/profile/Berenger_Ayebie/ publicati on/316554706_COURBES_ELLIPTIQUES_FORMULES_ADDITION_ET_DE_DOUBLEME NT_UNIFIEES/links/5903b0f6aca272116d2fba28/COURBES-ELLIPTIQUES FORMULES-ADDITION-ET-DE-DOUBLEMENT-UNIFIEES.pdf > (consulté en juin 2020).

[37] J. Wales et L. Sanger, Encyclopédie [en ligne] Disponible sur : <www.wikipedia .org/wiki/Courbe_elliptique >(Consulté le 20/8/2020).

[38] S. Ballet et L. Bonecaze , "*Cryptographie Avancée Courbes Elliptiques Application à la Cryptographie"*,[en ligne]. Marseille : École Polytechnique, 5ème année, cours,36p, Disponible sur : < http://alexis.bonnecaze.perso.luminy.univ-amu.fr/Cr yptoA vancee.pdf >(consulté en mars 2020).

[39] G. Harper , A. Menezes , et S.A. "Public-key cryptosystems with very small key lengths". In R.A. Rueppel[en ligne], *eurocrupt* , vol.658, pp 163– 173 Disponible sur :< https://link.springer.com/chapter/10.1007/3-540-47555-9_14 >(consulté le 27/8/2020).

[40] A.Menezes et A.Scott . " Elliptic curve cryptosystems and their implementation" [en ligne] of *cryptography*, vol.6, pp.209–224 Disponible sur : < https:/ /link .springer.com/article/10.1007%2FBF00203817>(consulté le 25/8/2020).

[41] R. Lercier . " Courbes elliptiques et cryptographie" [en ligne], *revue scientifique et technique de la défense,* 2004, pp 59-66 Disponible sur : < https://www. Resear ch gate.net/Publication/255644521 Courbes Elliptiques et crypto-graphie > (consulté le 22/8/2020).

[42] A. Sagheer. " *Elliptic Curves Cryptographic Techniques"* [en ligne]. Département du système d'information, Université de Anbar Ramadi-Iraq, 2012, 8p.Disponible sur:<https://www.researchgate.net/publication/260739576 Elliptic curvescryptogr aphic techniques> (consulté en juillet 2020).

[43] N. Melioni . " *Arithmétique pour la Cryptographie basée sur les Courbes Elliptiques"*. [en ligne] Thèse de doctorat en informatique, Université des Sciences et Techniques- Languedoc, 2007, 139p, Format PDF. Disponible sur : < http://meloni.univ-tln.fr/articles/These.pdf > (consulté le 1/9/2020).

[44] K.Wrya . " a new text encryption technique on elliptic curve cryptography" [en ligne]. *Journal of Engineering and Applied Sciences,* 2017, Vol.12, n°13, pp. 3329-3333 Disponible sur: < https://medwelljournals.com/abstract/?doi=jeasci.2017. 3329. 3333> (consulté le 25/7/2020).

[45] J.Teeriaho, 2011. "Cyclic *Group Cryptography with Elliptic Curves"* [en ligne]. Université des sciences appliquées, Rovaniemi, Finlande, 2011. 21 p. Disponible sur :<http://web.lapinamk.fi/jouko.teeriaho/brasov.pdf> (consulté le 20/07/2020).

[46] K. Lewin, " signal processing laboratory" [en ligne]. (2011, mise à jour 2019) Disponible sur :<http://splab.cz/download/databaze/ultrasound.com com> (consulté le 9/9/2020).

[47] T. Preston-Werner et C. Wanstrath, Github [en ligne]. (2008, mise à jour Aout 2020) Disponible sur : <https://github.com/ieee8023/covid-chestxray-dataset /tree/master/images.com > (consulté le 9/9/2020).

[48] N. Rutger, "*Tests de primalité : théorie et pratique"*, [en ligne], Université de Strasbourg et CNRS, Cours, 2011, 16p. Disponible sur :< http://irma.math.uni str a.fr/~noot/publications/primalite irem 2011 > (consulté en mars 2020).

[49] F. de Marcay, " *Algorithme d'Euclide "* [en ligne], Département de Mathématiques d'Orsay, Université Paris-Sud-France, Cours, 2014, 16p. Disponible sur :<https:// www.imo.universite-paris-saclay.fr/~merker/Enseignement/Algebre- effective/algorithme-euclide.pdf > (Consulté en mars 2020).

# Résumé

L'évolution rapide des technologies de télécommunications s'exprime aujourd'hui dans le domaine de la santé par la mise en place de nouveaux moyens de partage des images médicales des patients. Dans ce contexte, la question de la sécurité de ces images est particulièrement sensible en vue de son intégrité. L'objectif de ce mémoire est de contribuer à la protection de ces données en utilisant la cryptographie basée sur les courbes elliptiques (ECC) qui est une zone d'études moderne. Pour atteindre cet objectif, on a étudié des algorithmes de cryptographie asymétrique notamment ElGamel et RSA ainsi qu'un algorithme ECC sous deux formes : avec et sans groupement. Ces algorithmes sont appliqués sur des images médicales collectées de bases de données ouvertes et issues de différentes modalités d'imagerie médicale; à savoir : échographie, RX, scanner et IRM. Les résultats obtenus ont montré que l'algorithme ECC avec groupement est plus efficace que celui sans groupement, puisqu'il fournit des performances bien meilleures quant à la qualité et la rapidité de chiffrement/déchiffrement en particulier pour des images de grande taille. De ce fait, l'utilisation de l'ECC pour la sécurisation des images médicales est prometteuse.

# ملخص

يتم التعبير عن التطور السريع لتقنيات الاتصالات السلكية واللاسلكية حديثا في مجال الصحة من خلال تطبيق وسائل جديدة لتبادل الصور الطبية للمرضى. في هذا السياق، فإن مسألة أمن هذه الصور حساسة بشكل خاص في ضوء سلامتها. الهدف من هذه المذكرة هو المساهمة في حماية هذه البيانات باستخدام التشفير المعتمد على المنحنيات الإهليجية والتي تعتبر دراسة حديثة. لتحقيق هذا الهدف، قمنا بدراسة خوارزميات التشفير غير المتماثل بما في ذلك خوارزميات ElGamel و RSA بالإضافة إلى شكلين من خوارزمية التشفير باستخدام المنحنيات الاهليجية (ECC) بالتجميع وبدون التجميع. تطبيق هذه الخوارزميات على الصور الطبية التي تم جمعها من قواعد البيانات مفتوحة المصدر، باستخدام عدة طرق التصوير الطبي المختلفة؛ وهي: الموجات فوق الصوتية والأشعة السينية والماسح الضوئي والتصوير بالرنين المغناطيسي. أظهرت النتائج التي تم الحصول عليها أن خوارزمية التشفير للمنحنى الاهليجي مع التجميع أكثر فاعلية من ذلك الذي بدون التجميع، لأنها توفر أداءً أفضل بكثير من حيث جودة وسرعة التشفير وفك التشفير، ولا سيما للصور ذات الحجم الكبير. ولذلك، فإن استخدام التشفير للمنحنى الاهليجي لتأمين الصور يعد أمرًا واعدًا.

# Abstract

The fast evolution of telecommunications technologies is now being expressed in the healthcare field by the implementation of new ways of sharing the medical images of patients. In this context, the security matter of these images is highly sensitive to their integrity. The main objective of this thesis is to contribute to the protection of these data using cryptographic schemes based on elliptic curves (ECC) which is a modern field of study. To achieve this objective, asymmetric cryptography algorithms including ElGamel and RSA as well as an ECC algorithm were studied in two forms: with and without grouping. These algorithms are tested on medical images collected from open databases and from different medical imaging modalities; namely: ultrasound, X-ray, CT and MRI. The results showed that the ECC algorithm with grouping is more efficient than the one without grouping, since it provides much better performance in terms of quality and speed of encryption/decryption, especially for large images. As a result, the use of ECC for securing medical images is promising.