وزارة التعليم العالي والبحث العلمي

BADJI MOKHTAR –ANNABA
UNIVERSITY
UNIVERSITE BADJI MOKHTAR
ANNABA

جامعة باجي مختار
- عنابة -

Faculté des Sciences

Département de Mathématiques

Année : 2016/2017

THÈSE

Présenté en vue de l'obtention du diplôme de
DOCTORAT EN SCIENCES

L'IMAGERIE MEDICALE : TRANSPORT ET STOCKAGE NUMERIQUES SECURISES

Option
MATHEMATIQUES APPLIQUEES

Par
Moumen Abdelkader

DIRECTEUR DE THÈSE : Sissaoui Hocine Pr. U.B.M. ANNABA

Devant le jury

PRESIDENT :	Nouri Fatima Zohra	Prof.	U.B.M. ANNABA
RAPPORTEUR :	Haiour Mohamed	Prof.	U.B.M. ANNABA
RAPPORTEUR :	Maouni Messaoud	M.C.A	U. SKIKDA
EXAMINATEUR :	Bouhouche Salah	Dir. Rech.	CRTI ALGER
EXAMINATEUR :	Drai Radouane	Dir. Rech.	CRTI ALGER

ملخص

الهدف من هذه الرسالة هو اقتراح أساليب جديدة لحماية وتشفير الصور الرقمية.
الطرق المقترحة يجب أن تلبي معايير السلامة المعروفة في أوساط أمن المعلومات مثل السرية ، والتوثيق والتتبع.
الطرق المقترحة ينبغي أن تكون مقاومة ضد الهجمات المعروفة وتملك معايير قياس إحصائية قريبة من القيم المثلى
ومن بين الأهداف هو تصميم أساليب أقل تكلفة من حيث الموارد و وقت التشفير وضمان سلامة في نفس الوقت. هذه المقترحات ينبغي أيضاً أن توفر عدم الكشف عن الهوية في حالة تشفير متعدد المستقبلين.

كلمات مفتاحية : الصور الرقمية، التشفير، فك التشفير، تشفير متعدد المستقبلين، إخفاء رسائل في صور، التشفير غير المتناظر، التشفير المتناظر.

Résumé

Le but de cette thèse est de proposer des nouvelles méthodes de protection des images numériques.

Les méthodes proposées doivent satisfaire certains critères de sécurité comme la confidentialité, l'intégrité, l'authentification et la traçabilité. Les approches proposées doivent également avoir une résistance contre les attaques connues, et présentent des valeurs de mesures statistiques proches des valeurs optimales.

Ce travail de thèse va permettre : de concevoir des méthodes moins coûteuse en terme de ressource et temps de calcul, de garantir la sécurité et fournir l'anonymat s'il s'agit d'un chiffrement multi-récepteur.

Mots clés : Image numérique, cryptosystème, chiffrement, déchiffrement, la cryptanalyse, stéganogaraphie, stéganalyse, multi-réception, cryptographie symétrique, cryptographie asymétrique.

Abstract

The aim of this thesis is to propose new methods to protect digital images.

The methods proposed must satisfy the security criterias such as confidentiality, integrity, authentication and traceability. The proposed approaches must also have resistance against known attacks and present statistical measurement closed to the optimal values.

Among the objectives is to design methods less expensive in terms of resources, provides a good computational cost and ensure at the same time the security. Also provide the anonymity in the case of a multi-receiver encryption.

Keywords : Digital Imaging, cryptosystem, encryption, decryption, cryptanalyse, steganogaraphy, multi-receiver, asymmetric cryptography, symmetric cryptography.

Publications internationales :

1. **Abdelkader Moumen**, Mohamed Bouye and Hocine Sissaoui "New Secure Partial Encryption Method for Medical Images Using Graph Coloring Problem."Nonlinear Dynamics, Volume 82, Issue 3 , pp 1475-1482.
   Nonlinear Dynamics :
   http ://link.springer.com/journal/11071, **ISI impact factor 3.00**
   DOI : 10.1007/s11071-015-2253-4

2. **Abdelkader Moumen** and Hocine Sissaoui "Images Encryption Method using Steganographic LSB Method, AES and RSA algorithm."
   Nonlinear Engineering - Modeling and Application. Published Online : 2017-01-27
   https ://www.degruyter.com/view/j/nleng
   Elsevier - SCOPUS
   DOI : https ://doi.org/10.1515/nleng-2016-0010

3. L houssain El Fadil and **Abdelkader Moumen** "Anonymous Multi-Receiver Public Key Encryption Based on Lucas Sequences."
   Journal of Information Science and Engineering. Submitted 27/04/2017
   http ://www.iis.sinica.edu.tw/page/jise/Introduction.html

Communications :

1. "Using steganography in cryptography". ICCC 2015 International Conference on Coding and Cryptography. USTHB Algiers, Algeria 2-3 november 2015.

2. "Secure Partial Encryption Method for Medical images". The 10th Annual Scientific Research Day, 2014. Abha, KSA.

3. "Traffic flow mathematics models and applications". Algerian Mathematicians Congress - CMA2012, 7 and 8 March 2012, Annaba- Algeria.

À mes parents.

À ma femme.

À mes enfants, Adnen et Bayane.

À toute ma famille.

Remerciements

Je voudrai remercier avant tout, ALLAH de m'avoir faciliter ce travail et de m'avoir donner le courage et la volonté pour dépasser toutes les difficultés.

J'adresse mes remerciements aux personnes qui m'ont aidé et qui m'ont accompagné dans la réalisation de ce travail.

Tout d'abord, c'est à M. Sissaoui Hocine, professeur à l'Université de Badji Mokhtar de Annaba que j'adresse mes remerciements, je le remercie très vivement d'avoir accepté de diriger ce travail, il m'a guidé dans mon travail et m'a aidé à trouver des solutions pour avancer. Son expérience de la recherche, ses conseils et encouragements m'ont été très précieux tout au long de cette thèse. Je le remercie pour ces qualités scientifiques et humaines exceptionnelles, j'ai pour lui un grand respect.

Ensuite, mes remerciements et ma gratitude s'adresse aussi au professeur Nouri Fatima Zohra professeur l'Université de Badji Mokhtar Annaba qui me fait l'honneur d'être le président du jury.

Je remercie également tous les membres de jury de me faire l'honneur de participer à mon jury.

Je remercie très chaleureusement les membres de jury les professeurs Haiour Mohamed, Maouni Messaoud, Bouhouche Salah et Drai Radouane pour avoir accepté d'être examinateurs de cette thèse. Je les remercie d'avoir bien voulu s'intéresser à ce travail et en être des examinateurs.

Un grand merci à tous mes amis, mes collègues de l'université King Khalid à Abha en Arabie Saoudite, les membres de l'équipe crypto et traitement d'images, qui m'ont soutenu pendant la rédaction de cette thèse. Leurs encouragements m'ont été d'une grande utilité, j'ai partagé avec eux de bons moments lors des projets communs, j'ai eu l'occasion d'apprécier leurs grandes qualités scientifiques pour d'éclairantes discussions lors nos groupes de travail.

Enfin, je ne pourrais terminer sans remercier chaleureusement ma famille pour leurs soutiens au cours de toutes ces années.

Je remercie du fond du cœur ma femme, toujours a été à côté de moi, qui a toujours été d'un soutien et d'une patience exceptionnels.

A tous ceux que je n'ai pas cités ici et que j'ai rencontrés pendant ce travail.

Table des matières

1 Introduction générale **10**
- 1.1 Motivations . . . 10
- 1.2 Cryptologie . . . 11
- 1.3 Bref historique . . . 11
- 1.4 Cette thèse . . . 15

2 L'image numérique et l'imagerie médicale **17**
- 2.1 Introduction . . . 17
- 2.2 L'image matricielle . . . 17
- 2.3 L'image vectorielle . . . 18
- 2.4 L'image médicale . . . 18
- 2.5 Codage des couleurs . . . 20
  - 2.5.1 Les images binaires : . . . 20
  - 2.5.2 Les images en niveau de gris : . . . 20
  - 2.5.3 Les images couleurs : . . . 20
- 2.6 Les méthodes d'évaluation . . . 21
  - 2.6.1 Histogramme . . . 21
  - 2.6.2 Le coefficient de corrélation . . . 22
  - 2.6.3 L'analyse d'entropie . . . 23
  - 2.6.4 L'écart irrégulier . . . 24
  - 2.6.5 Résistance au bruit . . . 25
  - 2.6.6 NPCR et UACI . . . 25
- 2.7 Conclusion . . . 26

3 La sécurité **27**
- 3.1 Introduction . . . 27
- 3.2 Les termes de base utilisés en cryptographie . . . 28
- 3.3 Les objectifs de la cryptographie . . . 29
- 3.4 Classification des schémas cryptographique : . . . 30
  - 3.4.1 Classification selon les clés . . . 30
  - 3.4.2 Classification selon la structure de chiffrement . . . 32
  - 3.4.3 Classification selon le pourcentage de données cryptées . . . 34
- 3.5 Cryptographie symétrique : . . . 35

3.5.1 Data Encryption Standard (DES) . . . 36
3.5.2 L'algorithme AES (Advanced Encryption Standard) : . . . 36
3.6 Cryptographie à clé publique : . . . 39
3.6.1 Le problème du logarithme discret : . . . 42
3.6.2 Les fonctions à sens unique : . . . 42
3.6.3 Les fonctions à trappe : . . . 43
3.6.4 L'algorithme d'Euclide étendu : . . . 43
3.6.5 Le théorème des restes chinois : . . . 44
3.6.6 Procédé de Diffie-Hellman d'échange publique des clés : . . . 46
3.6.7 L'algorithme RSA (Rivest, Shamir Adleman) : . . . 47
3.6.8 La sécurité de RSA : . . . 50
3.6.9 La signature numérique . . . 52
3.6.10 Le certificat électronique . . . 53
3.7 La cryptanalyse . . . 54
3.7.1 Les principes de la cryptanalyse . . . 54
3.7.2 Les types de base de la cryptanalyse . . . 55
3.7.3 La cryptanalyse moderne : . . . 56
3.8 Conclusion . . . 57

4 Nouvelle méthode de chiffrement partiel des images médicales basée sur la coloration des graphes 60
4.1 Introduction : . . . 60
4.2 Coloration de graphe : . . . 61
4.2.1 Ensemble indépendant maximal . . . 62
4.2.2 L'algorithme DBG . . . 63
4.2.3 Résolution de GCP . . . 64
4.3 Notre approche . . . 64
4.4 L'analyse de sécurité : . . . 67
4.5 Résultats expérimentaux . . . 68
4.6 Conclusion . . . 71

5 Méthode de chiffrement des images basée sur la méthode stéganographique LSB et les algorithmes AES et RSA 72
5.1 Introduction . . . 72
5.2 Stéganographie et tatouage . . . 73
5.2.1 La stéganographie . . . 74
5.2.2 La stéganalyse . . . 77
5.2.3 Le tatouage numérique . . . 78
5.2.4 La méthode LSB (Least Significant Bit) . . . 79
5.3 Notre approche . . . 80
5.4 Résultats expérimentaux . . . 80
5.4.1 Effet du bruit : . . . 83
5.4.2 Analyse de l'espace clé : . . . 84

5.4.3 L'analyse de corrélation : 84
5.4.4 Analyse d'entropie : 85
5.4.5 Comparaison de la technique proposée et l'algorithme étudié dans [97] : 85
5.5 Conclusion 86

6 Un nouveau cryptosystème multi-récepteur à clé publique basé sur les suites de Lucas 87
6.1 Introduction 87
6.2 Le chiffrement à clé publique LUC : 88
6.2.1 Les suite récurrente linéaire : 88
6.2.2 Les suites de Lucas 89
6.2.3 L'algorithme de chiffrement monocast LUC : 93
6.3 Les résultats Principaux 95
6.3.1 Notations et Définitions 96
6.3.2 Les propriétés cryptographiques des suites de Lucas 97
6.3.3 Méthode et coût de calcul 99
6.3.4 Notre approche : Schéma de chiffrement multi-récepteur . . . 101
6.3.5 L'analyse de l'approche proposée 102
6.3.6 L'échange de clés de Lucas Diffie-Hellman étendue à un groupe d'utilisateurs 103
6.4 Conclusion 104

7 Conclusion et perspectives 107

Table des figures

1.1 Schéma de communication. 11
1.2 "Scytale" un ancien outil de chiffrement. 12
1.3 Le cylindre de Thomas Jefferson 1790. 13
1.4 Le chiffrement César : Décalage des lettres de l'alphabet. 13
1.5 La machine de chiffrement "Enigma", deuxième guerre mondiale. . . 13
1.6 La sécurité sous forme matérielle : (a) Le HSM, (b) USB d'authentification. 14

2.1 Exemple d'agrandissement sur une image matricielle. 19
2.2 Exemple d'agrandissement sur une image vectorielle. 20
2.3 (a) Image couleur, (b) Image en niveaux de gris, (c) Image binaire. . 21
2.4 (a) Image de niveaux de gris, (b) Histogramme. 22

3.1 Les étapes de chiffrement. 28
3.2 Classification des schémas cryptographique. 30
3.3 La fonction de hachage : fournit une empreinte courte de la donnée. . 32
3.4 Le chiffrement symétrique. 35
3.5 L'algorithme DES. 38
3.6 L'algorithme AES. 40
3.7 Le chiffrement asymétrique 40
3.8 La signature numérique. 58
3.9 Vérification de la signature numérique. 58
3.10 Exemple de certificat électronique. 59
3.11 La vérification du certificat électronique. 59

4.1 Exemple d'une coloration d'un graphe 62
4.2 Le graphe associé au bloc A. 67
4.3 Après le chiffrement et l'ajustement. 68
4.4 Bras : (a) L'image originale, (b) Image partiellement chiffrée, (c) Image déchiffrée. 70
4.5 Cancer du poumon : (a) L'image originale, (b) Image partiellement chiffrée, (c) Image déchiffrée. 70
4.6 Crâne : (a) L'image originale, (b) Image partiellement chiffrée, (c) Image déchiffrée. 70

4.7 Main : (a) L'image originale, (b) Image partiellement chiffrée, (c) Image déchiffrée. 71

5.1 (a) Le message, (b) L'image originale, (c) Stégo-objet. 74
5.2 (a) L'image, (b) L'image originale, (c) Stégo-objet. 74
5.3 Schéma Stéganographique. 76
5.4 Le tatouage numérique : (a) L'image originale, (b) L'image tatouée. . 78
5.5 Notre approche : Chiffrement AES-RSA-LSB. 81
5.6 Cancer du poumon : (a) L'image originale, (b) L'image chiffrée, (c) Stego-image, (d) L'image déchifrée. 83
5.7 Crâne : (a) L'image originale, (b) L'image chifrée, (c) Stego-image, (d) L'image déchifrée. 83
5.8 Main : (a) L'image originale, (b) L'image chifrée, (c) Stego-image, (d) L'image déchifrée. 83

6.1 L'échange de clés de Lucas Diffie-Hellmane étendue à un groupe d'utilisateurs. 106

Liste des tableaux

3.1 AES : Le nombre de tours/la taille de la clé/la taille des blocs 37
3.2 Comparaison chiffrement symétrique/asymétrique 41

4.1 Résistance au bruit de la méthode de chiffrement GCP. 69

5.1 Résistance au bruit du chiffrement AES-RSA-LSB. 84
5.2 Cancer du poumon : Analyse de corrélation entre deux pixels adjacents. 84
5.3 Crâne : Analyse de corrélation entre deux pixels adjacents. 85
5.4 Main : Analyse de corrélation entre deux pixels adjacents. 85
5.5 La valeur d'entropie : L'image originale, l'image chiffrée et l'image stégo-chiffrée. 85
5.6 Comparaison de la technique proposée et l'algorithme étudié dans [97]. 86

6.1 Exemple des premiers nombres de Lucas pour $P = 3$ et $Q = 1$. 92
6.2 Chiffrement multi-récepteur : comparaison des résultats avec d'autres schémas. 103

Chapitre 1

Introduction générale

Nos travaux de recherche portent sur le chiffrement des images et les sujets en relations directement ou indirectement. Ce chapitre contient introduction sur la cryptologie, les motivations des travaux proposés, bref historique, plan et les résultats de cette thèse.

1.1 Motivations

L'être humain est une créature sociale ! Son besoin de communication a existé depuis des milliers d'années bien avant l'invention du papier et des ordinateurs. Aujourd'hui, la technologie et la communication d'informations sont profondément intégrées dans de notre vie. On utilise de plus en plus les téléphones, l'Internet, les services bancaires mobiles et d'autres services. L'information est présente et utilisée sous de nombreuses formes : documents, audio, vidéos, photos, etc. Les progrès récents dans la technologie, en particulier dans l'industrie informatique et dans la communication a motivé les organisations pour remplacer leurs dossiers traditionnels, stockés et échangés manuellement, par des systèmes informatiques et des documents numériques leur offrant un stockage facile et une communication fluide.

Avec le développement rapide des technologies multimédias et des réseaux de communications et l'évolution des équipements qui sont capable d'acquérir, d'archiver et de transmettre des images et des vidéos à des coûts raisonnables, ce qui favorise leur utilisation dans plusieurs domaines, comme la vision sur ordinateur, l'imagerie médicale, systèmes multimédia, l'imagerie satellitaire, télémédecine, télésurveillance, etc. L'image occupe une place particulièrement importante. Ces données sont échangées via des canaux qui ne sont pas toujours sûrs, la plupart des cas ils sont transmis sur des réseaux ouverts, une grande partie de ces informations est confidentielle ou privée. En effet, ces données peuvent être facilement interceptées ou modifiées par des attaquants ou par des utilisateurs non autorisés. La sécurité de ces informations durant le transfert ou pendant le stockage est devenue plus importante et a attiré beaucoup d'attention.

1.2 Cryptologie

Les progrès importants dans la technologie et les énormes flux générés de données numériques ont donné naissance à de nouveaux problèmes. Parmi ces problèmes on trouve la protection des données. Le but traditionnel de la cryptographie est de concevoir des méthodes permettant de transmettre des données de manière sécurisée. La cryptographie moderne traite plus généralement les problèmes de sécurité des communications et des données stockées. La cryptographie consiste à utiliser les mathématiques pour transformer une donnée en clair en une donnée incompréhensible, le sens inverse de cette opération est le déchiffrement. La cryptologie ou la science du secret [95] comporte deux grandes branches : la cryptographie et la cryptanalyse, la figure **??** présente le schéma complet de la communication. La cryptographie est l'écriture secrète de l'information ou le chiffrement, et la cryptanalyse est l'analyse de cette dernière ou l'étude du niveau de sécurité des systèmes, c'est-à-dire se positionner comme un adversaire qui cherche à casser les codes secrets et retrouver le message original.

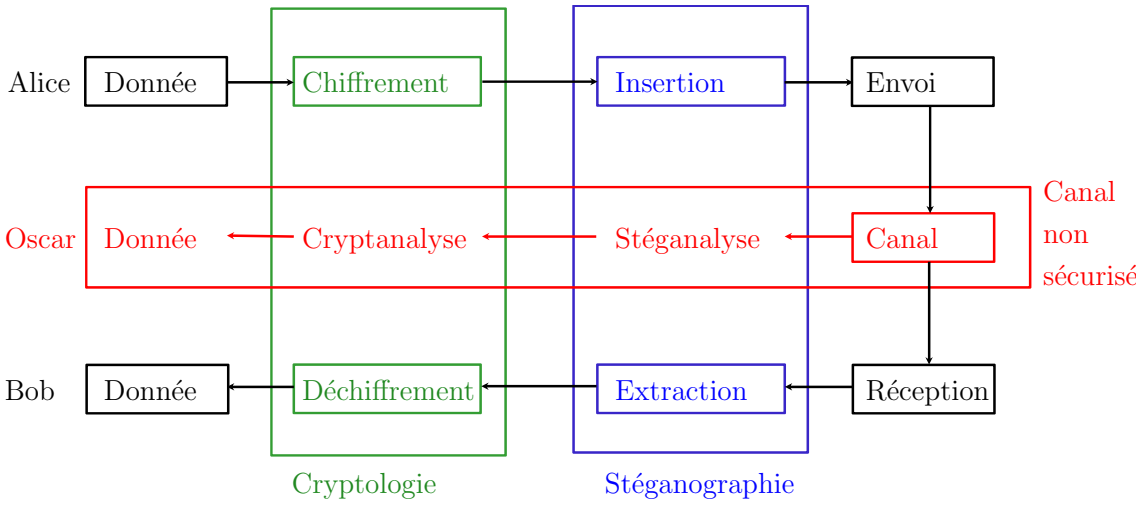


FIGURE 1.1: Schéma de communication.

Le but de la cryptographie est d'offrir un certain nombre de services de sécurité comme la confidentialité, l'intégrité et l'authentification [27, 50]. Des généralités sur la cryptographie seront présentées dans le chapitre 2 avec plus de détail.

1.3 Bref historique

La cryptographie est une science très ancienne qui date bien avant l'invention de l'ordinateur, elle est née au même moment que l'écriture. Vers 1900 ans avant J.-C., les Égyptiens ont commencé à modifier le texte pour garantir la protection

des messages. La méthode de chiffrement utilisée consistait simplement à supprimer quelques lettres et à remplacer certains mots par d'autres. Pendant des siècles, la cryptographie a été utilisée à des fins militaires pour assurer les correspondances [47, 95, 168].

Entre 100 et 44 avant J.-C, le dictateur de l'empire romain Jules César, a utilisé une nouvelle méthode pour protéger ses messages, connue sous le nom de chiffrement de César (Figure 1.4), l'une des méthodes les plus célèbres. Chaque lettre est remplacée par la troisième lettre suivante de l'alphabet. Au XIV siècle, le chiffrement était avec des dispositifs traditionnels comme le crayon et le papier. Le "scytale" ou "bâton de Plutarque" (Figure 1.2), est un bâton de bois, dont la forme est connue uniquement de l'émetteur et du destinataire du message. En 1790, Thomas Jefferson propose un cylindre de chiffrement composé de 26 roues (Figure 1.3), les 26 lettres de l'alphabet sont inscrit sur chaque roue dans un ordre aléatoire, l'expéditeur et le récepteur doivent avoir des cylindres identiques.

FIGURE 1.2: "Scytale" un ancien outil de chiffrement.

Dès le début de la cryptographie et jusqu'aux années 1960, les communications sécurisées ont été limitées à des applications militaires et diplomatiques [90].

Avant que les ordinateurs modernes aient été inventés [25, 93], la cryptographie sous forme matérielle est apparue sous forme d'une machine mécanique et électromécanique dans les années 1920. Connue sous le nom "Enigma" (Figure 1.5), inventée par un groupe de scientifiques allemands. Ce dispositif a été largement utilisé pour toutes les correspondances de l'armée allemande pendant la seconde guerre mondiale, avant d'être décryptée par les Britanniques avec l'aide de la Pologne en 1932.

Avec le progrès de l'informatique et le besoin de protéger l'information dans d'autres domaines que le militaire, la cryptographie sert de plus en plus dans des

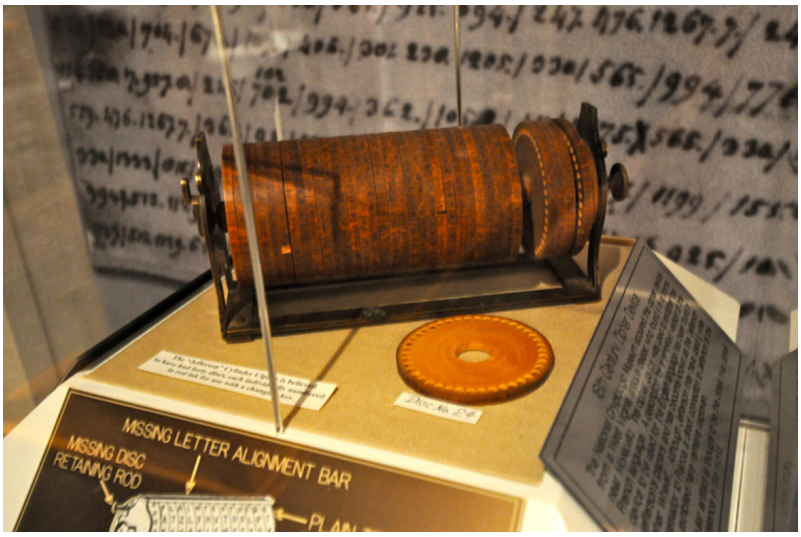


FIGURE 1.3: Le cylindre de Thomas Jefferson 1790.

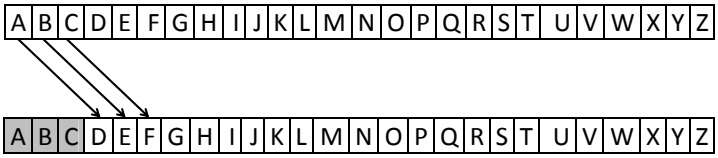


FIGURE 1.4: Le chiffrement César : Décalage des lettres de l'alphabet.

FIGURE 1.5: La machine de chiffrement "Enigma", deuxième guerre mondiale.

domaines variés. Naturellement, les chercheurs de différentes disciplines ont proposé autres solutions plus modernes et plus efficaces. A la fin des années 1960 et au début des années 1970, un physicien cryptographe allemand Horst Feistel a créé un algorithme de chiffrement pour IBM appelé le Réseau de Feistel [78], qui était une

structure symétrique utilisée dans la construction de chiffrement par blocs. Ce fut le premier réseau de cryptographie moderne conçu et commercialisé en 1973.

En 1977, le Bureau national américain de normalisation (National Institute of Standards and Technology NIST) a publié un algorithme de chiffrement basé sur l'algorithme de Feistel, connu sous le nom Data Encryption Standard (DES). DES est resté très présent dans la cryptographie et dans le monde académique, a été considéré comme une norme jusqu'à la fin de l'année 2000. En Janvier 1999, deux organismes l'EFF (Electronic Frontier Foundation) et DCTI (Distributed Computing Technologies, Inc) ont collaboré pour casser publiquement une clé DES en 22 heures et 15 minutes. En 2001, le NIST a remplacé DES en adoptant AES (Advanced Encryption Standard). AES a été développé par deux chercheurs belges Joan Daemen et Vincent Rijmen il remplace l'algorithme DES [94].

En 1978 Ron Rivest, Adi Shamir et Len Adleman [156] de l'Institut de Technologie du Massachusetts ont proposé le premier algorithme de sécurité à clé publique RSA [182] .La théorie du système à clef publique a marqué le début de la cryptographie moderne. Dans [48] Kahn donne une histoire complète de la cryptographie sans aborder les problèmes techniques.

Également, il y'a d'autres théories qui interviennent dans la cryptographie comme la théorie du chaos [170, 22, 191, 62] et les courbes elliptiques [176, 105, 145, 184, 185, 133]. Sous forme matérielle moderne, on trouve des dispositifs commes des USB d'authentification et le HSM (Hardware Security Module) (voir la figure 1.6). L'USB d'authentification c'est moyen d'authentification forte qui génère des mots de passes à validité limitée. Le HSM est un matériel électronique considéré comme très sécurisé offrant la possiblité stocker et protéger des clefs cryptographiques.

(a) (b)

FIGURE 1.6: La sécurité sous forme matérielle : (a) Le HSM, (b) USB d'authentification.

1.4 Cette thèse

Le plan de ce mémoire sera décliné en sept chapitres et sera organisé de la façon suivante :

Après une introduction générale dans ce premier chapitre. Dans le chapitre 2 nous étudions l'image numérique et l'image médicale et ses grandes catégories, les paramètres d'évaluation des images chiffrées serons également détaillées dans ce chapitre. Nous traitons l'état de l'art de la sécurité des images dans le Chapitre 3, après un rappel des notions de base, nous présentons les deux branches de la cryptologie : la cryptographie, la cryptologie et les différentes techniques utilisées.

On présentera ensuite, dans les Chapitre 4, 5 et 6 nos contributions principales dans cette thèse.

Ainsi, nous avons proposé dans le Chapitre 4, un nouvel algorithme de chiffrement partiel des images médicales, cette approche est basée sur la coloration de graphes. Le grand volume d'échange de données médicales a motivé le développement de nouvelles méthodes pour réduire le coût. Le chiffrement partiel est une approche pour réduire les ressources et le temps de calcul pour les énormes volumes de multimédia. Cet article présente une nouvelle approche sécurisée. Avant de chiffrer l'image, nous sélectionnons des pixels optimaux, cette sélection grâce à un algorithme de coloration de graphes. Ensuite, les pixels localisés vont être cryptés par un algorithme de chiffrement symétrique. Dans cette méthode, la clé et l'algorithme de chiffrement sont difficiles à détectés parce qu'il est difficile de prévoir les positions des pixels chiffrés. Les résultats expérimentaux montrent l'efficacité et la robustesse contre plusieurs attaques de notre proposition. D'autre part, on obtient un pourcentage acceptable de données chiffrées pour une meilleure sécurité avec un coût inférieur par rapport au cryptage total de l'image.

Nous proposons dans le Chapitre 5, un nouveau schéma de chiffrement des images. Les motivations de la technique proposée est de développer un algorithme qui est plus rapide que les techniques actuelles, et d'autre part nous voulons éliminer l'étape de partage de la clé secrète. Par conséquent, pour atteindre cette tâche, nous présentons une méthode qui utilise le chiffrement symétrique, chiffrement asymétrique et la théorie de la stéganographie. L'image est chiffrée en utilisant un algorithme symétrique, alors, la clé secrète est cryptée par un algorithme asymétrique. Ensuite, elle est cachée dans l'image chiffrée en utilisant les techniques de la stéganographie. Les résultats de l'analyse montrent que les valeurs de test sont très proches des valeurs optimales.

Dans le chapitre 6, on introduit un nouveau système de chiffrement multi-récepteur qui fournit l'anonymat des utilisateurs. Le chiffrement multi-récepteur a une grande importance dans de nombreux secteurs tels que les applications médicales, les votes

électroniques, les sondages, les référendums et les pétitions. La comparaison avec d'autres résultats montrent que la méthode proposée fournit l'anonymat et garantit un temps de calcul intéressant.

Finalement, dans le chapitre 7 une conclusion générale va résumer les objectifs atteints dans ce travail. Ainsi, nous rappelons les contributions apportées, nous suggérons également quelques pistes pour les futurs travaux de recherches et les perspectives à venir.

Chapitre 2

L'image numérique et l'imagerie médicale

2.1 Introduction

Bien avant l'invention de l'ordinateur, l'homme avait choisi un moyen simple de communication qui ne nécessite aucune connaissance particulière sinon celle de tracer, cette méthode est de dessiner et concevoir des images. Avant toute chose, mettons-nous d'accord sur le terme "image", la définition de l'image dans Larousse : « *image : n.f. (lat. imago) [. . .] Représentation imprimée d'un sujet quelconque* [. . .]». Pour un ordinateur le support d'affichage d'une image numérique est l'écran.

Le développement des médias de communication et des supports de stockage ont énormément transformé les moyens de communication. Les nouvelles technologies, sont basées essentiellement sur l'échange et le stockage des données multimédias et en particulier les images numériques. De ce fait, l'image numérique devient de plus en plus indispensable dans plusieurs domaines notamment la communication [162].

Dans ce chapitre nous étudions les grandes catégories d'images : les images matricielle (appelées aussi images bitmap ou raster) et les images vectorielles, l'image médicale sera également étudié. Ensuite, nous allons présenter les paramètres d'évaluation les plus connues des systèmes de chiffrement des images numériques.

2.2 L'image matricielle

Ce type d'images est très populaire et le plus répandu, une image numérique matricielle, appelé également l'image BITMAP, peut être considérée comme une matrice ou un ensemble ordonné de données numériques à deux ou trois dimensions. Les indices de ligne et colonne identifient les points dans l'image. Les éléments de la matrice sont les unités élémentaires de l'image, ils sont appelés des pixels (ou "

picture elements ", pixel est une abréviation de PICture ELement) [49, 162]. Si le nombre de lignes de cette matrice est m et n représente le nombre de colonnes, le produit $m \times n$ nous donne la taille de l'image. La résolution d'une image est définie par le nombre de pixels par unité de longueur. Donc, on peut construire une image 2D comme un tableau de valeurs dans lequel on fait correspondre une position sur un plan (x, y) et une couleur pour visualiser l'image sur un support électronique, les format les plus connues : JPEG, PNG, GIF.

2.3 L'image vectorielle

C'est une image numérique composée d'objets géométriques et créée à partir d'équations mathématiques (comme un cercle, arc de cercle, courbe, droite, polygone) et des paramètres (comme la position, les dimensions, la couleur). Chaque objet est définit mathématiquement par des équations et des attributs comme la position, la couleur, etc. Par exemple, l'image vectorielle d'un cercle est définie par des attributs de types : position du centre, rayon, une droite : tracée entre les points (x_1, y_1) et (x_2, y_2). On ne peut pas présenter toutes les images de façon vectorielle, c'est notamment le cas des photos réalistes qui sont des images matricielles. Une image vectorielle ne peut pas être affichée directement sur un écran. Elle doit auparavant être transformée en image de type matricielle.

Ces images sont essentiellement utilisées pour réaliser des schémas ou des plans dans les logiciels industriels de comme : PAO (Publication assistée par Ordinateur), DAO (Dessin Assisté par Ordinateur) , AutoCAD, CATIA, Illustrator et les outils de conception de 3D (comme 3DSMax, Maya). Les formats les plus connus sont : EPS, EMF et WMF (Métafichiers Windows). Contrairement aux images matricielles, les images vectorielles car elles sont constituées uniquement d'entités mathématiques, ont la propriété de pouvoir être agrandies sans limite et sans perte de qualité, chaque ligne et chaque forme est recalculée dynamiquement (Voir les figures 2.1 et 2.2).

2.4 L'image médicale

L'imagerie médicale est un ensemble de techniques consistant à mettre en image les différentes régions du corps humain. L'usage de l'imagerie médicale permet une investigation de plus en plus profonde des organes humains grâce aux systèmes de radiologie de plus en plus performants, sont également utilisées dans la recherche biomédicale pour mieux comprendre le fonctionnement de l'organisme. Les débuts de l'imagerie médicale sont la conséquence des travaux de Wilhelm Röntgen sur les rayons X en 1895, il a réalisé les premiers clichés anatomiques radiographiques sur sa femme Anna Berthe Roentgen. Il reçoit le prix Nobel de physique en 1901. Il existe plusieurs types d'imageries médicales qui sont plus ou moins adaptées en fonction des zones à étudier. On distingue notamment [5] :

— La radiologie, qui utilise les rayons X.

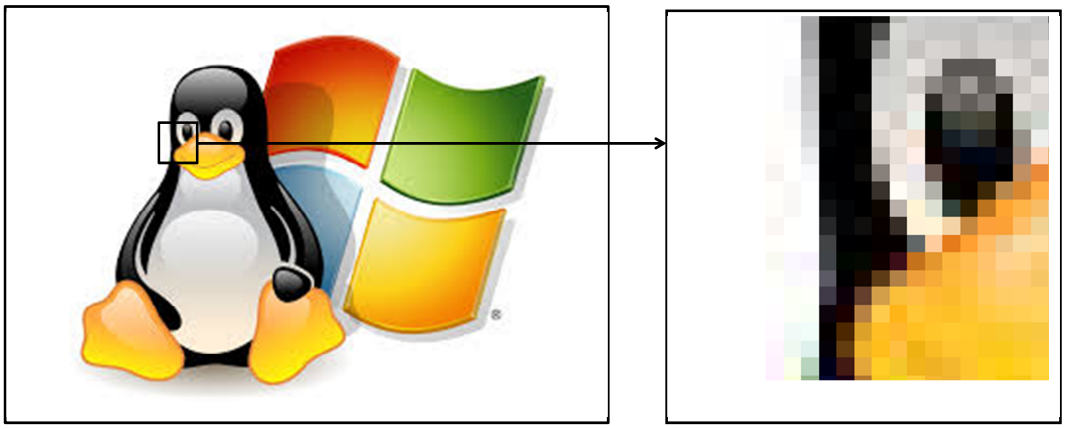


FIGURE 2.1: Exemple d'agrandissement sur une image matricielle.

— L'échographie, qui se sert des ultrasons pour explorer les organes.
— L'imagerie par résonance magnétique (IRM).

Les images médicales sont des images réelles, ils peuvent pas être calculées, donc ils sont des images matricielles, dans la plupart des cas ce sont des images en niveaux de gris. L'évolution des technologies du multimédia et des communications a des conséquences dans le domaine de la santé par la mise à disposition de nouveaux moyens de partage et d'accès distant et comme le PACS (Picture Archiving and Communication Systems), et l'adoption des nouvelles standarts et normes internationales. Le besoin d'un standard est apparu suite au developement des media numériques et des réseaux d'images. La communauté médicale a activement proposé des standards pour échanger numériquement le dossier patient et notamment les images médicales, parmi les objectifs de ces normes, rendre les solutions logicielles plus performantes. Un standart d'échange de l'information médicale est une convention entre les professionnels de la santé pour accéder et échanger de façon fluide et sécurisé les données. Parmi les standarts existant sur le marché on peut citer [37, 115, 135, 161, 180] :

— **DICOM** (Digital Imaging and Communication in Medicine) [41].
— **IHE** (Integrating the Healthcare Enterprise) [86].
— **SIH** (Systèmes d'Information Hospitaliers).
— **SIR** (Systèmes d'Information Radiologique).
— **HL7** (Health Level 7) [79].
— **ACR-NEMA** [83, 136].

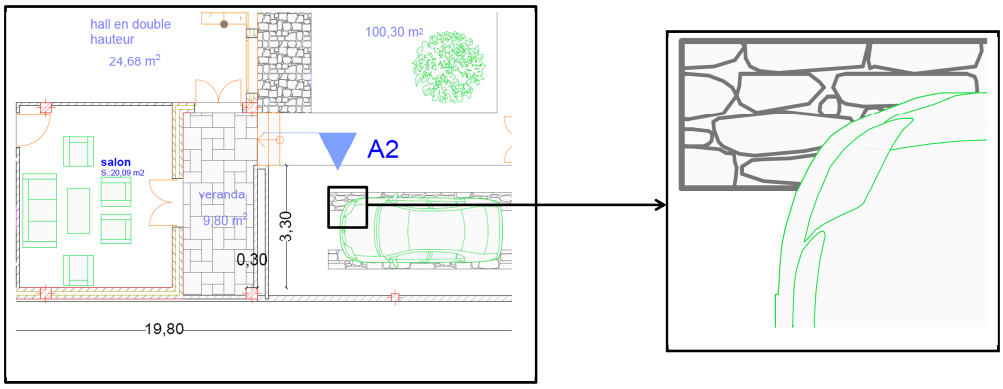


FIGURE 2.2: Exemple d'agrandissement sur une image vectorielle.

2.5 Codage des couleurs

Pour une image numérique, on peut distinguer trois grands types de couleurs [162] (figure 2.3) :

2.5.1 Les images binaires :

Sont des matrices de pixels où le contenu de chaque élément ne peut prendre que les valeurs 0 pour le noir ou 1 pour le blanc. Donc, le nombre de couleurs n'est que de 2 et le rendu de l'image est parfois suffisant dans certains cas.

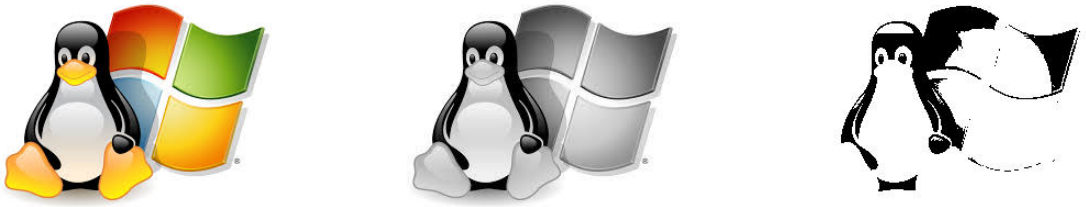
2.5.2 Les images en niveau de gris :

Sont codées généralement sur 8 bits (correspondant à 1 octet), et dans ce cas nous obtenons 256 intensités comprises entre 0 et 255 qui représente respectivement le noir et le blanc. C'est une image qui offre plusieurs niveaux d'intensité allant du noir au blanc. Le codage en niveau de gris offre plus de nuances que le simple noir et blanc.

2.5.3 Les images couleurs :

Dans ce codage l'image est décomposé en générale en trois plans : rouge, vert et bleu. La couleur d'un pixel est obtenue comme le ferait le peintre, en mélangeant les couleurs fondamentales. Chaque pixel est représenté par un vecteur constitué de 3 composantes rouge, vert et bleu qui considère l'image comme une superposition de trois plan monochromes traités indépendamment. L'image couleur peut être codée sur 4 bits (image en 16 couleurs), 8 bits (image en 256 couleurs) ou 24 bits pour une

image en 16 millions de couleur ($16777216 = 2^{24}$). Il existe autres types de codages couleurs, les plus connus sont : TSL, CMY, CIE, YUV et YIQ.



(a) (b) (c)

FIGURE 2.3: (a) Image couleur, (b) Image en niveaux de gris, (c) Image binaire.

2.6 Les méthodes d'évaluation

Chiffrer une image numérique change les pixels par rapport à l'image originale. Un algorithme de chiffrement robuste doit faire ces changements de façon irrégulière et maximiser en même temps la différence entre les valeurs des pixels de l'image original et l'image chiffrée. Autrement dit l'image cryptée doit être indépendante de l'image originale et l'image finale ne doit pas révéler les caractéristiques de l'image claire.

L'une des mesures les plus anciennes et les plus connues est l'inspection visuelle, avec l'avancement des techniques de de cryptanalyse l'inspection visuelle n'est plus suffisante pour examiner la puissance d'un algoritme de chiffrement. Par conséquent, le recours a des facteurs quantitatives est nécessaire pour mieux juger un cryptosysteme [34, 166].

Les facteurs qui mesurent la qualité des techniques de chiffrement peuvent être classées en deux familles [183] :

1. **La corrélation :** Cette famille mesure la capacité de l'algorithme d'avoir une corrélation faible entre l'image claire et l'image cryptée. Dans cette famille cinq mesures serons étudiés : l'histogramme, le coefficient de corrélation, l'entropie, l'écart irrégulier et la résistance au bruit.
2. **La diffusion :** Cette deuxième famille évalue les caractéristiques de diffusion de l'algorithme. Dans Cette famille, deux mesures NPCR et UACI serons étudié.

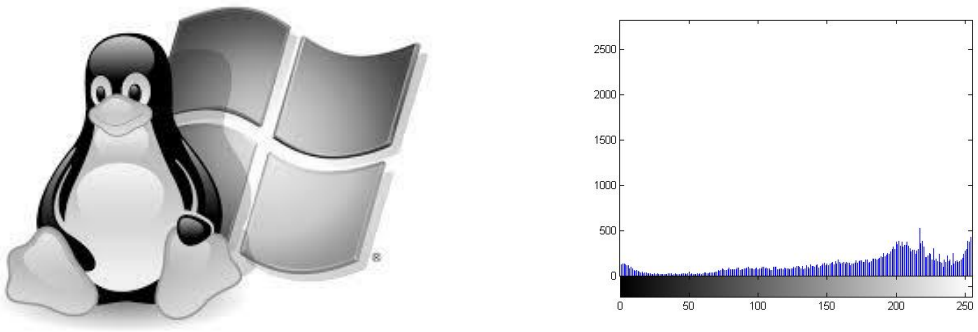
Dans cette section, nous allons discuter les deux familles de paramètres d'évaluation.

2.6.1 Histogramme

L'histogramme d'une image est une fonction discrète qui représente la répartition du nombre de pixels dans une image en fonction de leur intensité (figure 2.4), à

chaque valeur on associe le nombre de pixels dans l'image avec ce niveau. Dans un histogramme chaque barre verticale représente le nombre de fois de niveau de gris correspondant [112, 122]. Dans un schéma de chiffrement on utilise souvent l'histogramme de déviation pour mesurer l'écart entre l'image originale et l'images cryptée [45]. Pour un algorithme de chiffrement fiable, l'histogramme de l'image chiffrée doit avoir les deux propriétés :

1. Il doit être tout à fait différent de l'histogramme de l'image originale.
2. Pour empêcher la fuite d'informations à un adversaire, l'histogramme de l'image chiffrée doit avoir une distribution uniforme.



(a) (b)

FIGURE 2.4: (a) Image de niveaux de gris, (b) Histogramme.

2.6.2 Le coefficient de corrélation

Le coefficient de corrélation détermine la relation et le degré de similitude entre deux variables. Dans un cryptosyteme de chiffrement des images, la corrélation est utilisée pour mesurer la différence de deux images [9, 140, 148], on calcule la corrélation entre les pixels aux mêmes endroits dans l'image claire et l'image chiffrée. La corrélation est une mesure utile pour juger la qualité de chiffrement [13, 84].

Pour un chiffrement fiable le coefficient de corrélation CC doit être très proche du zéro. Ainsi, le succès du processus de cryptage signifie des petites valeurs du CC, et l'image cryptée est totalement aléatoire et hautement non corrélée [13, 165]. Cela garantit que l'algorithme est résistant contre l'attaque de corrélation des pixels.

Si le coefficient de corrélation est proche de 1, cela signifie que l'image originale et l'image chiffrée sont très dépendants et le processus de cryptage a échoué à cacher les détails de l'image originale de sorte que l'image claire peut être reproduite facilement à partir du cryptée [80, 140].

Le coefficient de corrélation peut être obtenu à partir de la formule [196, 70, 85, 112, 148, 12, 140, 80] :

$$CC = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{n=1}^{N} (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{n=1}^{N} (x_i - E(x))^2} \sqrt{\sum_{n=1}^{N} (y_i - E(y))^2}} \tag{2.1}$$

Où $E(x) = \frac{1}{N} \sum_{n=1}^{N} x_i$, x et y sont des valeurs de pixel du même indice de l'image originale et de l'image chiffrée respectivement.

Pour tester la corrélation entre deux pixels adjacents horizontalement (verticalement ou diagonalement) de l'image chiffrée, nous utilisons la même formule où x et y sont les valeurs des deux pixels adjacents. Pour un chiffrement fiable, le coefficient de corrélation des pixels adjacents doit être également très proche du zéro.

2.6.3 L'analyse d'entropie

L'entropie de l'information est un autre facteur non négligeable pour évaluer la résistance d'un système cryptographique. L'entropie de l'information $H(s)$ d'une source s peut être calculée par la formule [202] :

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i) log_2 \frac{1}{P(s_i)} \text{ bits}, \tag{2.2}$$

où $P(s_i)$ représente la probabilité du symbole s_i.

$$P(s_i) = \frac{\text{le nombre de } s_i \text{ dans l'image chiffrée}}{2^N}. \tag{2.3}$$

Par l'entropie, nous pouvons évaluer le degré d'incertitude et le caractère aléatoire du système [195].

Si tous les symboles s_i ont la même probabilité, i.e.

$$P(s_i) = \frac{1}{2^N} \text{ pour } (i = 0, 1, \cdots, 2^N - 1). \tag{2.4}$$

Alors

$$\begin{aligned} H(s) &= \sum_{i=0}^{2^N-1} P(s_i) log_2 \frac{1}{P(s_i)} \text{ bits} \\ &= \sum_{i=0}^{2^N-1} \frac{1}{2^N} log_2 2^N \text{ bits} \\ &= 2^N \frac{1}{2^N} log_2 2^N \text{ bits} \\ &= N \text{ bits}. \end{aligned} \tag{2.5}$$

Pour une image de $2^8 = 256$ intensités, la valeur idéale de l'entropie est $N = 8$. Pour un système de chiffrement résistant aux attaques d'entropie, l'entropie du système de chiffrement doit être proche de la valeur idéale. Cela signifie que la fuite d'informations dans le processus de chiffrement est négligeable et que le système de cryptage est sécurisé contre l'attaque d'entropie. Si la valeur de l'entropie est loin de la valeur idéale, (8 pour une image en niveaux de gris), alors il existe un certain degré de prévisibilité dans le système qui menace la sécurité.

2.6.4 L'écart irrégulier

Les paramètres précédents sont utiles pour juger de la qualité d'un algorithme de chiffrement, mais ils ne sont pas suffisants car qu'ils ne conservent aucune information sur les positions des pixels. Un bon algorithme de chiffrement devrait modifier les positions des pixels d'une manière aléatoire et uniforme. Cela permet d'éviter la situation dans laquelle certains pixels seront soumis à un grand changement alors que d'autres pixels feront l'objet d'un petit changement [80].

L'écart irrégulier repose sur le calcul de la divergence provoquée par le processus de chiffrement [80, 203]. Le calcul de l'écart irrégulier ID peut être résumé dans les étapes suivantes [9, 140, 148] :

1. Trouver la matrice D qui représente la différence absolue entre la valeur des pixels avant et après le chiffrement :

$$D = |I - J| \tag{2.6}$$

2. Construire l'histogramme 'H' de la matrice D :

$$H = \text{histogramme}(D) \tag{2.7}$$

3. Trouver la valeur moyenne M_H de l'histogramme H :

$$M_H = \frac{1}{256} \sum_{i=0}^{255} h_i \tag{2.8}$$

4. Estimer l'écart absolu H_D entre l'histogramme et la valeur moyenne M_H :

$$H_D(i) = |h_i - M_H| \tag{2.9}$$

5. L'écart irrégulier DI est calculé comme suit :

$$ID = \sum_{i=0}^{255} H_D(i). \tag{2.10}$$

L'écart irrégulier ID donne une indication sur la divergence qui a subit chaque pixel de l'image originale [140]. Si l'écart irrégulier est proche d'une distribution uniforme, alors c'est un bon paramètre d'un l'algorithme résistant aux attaques statistiques [80].

2.6.5 Résistance au bruit

Le bruit est présent dans la plupart des images, un bon système de chiffrement doit être robuste contre le bruit. Si l'image décrypté est très similaire à l'image originale, alors le système de cryptage est résistant contre le bruit. Pour mesurer le bruit on compare le $PSNR$ (Peak Signal to the Noise Ratio) de l'image originale et l'image cryptée, le $PSNR$ est donné par la formule [130] :

$$PSNR = 10 \times \log_{10} \frac{255 \times 255 \times M \times N}{\sum_{i=1}^{M} \sum_{j=1}^{N} (P_{ij} - Q_{ij})^2}(dB),$$

où P_{ij} et Q_{ij} sont les pixels de la ligne i et la colonne j de l'image originale et l'image chiffrée, respectivement, M le nombre de lignes et N le nombre de colonnes de l'image.

2.6.6 NPCR et UACI

Dans la cryptographie, la diffusion est une propriété souhaitable qui est introduite par C.E Shannon dans son papier publié en 1949 [35]. Un bon cryptosystème doit assurer une bonne diffusion, cela signifie que si un seul bit du l'image est modifié, le chiffrement devrait changer complètement l'image d'une manière imprévisible. Ce phénomène est appelé également l'effet d'avalanche, un petit changement de clé ou l'image provoque un changement significatif dans l'image cryptée.

Un algorithme robuste doit être très sensible aux petits changements [118, 198]. L'adversaire peut faire un léger changement sur l'image claire, puis observe le changement de résultat. De cette façon, si les paramètres de diffusion sont faibles, il peut trouver une relation significative entre l'image originale et l'image chiffrée.

Si l'algorithme présente une bonne diffusion, la relation entre l'image cryptée et l'image originale est trop complexe et l'attaquant ne peut pas prévoir facilement les changements. Donc cette attaque deviendrait inefficace et pratiquement inutile.

Afin de mesurer la diffusion dans un cryptosystème, on modifie un bit dans l'image claire, puis on calcule la différence résultante du processus de chiffrement [7]. Pour tester l'influence de ce changement deux mesures peuvent être utilisées : $NPCR$ et $UACI$ [16, 26, 122, 148, 201, 91, 87, 82, 199].

Nous prenons deux images cryptées, C_1 et C_2, les images originales correspondant ont un seul pixel de différence. Nous définissons également une matrice D qui a la même taille que C_1 et C_2 :

$$D(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j) \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{2.11}$$

La première mesure est le $NPCR$ (Number of Pixels Change Rate) est définit par la formule :

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%. \tag{2.12}$$

Où M et N sont la largeur et la hauteur de C_1 et C_2 respectivement. Le $NPCR$ mesure le pourcentage des pixels différents dans les deux images. Le $NPCR$ peut également être définie par le taux de variance des pixels dans l'image cryptée provoqués par le changement d'un seul pixel dans l'image originale.

La deuxième mesure est le $UACI$ (Unified Average Change Intensity) est définit par :

$$UACI = \frac{1}{M \times N} \left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100\%. \tag{2.13}$$

$UACI$ mesure l'intensité moyenne de la différence entre les deux images. Le $NPCR$ et le $UACI$ sont conçus pour analyser le nombre de changements de pixels et le nombre de changement moyen d'intensité. Des valeurs de $NPCR$ et $UACI$ grandes indiquent une résistance élevée aux attaques différentielles.

2.7 Conclusion

Dans ce chapitre, nous avons présenté des généralités sur les images numériques, leurs classifications, les standarts d'imagerie médicale les plus répandus. Nous avons parcouru les tests contre les attaques les plus courantes en cryptographie [112, 122, 167, 177]. Il existe d'autres analyses qui peuvent être appliquées, entre autres : le temps de traitement et la sensibilité de la clé.

Dans le chapitre suivant, nous allons aborder les questions liées à la sécurité des images numériques, nous détaillons les deux grandes branches de la cryptologie : la cryptographie et la caryptanalyse.

Chapitre 3

La sécurité

3.1 Introduction

La cryptographie n'est plus utilisée uniquement pour protéger les correspondances diplomatiques et militaires. Aujourd'hui, le chiffrement des images a des applications dans divers domaines, la communication sur internet, systèmes multimédia, l'imagerie médicale et la télémédecine.

La cryptographie a pour but de protéger les données et d'assurer la sécurité des communications et des informations stockées en présence d'un adversaire. Elle propose un ensemble de techniques et d'algorithmes permettant d'offrir des services de confidentialité, d'authentification et d'intégrité. Le mot cryptographie provient du grec "krypto" signifie je cache et "graphe" signifie le document [168].

La cryptologie c'est la science qui étudie la sécurité des données. On peut diviser la cryptologie en deux principales branches : la cryptographie et la cryptanalyse, la cryptographie est un processus qui rend incompréhensible une donnée secrète, et la cryptanalyse et chercher les failles de ce processus.

Dans un tel contexte, la question de la sécurité des données est particulièrement sensible et des solutions de protection des contenus numériques doivent être élaborées, avoir un moyen sûr et fiable pour échanger ces données devient une nécessité et les questions de sécurité doivent être examinées attentivement.

Dans ce chapitre nous étudions la question de sécurité et le chiffrement des données numériques.

3.2 Les termes de base utilisés en cryptographie

La figure 3.1 resume les étapes de chiffrement, un système cryptographique est composé généralement des ensembles suivants :

M : ensemble fini d'objets clairs (plain texts).

C : ensemble fini d'objets chiffrés (cipher texts).

K : ensemble fini de clés (key space).

E : ensemble fini de règles ou de fonctions de chiffrement (encryption rules).

D : ensemble fini de règles ou de fonctions de déchiffrement (decryption rules).

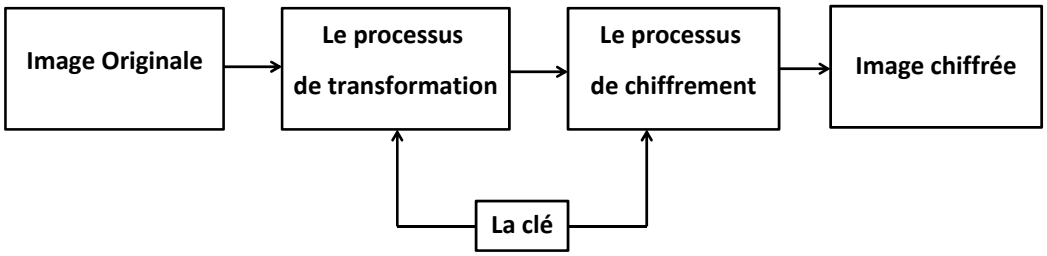


FIGURE 3.1: Les étapes de chiffrement.

Parmi les termes les plus utilisés en cryptographie on peut citer :

Le chiffrement (cryptage) : Un processus de conversion d'objet en clair en objet chiffré, c'est-à-dire transformer une donnée lisible (ou claire) en une donnée illisible ou incompréhensible. L'émetteur doit chiffrer un message M avant de le transmettre, il construit un texte chiffré C au moyen d'une fonction de chiffrement $C = E(M)$ qui dépend d'une clé k.

Le déchiffrement (décryptage) : Le processus inverse de chiffrement, récupération d'une donnée claire à partir d'une donnée chiffrée, la fonction de déchiffrement $D(C)$ possède la propriété d'être l'inverse à gauche de la fonction E. Le processus de déchiffrement nécessite : un algorithme de déchiffrement et une clé.

Cryptosystème : Le système cryptographique, l'ensemble des règles et méthodes pour chiffrer et déchiffrer.

Cryptographie : Une science qui vise à créer des données chiffrées à partir des méthodes de chiffrement.

Cryptanalyse : (Crypto-Analyse) une technique qui étudie les cryptosystème en vue de les rendre messages chiffrés lisibles. Autrement dit, briser les systèmes cryptographiques.

Le message clair (Plaintext) : Ce que nous avons avant le chiffrement, c'est-à-dire l'objet d'origine lisible que la personne souhaite communiquer avec le destinataire.

Texte chiffré (Ciphertext) ou Cryptogramme : Le résultat du processus du chiffrement, ou la donnée en clair transformée qui devienne vide de sens.

Clé (Key) : Une chaine de caractère utilisée au moment de chiffrement et de déchiffrement. La sélection de la clé dans la cryptographie est très importante étant donné que la sécurité de l'algorithme de chiffrement en dépend directement [108] (le principe de Kerchhoffs).

La Stéganographie : Est une branche particulière de la cryptographie consiste à camoufler ou masquer la présence d'un message dans un support (texte, image, etc.).

Le tatouage numérique : ou marquage numérique (watermarking en Anglais) utilisé principalement pour la protection de droit d'auteur. On insert un message (le nom propriétaire ou la marque) dans la donnée, il difficile de supprimer la donnée insérée.

3.3 Les objectifs de la cryptographie

La cryptographie est l'étude des techniques utilisées pour accomplir les quatre objectifs suivants [27, 50] : La confidentialité, l'intégrité, l'authentification et la traçabilité.

Confidentialité : Est le sujet le plus ancien auquel la cryptographie ait tenté de trouver des réponses. C'est l'objectif traité et appliqué tout au long de l'histoire de la cryptographie. La confidentialité consiste à interdire l'accès à des personnes non autorisées. La solution est de rendre les données confidentielles illisibles tout en y assurant que le destinataire pourra retrouver les données originales.

Intégrité : L'intégrité des données garantit que l'information n'a pas été modifiée entre le moment de dépôt et le moment de la récupération, ou entre le moment d'envoi et le moment de la réception. Le but est de détecter facilement les modifications si l'information à été interceptée et modifiée. Le problème de l'intégrité peut apparaître dans le cas du partage de ressources et dans le cas d'envoi d'une donnée sur un canal susceptible d'être non sécurisé. Parmi les instruments de contrôle d'intégrité on trouve les fonctions de hachage (voir la section 3.4.1) et le marquage fragile (voir la section 5.2.3).

Authentification : L'authentification est un problème ancien qui a trouvé des réponses dans la cryptographie moderne. La cryptographie apporte un ensemble de techniques qui permet d'authentifier l'émetteur d'une donnée et de s'assurer de l'identité d'une personne souhaitant accéder à cette donnée.

Traçabilité (non-répudiation) : Dans certains échanges électroniques il n'existe pas de témoignage sur les actions sur les données échangées ou archivées. La traçabilité consiste à tracer toute action sur les documents. Donc c'est une façon d'empêcher une entité de nier la participation dans un échange électronique.

3.4 Classification des schémas cryptographique :

Les algorithmes de chiffrement peuvent être classés de différentes façons ; selon la structure des algorithmes, en fonction des clés, ou selon le pourcentage des données chiffrées [61] (voir la figure 3.2).

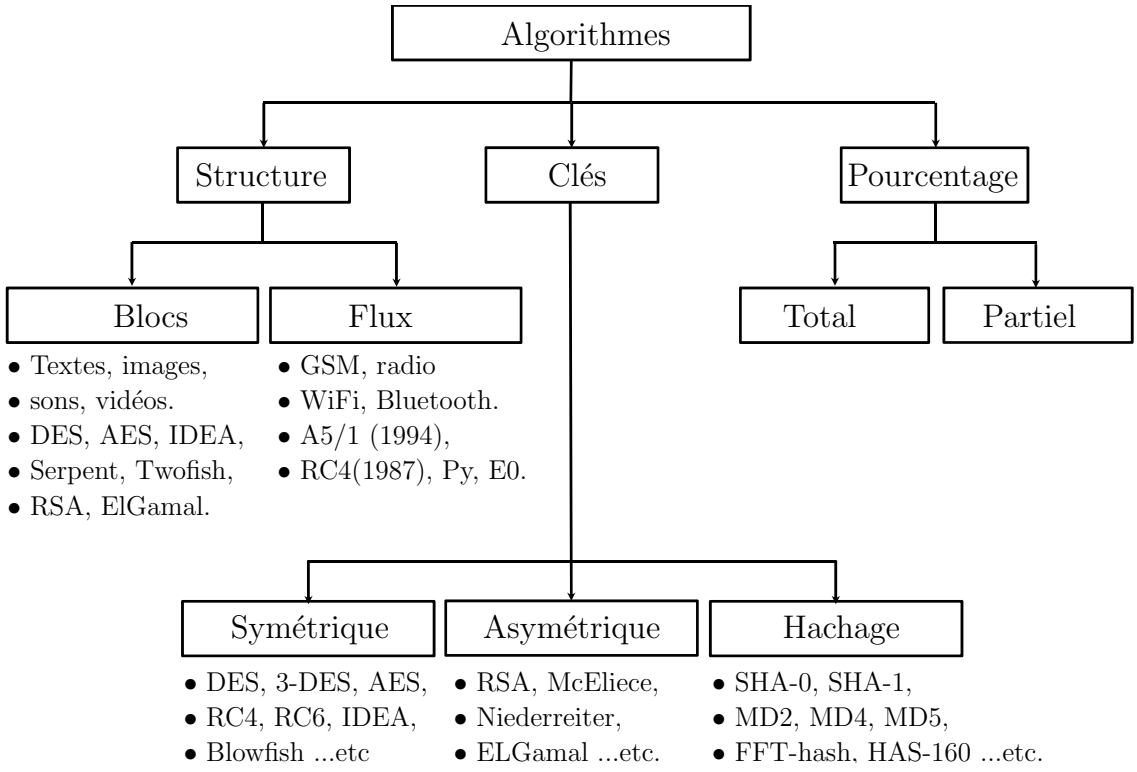


FIGURE 3.2: Classification des schémas cryptographique.

3.4.1 Classification selon les clés

De façon générale, il existe trois types de systèmes de chiffrement, symétriques, asymétrique et le hachage :

1- Chiffrement symétrique

Appelé aussi le chiffrement à clé secrète est la branche la plus ancienne de la science du secret. On utilise la même clé pour chiffrer et déchiffrer, l'expéditeur et le destinataire doivent partager la même clé pour pouvoir effectuer le chiffrement et le déchiffrement (voir la section 3.5).

2- Chiffrement asymétrique

Appelé aussi chiffrement à clé publique est un système où chaque interlocuteur dispose d'une paire de clés, une publique pour le chiffrement et une privée pour le déchiffrement. La cryptographie à clé publique sera présentée avec plus de détail dans la section 3.6.

3- Les fonctions de hachage

On peut définir une fonction hachage appelée parfois fonction à sens unique ou fonction de condensation comme suit :

Définition 3.4.1. *Une fonction mathématique qui associe une donnée de longueur arbitraire à une sortie de taille fixe est dite fonction de hachage.*

La sortie de la fonction hachage est appelée la valeur du hachage ou un résumé de la donnée ou l'empreinte (voir la Figure 3.3). La fonction de hachage doit être à sens unique, c'est-à-dire très difficile ou impossible de trouver la donnée en clair à partir du hach, cette fonction ne demande aucune clé et calcule une empreinte courte de la donnée. Elle doit aussi être sensible pour toute modification, c'est-à-dire une petite modification de la donnée entraîne une grande modification de l'empreinte. Autrement dit, deux données différentes n'ont pas la même valeur de hachage. Parmi les fonctions les plus connues, on peut citer les familles SHA (SHA-0, SHA-1, SHA-2, SHA-3), les familles MD (MD2, MD4, MD5, MD6), FFT-hash, HAS-160, RIPEMD, Whirlpoo ...etc.

Les utilisations les plus courantes des fonctions de hachage sont :

1- La vérification de l'intégrité : Pour vérifier l'intégrité d'une donnée, on teste si la donnée reçue possède le même hach que la donnée originale.

2- La signature numérique : La signature numérique sera plus efficace et plus rapide si on signe le hach de la donnée au lieu de signer la donnée entière.

3- L'authentification : Pour avoir une base de données des mots de passe plus sécurisée, on ne les stocke pas en clair, on stock que le hach. Au moment de l'authentification, on compare le hach de la valeur entrée par l'utilisateur et hach stocké.

Pour plus d'informations sur les fonctions de hachage le lecteur pourra consulter [1, 2, 24, 108, 88, 89, 157, 139, 178].

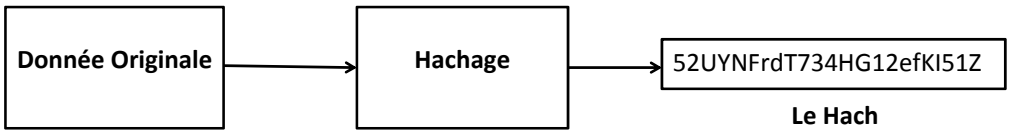


FIGURE 3.3: La fonction de hachage : fournit une empreinte courte de la donnée.

3.4.2 Classification selon la structure de chiffrement

En cryptographie symétrique moderne les algorithmes de chiffrement peuvent être classés en fonction de la structure en deux grandes catégories : chiffrement par blocs et chiffrement par flux.

Chiffrement par blocs :

Le chiffrement par bloc (en anglais block cipher) est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique. Les chiffrements par blocs ont un principe simple, le découpage des données en blocs de taille généralement fixe. Pour chaque bloc X_i de n bits, la taille de bloc est comprise entre 32 et 512 bits, dans le milieu des années 1990 le standard était de 64 bits mais depuis 2000, le standard est devenu 128 bits. Les blocs sont ensuite chiffrés les uns après les autres. L'algorithme de chiffrement est appliqué pour obtenir un bloc chiffré Y_i de même taille, le chiffrement d'un bloc se fait avec la même clé.

Le chiffrement par blocs présente les caractéristiques suivantes [179] :

1. Taille de bloc variable : tailles de blocs inférieur signifient une sécurité élevée.
2. Taille de clé variable : tailles de clés supérieures signifient une sécurité élevée.
3. La multiplication de nombre de tours : augmente la sécurité.

Une liste non-exhaustive de chiffrements par bloc :

1. DES, conçu dans les années 70.
2. AES, le remplaçant de DES.
3. Blowfish, Serpent et Twofish, des alternatives à AES.

Chiffrement par flux :

Le chiffrement par flux, appelé également chiffrement à flot ou chiffrement à la volée (stream cipher en anglais), est la deuxième catégorie de chiffrement moderne en cryptographie symétrique. Contrairement au chiffrement par blocs, le chiffrement par flux, consiste à chiffrer les bits individuellement, il est conçu pour être plus rapide qu'un chiffrement par bloc et économique en terme de ressources. Un chiffrement par flot traite les données de longueur quelconque, il n'a pas besoin de les découper en blocs, ou de lire la donnée en entier ni d'avoir sa longueur au préalable.

Une liste non-exhaustive de chiffrements par flot :

1. A5/1 : publié en 1994, utilisé dans les téléphones mobiles de type GSM, les communications par radio.
2. RC4 : le plus répandu, conçu en 1987 par Ronald Rivest, utilisé notamment sur le WiFi.
3. Py : un algorithme développé par de Eli Biham.
4. E0 : utilisé sur le protocole Bluetooth.

Nous donnons les définitions du générateur de nombres pseudo-aléatoires et l'opérateur logique XOR (le ou exclusif), des outils beaucoup utilisés dans le chiffrement par flot.

Définition 3.4.2. ***Un générateur de nombres pseudo-aléatoires****, pseudorandom number generator (PRNG) en anglais, est un algorithme qui génère une suite de nombres présentant certaines propriétés du hasard.*

Il existe plusieurs types de générateurs de nombres pseudo aléatoires, on peut citer entre autres [27, 54, 101] :

— La méthode de Von Neumann (1946).
— La méthode de Fibonacci.
— La méthode de congruences introduite par Lehmer.
— La méthode Yarrow inventée par Bruce Schneier, John Kelsey et Niels Ferguson.
— Le générateur Fortuna inventé par Bruce Schneier et Niels Ferguson.
— Blum Blum Shub (BBS) proposé en 1986 par Lenore Blum, Manuel Blum et Michael Shub.
— ISAAC son auteur Bob Jenkins (1996).

Exemple 3.4.3.

Générateur Congruentiel Linéaire (LGC) : C'est le plus ancien et le mieux connu, simple à implémenter, temps d'exécution court. Le LGC est une suite mathématique définie de la manière suivante :

$$X_{n+1} \equiv (aX_n + c) \pmod{m} \tag{3.1}$$

Où **mod** désigne l'opérateur modulo : le reste de la division entière.

Le premier élément de la suite est X_0, appelé la graine qui engendrera tous les autres nombres pseudo-aléatoires.

Les coefficients $< a, c, m >$ (respectivement : multiplicateur, incrément, modulo) définissent un Générateur Congruentiel Linéaire.

L'opérateur logique XOR, ou OU exclusif, peut se définir comme suit :

Définition 3.4.4. ***L'opérateur logique XOR :*** *Le résultat est VRAI si les deux opérandes A et B ont des valeurs distinctes.*

$$\textit{Nous écrivons : } X = A \oplus B \tag{3.2}$$

Exemple 3.4.5.

Utilisation de l'opérateur XOR en cryptographie :
$M = 0110101011010100$ (message en clair).
$K = 0101011011100110$ (la clé secrète).
Chiffrement : $C = M \oplus K = 0011110000110010$ (message chiffré).
Déchiffrement : $M = C \oplus K = 0110101011010100$ (message déchiffré).

Dans la plupart des cas dans de chiffrement par flux on opère le XOR entre un bit résultant du PRNG et un bit provenant de la donnée. L'opération XOR est choisi pour sa simplicité [94], il n'est pas la seule opération possible. L'opération d'addition dans un groupe est également envisageable, par exemple : l'addition entre deux octets, modulo 256.

On distingue deux types de chiffrement par flux [17] :

1. **Synchrone :** Le flot de chiffrement se déroule indépendamment du texte.
2. **Auto-synchronisant :** le flot de chiffrement est produit à partir de la clé et d'un nombre fixe de caractères du flux chiffré.

Le chiffrement par flux se caractérise par [169] :

1. La sécurité repose sur les propriétés du PRNG.
2. Le PRNG est imprévisible, le prochain bit est difficile à prévoir.
3. Chiffrements par flux est plus rapide et consomme moins de ressources comparativement avec le chiffrement par bloc.

3.4.3 Classification selon le pourcentage de données cryptées

Les premiers systèmes de chiffrement étaient destinés principalement pour chiffrer les textes, le principe pour ces systèmes est chiffrer le texte entièrement. Avec le changement de mode de communication et l'arrivée du multimédia, les anciens systèmes ne sont plus appropriés pour les images et la vidéo à cause de la quantité et la taille énorme. Les chercheurs ont pensé à d'autres systèmes de chiffrement basés sur le pourcentage de données cryptées pour réduire le coût. En fonction du pourcentage des données cryptées, le chiffrement peut être divisé en deux groupes : chiffrement total et chiffrement partiel.

Le chiffrement total :

Consiste à chiffrer tous les bits de la donnée, dans ce type de chiffrement on ne distingue pas entre les parties sensibles et les parties non sensibles de la donnée. Le processus de chiffrement et de déchiffrement est lent. Ce type consomme plus de ressources, il est coûteux en terme de temps, d'où la naissance du chiffrement partiel.

Le chiffrement partiel :

Le chiffrement partiel ou sélectif est une approche récente qui a pour but réduire le temps de calcul. Il consiste à chiffrer uniquement un sous-ensemble des données. L'objectif du chiffrement sélectif est de réduire la quantité de données à crypter tout en conservant un niveau de sécurité suffisant. Par exemple, pour les images médicales, pour avoir un bon niveau de confidentialité, au minimum 12.5% des données doivent être chiffrées [172]. Dans la vidéo surveillance, il suffit juste de cacher les visages. Pour les images captées par les radars de contrôle de vitesse ou le contrôle d'accès, il suffit de chiffrer la zone où se trouve l'information.

De nombreuses recherches ont proposé des algorithmes qui combinent le chiffrement sélectif avec d'autres processus tel que la compression pour réduire le temps de traitement global [46, 137, 200]. Pour plus d'informations sur le chiffrement sélectif et les algorithmes proposés le lecteur pourra consulter [23, 77, 149, 150, 125, 126, 172].

3.5 Cryptographie symétrique :

Ou le chiffrement à clé secrète est la plus importante branche et la plus utilisée dans nos jours à cause de sa rapidité et la simplicité d'implémentation. Dans cette branche on utilise la même clé pour chiffrer et déchiffrer, l'expéditeur et le destinataire doivent partager la même clé pour pouvoir éffectuer le chifrement et le déchiffrement (voir la figure 3.4), cette clé est appelée "clé secrète" et doit être échangée via un canal sécurisé. Les algorithmes symétriques les plus connues sont le DES, 3-DES, AES, RC4, RC6, Blowfish ...etc [94, 138, 189, 77].

La sécurité du système symétrique repose sur l'algorithme lui-même et la clé secrète, le plus gros problème de cette technique est l'échange de la clé secrète, ce problème d'échange de la clé est spécifique de la cryptographie symétrique. La sécurité d'un tel système dépend de la clé, également dépend de la longueur de clé, plus la clé est longue plus le système est sûr.

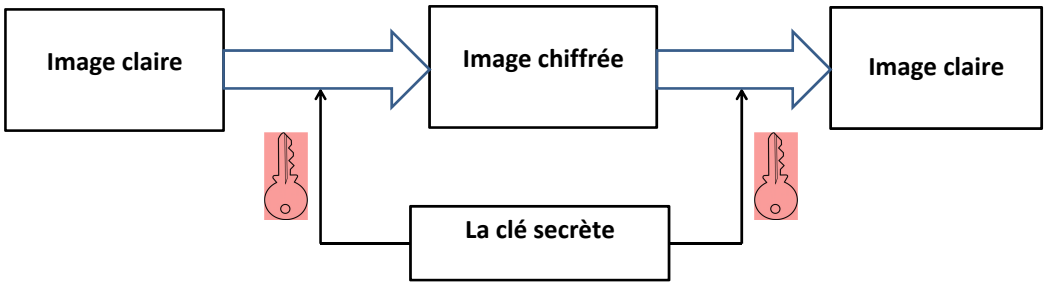


FIGURE 3.4: Le chiffrement symétrique.

3.5.1 Data Encryption Standard (DES)

Nous décrivons dans cette section le "Data Encryption Standard" qui a été l'un des systèmes de chiffrement les plus utilisés. Notamment pour chiffrer les mots de passe sous Unix. Le DES a été conçu dans les années 70 par IBM pour être un système de chiffrement à clé secrète (à l'époque sûr). Le DES utilise des clés de 56 bits. Son emploi n'est plus recommandé aujourd'hui, du fait de sa lenteur à l'exécution et de son espace de clés trop petit.

Quand il est encore utilisé c'est généralement en Triple DES, ce qui ne fait rien pour améliorer ses performances. Le premier standard DES est publié par FIPS le 15 janvier 1977 sous le nom FIPS PUB 46 [27, 50].

Historique

En 1975, DES est officialisé, deux ans plus tard DES devient un standard FIPS le 15 janvier 1977 sous le nom FIPS PUB 4. Ce système de chiffrement symétrique fait partie de la famille des chiffrements itératifs par blocs, plus particulièrement il s'agit d'un schéma de Feistel (du nom de Horst Feistel à l'origine du chiffrement Lucifer). DES a été construit pour fonctionner aussi bien de façon logicielle que matérielle.

En 2005 DES est retiré des standards FIPS suite à plusieurs attaques réussies. Ainsi, en 1998 la clé DES à été cassé en 56 heurs, puis en Janvier 1999, l'EFF (Electronic Frontier Foundation) et DCTI (Distributed Computing Technologies, Inc) ont collaboré pour casser une clé DES en 22 heures et 15 minutes.

Fonctionnement

L'algorithme DES transforme un bloc de 64 bits en un autre bloc de 64 bits. Il manipule des clés de 56 bits [50].

3.5.2 L'algorithme AES (Advanced Encryption Standard) :

Adopté par le gouvernement des États-Unis en 2001. AES est l'œuvre de deux chercheurs belges Joan Daemen et Vincent Rijmen pour remplacer les algorithmes DES et 3DES [94], facile à implémenter, consomme peu de mémoire et flexible pour supporter des clés de 128, 192 ou 256 bits. L'algorithme AES est un ensemble d'étapes répétées plusieurs fois (tours), ces étapes sont des transformations linéaires et non-linéaires. Le nombre de tours dépend de la taille de la clé et de la taille des blocs [189] (voir le tableau 3.1).

L'algorithme AES est composé de quatre opérations de base (voir la figure 3.6) fonctionnent sur un tableau d'octets organisés en une matrices 4×4. Pour le chiffrement total, les données sont transmises par nombre de tours ($Nr = 10, 12, 14$). Ces tours sont régies par les transformations suivantes [77, 94, 189] :

Algorithm 1: DES

Début

1. Inputs : Un message M de 64 bits, une clé K de 56 bits.
2. Output : Un cryptogramme C de 64 bits.
3. Une permutation initiale IP donnant le message "permuté" M.
4. Découper M en deux parties de 32 bits : L qui représente la partie gauche, R la partie droite.
5. Exécuter 16 itérations de la fonction f (figure 3.5), ces itérations combinent des opérations de substitutions et des transpositions en trois étapes :
   (a) **Étape 1 :** Appliquer au bloc une permutation initiale IP.
   (b) **Étape 2 :** Modifier les parties gauches et droites comme suit :

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \text{ pour } 1 \leq i \leq 16.$$

   f une fonction qui prend en entrée les 32 bits de la partie droite et 48 bits de la clé de tour et fournit une sortie de 32 bits. La fonction f est définie en utilisant huit permutations appelées S-boxes [17, 27, 50] (S pour substitution en anglais) qui associent à 6 bits d'entrée 4 bits de sortie. Chaque clé de tour K_i contient un sous-ensemble différent des 56 bits de la clé et on obtient un pré-cryptogramme $C = (R_{16}, L_{16})$.
   (c) **Étape 3 :** Enfin, le pré-cryptogramme $C = (R_{16}, L_{16})$ subit la permutation inverse de la permutation initiale IP^{-1} et donne le cryptogramme final.

Fin.

	La longueur de la clé	La taille de bloc	Le nombre de tours
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

TABLE 3.1: AES : Le nombre de tours/la taille de la clé/la taille des blocs

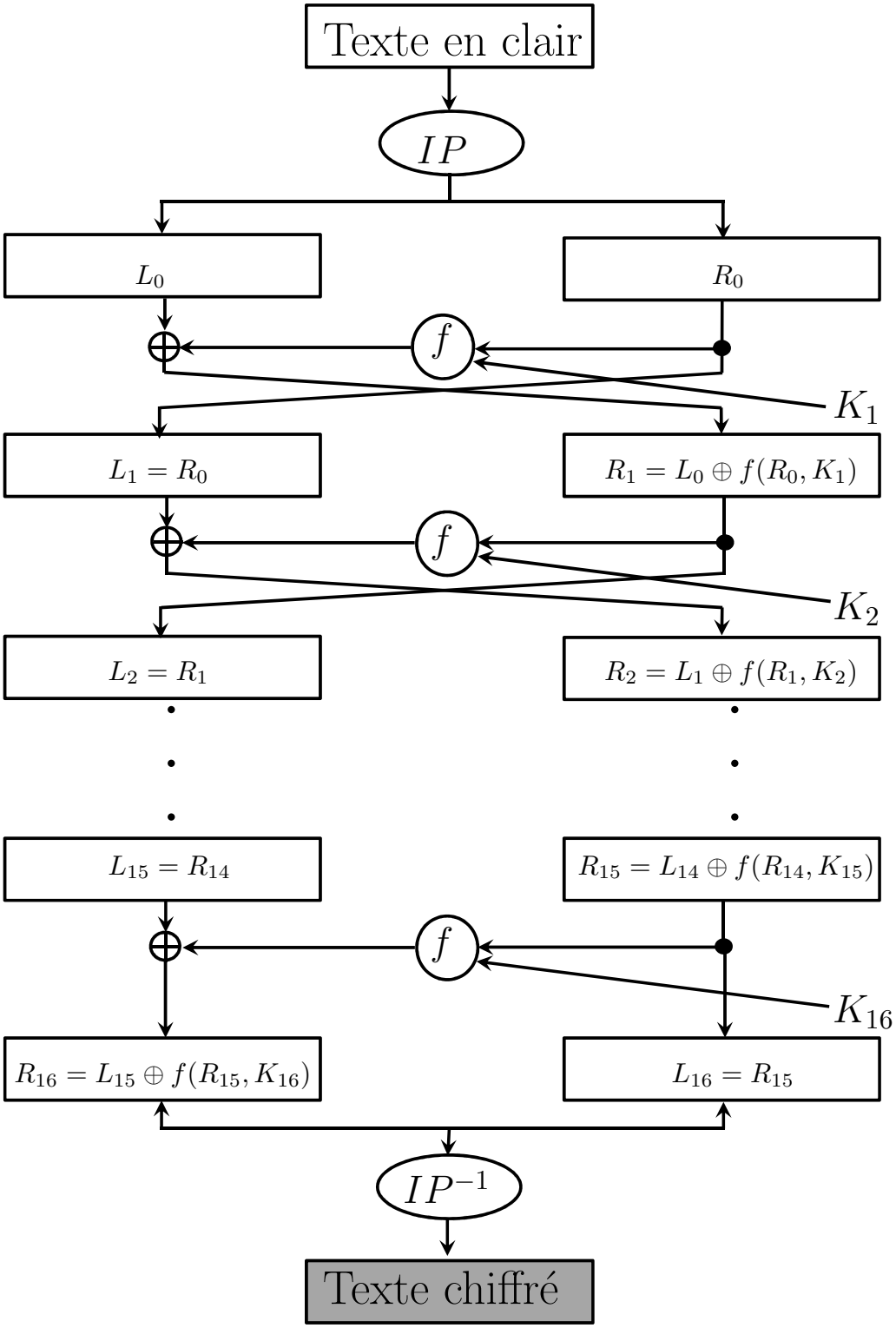


FIGURE 3.5: L'algorithme DES.

(i) SubBytes : Une transformation non linéaire des octets. Chaque octet est remplacé par une matrice dite "s-box".

(ii) ShiftRows : Il s'agit d'un simple décalage cyclique de chaque ligne de la matrice de données vers la gauche.

(iii) MixColumns : Combinaison linéaire de la matrice, où la matrice de données est multipliée par une autre matrice pour réordonner les colonnes.

(iv) AddRoundKey : Est un simple XOR (le ou exclusif) entre la donnée et une partie de clé secrète.

3.6 Cryptographie à clé publique :

Le chiffrement asymétrique appelé également chiffrement à clé publique est un système où chaque interlocuteur dispose d'une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement. La théorie du système asymétrique, publiée par Diffie et Hellman en 1976 [186] a marqué le début de la cryptologie moderne. Ils ont inventé une nouvelle idée pour crypter, chaque utilisateur a deux clés différentes, une privée et une autre publique (c.f Fig 3.7). Les clés sont nécessaires pour le processus de chiffrement et de déchiffrement de telle sorte que la connaissance de la clé publique ne permette pas de retrouver facilement la clé privée. Plus précisément si le propriétaire de la paire de clés diffuse la clé publique, mathématiquement il est impossible de déduire la clé privée à partir de la clé publique. Donc le propriétaire est la seule personne capable de déchiffrer un document chiffré puisque seule la clé privée peut déchiffrer. Parmi les algorithmes asymétriques on peut citer le RSA [156], McEliece, Niederreiter [179], ELGamal [181] ...etc.

Cette branche de la cryptographie présente deux intérêts majeurs :

1. Elle supprime le problème de transfère sécurisé de la clé.
2. Elle permet l'implémentation de la signature électronique (voir la Section 3.6.9).

Le chiffrement asymétrique ne remplace pas le chiffrement symétrique, les algorithmes asymétriques nécessitent un temps de calcul important contrairement aux algorithmes symétriques. Il n'est pas préférable d'utiliser le chiffrement asymétrique pour un volume important de données comme des images, par exemple le RSA est 1500 fois plus lent que l'algorithme symétrique DES [50]. Le tableau (3.6) présente les différences entre le chiffrement symétrique et le chiffrement asymétrique [190].

On va présenter dans cette section le principe général du chiffrement à clé publique et les outils métamathématiques nécessaires, l'algorithme du système RSA sera également présenté avec des exemples [17, 50, 73, 114].

Un cryptosystème à clef publique s'appuie sur une fonction dite à sens unique, elle même basée sur le problème suivant dit "Le problème du logarithme discret".

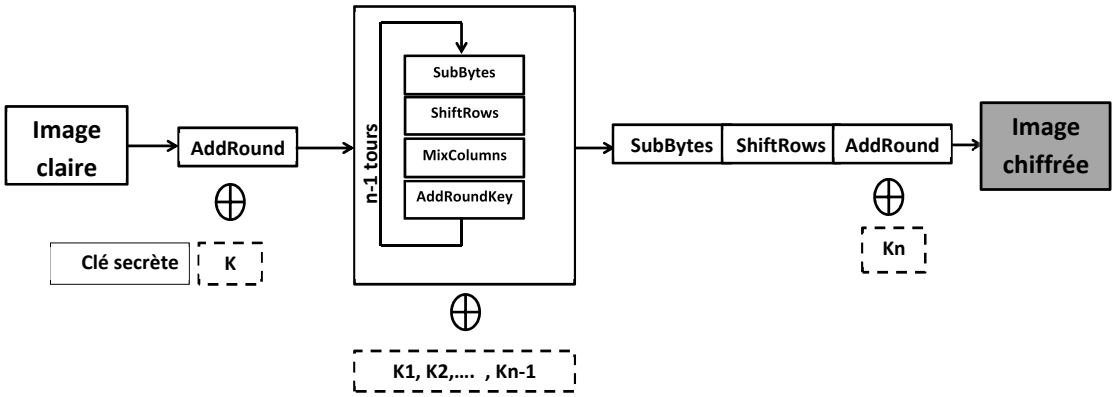


FIGURE 3.6: L'algorithme AES.

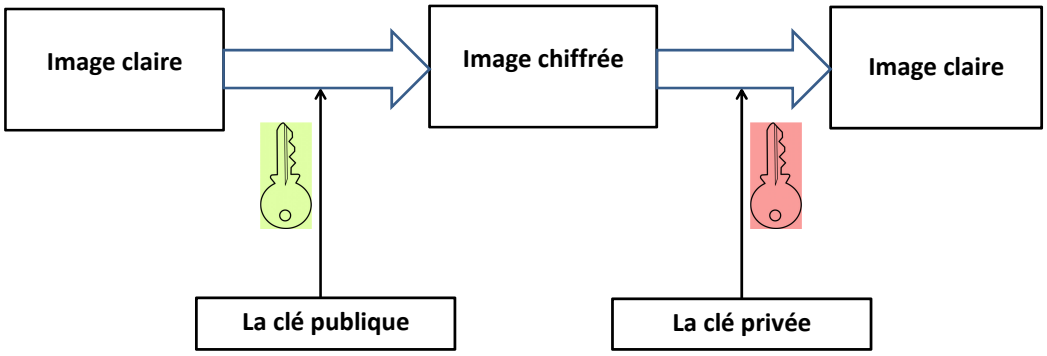


FIGURE 3.7: Le chiffrement asymétrique

Le chiffrement symétrique	Le chiffrement asymétrique
1. Le même algorithme avec la même clé peut être utilisé pour le chiffrement et le déchiffrement. 2. L'expéditeur et le destinataire doivent partager l'algorithme et la clé. 3. La clé doit être gardée secrète. 4. Il doit être impossible de déchiffrer si la clé et l'algorithme ne sont pas disponible. 5. La connaissance de l'algorithme et des échantillons de la donnée chiffrée doit être insuffisante pour déterminer la clé. 6. Algorithme rapide et consomme moins de ressources.	1. Le même algorithme est utilisé dans le processus avec un couple de clés, une clé pour le chiffrement et l'autre pour le déchiffrement. 2. L'émetteur et le récepteur doivent avoir chacun une paire de clés. 3. La clé de déchiffrement doit être gardée privée. 4. Il doit être impossible de déchiffrer si la clé et l'algorithme ne sont pas disponibles. 5. Pour un récepteur légitime la connaissance de l'algorithme et la clé de chiffrement et des échantillons de la donnée chiffrée doivent être suffisantes pour déterminer la clé de déchiffrement. 6. Plus lent que le chiffrement symétrique [27].

TABLE 3.2: Comparaison chiffrement symétrique/asymétrique

3.6.1 Le problème du logarithme discret :

Soit G un groupe cyclique d'ordre n engendré par $g \in G$, i.e. :

$$G = g_0,\ g,\ g_2, \cdots,\ g_{n-1},$$

et $g_n = g_0 = 1$, le neutre de G.

Définition 3.6.1. ***Le problème du logarithme discret :*** *Soit G un groupe cyclique d'ordre n engendré par g. Le problème du logarithme discret sur G est le suivant :*

$$g \in G \text{ et } y \in < g >,\ \textit{trouver un entier } x \textit{ tel que } g^x = y. \tag{3.3}$$

Pour les groupes multiplicatifs de $GF(p)$ ou $GF(p^2)$ avec p et g fixe choisis avec soin, l'algorithme rapide pour résoudre le problème du logarithme discret prend un temps d'exécution "sous-exponentiel" [134]. Par conséquent, un système cryptographique dans lequel la sécurité est fondée sur le problème du logarithme discret est considéré comme sûr.

Les théorèmes suivants expriment la difficulté théorique du problème du logarithme discret [134].

Théorème 3.6.2. ***[Shoup, 1997]*** *Dans un groupe générique d'ordre n premier, la résolution du problème du logarithme discret nécessite au moins $\sqrt{n}$ multiplications.*

Théorème 3.6.3. *Soit p un nombre premier. Il existe un algorithme sous-exponentiel avec $a = 1/3$ qui permet de résoudre le problème du logarithme discret dans les groupes du type $(\mathbb{Z}/p\mathbb{Z})^\star$.*

3.6.2 Les fonctions à sens unique :

Définition 3.6.4. ***La fonction à sens unique :***
Considérons deux ensembles arbitraires X et Y et une fonction $f : X \longrightarrow Y$.
Soit $f(X)$ l'ensemble image de l'ensemble X par f.
La fonction f est dite ***à sens unique*** *si pour tout x de X, il est facile de calculer $f(x)$ et s'il est difficile de trouver, pour la plupart des $y \in f(X)$ un $x \in X$ tel que $f(x) = y$.*

Exemple 3.6.5. *Soit $X = Y = \mathbb{Z}_{29}$, considérons la fonction f définie par :*

$$f : X \longrightarrow Y$$

$$x \longmapsto f(x) \equiv 2^x \pmod{29} \tag{3.4}$$

(a) *Nous calculons facilement $f(5)$, nous avons besoin de 3 opérations pour calculer $f(5) = 2^5 \pmod{29}$, en effet :*

1. *Nous pouvons calculer d'abord : $2^2 = 2 \times 2 = 4$.*

2. *Ensuite :* $2^4 = 4 \times 4 = 16$.

3. *Enfin :* $2^5 = 16 \times 2 = 32 \equiv 3 \pmod{29}$.

(b) *D'autre part, nous avons besoin de* 22 *multiplications pour calculer l'image inverse de* 5, *i.e, trouver* $x \in X$ *tel que* $f(x) = 5$, *en effet :*
$2^1 \equiv 2 \pmod{29}$, $2^2 \equiv 4 \pmod{29}$, $2^3 \equiv 8 \pmod{29}$, $\cdots$, $2^{22} \equiv 5 \pmod{29}$.

Exemple 3.6.6. *Un autre exemple plus complexe, considérons la fonction :*

$$f(x) \equiv 3^x \pmod{n} \tag{3.5}$$

Où $n = 279983311221378 \cdots\cdots\cdots\cdots 1823983$ *un nombre très grand.*
Calculer l'image inverse est beaucoup plus compliqué que de calculer l'image directe.

3.6.3 Les fonctions à trappe :

Définition 3.6.7. *Une fonction à sens unique* $f : X \longrightarrow Y$ *est dite* ***à trappe*** *si :*
- *Elle peut être calculée efficacement dans le sens direct.*
- *Le calcul dans le sens inverse est aussi possible si on dispose une information secrète -la trappe- qui permet de construire une fonction* g *telle que* $g \circ f = Id$.
- *Il est facile de calculer l'image par* f *de n'importe quelle entrée mais calculatoirement impossible d'inverser* f *sans connaître* g.
- *Il doit être facile de générer des couples* (f, g).
- *La publication de* f *ne doit rien révéler sur* g.

Exemple 3.6.8. *L'exemple le plus élémentaire d'une fonction à trappe est la factorisation d'un entier.*
Considérons $f(p, q) = p \times q$ *où* p *et* q *deux nombres premiers. Il est simple de calculer* $f(1093, 1039) = 1135627$.
Pour calculer l'image inverse de 1135627 *pourrait prendre plus de temps. Si les deux nombres premiers sont choisis suffisamment grand même plusieurs d'ordinateurs ne sont pas suffisants pour arriver aux deux facteurs.*

3.6.4 L'algorithme d'Euclide étendu :

L'algorithme d'Euclide est utilisé pour calculer du $PGCD$ de deux entiers positifs a et b, il s'agit d'une divisions en cascade, les résultats de l'une servent pour la suivante, le reste trouvé avant le reste nul est le $PGCD$ (Plus Grand Commun Diviseur). L'algorithme d'Euclide étendu est particulièrement utilisé lorsque on souhaite calculer calculer l'inverse de $b \pmod{n}$ s'il existe et les coefficients de Bézout.

Définition 3.6.9. *L'inverse* $b \pmod{n}$ *est le nombre entier* b^{-1} *tel que :*

$$b \cdot b^{-1} \pmod{n} = 1.$$

Définition 3.6.10. *Les coefficients de Bézout sont deux entiers u et v tels que :*

$$au + bv = PGCD(a, b).$$

Proposition 3.6.11. *Un entier a est inversible modulo n si et seulement si :*

$$PGCD(a, n) = 1$$

.

Exemple 3.6.12. *Pour calculer* $12^{-1} \pmod{67}$.
Remarquons que le $PGCD(12, 67) = 1$, *en effet, par l'algorithme d'Euclide on trouve :*

$$\begin{aligned} 67 &= 5 \cdot 12 + 7 \\ 12 &= 1 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

En suite on cherche les coefficients de Bézout (on repars en arrière) :

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(7 - 5) \\ &= -2 \cdot 7 + 3 \cdot 5 \\ &= -2 \cdot 7 + 3(12 - 7) \\ &= 3 \cdot 12 - 5 \cdot 7 \\ &= 3 \cdot 12 - 5(67 - 5 \cdot 12) \\ &= -5 \cdot 67 + 28 \cdot 12. \end{aligned}$$

Nous avons :

$$\begin{aligned} -5 \cdot 67 + 28 \cdot 12 &= 1 \\ 28 \cdot 12 &\equiv 1 \pmod{67} \\ 28 &\equiv 12^{-1} \pmod{67}. \end{aligned}$$

Donc l'inverse de $12 \pmod{67}$ *est* 28.

3.6.5 Le théorème des restes chinois :

Nous donnons le théorème des restes chinois utilisé dans l'algorithme RSA.

Théorème 3.6.13. *Soient $m_1, m_2 \cdots, m_n$ des entiers supérieurs à 2 deux-à-deux premiers entre eux. Alors, pour tous entiers $a_1, a_2 \cdots, a_n$ des entiers, le système*

d'équations :

$$\begin{cases} x = a_1 \pmod{m_1} \\ x = a_2 \pmod{m_2} \\ \cdot \ \cdot \ \cdot \\ \cdot \ \cdot \ \cdot \\ \cdot \ \cdot \ \cdot \\ x = a_n \pmod{m_n} \end{cases}$$

admet une unique solution x modulo :

$$M = m_1 \times \cdots \times m_n$$

et qui est donnée par la formule :

$$x = a_1 M_1 y_1 + \cdots + a_n M_n y_n$$

où $M_i = \frac{M}{m_i}$ et $y_i = M_i^{-1} \pmod{m_i}$ pour tout i compris entre 1 et n.

Exemple 3.6.14. *Pour trouver x le plus petit entier positif tel que :*

$$\begin{cases} x = 3 \pmod{17} \\ x = 4 \pmod{11} \\ x = 5 \pmod{6} \end{cases}$$

On applique le théorème chinois on a :

$$\begin{cases} M = 17 \times 11 \times 6 = 1122 \\ M_1 = 66 \\ M_2 = 102 \\ M_3 = 187 \end{cases}$$

L'inversion de M_1, M_2 et M_3 par l'algorithme d'Euclide donne :

$$\begin{cases} y_1 = 8 \\ y_2 = 4 \\ y_3 = 1 \end{cases}$$

Donc la solution x :

$$x = 3 \times 66 \times 8 + 4 \times 102 \times 4 + 5 \times 187 \times 1 \pmod{1122} = 785 \pmod{1122}.$$

3.6.6 Procédé de Diffie-Hellman d'échange publique des clés :

C'est une méthode par laquelle deux personnes nommées conventionnellement *Alice* et *Bob* peuvent se mettre d'accord sur un nombre (clé de chiffrement) sans qu'une troisième personne appelée *Oscar* puisse découvrir ce nombre en écoutant.

On s'intéresse ici au cryptosystème à **"clefs publiques"** utilisé pour un échange publique de clé, dit protocole de **Diffie-Hellman** du nom de ses deux inventeurs Diffie et Hellman [186]. Ce cryptosystème est celui induit par la fonction modulaire à sens unique définit par :

$$\mathbb{Z} \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\star$$

$$x \longmapsto f(x) = g^x \tag{3.6}$$

où p est premier et suffisamment grand pour que le problème du calcul de logarithme discret soit "difficile". L'élément g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\star$.

Le principe de cet algorithme se résume dans les points suivants :

1. *Alice* et *Bob* conviennent à un p premier très grand, de tel sorte que le calcul du logarithme discret dans $(\mathbb{Z}/p\mathbb{Z})^\star$ est un "problème difficile", dont g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\star$, qui seront publiques.
2. *Alice* choisit une clé privée a, et envoie à Bob : $g^a \pmod p$.
3. *Bob* choisit une clé privée b, et envoie à Alice : $g^b \pmod p$.
4. *Bob* et Alice utilisent leurs clés privées pour trouver la clé de chiffrement commun : $k = (g^a \pmod p)^b \pmod p = (g^b \pmod p)^a \pmod p$.

Exemple 3.6.15. *Un exemple explicite de l'opération :*

1. *Alice et Bob conviennent à un groupe d'ordre* $p = 23$ *et* $g = 3$ *un générateur de* $(\mathbb{Z}/p\mathbb{Z})^\star$.

2. *Alice choisit un nombre secret* $a = 6$.

3. *Alice envoie à Bob la valeur :* $g^a \pmod p = 3^6 \pmod{23} = 16$.

4. *Bob choisit à son tour un nombre secret* $b = 15$.

5. *Il envoie à Alice la valeur :* $g^b \pmod p = 3^{15} \pmod{23} = 12$.

6. *Alice et Bob peuvent maintenant calculer la clé secrète :*
   $(3^{15} \pmod{23})^6 \pmod{23} = (3^6 \pmod{23})^{15} \pmod{23} = 9$.

Le procédé de Diffie-Hellman peut être étendu sur un groupe d'utilisateurs, on appelle ce groupe les utilisateurs autorisés. Ces utilisateurs peuvent se mettre d'accord sur une clé de chiffrement sans qu'une personne hors de ce groupe puisse la découvrir.

3.6.7 L'algorithme RSA (Rivest, Shamir Adleman) :

On s'intéresse ici au cryptosystème à "clefs publiques", dit RSA du nom de ses trois inventeurs Rivest, Shamir et Adleman [156]. Le premier système asymétrique solide et le plus populaire pour le chiffrement des données numériques. L'algorithme RSA a été publié en 1977 par Ron Rivest, Adi Shamir et Len Adleman de l'Institut de Technologie du Massachusetts (MIT). RSA est basé sur la difficulté de factoriser de grands nombres premiers, c'est-à-dire. la décomposition en produit de facteurs premiers. Par exemple factoriser un nombre à 200 chiffres demande 4 milliards d'années de calcul machine. Ce cryptosystème est celui induit par la fonction modulaire à sens unique et à trappe définit par :

$$\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

$$x \longmapsto f(x) = x^e$$

où n et e sont fixés.

Depuis sa parution, le cryptosystème RSA a fait l'objet de nombreuses études mettant en évidence certaines vulnérabilités, mais aucune n'a permis un cassage total. Les attaques mises en œuvre ont surtout montré le danger d'une utilisation incorrecte de RSA.

Les opérations de base de RSA sont : la génération des clefs, le chiffrement et le déchiffrement (voir l'algorithme 2) :

La génération des clefs :

Contrairement au chiffrement symétrique, le chiffrement à clé publique utilise une paire de clés, publique K_{pub} et privée K_{pr}, la fabrication des clés se fait comme suit :

1. Choisir des grands nombres premiers p et q (généralement plus de 100 chiffres).
2. Calculer $n = pq$.
3. Calculer la fonction d'Euler $\varphi(n) = (p-1)(q-1)$.
4. Choisir un entier $e \in \mathbb{Z}^\star$, tel que :

$$\text{PGCD } (e, \varphi(n)) = 1. \tag{3.7}$$

5. Choisir un nombre d, tel que $d.e \equiv 1 \pmod{\varphi(n)}$.

   La clé publique : la paire (n, e), permet à chacun de chiffrer un message.
   La clé privée : la paire (n, d), permettant à celui qui la possède de déchiffrer un message chiffré.

Remarques :

1. $\varphi(n)$ est l'ordre du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\star$.

2. On appelle n le module RSA.
3. On appelle e l'exposant de chiffrement et d l'exposant de déchiffrement.
4. On appelle $\varphi(n)$ la fonction ou l'indicateur d'Euler.
5. Le calcul $d = e^{-1} \pmod{n}$ se fera en utilisant l'algorithme d'Euclide étendu 3.6.4.
6. Seule la personne possédant l'exposant privé de déchiffrement peut déchiffrer le message.

Le processus de chiffrement :

Si M est le message claire $M < n$, Pour chiffrer $M \in \mathbb{Z}/n\mathbb{Z}$, on calcule le cryptogramme C comme suit :

$$C = M^e \pmod{n}. \tag{3.8}$$

Ainsi, comme le module n et l'exposant e sont publiques, tout le monde peut chiffrer un message pour le destinataire ayant comme clé publique (n, e).

L'algorithme de chiffrement RSA conduit à définir la fonction de chiffrement :

$$\begin{aligned} f : (\mathbb{Z}/n\mathbb{Z})^\star &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^\star \\ x &\longmapsto x^e \pmod{n}. \end{aligned} \tag{3.9}$$

Le processus de déchiffrement :

Si l'entier d est connu, la fonction de chiffrement RSA f peut être facilement inversée :

$$f^{-1}(y) = y^d \pmod{n}. \tag{3.10}$$

ou encore

$$\begin{aligned} f^{-1} : (\mathbb{Z}/n\mathbb{Z})^\star &\longrightarrow (\mathbb{Z}/n\mathbb{Z})^\star \\ x &\longmapsto x^d \pmod{n}. \end{aligned} \tag{3.11}$$

Pour déchiffrer le cryptogramme $C = M^e$, on calcule :

$$M = C^d \pmod{n}. \tag{3.12}$$

Seule la personne possédant la clé privée (n, d) de déchiffrement peut déchiffrer le message.

Exemple 3.6.16. ***Le chiffrement RSA :***

La génération des clefs :

1. Bob choisit les nombre premiers $p = 101$ et $q = 113$.

Algorithm 2: RSA

Début

1. **Généralement de la paire de clés :**
   — Choisir des grands nombres premiers p et q.
   — La clé privée : Le couple (p, q), les deux nombres premiers p et q.
   — la clé publique : Le couple (n, e), $n = pq$ et un entier e premier avec $\varphi(n) = (p-1)(q-1)$.
2. **Chiffrement :** Si M le texte clair et C le texte chiffré :

$$C = M^e \pmod{n}.$$

3. **Déchiffrement :** S'appuie sur la fonction inverse :

$$M = C^d \pmod{n},$$

tel que $e.d = 1 \bmod \varphi(n)$

Fin.

2. Donc l'exposant RSA $n = p.q = 11413$ et la fonction d'Euler $\varphi(n) = 100 \times 112 = 11200$.
3. Bob peut choisir $e = 3533$ comme exposant de chiffrement. Il vérifie en utilisant le théorème des restes chinois que $PGDC(\varphi(n), e) = 1$, en même temps il calcule $d = e^{-1} \bmod \varphi(n)$.

$$d = e^{-1} \pmod{11200} = 6597.$$

Donc

$$d = 6597.$$

La clé publique de Bob : $(n, e) = (11413, 3533)$.
La clé privée de Bob : $(n, d) = (11413, 6597)$.

Le chiffrement :
Bob publie sa clé publique $(n, e) = (11413, 3533)$, Alice souhaite envoyer le message claire $M = 9726$ à Bob. En général on envoie le code ASCII du message et le récepteur recevra un code ASCII, ensuite il va le convertir en chaine de caractère.

Alice va chiffrer le message avant de l'envoyer en calculant son cryptogramme C :

$$\begin{aligned} C &= M^e \pmod{n} \\ C &= (9726)^{3533} \pmod{11413} \\ &= 5761. \end{aligned}$$

Le déchiffrement :
Bob reçoit le message chiffré $C = 5761$, il utilise sa clé privée $(n, d) = (11413, 6597)$ pour le déchiffrer comme suit :

$$\begin{aligned} M &= C^d \pmod{n} \\ &= (5761)^{6597} \pmod{11413} \\ &= 9726. \end{aligned}$$

De cette façon il obtient le message clair.

3.6.8 La sécurité de RSA :

La sécurité de RSA est basée sur le fait que la fonction de chiffrement :

$$f(x) = x^e \pmod{n}$$

est une fonction à sens unique puisque il est difficile déchiffrer un message clair. C'est une fonction à trappe aussi, puisque *Bob* a l'information d, donc pourra déchiffrer facilement.

Remarque 3.6.17.

Pour calculer d à l'aide de e et n, il faut trouver l'inverse de e modulo $\varphi(n)$, ce qui nécessite la connaissance de p et q, c'est-a-dire la factorisation de n.

Remarque 3.6.18.

La sécurité de cet algorithme repose sur les deux points :

1. Casser RSA nécessite la factorisation du nombre n.
2. La factorisation de ce nombre est un problème difficile, nécessite des milliards d'années si p et q sont grands.

Remarque 3.6.19.

Pour que la factorisation de n soit un problème difficile, il faut qu'un certain nombre de conditions soit remplies :

1. Les nombres p et q doivent être grands, une longueur de clé de 1024 bits offre une bonne garantie de sécurité.
2. Il faut que $p - q$ aussi soit grand pour contrer la méthode de factorisation de Fermat.
3. Il faut que les nombres $p \pm 1$ et $q \pm 1$ aient chacun un grand facteur premier (environs 100 bits), pour résister à la méthode de factorisation de Pollard.
4. Il faut que les ordres de e modulo $p - 1$ et $q - 1$ soient aussi grands, pour faire face contre l'attaque cyclique.

Lemme 3.6.20. *Si la fonction d'Euler $\varphi(n)$ est connue, alors nous pouvons factoriser n.*

Démonstration. Nous avons :

$$\begin{aligned}\varphi(n) &= (p-1)(q-1)\\ &= pq - p - q + 1\\ &= pq - (p+q) + 1\\ &= n - (p+q) + 1\\ \text{et } (p+q) &= n - \varphi(n) + 1.\end{aligned}$$

Posons $S = p + q$, donc $S = n - \varphi(n) + 1$.
Pour factoriser n il suffit de déterminer p et q à partir de leurs somme S et leurs produit n. Nous définissons le polynôme :

$$f(x) = (x-p)(x-q) = x^2 - Sx + n. \tag{3.13}$$

Donc, nous pouvons trouver p et q :

$$\begin{cases} p = \dfrac{S + \sqrt{S^2 - 4n}}{2} \\ q = \dfrac{S - \sqrt{S^2 - 4n}}{2}. \end{cases} \tag{3.14}$$

□

L'algoritme RSA est basé sur le thèorème suivant [156] :

Théorème 3.6.21. *Soit p et q deux nombres premier différents, $n = pq$, considérons deux entiers e et d tels que $ed = 1 \pmod{(p-1)(q-1)}$. Pour tout entier $0 \leq m < n$ nous avons :*

$$m^{ed} = m \pmod{n}. \tag{3.15}$$

Démonstration. Soit m un entier tel que $0 \leq m < n = pq$:

Premier cas : Si m et $n = pq$ sont premiers entre eux, alors l'ordre du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\star$ est $(p-1)(q-1)$ et $m \in (\mathbb{Z}/n\mathbb{Z})^\star$. Il résulte de la théorie des groupes $m^{ed} = m \pmod{n}$.

Deuxième cas : Si m est non premier avec $n = pq$, alors m est un multiple de p ou q. Supposons que $m = p^\alpha r$ tel que $PGCD(p, r) = 1$ et $\alpha \leq 1$.

Puisque $m < n$, $1 \leq r < q$ et $PGCD(p, r) = 1$.
Alors

$$PGCD(r, n) = 1 \text{ et } r^{ed} \equiv r \pmod{n}. \tag{3.16}$$

Par conséquent

$$m^{ed} = (p^\alpha r)^{ed} \equiv (p^\alpha)^{ed} r \pmod{n}. \tag{3.17}$$

Il est clair que

$$(p^{\alpha})^{ed} \equiv p^{\alpha} \pmod{p}. \tag{3.18}$$

Puisque p et q sont distincts :

$$(p^{q-1}) \equiv 1 \pmod{q}. \tag{3.19}$$

Nous savons qu'il existe $k \in \mathbb{Z}$ tel que : $ed = 1 + k\varphi(n)$ où $\varphi(n) = (p-1)(q-1)$. Donc

$$\begin{aligned}(p^{\alpha})^{ed} &= (p^{\alpha})^{1+k\varphi(n)} \\ &= p^{\alpha}(p^{\alpha})^{k(p-1)(q-1)}.\end{aligned} \tag{3.20}$$

D'autre part

$$\begin{aligned}(p^{\alpha})^{k(p-1)(q-1)} &= (p^{q-1})^{k\alpha(p-1)} \\ &\equiv 1^{k\alpha(p-1)} \pmod{q} \\ &\equiv 1 \pmod{q} \text{ (à partir de l'équation 3.19).}\end{aligned} \tag{3.21}$$

Aussi

$$\begin{aligned}(p^{\alpha})^{ed} &= (p^{\alpha})^{1+k\varphi(n)} \\ &= p^{\alpha}(p^{\alpha})^{k(p-1)(q-1)} \\ &= p^{\alpha} \pmod{q}.\end{aligned} \tag{3.22}$$

Puisque p et q sont premiers entre eux, à partir de (3.18) et (3.22) nous avons :

$$(p^{\alpha})^{ed} \equiv p^{\alpha} \pmod{n}. \tag{3.23}$$

Conclusion : de (3.16) et (3.23) nous avons :

$$\begin{aligned}m^{ed} &= (p^{\alpha}r)^{ed} \\ &\equiv (p^{\alpha})^{ed}r^{ed} \pmod{n} \\ &\equiv p^{\alpha}r \pmod{n} \\ &= m.\end{aligned} \tag{3.24}$$

Le cas si m est a multiple de q est identique au cas m est multiple de p. □

3.6.9 La signature numérique

Une application intéressante de la cryptographie à clé publique est la signature numérique, la signature numérique est l'utilisation à l'envers d'un algorithme de chiffrement asymétrique (Figures 3.8 et 3.9). Dans le chiffrement à clé publique, on chiffre avec la clé publique du destinataire, personne sauf le destinataire pourra déchiffrer. Au contraire dans la signature numérique, l'expéditeur signe le document avec sa clé privée, tout le monde pourra donc vérifier la signature puisque tout monde dispose de la clé publique.

Une signature numérique est adoptée de plus en plus dans plusieurs pays et dans plusieurs domaines tels que le commerce électronique et l'échange des documents réglementaires, elle a les mêmes conséquences juridiques qu'une signature manuscrite (Décret Français du 31 mars 2001 sur la signature électronique) [182].

La signature numérique doit garantir les propriétés suivantes :

1. Identifier l'émetteur du message, seul le propriétaire de la clé privé peut signé.
2. N'importe qui peut vérifier l'authenticité avec la clé publique.
3. Assurer l'intégrité du document, le document n'ait pas été modifié.
4. Garantir que l'expéditeur ne peut pas nier avoir envoyé le message.
5. Une signature numérique n'est pas réutilisable ou falsifiable.

Pour une signature numérique efficace et plus rapide on ne signe pas le message en entier, on signe que le hach.

3.6.10 Le certificat électronique

L'échange numérique des données nécessite le partage des clés publiques. Dans un tel système on risque de confondre une fausse clé avec une clé authentique. Il y a aussi le risque qu'un intercepteur non autorisé utilise l'identité de quelqu'un d'autre. Il est essentiel de s'assurer qu'on crypte vers la bonne personne.

Comment savoir qu'on a la bonne clé publique ? Le certificat numérique nous permet de s'assurer que la clé publique qu'on utilise appartient au bon utilisateur. Le certificat numérique est une sorte de garantie de la validité des informations identifiant le possesseur de la clé. Elle permet l'identification de façon unique la personne, l'entité ou l'ordinateur. Le certificat peut être vu comme une carte d'identité numérique. Elle garantit l'association entre une identité et une clé publique.

Dans les signatures numériques les certificats attestent le lien entre les données de vérification de signature électronique et le signataire. La législation en France ne permet pas de signer électroniquement un document sans avoir un certificat électronique [1].

Le certificat numérique est fournie par un organisme (ou plusieurs) de confiance appelé l'autorité de certification ou délivré au sein d'une entreprise (Figures 3.10 et 3.11). L'autorité de certification fait foi de tiers de confiance et garantie le lien entre l'identité physique et l'identité numérique, elle fonctionne comme un service de gestion des cartes d'identité dans une mairie. Les certificats sont créés et signées avec la clé privée de l'autorité, puis livrées au demandeur sous forme d'une document électronique a stocker sur un pc, usb ou une carte à puce.

La signature du certificat par l'autorité est une déclaration que ces informations ont été attestées par un (ou plusieurs) tiers de confiance. L'utilisation des certificats

1. Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.
http ://www.legifrance.gouv.fr/

est présente en général dans les sites e-commerce, les sites de banques et au sein des entreprises.

Le certificat électronique contient en général des informations concernent l'expéditeur et l'identité et la signature de l'autorité de certification :

— Des informations sur le porteur du certificat (nom, prénom, email, identifiant, entreprise,...)
— L'identité et signature de l'autorité qui a émis le certificat.
— La date de validité du certificat.
— La clé publique du porteur du certificat.
— Les algorithmes utilisés.

3.7 La cryptanalyse

Si déchiffrer consiste à retrouver le texte clair en connaissant la clef et l'algorithme, cryptanalyser c'est tenter retrouver le texte clair sans avoir connaissance de la clef. La cryptanalyse ou que fait Oscar est la science ou l'art qui regroupe tous les moyens de déchiffrer une donnée cryptée lorsque la clé est inconnue, elle s'est développée parallèlement à la cryptographie.

Parmis les objectifs de la cryptanalyse est de mesurer les faiblesses et la robustesse d'un cryptosystème face aux attaques, d'en découvrir le secret et décrypter les textes chiffrés [17, 50]. Ainsi, la tâche principale de la cryptanalyse est de reconstruire la clef de chiffrement, ou une forme équivalente qui peut avec succès déchiffrer totalement ou partiellement une donnée chiffrée.

3.7.1 Les principes de la cryptanalyse

Les techniques de la cryptanalyse sont basées sur l'hypothèse suivante, connue sous le nom "Le principe de Kerchhoffs"(voir [8]), qui affirme que l'opposant connaît le système cryptographique utilisé et que la sécurité de système de protection est basée sur la clé sécrète ou la clé privée. Auguste Kerchhoffs donne les principes de bases de la cryptographie à clef sécrète. Pour Auguste Kerchhoffs une méthode cryptographique est distingué à assurer pour un temps illimité la correspondance. Un cryptosystème ou une application de chiffrement sûre doit remplir certaines conditions [8] :

1. Le cryptosystème doit être mathématiquement indéchiffrable.
2. La possibilité de modifier la clé par les utilisateurs.
3. Il faut que l'algorithme soit applicable à la correspondance télégraphique.
4. Il faut que le cryptosystème soit portatif et que son fonctionnement n'exige pas le concours de plusieurs personnes.
5. L'utilisation du l'algorithme doit être facile.

3.7.2 Les types de base de la cryptanalyse

En fonction d'informations connues par les cryptanalystes on peut distinguer différents types de base de cryptanalyses (liste non exhaustive) [50] :

1. **L'attaque à texte chiffré seul (Ciphertext-only attack) :** Dans ce scénario l'attaquant a seulement accès à des textes chiffrés de plusieurs messages et tente de les analyser afin de déduire la clé ou découvrir le texte clair. En pratique, ce scénario est le plus courant puisque le texte chiffré est facile d'être intercepté. L'objectif le plus important des cryptosystèmes est de résister contre ce type d'attaque.
2. **L'attaque à texte clair connu (Known-plaintext attack) :** L'adversaire connaît à la fois des parties du texte chiffré et le texte correspondant en clair. Cela peut aider à déterminer la clé ou une partie de la clé. Ce scénario est le plus courant dans la cryptanalyse moderne.
3. **L'attaque à texte clair choisi (Chosen-plaintext attack) :** Dans ce cas, le cryptanalyste a accès à l'algorithme ou la machine de chiffrement, il choisit des textes clairs, il peut produire la version chiffrée de ce texte. La différence principale par rapport l'attaque à texte clair connu est que le cryptanalyste peut choisir le texte à chiffrer. L'adversaire peut utiliser les paires des messages clairs et chiffrés pour obtenir la clé secrète ou une partie de cette clé. On trouve l'attaque à texte clair choisi principalement dans des implémentations matérielles ou la clef secrète est protégée physiquement telles que les cartes à puce, usb, etc.
4. **L'attaque à texte chiffré choisi (Chosen-ciphertext attack) :** L'ennemi a accès au dispositif de déchiffrement, il a la possibilité de choisir les textes à déchiffrer sans connaître la clef. De la même manière que l'attaque précédente, l'adversaire tente d'obtenir la clef secrète ou une partie de la clef en analysant les paires des textes clairs et chiffrés obtenus. Cette attaque est populaire dans la cryptographie asymétrique puisque la clef publique est connue.
5. **L'attaque par force brute (Brute-force attack) ou l'attaque exhaustive :** l'attaquant essaie toutes combinaisons de clefs possibles jusqu'à l'acquisition du texte clair. Dans un cryptosystème solide il doit être mathématiquement impossible de tester toutes les combinaisons.

Dans les attaques citées ci-dessus, l'attaque à texte chiffré seul est la plus facile et la plus connue du fait que le canal de communication est généralement accessible par les attaquants. Les attaques par texte choisi sont possibles quand un attaquant peut accéder à l'algorithme de chiffrement, ou s'il peut réussir à deviner les textes en clair ou certains segments. Ces attaques sont devenues de plus en plus fréquentes dans monde le numérique d'aujourd'hui.

3.7.3 La cryptanalyse moderne :

La création de techniques modernes de chiffrement a fait ressortir des nouvelles méthodes de cryptanalyse. Nous pouvons grouper ces nouvelles techniques en deux grandes familles.

1. **Cryptanalyse différentielle :** L'idée originale pour la cryptanalyse différentielle vient d'Eli Biham et Adi Shamir en 1991 [58], qui a publié un certain nombre de résultats dans les années 1980 sur la cryptanalyse de plusieurs algorithmes de chiffrement et de fonctions de hachage. L'attaque différentielle est une attaque par texte clair choisi. L'idée de cette attaque consiste à étudier un grand nombre de couples de textes clairs X et X' avec une légère différence fixée ΔX (un bit par exemple). Ensuite, on analyse statistiquement le comportement et la propagation de différences des textes chiffrés, on tente de prédire le comportement avec une forte probabilité. Ce type d'attaque a été utilisé largement sur les familles DES et les familles MD de fonctions de hachage, [81, 121, 43, 59, 192, 193, 194]. Par exemple, l'attaque différentielle peut casser l'algorithme DES après 2^{47} couples de texte choisi. Il existe plusieurs variantes des cryptanalyses différentielles, nous pouvons distinguer : différentielle tronquée, différentielle d'ordre supérieur et différentielles impossibles [51, 60, 110, 111, 147].
2. **Cryptanalyse linéaire :** Cette technique de cryptanalyse a été introduite par A. Crofdir et H. Gilbert, a été appliquée par un chercheur de Mitsubishi Electric Mitsuri Matsui en 1993 [50] pour casser l'algorithme DES . C'est une attaque à texte clair connu. Le principe dans cette attaque consiste à chiffrer plusieurs fois un texte avec des clefs différentes afin de collecter un grand nombre de couples (texte clair, texte chiffré) et construire une immense table qui contient toutes les versions chiffrées de ce message. Pour trouver la clef de chiffrement on cherche le message intercepté dans cette table. Puisque la table est très grande cette recherche prendra un temps énorme, pour réduire la taille de la table et temps de recherche, on réalise des approximations linéaires pour simplifier le tableau. L'idée principale et de chercher des relations linéaires de dépendance de probabilités exceptionnelles entre les bits d'entrée et de sortie. Ce type de cryptanalyse a été amélioré par Eli Biham en 2002.

Les deux grandes familles d'attaques présentées précédemment sont les plus connues sur les algorithmes de chiffrement par blocs, leur efficacité a été démontré contre plusieurs algorithmes. Il existe beaucoup d'autres classes d'attaques, on peut citer entre autres l'attaque boomerang, l'attaque rectangle, la cryptanalyse différentielle-linéaire la cryptanalyse ξ^2, la cryptanalyse quadratique, la cryptanalyse modulo n, compromis temps/mémoire, l'attaques sur les modes opératoires, l'attaques par canaux auxiliaires et beaucoup d'autres.

3.8 Conclusion

Dans ce chapitre, nous avons présenté des généralités sur la cryptographie, les thèmes base utilisés en cryptographie, les objectifs de la cryptographie et la classification des algorithmes, cette classification est non-exhaustive, il existe d'autres types d'algorithmes comme les algorithmes chaotique [22, 62, 109, 170, 191], comme son nom l'indique, la cryptographie chaotique repose sur l'utilisation du chaos. Également, il y a d'autres techniques qui interviennent dans le cryptages des images comme la stéganographie et le tatouage numérique [187]. La théorie des courbes elliptiques et la théorie des codes correcteurs qui sont utilisées aussi pour développer de nouveaux algorithmes à clé publique [105, 145, 133, 176, 184, 185].

Nous avons évoqué également dans ce chapitre la deuxième branche de la cryptologie, la cryptanalyse, ses principes et les différents types d'attaques.

Dans les chapitres suivants, nous allons présenter nos contributions à la sécurité des images numériques.

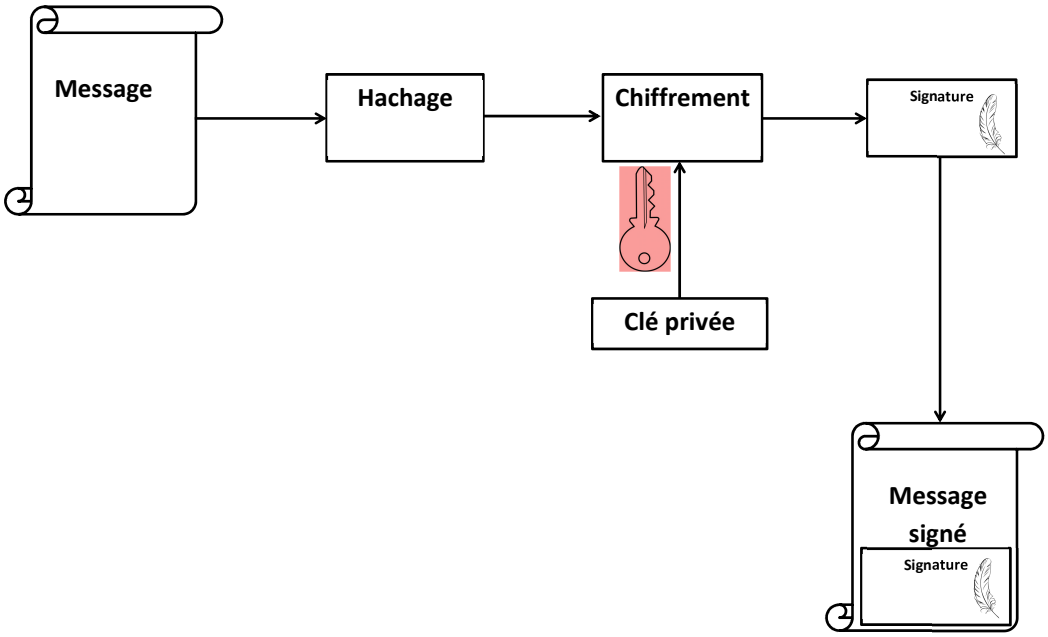


FIGURE 3.8: La signature numérique.

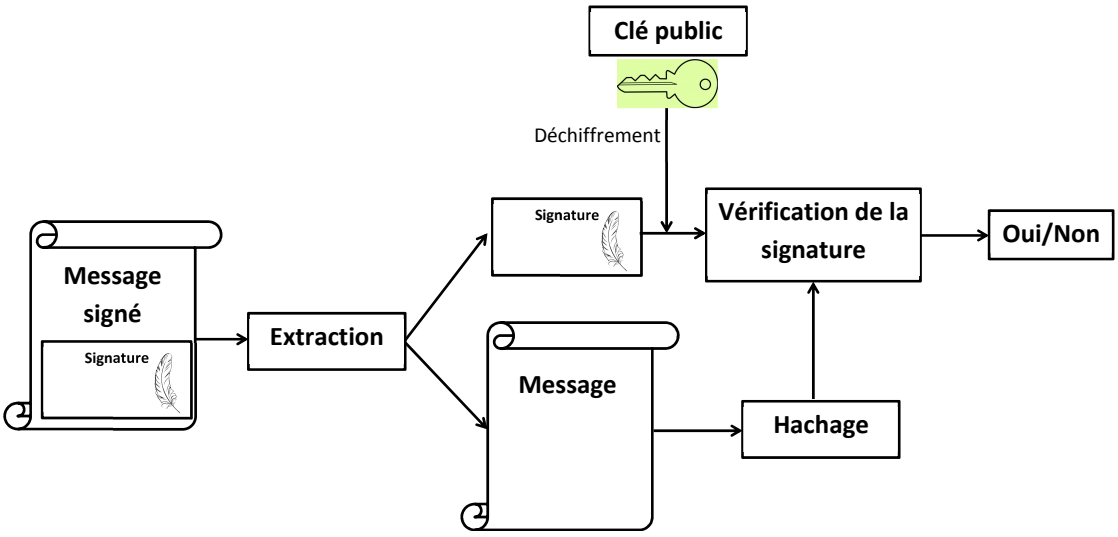


FIGURE 3.9: Vérification de la signature numérique.

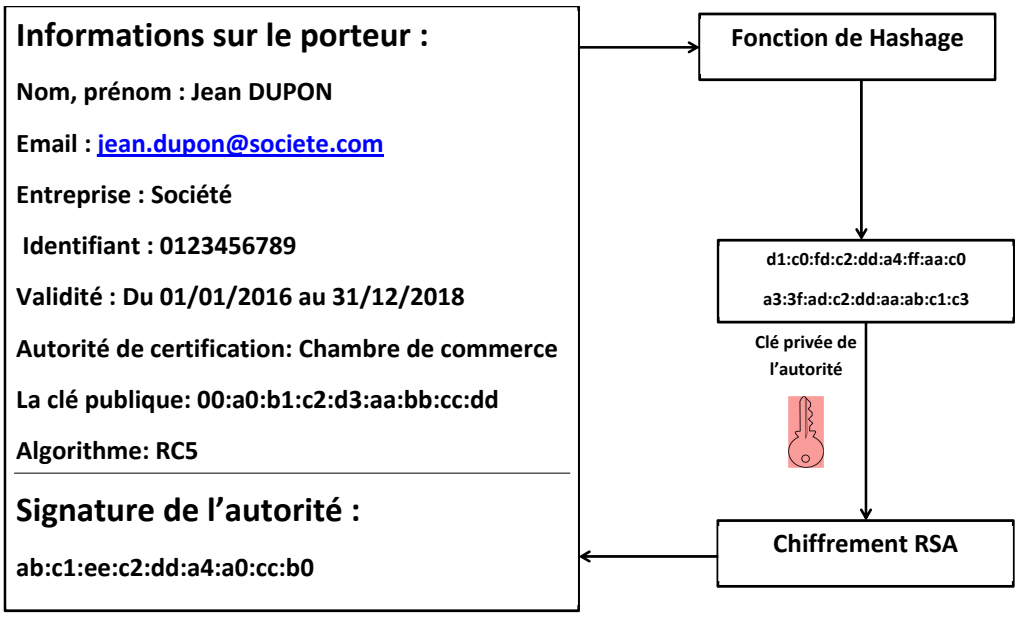


FIGURE 3.10: Exemple de certificat électronique.

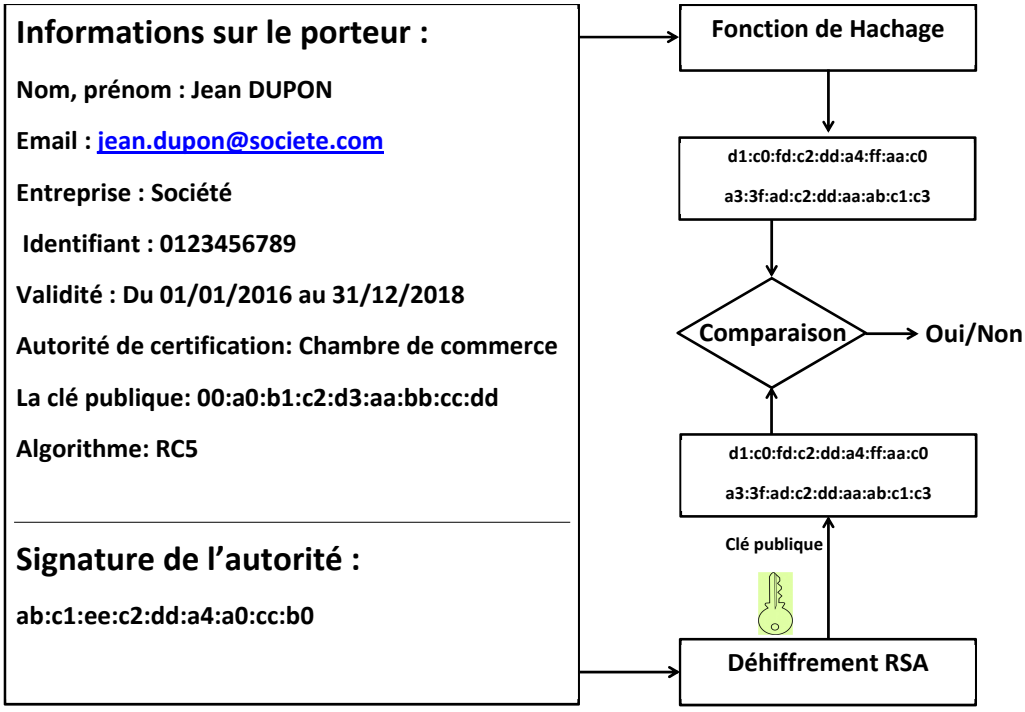


FIGURE 3.11: La vérification du certificat électronique.

Chapitre 4

Nouvelle méthode de chiffrement partiel des images médicales basée sur la coloration des graphes

4.1 Introduction :

Ce chapitre est l'objet de la publication [23].

Le trafic d'images numériques a été rapidement augmenté dans les réseaux ces dernières années. La sécurité des images est devenue importante pour de nombreux secteurs, à savoir pour les applications médicales. À l'heure actuelle, la transmission d'images médicales est une routine quotidienne, l'usage de l'imagerie médicale par les professionnels de la santé a évolué d'une façon remarquable, du fait du développement des technologies numériques. Elle permet une investigation de plus en plus profonde des organes humains grâce aux systèmes de radiologie davantage performants. L'approche numérique induite par l'utilisation des outils informatiques induit des traitements sur des images en très haute définition, ainsi une modalité de type scanner produit des images de taille de l'ordre du 10 Mo et un examen complet atteint 500 Mo.

Au vu des lois protégeant les données médicales des patients notamment en ce qui concerne l'accès et la confidentialité, les professionnels de santé ont l'obligation de sauvegarder ces images selon des contraintes de temps. Ces images peuvent être échangées entre les professionnels de la santé, ce qui les conduits à garantir la confidentialité lors des transferts.

Ainsi, l'échange de ces informations numériques dans les applications médicales posait le problème de sécurité. Le volume important des données échangées posait également le problème de temps de traitement. Le grand volume des données a motivé le développement de nouvelles méthodes pour réduire le coût de calcul. Le chiffrement partiel est une approche pour réduire les ressources et le temps de traitement. Les chercheurs de plusieurs disciplines ont développé plusieurs algorithmes de chiffrement partiel basés sur plusieurs techniques [14, 19, 77, 92, 120, 189].

Contrairement à la méthode de chiffrement total, le chiffrement partiel (également appelé le chiffrement sélectif) est une approche utilisée pour réduire le temps de traitement. Par conséquent, un sous-ensemble des données sera chiffré. Le but de cette approche consiste à réduire la quantité des données chiffrées tout en conservant un niveau de sécurité suffisant. Par exemple, pour une image médicale un minimum de $12,5\%$ des données doit être chiffré pour avoir un bon niveau de confidentialité [172]. De nombreuses recherches ont proposé des algorithmes qui combinent le chiffrement sélectif avec d'autres techniques telle que la compression [46, 137, 200].

Nous avons présenté dans cet article une nouvelle approche sécurisée pour chiffrer partiellement les images médicales en utilisant le problème de coloration de graphes. Avant de chiffrer l'image, nous utilisons un problème de coloration de graphes pour localiser et sélectionner des positions optimales. La clé de la méthode cryptographique est difficile à détecter puisque il est difficile de prévoir les pixels chiffrés. Le graphe (les pixels sélectionnés pour le chiffrement) est différent pour chaque image ce qui rend plus difficile le travail des adversaires. Nous avons obtenu un pourcentage acceptable des données chiffrées pour une sécurité suffisante des images médicales avec un coût plus faible par rapport au chiffrement total.

Dans ce chapitre, nous allons présenter le problème de coloration de graphes et une description de la méthode DBG (De Bruijn Graph). Nous décrivons notre approche et fournirons des analyses de sécurité et des résultats expérimentaux.

4.2 Coloration de graphe :

Le problème de la coloration de graphes (Graph Coloring problem en anglais : GCP) est parmi les problèmes d'optimisation combinatoire les plus étudiés en informatique et en mathématiques. La coloration de graphes est un sujet très actif de la théorie des graphes, il fait objet de plusieurs applications dans de nombreux domaines tels que, la télécommunication, la bioinformatique et l'Internet. Le GCP est lié aussi à plusieurs applications traditionnelles dans des domaines variés, comme le problème d'emploi du temps [52], l'ordonnancement des taches [119], l'optimisation des chaines logistiques [11], l'affectation des registres dans les compilateurs [123], la gestion du trafic aérien [141] et l'affectation de fréquences dans les réseaux de communications [4]. La coloration de graphes a été aussi appliquée pour modéliser et résoudre des problèmes en mathématiques et statistiques [124]. Plusieurs méthodes et algorithmes sont proposés pour résoudre le problème de coloration, les premiers algorithmes heuristiques utilisés sont les algorithmes constructifs dont le principe est d'affecter à chaque sommet la plus petite couleur possible en parcourant de façon séquentielle tous les sommets du graphe. Les algorithmes constructifs fréquemment employés et les plus connus sont RLF [68] et DSATUR [42]. Un nombre important de recherches ont été destinés pour la résolution du problème de coloration, parmi ces méthodes nous trouvons la recherche TABU qui occupe la première place puisque

plusieurs auteurs ont introduit cette technique dans leurs travaux [6, 163].

Définition 4.2.1. *La coloration d'un graphe consiste à associer une couleur à chaque sommet de manière que deux sommets adjacents ne possèdent pas la même couleur. Si le graphe contient une arête (x, y), alors x et y ont des couleurs différentes (voir la figure 4.1).*

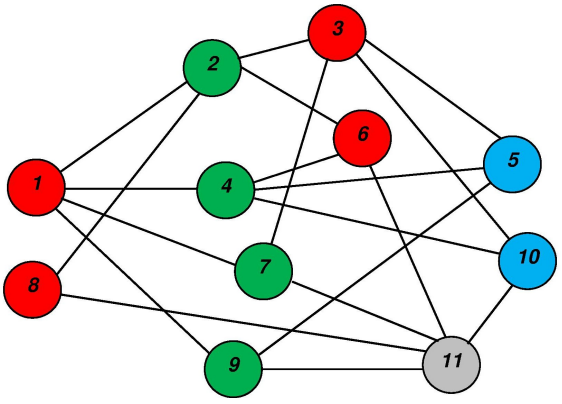


FIGURE 4.1: Exemple d'une coloration d'un graphe

Définition 4.2.2. *Une k-coloration valide des sommets d'un graphe $G = (V, E)$ est une application $c : V \longrightarrow \{1, \cdots, k\}$, telle que $c(x) \neq c(y)$ $\forall (x, y) \in E$, la valeur $c(x)$ associée au sommet x est appelée couleur de x.*

Si $(x, y) \in E$ et $c(x) = c(y)$ on dit que x et y sont en conflit. Les sommets ayant la même couleur définissent une classe de couleur de telle sorte qu'il n'existe pas d'arête entre deux sommets de la même classe. Comme chaque classe de couleur est un ensemble indépendant de G, une coloration peut être vue comme une partition de V en ensembles indépendants.

Définition 4.2.3. *Le nombre chromatique d'un graphe G noté $\chi(G)$, est le plus petit nombre de couleurs différentes utilisées pour colorier tous les sommets de G avec une coloration valide.*

4.2.1 Ensemble indépendant maximal

Définition 4.2.4. *Un ensemble indépendant dans un graphe $G = (V, E)$ est un sous-ensemble $S \subseteq V$ de sommets deux à deux non adjacents.*

Le problème d'ensemble indépendant maximal est né en même temps que le problème de coloration de graphes. Ainsi, il est normal dans des problèmes de coloration de rechercher des moyens de restructurer les ensembles (couleurs) indépendants, qui

correspondent à différentes couleurs données, le but est d'augmenter la taille de l'ensemble indépendant pour réduire ainsi le nombre des ensembles et par la suite le nombre de couleurs.

Nous considérons un graphe non-orienté $G = (V, E)$, où $V = \{1, \cdots, k\}$ est l'ensemble de sommets du graphe, E est l'ensemble des arêtes. Pour chaque sommet $i \in V$ on définit les sommets liées à ce sommet i :

$$\begin{array}{l} nodestar(i) = \{j : \{i, j\} \in E\} \\ d_i = card(nodestar(i)). \end{array} \tag{4.1}$$

La formulation usuelle de la programmation mathématique du problème de l'ensemble indépendant maximal se fait comme suit :

1. On associe une variable binaire x_i à chaque sommet $i \in V$.
2. $x_i = 1$ si et seulement si le sommet i est choisi comme élément de l'ensemble indépendant S.

Donc, le problème peut être exprimé sous forme d'un problème de la programmation en nombres entiers :

$$(IP) \begin{cases} max\ x_0 = \sum(x_i : i \in V) \\ x_i + x_j \leq 1, \{i, j\} \in E \\ x_i\ binaire, i \in V. \end{cases} \tag{4.2}$$

Pour produire rapidement une solution approchée de ce type de problème, nous utilisons l'heuristique de la contrainte de substitution (surrogate en Anglais). Cette méthode est obtenue en remplaçant l'ensemble des contraintes par une seule contrainte qui est une combinaison linéaire des contraintes originales. Pour le problème (IP), nous faisons une simple sommation de toutes les contraintes comme suit :

$$\sum(d_i x_i : i \in V) \leq d_0. \tag{4.3}$$

Le problème de substitution associé à (IP) devient :

$$(SC) \begin{cases} max\ x_0 = \sum(x_i : i \in V) \\ \sum(d_i x_i : i \in V) \leq d_0 \\ x_i\ binaire, i \in V. \end{cases} \tag{4.4}$$

4.2.2 L'algorithme DBG

Soit $G = (V, E)$ un graphe non-orienté et $w = (w_1, ..., w_m)^t$ le facteur de la contrainte de substitution, où m désigne le nombre d'arêtes. On choisit la variable $x_r = 1$. S'il existe $j \in nodestar(r)$ et $1 \leq k \leq m$, tel que $a_{k,j} = 1$, alors $w_k = 0$, pour tout $1 \leq j \leq n$ et pour tout $1 \leq k \leq m$ [171].

Algorithm 3: DBG

1. Début.
2. Poser $w = (1, ..., 1)^t$ et $V' = \emptyset$.
3. Calculer la contrainte de substitution $wA = \sum_{w_k \neq 0} (a_{k,.})$.
4. i=indice(min$(w^t A) : (wA^t)_i \neq 0$).
5. $x_i = 1$ et $V' = V' \cup \{i\}$.
6. Pour tout $j \in nodestar(i)$.
7. Si $a_{k,j} = 1$ alors $w_k = 0$.
8. Si $\sum_{k=1}^{d_0} w_k = 0$ stop.
9. Autrement retourner à l'étape 2.
10. Fin pour.
11. Fin.

4.2.3 Résolution de GCP

La décomposition du graphe G sous forme d'ensembles indépendants $X_1, X_2, ..., X_k$ nous donne une k-coloration valide en donnant à chaque ensemble X_i la couleur i, $1 \leq i \leq k$. Nous proposons une k-coloration au problème GCP utilisant l'heuristique DBG pour construire k classes de couleurs du graphe G.

4.3 Notre approche

Nous utilisons le problème de coloration de graphe pour augmenter la sécurité et rendre la détection de la clé chiffrement une tâche difficile.

Dans l'approche proposée, quelques pixels de l'image originale seront sélectionnés et chiffrés. Nous considérons la matrice de pixels associé à l'image claire, notre algorithme traite l'image par blocs, chaque ligne de pixels est considérée comme bloc. Nous utilisons l'algorithme de coloration de graphe décrit précédemment pour déterminer les positions des pixels qui seront chiffrés.

Chaque ligne de la matrice associée correspond à un graphe non orienté $G = (V, E)$, où V désigne l'ensemble des sommets, E l'ensemble des arêtes de telle sorte que deux sommets x et y sont adjacents si la différence entre deux pixels p_i et p_j est inférieur à un seuil s, où $i \neq j$ et $i, j = 1, \cdots, card(V)$.

$$| p_i - p_j | < s \tag{4.5}$$

Chaque classe de couleur C correspond à un ensemble indépendant. Dans notre

Algorithm 4: Coloration de graphe

1. While $V \neq \emptyset$.
2. Appliquer l'algorithme (DBG) pour trouver une approximation de l'ensemble maximal indépendant V' :
   a. Soit $w = (1, ..., 1)^t$ et $V' = \emptyset$.
   b. Calculer la contrainte de substitution $wA = \sum_{w_k \neq 0} (a_{k,.})$.
   c. Posons $i = index(\min(wA) : (wA)_i \neq 0)$, soit $x_i = 1$ and $V' = V' \cup \{i\}$.
   d. Pour tout $j \in nodestar(i)$ si $a_{k,j} = 1$, alors $w_k = 0$, if $\sum_{k=1}^{m} w_k = 0$ stop.
   Sinon revenir à l'étape **b**.
3. $V = V \backslash V'$.
4. Si les sommets de V sont disjoints stop, sinon aller à 2.
5. Fin boucle while.

cas, nous chiffrons un sous-ensemble des premières classes de couleurs qui représente au moins $12,5\%$ de l'image. Le choix de la valeur de seuil s est lié aux valeurs de pixels dans chaque bloc. Le calcul de la valeur de seuil s du bloc H_l se fera par la formule :

$$s_l = \lceil \frac{(\sum |p_i^l - p_i^{l+1}|)}{(Card(V) - 1)} \rceil. \tag{4.6}$$

Où $\lceil x \rceil$ est la partie entière de x.

Correction

Après le chiffrement de l'image on applique un ajustement sur les pixels du bloc H_l afin de maintenir le même graphe tel qu'il était avant le processus chiffrement. Pour cela, nous recherchons les sommets liés à chaque sommet : noté $nodestar(x)$. Ensuite, nous ajoutons la même valeur (voir l'exemple 4.3.1). De cette façon, nous garantissons que le destinataire aura le même graphe tel qu'il était avant le chiffrement.

Nous donnes un exemple concret de l'opération.

Exemple 4.3.1. *(figures 4.2 et 4.3)*

Sélection :

1 Considérons un bloc A de pixels (figure 4.2).

2 Calculer le seuil correspondant au bloc A, nous obtenons $s = 2$ (formule 4.6).

3 Construire le graphe $G = (V, E)$ associée au bloc A, $(i, j) \in E$ si $|p_i - p_j| < 2$ (figure 4.2).

Algorithm 5: GCPCrypt

1. Input : Une image originale I, une clé de chiffrement AES_{key}
2. Output : image cryptée I'.
3. Posons la matrice des pixels de taille $N = N_1 \times N_2$ associée à l'image originale.
4. Divisez I sous la forme de N blocs l_l de même tailles.
5. $l \leftarrow 1$.
6. While $l \leq N$.
7. Calculer $s_l = \lceil \frac{(\sum |p_i^l - p_i^{l+1}|)}{(Card(H_l) - 1)} \rceil$.
8. Pour chaque bloc H_l sélectionner les premières classes de couleurs C'_{H_l} en utilisant l'algorithme DBG, tel que le pourcentage $P(C'_{H_l}) \geq 12.5\%$.
9. Chiffrer tous les pixels des classes de couleurs C'_{H_l} en utilisant l'algorithme de chiffrement AES : $p'_{C'_{H_l}} = p_{C'_{H_l}} + AES_{key}$.
10. Ajuster le bloc H_l :
    (a) Pour $i = 1$ à card(C_{H_l}) faire
    (b) $add = p'_i - p_i$
    (c) $p_{nodestar(i)} \leftarrow p_{nodestar(i)} + add$
    (d) Fin de la boucle pour.
11. $l \leftarrow l + 1$.
12. $I'(l) \leftarrow H_l$.
13. Fin de la boucle While.
14. Retourner I'.

4 Appliquer l'algorithme de coloration de graphe (l'algorithme 4), nous obtenons la première classe de couleur $C = (1, 4)$, nous avons deux positions optimales 1 et 4, le pourcentage des pixels sélectionnés est $P = \frac{2}{6} = 33.33\%$. Donc, chiffrer cette classe de couleur est suffisant pour ce bloc.

Chiffrement :

5 Chiffrer les positions sélectionnées 1 et 4 par l'algorithme AES.

6 Ajustement :

Nous ajustons les autres pixels pour maintenir le même graphe, on obtient un nouveaux bloc A'.

Ainsi, les valeurs de pixels associées à la classe $(1, 4)$ avant le chiffrement sont 103, 105, et après le chiffrement 101, 106. La correction du bloc est réalisé en modifiant les valeurs de pixels associées aux sommets reliés à la classe $(1, 4)$

(Figure 4.2).

La valeur de pixel associée aux sommet 1 a été incrémentée par 2, puis les valeurs de pixels associées à $nodestar(1) = (3, 6)$ sont également décrémentées par 2.

La valeur de pixel associée au vertex 4 a été incrémentée par 1, de sorte que les valeurs de pixels associées à $nodestar(4) = (2, 3, 5, 6)$ sont également incrémentée par 1.

Déchiffrement :

7 Le destinataire reçoit le bloc A', il va obtenir la valeur de seuil $s = 4$. Le récepteur pourrait construire le graphe associé à A' qui sera identique au bloc A (Figure 4.3).

Ensuite, le récepteur appliquera l'algorithme de coloration il obtient la même classe $(1, 4)$ associée aux valeurs de pixels 101 et 106. Le récepteur appliquera la correction inverse sur $nodestar(1) = (3, 6)$ et $nodestar(4) = (2, 3, 5, 6)$ pour obtenir l'image original.

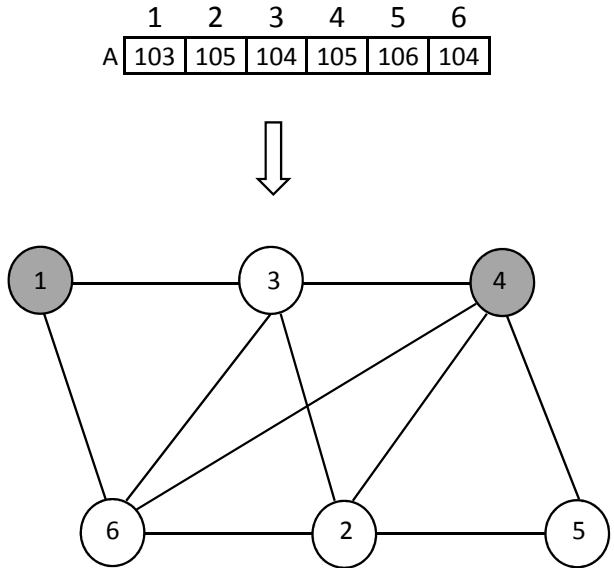


FIGURE 4.2: Le graphe associé au bloc A.

4.4 L'analyse de sécurité :

Le coût de calcul est élevé si nous appliquons le chiffrement total, en particulier dans les centres de radiologie où le volume d'images médicales généré dépasse des millions de gigaoctets. Dans cet article, nous avons adopté une solution de chiffrement sélectif, pour obtenir un bon niveau de sécurité, nous traitons uniquement les premières classes de couleur qui présente au moins $12,5\%$ des données [172].

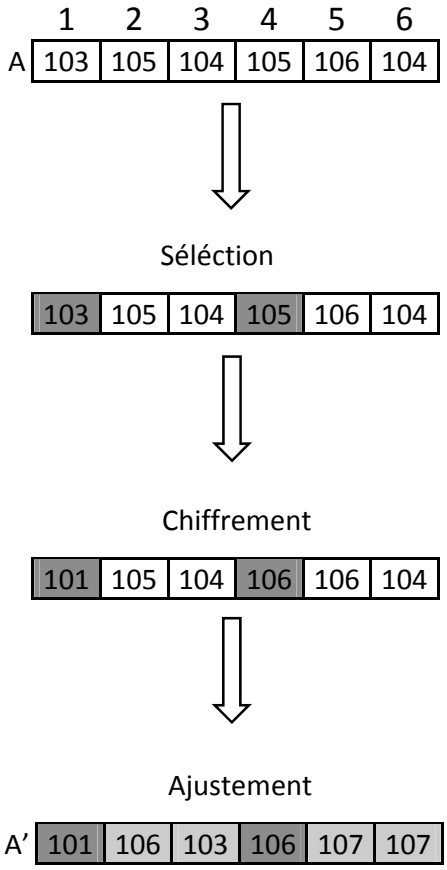


FIGURE 4.3: Après le chiffrement et l'ajustement.

D'autre part, les images médicales chiffrées avec un $PSNR < 30\ dB$ le diagnostic médical sera compliqué [107]. L'utilisation d'un problème de coloration de graphe rend plus difficile la localisation des pixels chiffrés, ce qui augmente la sécurité.

4.5 Résultats expérimentaux

Nous avons testé et évalué notre algorithme sur plusieurs images en niveaux de gris. Nous avons choisi quatre images qui sont présentées dans les figures 4.4, 5.6, 5.7 et 5.8.

Pour le processus de chiffrement, nous avons appliqué le chiffrement par flot en utilisant l'algorithme AES en mode OFB (Output Feedback Block) avec une clé de longueur 128 bit. Nous avons utilisé l'algorithme DBG pour le problème de coloration de graphe. Cette approche peut être également utilisée avec d'autres valeurs de longueur de clé et avec d'autres modes de chiffrement.

Pour notre cas, nous avons testé deux paramètres d'évaluation importants pour mesurer la robustesse de l'algorithme, le premier est le pourcentage P des pixels

Algorithm 6: GCPDecrypt

1. Input : image cryptée I'.
2. Output : image déchiffrée I.
3. Diviser I en N blocs H_l de la même taille.
4. $l \leftarrow 1$.
5. While $l \leq N$.
6. Calculer $s_l = \lceil \frac{(\sum p_i^l - p_i^{l+1})}{(Card(H_l) - 1)} \rceil$.
7. Pour chaque bloc H_l sélectionner les premières classes de couleurs C'_{H_l} en utilisant l'algorithme 4, qui garantissent un pourcentage $P(C'_{H_l}) \geq 12.5\%$.
8. Appliquer l'algorithme AES pour déchiffrer chaque pixel du bloc C'_{H_l}.
9. $l \leftarrow l + 1$.
10. $I(l) \leftarrow H_l$.
11. Fin de la boucle While.
12. Retourner I.

.

chiffrés défini comme suit :

$$P = \frac{\text{le nombre des pixels chiffrés}}{\text{le nombre total des pixels}}, \tag{4.7}$$

et le second est le PSNR (Peak Signal to the Noise Ratio) qui est utilisé pour évaluer la qualité de image médicale chiffrée (voir la section 2.6.5, page 25).

Le tableau 5.1, montre les résultats de notre méthode appliquée aux images sélectionnées. Nous obtenons des résultats comparables (en termes de pourcentage de données cryptées et PSNR) avec la méthode utilisée par W. Puech et J.-M. Rodrigues qui utilise des coefficients du transformée en cosinus discrète DCT (Discrete Cosine Transform) [189].

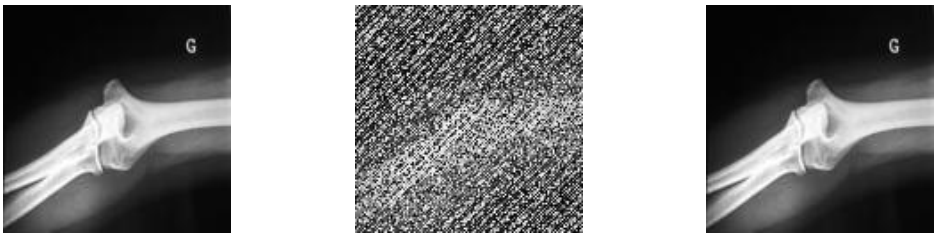
	la taille de l'image	données chiffrées %	PSNR (dB)
Bras	128×128	$20,31$	21.63
Cancer du poumon	256×256	$19,31$	22.11
Crâne	256×256	$25,00$	26.32
Main	512×512	$18,73$	19.64

TABLE 4.1: Résistance au bruit de la méthode de chiffrement GCP.

Pour les images sélectionnées, nous avons obtenu un pourcentage des données

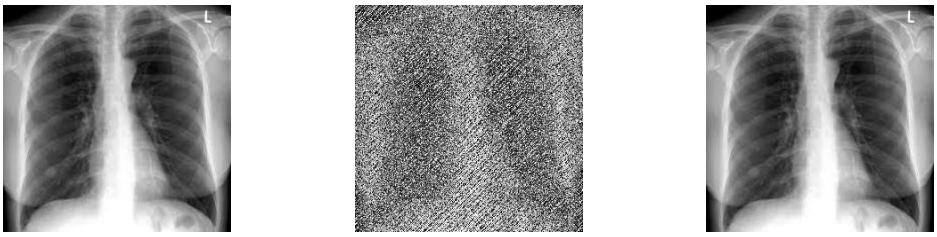
chiffrées plus de $12,5\%$. Cela permettra de garantir un bon niveau de confidentialité pour une image médicale [172]. D'autre part, nous avons obtenu un ($PSNR < 30\ dB$) qui garantit un diagnostic médical difficile [107] en cas d'attaque.

Nous avons atteint un bon niveau de sécurité pour le traitement des images médicales et un gain de temps de calcul. Contrairement à la méthode utilisée dans [189], nous pouvons augmenter le pourcentage de données cryptées selon le besoin en augmentant les classes de couleurs cryptées.



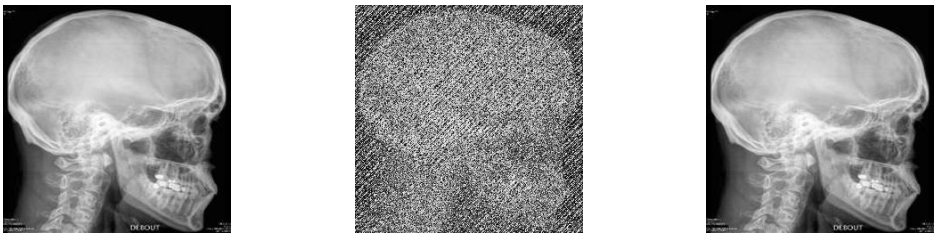
(a) (b) (c)

FIGURE 4.4: Bras : (a) L'image originale, (b) Image partiellement chiffrée, (c) Image déchiffrée.



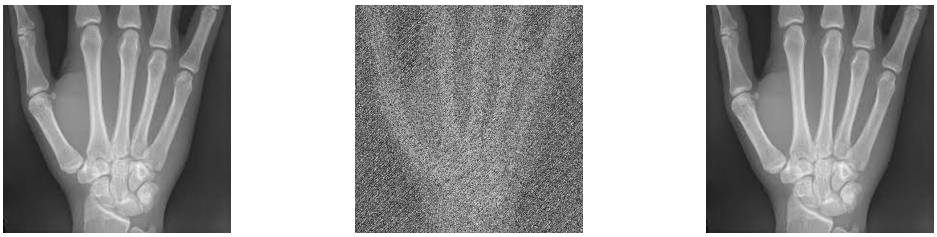
(a) (b) (c)

FIGURE 4.5: Cancer du poumon : (a) L'image originale, (b) Image partiellement chiffrée, (c) Image déchiffrée.



(a) (b) (c)

FIGURE 4.6: Crâne : (a) L'image originale, (b) Image partiellement chiffrée, (c) Image déchiffrée.



(a) (b) (c)

FIGURE 4.7: Main : (a) L'image originale, (b) Image partiellement chiffrée, (c) Image déchiffrée.

4.6 Conclusion

Dans cet article, nous avons introduit une nouvelle méthode de chiffrement des images médicales. Notre approche est basée sur le problème la coloration de graphes. Le problème de coloration de graphes est utilisé pour localiser quelques positions optimales des pixels que nous chiffrons ensuite, le but de cette sélection est d'obtenir un niveau de confidentialité élevé. Enfin, nous avons appliqué un ajustement approprié des valeurs de pixels pour faciliter la localisation des pixels chiffrés par le destinataire. Ce processus d'ajustement des pixels va compliquer l'application des méthodes de cryptanalyse.

Les résultats expérimentaux montrent clairement que notre algorithme proposé donne de bons paramètres d'évaluation P et $PSNR$.

Chapitre 5

Méthode de chiffrement des images basée sur la méthode stéganographique LSB et les algorithmes AES et RSA

5.1 Introduction

Ce chapitre est l'objet de la publication [15].

La vulnérabilité de la communication des images numériques est une question extrêmement importante de nos jours, en particulier lorsque les images sont communiquées par des canaux non sécurisés. Pour améliorer la sécurité des communications, de nombreux cryptosystèmes ont été présentés dans la littérature. Nous pouvons classer ces cryptosystèmes en deux grandes branches dites symétriques et asymétriques (voir les sections 3.5 et 3.6).

La première branche, les algorithmes symétriques les plus connus sont AES (Advanced Encryption Standard), DES (Data Encryption Standard) et 3-DES [138]. Ces techniques sont économiques et relativement sûres. Le plus grand problème avec ces algorithmes est l'échange et le stockage de la clé secrète.

La deuxième branche est le chiffrement asymétrique ou le chiffrement à clé publique [56]. Le même algorithme est utilisé pour le chiffrement et le déchiffrement avec une paire de clés, publique pour le chiffrement et privée pour lé déchiffrement. Il est impossible de calculer la clé privée à partir de la clé publique. Des systèmes asymétriques tels que RSA (Rivest, Shamir and Adleman) [56] nécessite l'utilisation de grands nombres (généralement plus grand que 512 bits), ce qui est inapproprié pour chiffrer des images [38, 164]. Cette branche cryptographique a un intérêt majeur, elle supprime le problème de transfert de la clé, mais elle ne peut pas remplacer les algorithmes symétriques parce que son temps de calcul est relativement long. Pour une grande quantité de données, il n'est pas préférable d'utiliser un chiffrement asymétrique [27, 50].

La stéganographie peut être également une solution pour augmenter la sécurité. La stéganographie est une technique utilisée pour cacher les données secrètes dans des médias de façon imperceptible. On peut trouver dans la littérature de nombreuses méthodes stéganographiques efficaces [57]. Parmi les méthodes les plus connues on trouve LSB (Least Significant Bit). Dans l'algorithme LSB, on insère des données en remplaçant les bits du poids faible par les bits de l'information à cacher.

Nous proposons dans ce chapitre une nouvelle technique de chiffrement des images basée sur la cryptographie symétrique, la cryptographie asymétrique et les techniques de la stéganographie. Les algorithmes symétriques sont plus rapides comparant avec les algorithmes asymétriques, l'inconvénient du chiffrement symétrique est l'obligation du partage de la clé secrète, le grand avantage des techniques asymétriques est l'élimination de transmission de la clé privée, mais les algorithmes asymétriques ne sont pas appropriés pour chiffrer les données de grand volume comme les images, à cause du temps de traitement qui est très long, par exemple le RSA est 1500 fois plus lent que l'algorithme symétrique DES [50]. La stéganographie ou la technique de cacher des messages, pourra également être utilisée dans la cryptographie. Nous proposons une technique basée sur les trois techniques, le chiffrement symétrique AES, le chiffrement asymétrique RSA et la méthode stéganoraphique LSB, notre approche profite des avantages des deux classes de chiffrement : les algorithmes symétriques et asymétriques, évite en même temps les inconvénients, c'est-à-dire, la méthode proposée profite de la vitesse des algorithmes symétriques et la sécurité des algorithmes asymétriques, et évite en même temps le partage de la clé et la non rapidité des méthodes asymétriques. La méthode proposée regroupe la sécurité des méthodes RSA, AES et LSB.

Les résultats de l'analyse montrent que les paramètres d'évaluation sont proches des valeurs optimales, également ces paramètres sont comparables avec celles présentées dans [97].

Dans la section 5.2, nous présentons une introduction à la stéganographique et l'algorithme LSB. Ensuite, nous décrivons l'approche proposée dans la section 5.3 et nous fournissons une analyse expérimentale dans la section 5.4. Enfin, nous donnons notre conclusion dans la section 5.5.

5.2 Stéganographie et tatouage

Etymologie grecque du mot stéganographie est "stego" le secret et "graphia" l'écriture. La stéganographie est la science pour cacher de façon imperceptible des informations secrètes dans des médias. Le principal but du tatouage numérique (watermarking en Anglais) est la protection des droits d'auteur en ajoutant des informations de copyright visibles ou non visibles. On peut trouver dans la littérature plusieurs techniques de stéganoraphie [57, 146, 174], et de tatouage numérique [53, 63, 65, 152, 175]. Cette section a pour objectif la compréhension de ces techniques. Nous donnons également l'algorithme LSB utilisé dans nos travaux. LSB est parmi

les méthodes les plus connues [39, 18, 57, 96, 98].

5.2.1 La stéganographie

Contrairement à la cryptographie, la stéganographie est l'art de la dissimulation de communications. La stéganographie n'a pas pour objectif seulement de sécuriser une communication, mais d'en cacher même l'existence (figures 5.1 et 5.2). Dans certaines situations, le faite de vouloir transmettre des données de manière chiffrée sera jugé comme suspect et attire la curiosité des adversaires. La stéganographie arrive en renforcement au chiffrement de données.

Nous présentons tout d'abord un historique des techniques de stéganographie. Nous posons ensuite les bases de la stéganographie moderne et mettons en évidence les propriétés stéganographiques. Nous en déduisons ainsi les services de sécurité offerts par de telles techniques ainsi que les règles fondamentales de leur mise en œuvre.

(a) (b) (c)

FIGURE 5.1: (a) Le message, (b) L'image originale, (c) Stégo-objet.

(a) (b) (c)

FIGURE 5.2: (a) L'image, (b) L'image originale, (c) Stégo-objet.

Histoire de la stéganographie

La première apparition de stéganographie répertoriée vient d'une histoire Grecque datant du 5ème siècle avant Jésus-Christ [99]. Afin de communiquer secrètement les

chefs de guerre utilisèrent des esclaves. Ils leurs tatouaient sur le crâne rasé et ensuite les cheveux repoussent. L'esclave était envoyé chez le correspondant. Une fois rasé le message était lisible.

En Chine ancienne, les messages étaient écrits sur de la soie, qui était ensuite roulée en boule, elle même recouverte de cire. Un messager devait avaler cette boule. Dès le Ier siècle av. J.-C. Les romains utilisaient l'encre invisible, qui fut la plus utilisée des méthodes de stéganographie à travers les siècles. On écrit, au milieu des textes écrits à l'encre, un message à l'aide de jus de citron, de lait ou de certains produits chimiques. Il est invisible à l'œil, mais une simple flamme, ou un bain dans un réactif chimique, révèle le message.
Les premiers ouvrages traitant la stéganographie datent du XVI^{me} siècle. En 1499, l'abbé Jean Trithéme (1462-1516) publie le premier traité de stéganographie, intitulé Steganographia [104]. Un scientifique allemand, Gaspart Schott (1608-1666) explique dans son livre Schola Steganographica [99] comment dissimuler des messages en utilisant des notes de musique.

La Stéganographie Moderne

La stéganographie dite moderne adaptée aux données numériques, est relativement jeune. Elle suit le développement d'Internet. Le socle de la stéganographie moderne a été posé par G. J. Simmon en 1983 [74] en définissant. La première édition d'Information Hiding datée de 1969 [28]. En 1997, l'une des premières thèses dans le domaine de dissimulation d'information est soutenue [132]. Le lecteur trouvera son bonheur dans les ouvrages [48, 72, 66, 103, 153, 142, 144, 175].

Architectures Stéganographique

Dans une architecture stéganographique, il y a principalement deux éléments (voir la figure 5.3) :

1. **Le processus de dissimulation :** l'insertion du message dans la donnée couverture.
2. **Le processus d'extraction :** l'extraction du message de la donnée couverture.

De manière générale, il existe trois type de protocoles de stéganographie :

1. La stéganographie pure : le secret de dissimulation des données ne réside que dans l'algorithme utilisé à cet effet.
2. La stéganographie à clé secrète : l'échange de données confidentielles nécessite, au préalable, l'échange d'une clé secrète que l'on ne partagera qu'avec notre interlocuteur.
3. La stéganographie à clé publique : similaire à la cryptographie asymétrique. La personne voulant envoyer des données à son interlocuteur, sans éveiller de soupçons, utilisera la clé publique de ce dernier. Le récepteur sera le seul à pouvoir en extraire son contenu à l'aide de sa clé privée.

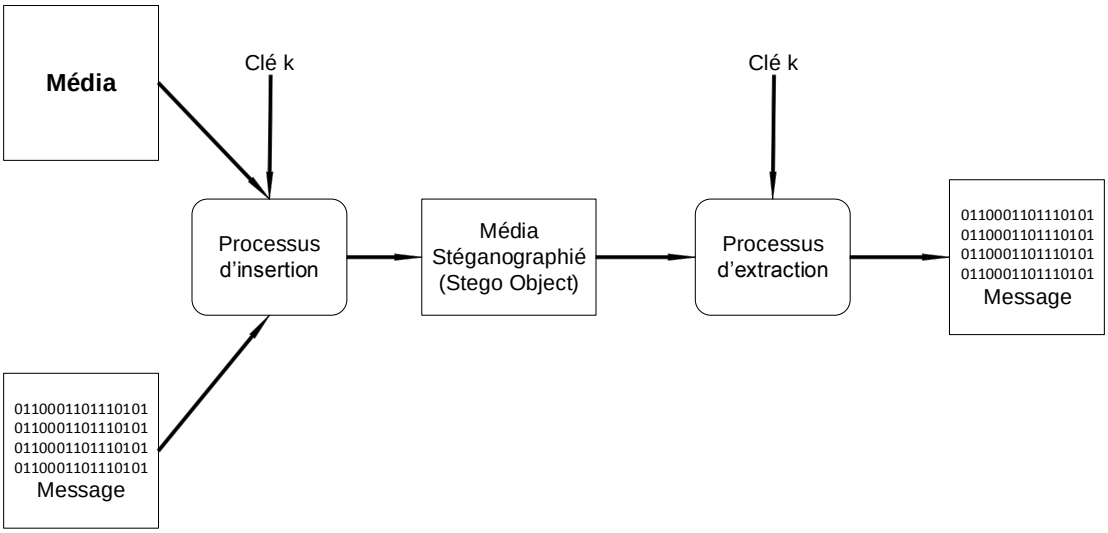


FIGURE 5.3: Schéma Stéganographique.

Caractéristiques d'un Schéma Stéganographique

Trois critères permettent d'évaluer les schémas stéganographiques : la capacité, la transparence et la robustesse.

1. La capacité : correspond à la quantité d'informations dissimulées dans dans le support.
2. La transparence : ou l'imperceptibilité, c'est-à-dire la probabilité que le stégo-objet soit détecter ou non. L'imperceptibilité dépend du nombre de modifications ou de changements qui a subit l'objet de couverture.
3. La robustesse : un schéma stéganographique est robuste si le stégo-objet reste normal après les transformations.

Un système stéganographique sûr et fiable a pour objectif envoyer le maximum d'informations sans qu'un adversaire puisse les détecter. La robustesse est importante pour le tatouage numérique (c.f la section 5.2.3). C. Cachin [32, 33] et R. Chandramouli [158, 159, 160] ont abordé les caractéristiques des algorithmes stéganographiques.

Techniques Stéganographiques

Il existe plusieurs techniques pour mettre en place des schémas stéganographiques. Nous décrivons ici ces techniques en fonction du type de support, ensuite nous allons détailler la méthode utilisée dans nos travaux il s'agit de la méthode LSB (Least Significant Bit).

1. La stéganographie sur images :

— Usage des bits de poids faible d'une image (LSB).
— Manipulation de la palette de couleurs d'une image.
— Message caché dans les choix de compression d'une image.

2. Dans un texte :
   — Modulation fine d'un texte.
   — Marquage de caractères.
   — Codage sous forme d'une apparence de spam.
3. Dans un fichier :
   — Dans les fichiers son, il existe à peu près les mêmes possibilités de cacher des messages que dans les fichiers images.
4. Fichiers HTML.
5. Canaux cachés HTTP, IP, TCP, où cachés DNS.
6. Rajout de données (EOF, en-têtes, ...) : Les données cachées consistent en un fichier image rajouté juste sous le marqueur EOF d'un fichier.

Parmi les techniques de stéganographie les plus dédiées aux images, on peut citer (liste non exhaustive) :

— **L'algorithme Outguess :** parmi les premiers algorithmes de stéganographie applicables aux images [146].
— **La méthode LSB (Least Significant Bit) :** le plus répandu dans monde de dissumulation d'informations [18, 39, 57, 96, 98], LSB sera présenté avec plus de détail dans la section 5.2.4 page 79.
— **L'algorithme F5 :** basé sur les coefficients DCT quantifiés, proposé par A.Westfeld en 1999 [20, 21].
— **JPHide et JPSeek :** est un algorithme conçu par A. Latham en 1999 [10, 143].

5.2.2 La stéganalyse

Contrairement à la cryptanalyse, dont le but est de déchiffrer les données ayant été chiffrées. La stéganalyse à pour but d'extraire ou de supprimer les messages insérés. La plupart des techniques stéganalyse recherche des artefacts créés par le processus stéganographique. Certains programmes laissent derrière eux des fichiers permettant de caractériser leur passage.

On peut trouver dans la littérature deux catégories d'attaques, spécifique et universelle [18, 98, 100].

L'attaque spécifique : Un attaquant qualifié de spécifique s'il cible un schéma de stéganographie particulier. Les attaques spécifiques se basent sur la détection d'irrégularité statistique du stégo-objet et la comparaison des distributions statistiques. Les méthodes les plus connues, on peut citer, entre autres : l'analyse du χ^2 de Andreas Westfeld et Andreas Pfitzmann [18], la métode RS développée par Fridrich, Miroslav Goljan et Rui Du [98], la steganalyse de

l'algorithme Outguess publiée par Jessica Fridrich, Miroslav Goljan et Dorin Hogea [100].

L'attaque universelle : Les techniques universelles, aussi appelées "blind steganography", sont essentiellement basées sur des architectures de type réseaux de neurones. Le principe étant de soumettre une base d'entraînements aussi diversifiée que possible, afin qu'il puisse détecter un large panel de techniques stéganographiques. Contrairement aux techniques plus spécifiques, les résultats de ce type d'architecture est de type binaire (stéganographié/non stéganographié). Ils sont moins efficaces comparativement à une technique spécifique.

On peut trouver dans la littérature plusieurs attaques universelles récentes comme : le distingueur linéaire de Fisher [71], le schéma de stéganalyse universelle adapté au domaine fréquentiel compressé [102] et l'algorithme RS proposé par J. Fridrich,M. Goljan et R. pour détecter l'utilisation de LSB [106].

Les règles de bases minimales pour faire face à des attaques sont :

1. C'est l'émetteur qui doit générer le support de couverture.
2. Pour éviter les attaques par différence et les attaques visuelles, le support de couverture doit être utilisé qu'une seule fois et détruit après utilisation.

5.2.3 Le tatouage numérique

Le tatouage numérique (appelés quelques fois le marquage numérique ou le watermarking en Anglais) est une discipline très récente [53, 63]. Contrairement à la stéganographie, les outils de tatouage numérique, sont utilisés principalement pour la protection de droit d'auteur, sont principalement développés afin d'avoir une grande robustesse, i.e difficile de supprimer la donnée insérée. L'adversaire ne s'intéresse pas au contenu inséré lui même, son unique objectif est la suppression de ce contenu sans modifier l'image. Le message inséré peut être le nom propriétaire ou la marque (figure 5.4).

(a) (b)

FIGURE 5.4: Le tatouage numérique : (a) L'image originale, (b) L'image tatouée.

On distingue généralement trois types de tatouage : visibles, invisibles et fragiles.

1. Le tatouage visible : par exemple ajouter la marque dans une image pour protéger les droits.
2. Le tatouage invisible : on insère le message d'une manière imperceptible. Le tatouage invisible peut être considéré comme une forme de stéganographie. Il est utilisé pour protéger les droits de façon invisible.
3. Le tatouage fragile : C'est un tatouage de type invisible, il est utilisé pour vérifier l'intégrité du document, c'est-à-dire vérifier si le contenu n'a pas été modifié par un tiers.

Le lecteur intéressé par les techniques du tatouage numérique pourra se référer aux ouvrages [31, 142, 175].

5.2.4 La méthode LSB (Least Significant Bit)

Pour chaque pixel, la couleur est codée avec trois octets : rouge, vert et bleu, chaque octet est codé sur 8 bits. Chaque octet indique l'intensité de la couleur, et le rang est de 0 à 255. La stéganographie LSB (Least Significant Bit) consiste à dissimuler l'information dans des bits de poids faibles d'un support numérique. Historiquement, la stéganographie LSB adaptée aux images fixes non compressées est l'une des premières techniques stéganographiques même l'une des plus employées encore aujourd'hui.
Utiliser LSB revient à remplacer certaines données déjà présentes dans un fichier par l'information à cacher. Cette méthode peut sembler simpliste, mais il faut faire attention à ne pas supprimer de données importantes qui rendraient impossible la lecture du stégo-objet final. Typiquement, on substitue les données non primordiales par notre message. Le destinataire extrait l'information s'il connait les positions où le message a été substitué. Puisque seules des modifications mineures ont été apportées dans le processus de dissimulation, l'émetteur présume qu'elles ne seront pas détectées par un attaquant passif.

Exemple 5.2.1.

On veux cacher la lettre A dans 3 pixels. Soit le code binaire des 3 pixels (9 octets) :

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

La valeur binaire de A est 10000011. En insérant la valeur binaire de A dans les 3 pixels, on obtiendrait le résultat suivant :

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

Parmi les 8 bits utilisés, les bits soulignés sont ceux qui ont été modifiés et en gras les bits de poids faible nécessaire pour comprendre le message entier. Cette modification est imperceptible pour l'œil humain, car la luminance de ces pixels aura varié d'au plus 1.

Une approche plus sophistiquée de cette méthode réside dans l'utilisation d'un générateur de nombres pseudo-aléatoires pour étaler le message secret sur l'image. Si les deux participants à la communication partage une clé k utilisable comme graine pour un générateur de nombres aléatoires, ils peuvent créer une suite aléatoire. Ainsi, la distance entre deux bits encapsulés est déterminée aléatoirement. Puisque le récepteur a accès à la graine k et a connaissance du générateur de nombres pseudo aléatoires.

5.3 Notre approche

Les méthodes asymétriques sont inappropriées pour les images car le temps de calcul est long. Mais ils sont plus sécurisées que les méthodes symétriques car ils suppriment l'échange de la clé secrète.

Pour les données énormes, il n'est pas économique d'utiliser les méthodes asymétriques comme RSA, par exemple l'algorithme symétrique DES est 1500 fois plus rapide que RSA [27, 50].

Pour profiter de la vitesse du chiffrement symétrique, de la sécurité du chiffrement asymétrique et des méthodes stéganographiques, nous proposons un algorithme qui combine les méthodes AES, RSA et LSB. En premier lieu, nous chiffrons l'image originale en utilisant AES et une clé secrète k générée aléatoirement. Ensuite, cette clé secrète est chiffrée à l'aide de RSA. Enfin, la clé secrète chiffrée k' est cachée dans l'image chiffrée en utilisant la méthode LSB (Figure 5.5).

L'approche proposée élimine le partage de la clé pendant le processus de chiffrement. La force de notre technique est basée sur les points positifs de RSA, AES et LSB.

5.4 Résultats expérimentaux

Nous analysons l'algorithme proposé sur plusieurs images en niveaux de gris de différentes tailles afin d'évaluer sa force. Nous avons choisi trois images qui sont présentées dans les figures 5.6, 5.7 et 5.8. Pour le chiffrement, nous avons appliqué un chiffrement par flux en utilisant l'algorithme AES en mode OFB (Output Feedback Block) avec une clé k de longueur 128 bits. La clé k a été chiffrée avec l'algorithme

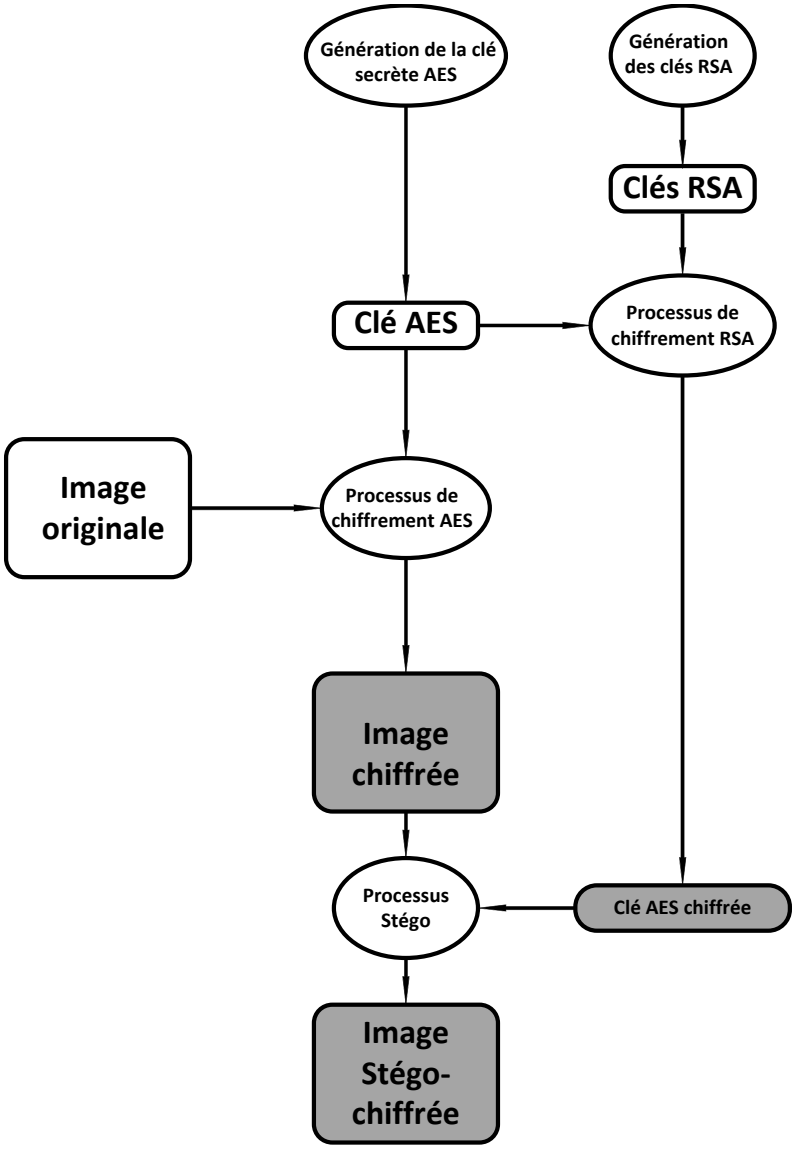


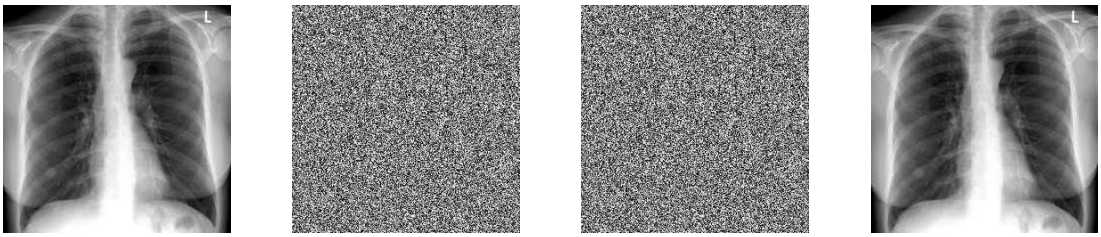
FIGURE 5.5: Notre approche : Chiffrement AES-RSA-LSB.

Algorithm 7: Schéma de chiffrement proposé

1. Nécessaire : AES, RSA, LSB.
2. Input : Image originale I.
3. Output : Image Stego-chiffrée I_2.
4. Générer aléatoirement une clé secrète "k".
5. Chiffrer l'image I utilisant l'algorithme AES et la clé secrète "k".
6. Chiffrer la clé secrète "k" utilisant l'algorithme RSA.
7. Cacher la clé de chiffrée "k'" utilisant LSB dans l'image chiffrée I_1.
8. Retourner l'image stego-chiffrée I_2.

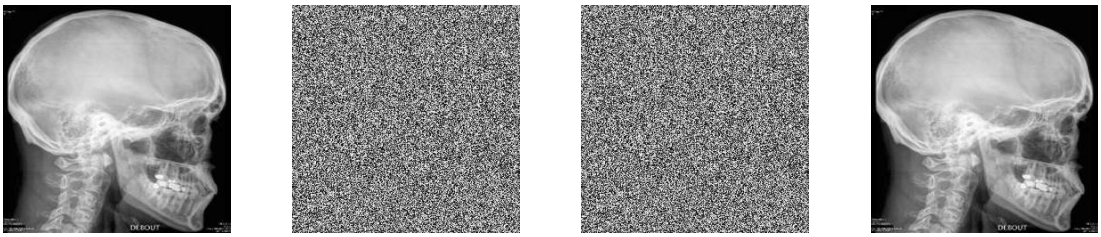
Algorithm 8: Schéma de déchiffrement proposé

1. Nécessaire : AES, RSA, LSB.
2. Input : Image Stego-chiffrée I_2.
3. Output : Image déchiffrée I.
4. Extraire de l'image I_2 en utilisant LSB la clé secrète chiffrée "k'".
5. Déchiffrer en utilisant l'algorithme RSA la clé secrète "k'".
6. Déchiffrer l'image I_1 utilisant l'algorithme AES et la clé secrète "k".
7. Retourner l'image déchiffrée I.



(a) (b) (c) (d)

FIGURE 5.6: Cancer du poumon : (a) L'image originale, (b) L'image chiffrée, (c) Stego-image, (d) L'image déchifrée.



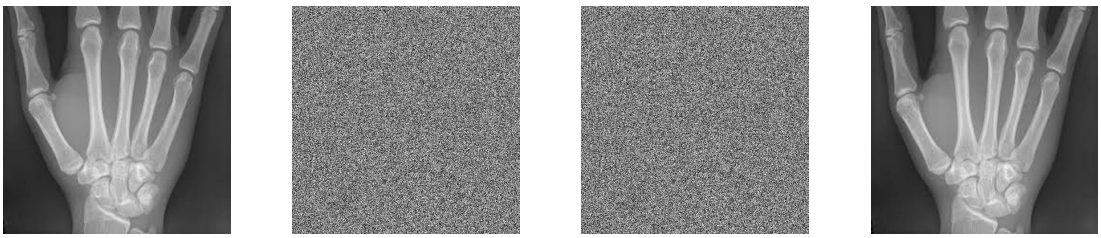
(a) (b) (c) (d)

FIGURE 5.7: Crâne : (a) L'image originale, (b) L'image chifrée, (c) Stego-image, (d) L'image déchifrée.

RSA. Ensuite, en utilisant la méthode LSB, la clé chiffrée k' est caché dans l'image chiffrée (Figure 5.6.b.). Après l'extraction de la clé secrète et le déchiffrement (Figure 5.6.c.) nous obtenons l'image déchiffrée (Figure 5.6.d.).

5.4.1 Effet du bruit :

Tous les types de données numériques, y compris les images, contiennent du bruit. Dans un cryptosystème si l'image déchiffrée est similaire à l'image d'origine, alors le système de cryptage est résistant contre le bruit. Après déchiffrement de l'image stego-chiffrée, nous avons observé que la qualité de l'image finale est bonne (PSNR



(a) (b) (c) (d)

FIGURE 5.8: Main : (a) L'image originale, (b) L'image chifrée, (c) Stego-image, (d) L'image déchifrée.

Les images	La taille de l'image	PSNR de l'image déchiffrée (dB)
Cancer du poumon	256×256	52.42
Crâne	256×256	52.87
Main	512×512	53.81

TABLE 5.1: Résistance au bruit du chiffrement AES-RSA-LSB.

	L'image originale	L'image chiffrée	L'image Stégo-chiffrée
Horizontal	0.9603	0.0915	0.0045
Vertical	0.9251	0.0152	0.0204
Diagonal	0.9143	0.0012	0.0425

TABLE 5.2: Cancer du poumon : Analyse de corrélation entre deux pixels adjacents.

$>$ 50 dB) qui garantit que l'algorithme proposé a une bonne résistance contre le bruit. Les résultats expérimentaux sont présentés dans le tableau 5.1.

5.4.2 Analyse de l'espace clé :

Pour un cryptosystème sécurisé, l'espace clé doit être suffisamment grand pour être sûr que l'attaque de force brute est impossible. Dans notre cas, puisque nous utilisons le système de cryptage RSA pour chiffrer la clé secrète AES, l'espace clé est au moins le même que RSA c-à-d 2^{80} à cause de l'utilisation de RSA. D'autre part, la clé est différente pour chaque image puisque elle est générée aléatoirement pour chaque image. Si la clé est cassée pour une image, il faudra la casser pour chaque image, donc, l'espace clé est $2^{80} \times$ *le nombre d'images*. Il n'est pas possible de déchiffrer le cryptosystème avec la technologie actuelle. .

5.4.3 L'analyse de corrélation :

Si le coefficient de corrélation entre les pixels adjacents dans l'image originale et l'image chiffrée est proche de 1, cela signifie que l'image originale et l'image chiffrée sont très dépendantes l'une de l'autre, i.e. l'image originale peut être facilement reproduite à partir de l'image chiffrée [80, 140], et le processus de chiffrement a échoué à cacher les détails de l'image originale. Les valeurs du coefficient de corrélation proches du zéro signifient une bonne résistance contre les attaques de corrélation.

Nous avons testé la corrélation entre les pixels adjacents dans l'image originale et l'image chiffrée. Nous avons obtenu une corrélation négligeable, il est donc difficile de casser l'algorithme en utilisant des attaques de corrélation. Les résultats sont donnés dans les tableaux 5.2, 5.3 et 5.4.

	L'image originale	L'image chiffrée	L'image Stégo-chiffrée
Horizontal	0.9412	0.0065	0.0256
Vertical	0.9545	0.0376	0.0087
Diagonal	0.9205	0.0189	0.0141

TABLE 5.3: Crâne : Analyse de corrélation entre deux pixels adjacents.

	L'image originale	L'image chiffrée	L'image Stégo-chiffrée
Horizontal	0.9625	0.0075	0.0258
Vertical	0.9348	0.0526	0.0084
Diagonal	0.9066	0.0185	0.0213

TABLE 5.4: Main : Analyse de corrélation entre deux pixels adjacents.

5.4.4 Analyse d'entropie :

L'entropie de l'information est un outil important pour analyser la robustesse d'un système de chiffrement. Par l'entropie nous pouvons montrer le degré d'incertitudes du système [195]. La valeur optimale de l'entropie est 8. Pour qu'un cryptosystème soit invulnérable, l'entropie doit être proche de la valeur optimale. L'algorithme proposé répond à cette analyse avec des bons paramètres comme le montre le tableau 5.5.

5.4.5 Comparaison de la technique proposée et l'algorithme étudié dans [97] :

Nous comparons le coefficient de corrélation et la valeur d'entropie de notre schéma avec l'algorithme AES étudié dans [97] (voir le tableau 5.6). A partir du tableau 5.6, on peut constater que les analyses du schéma proposé sont comparables avec celles de l'algorithme AES présenté dans [97]

Image	L'image originale	L'image chiffrée	L'image stégo-chiffrée
Cancer du poumon	7.5605	7.7625	7.7812
Crâne	7.2856	7.6115	7.6822
Main	6.8644	7.7365	7.8275

TABLE 5.5: La valeur d'entropie : L'image originale, l'image chiffrée et l'image stégo-chiffrée.

Analyse statistique	La technique proposé (hand.jpg)		AES [97]	
Images	L'image originale	L'image stégo-chiffrée	Plain Image	L'image chiffrée
Horizontal Cor	0.9625	0.0258	0.9282	−0.0067
Vertical Cor	0.9348	0.0084	0.9644	0.0504
Diagonal Cor	0.9066	0.0213	0.9116	−0.0156
L'entropie		7.8275		7.9975

TABLE 5.6: Comparaison de la technique proposée et l'algorithme étudié dans [97].

5.5 Conclusion

Dans cet article, nous avons introduit une nouvelle méthode de chiffrement des images. Notre approche est basée sur le chiffrement symétrique, le chiffrement asymétrique et la stéganographie. Premièrement, nous utilisons le chiffrement symétrique pour chiffrer l'image. Ensuite, nous employons un algorithme asymétrique pour la sécurité de la clé. Dans la dernière étape, nous cachons la clé chiffrée dans l'image chiffrée en utilisant la méthode steganographique LSB.

Les résultats de l'analyse de la sécurité sont présentés dans les tableaux 5.1, 5.2, 5.3, 5.4, 5.5 et 5.6. On peut constater que l'algorithme proposé est invulnérable contre les attaques les plus connues. Nous pouvons donc l'utiliser pour un chiffrement sécurisé et économique des données de grand volume.

Chapitre 6

Un nouveau cryptosystème multi-récepteur à clé publique basé sur les suites de Lucas

6.1 Introduction

Ce chapitre est l'objet de la soumission [113].

Le chiffrement multi-récepteur permet à un expéditeur d'une donnée de la chiffrer et de la transmettre via des canaux non sécurisés à un ensemble d'utilisateurs autorisés. Personne hors de ce groupe d'utilisateurs ne peut déchiffrer le message. Le chiffrement multi-récepteur a une grande importance dans de nombreux secteurs tels que la diffusion de communication, informatique en nuage (cloud computing), les communications sans fil, les applications sur les réseaux, le vote électronique, la loterie et les applications médicales.

De nombreuses applications de nos jours utilisent l'échange multi-récepteur puisque le chiffrement standard avec un récepteur unique n'est pas approprié. La motivation principale du chiffrement multi-récepteur est d'assurer la sécurité des communications dans un groupe.

Dans cet article, nous avons proposé un schéma de chiffrement multi-récepteur à clé publique basé sur les suites de Lucas. Les résultats de l'analyse montre que notre approche est plus efficace par rapport aux systèmes existants et satisfait anonymat des récepteurs.

Il y a plusieurs schémas de chiffrement multi-récepteur proposés dans la littérature basés sur différentes techniques [3, 69, 129, 30, 76, 117, 173, 197]. En 1993 Smith et Lennon [154], ont été les premiers à introduire un cryptosystème utilise les suites linéaires, dans lequel ils utilisent une nouvelle fonction à trappe basé sur les suites de Lucas. Ils ont suggéré que des suites linéaires du second ordre pourraient être utilisées à la place de l'exponentiation utilisé dans RSA. Par exemple le chiffrement à clé publique ElGamal [181] peut être formulé par les fonctions de Lucas [55, 64]. Également, l'échange de clé de Diffie-Hellman peut être construit par les fonctions

de Lucas [186]. Deux ans plus tard, Chi-Sung et al ont montré que la sécurité des fonctions Lucas est équivalente aux problèmes de logarithme discret [36]. En 2012, El Fadil a proposé un système de chiffrement basé sur les suites linéaires du second ordre dans lequel la sécurité sémantique est assurée [116].

Smith et Lennon [154] ont montré que le principal avantage de leur cryptosystème est l'utilisation des fonctions de Lucas à la place de l'exponentiation. Cela le rendrait invulnérable contre les attaques connues qui menacent la sécurité des cryptosystèmes plus traditionnels comme RSA et Diffie Hellman [40]. Puisque les fonctions Lucas peuvent être considérées comme une généralisation de la fonction exponentielle, toute attaque réussie sur les systèmes basés sur les fonctions de Lucas sera automatiquement réussis sur celles basées sur l'exponentiation [36].

Dans cet article nous avons proposé un nouveau schéma de chiffrement multi-récepteur à clé publique basé sur les suites de Lucas. Les résultats des analyses montrent que le modèle proposé garantit l'anonymat, résistant contre les attaques connues et efficace en terme de temps de calcul. Nous avons proposer également dans cet article un schéma d'échange Diffie-Helman basé sur les suites de Lucas.

Ce chapitre est organisé comme suit, dans la Section 6.2, nous donnons une description du chiffrement à clé publique LUC. Dans la même section, nous allons définir les suites linéaires du second ordre dite "les suites de Lucas", leurs propriétés serons également discutées. Ensuite, nous présentons nos résultats avec l'analyse de la sécurité dans la Section 6.3. Enfin, nous donnons notre conclusion dans la Section 6.4.

6.2 Le chiffrement à clé publique LUC :

LUC est un cryptosystème a clé publique développé par un groupe de chercheurs Basés en New Zéland [154, 155]. Comme tout les cryptosystèmes à clé publique, LUC peut être utilisé pour le chiffrement, la signature numérique et l'échange de clés.

LUC est basé sur l'utilisation les grands nombres de la suite de Lucas. Nous commençons par une vue générale sur la suite de Lucas qui est un cas particulier des suites récurrentes linéaires. Ensuite, nous présenterons les propriétés des suites de Lucas.

6.2.1 Les suite récurrente linéaire :

Définition 6.2.1. *On appelle suite récurrente linéaire d'ordre p toute suite à valeurs dans un corps commutatif K définie pour tout $n \geq n_0$ par une relation de récurrence linéaire de la forme :*

$$\forall n \geq n_0 \quad u_{n+p} = a_0 u_n + a_1 u_{n+1} + \cdots + a_{p-1} u_{n+p-1} \tag{6.1}$$

où $a_0, a_1, \cdots a_{p-1}$ sont p scalaires fixés de K (a_0 non nul).

L'expression du terme général d'une telle suite est possible si on est capable de factoriser un polynôme qui lui est associé, appelé le polynôme caractéristique.

Définition 6.2.2. *Le polynôme caractéristique associé à une suite récurrente linéaire est donnée par la formule :*

$$\begin{aligned} f(X) &= X^p - \sum_{i=0}^{p-1} a_i X^i \\ &= X^p - a_{p-1}X^{p-1} - a_{p-2}X^{p-2} - \cdots - a_1 X - a_0. \end{aligned} \tag{6.2}$$

Remarque 6.2.3. *Le degré du polynôme caractéristique est ainsi égal à l'ordre de la relation de récurrence. En particulier, dans le cas des suites d'ordre 2, le polynôme est de degré 2 et peut donc être factorisé à l'aide du discriminant.*

Exemples 6.2.4.

1. **La suite géométrique :** La suite récurrente linéaire d'ordre 1 est une suite géométrique, la relation de récurrence est $u_{n+1} = qu_n$ et le terme général est $u_n = u_{n_0} q^{n-n_0}$.
2. **Suite récurrente linéaire d'ordre 2 :** a et b étant deux scalaires fixés de K avec b non nul, la relation de récurrence est :

$$u_{n+2} = au_{n+1} + bu_n. \tag{6.3}$$

3. **Suite de Fibonacci :** L'exemple type d'une récurrence linéaire à deux termes (ordre 2) est la célèbre suite de Fibonacci définie pour $a = b = 1$ par :

$$u_o = u_1 = 1 \text{ et } u_{n+2} = u_n + u_{n+1}. \tag{6.4}$$

6.2.2 Les suites de Lucas

Les suites de Lucas sont deux suites d'entiers u_n et v_n générées par deux entiers P et Q premiers entre eux. La théorie de suites de Lucas est développée par le mathématicien français Édouard Lucas en 1878 [190]. Les termes de cette suite sont appelés les nombres de Lucas. Nous donnons la définition des suites des Lucas et la factorisation de son polynôme caractéristique. Plus de détails sur les suites de Lucas peut être trouvé dans le livre de Ribenboim [151] et les papiers de Smith. P [154, 155].

Définition 6.2.5. *Soit P et Q entiers non nuls premiers entre eux. Les suites de Lucas $u(P,Q)$ et $v(P,Q)$ sont définies par les relations récurrentes linéaires :*

$$u_{n+2}(P,Q) = Pu_{n+1} - Qu_n,\ u_0 = 0,\ u_1 = 1,\ n \in \mathbb{N}. \tag{6.5}$$

$$v_{n+2}(P,Q) = Pv_{n+1} - Qv_n,\ v_0 = 2,\ v_1 = P,\ n \in \mathbb{N}. \tag{6.6}$$

Étant donné que (6.5) et (6.6) sont linéaires, ils sont tous deux résolubles en déterminant les racines de l'équation caractéristique :

$$X^2 - PX + Q = 0 \tag{6.7}$$

Soit $D = P^2 - 4Q$ le discriminant de (6.7). Les racines de (6.7) peut être calculé comme suit :

$$\alpha = \frac{P + \sqrt{D}}{2},\ \beta = \frac{P - \sqrt{D}}{2}. \tag{6.8}$$

Les racines de l'équation caractéristique (6.7) α et β satisfont :

$$\alpha + \beta = P\ , \alpha\beta = Q, \tag{6.9}$$

Le discriminant D ce peut être écrit :

$$D = (\alpha - \beta)^2. \tag{6.10}$$

En fonction de α et β (6.8), on peut décrire explicitement la suite de Lucas comme :

$$u_n(P, Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta},\ n \in \mathbb{N}. \tag{6.11}$$

Ainsi, si c_1 et c_2 de deux entiers quelconques, alors la suite $(c_1\alpha^n + c_2\beta^n)$ à la propriété suivante :

$$\begin{aligned} P(c_1\alpha^{n-1} + c_2\beta^{n-1}) - Q(c_1\alpha^{n-2} + c_2\beta^{n-2})) &= c_1\alpha^{n-2}(P\alpha - Q) + c_2\beta^{n-2}(P\beta - Q) \\ &= c_1\alpha^{n-2}(\alpha^2) + c_2\beta^{n-2}(\beta^2) \text{ par (6.7)} \\ &= c_1\alpha^n + c_2\beta^n. \end{aligned}$$

Donc, la suite $(c_1\alpha^n + c_2\beta^n)$ satisfait la relation récurrente linéaire (6.5), et toute suite u_n satisfait la relation (6.5) s'écrit sous la forme :

$$u_n(P, Q) = c_1\alpha^n + c_2\beta^n,\ \text{où } u_0 = c_1 + c_2,\ u_1 = c_1\alpha + c_2\beta$$

Par conséquent la suite de Lucas u_n s'écrit :

$$u_n(P, Q) = \frac{\alpha^n - \beta^n}{\alpha - \beta},\ (\text{pour } c_1 = \frac{1}{\alpha - \beta},\ c_2 = -\frac{1}{\alpha - \beta}),\ u_0 = 0,\ u_1 = 1,$$

et la suite la suite v_n de Lucas s'écrit :

$$v_n(P, Q) = \alpha^n + \beta^n,\ (\text{pour } c_1 = c_2 = 1)\ ,\ v_0 = 2,\ v_1 = \alpha + \beta = P,\ n \in \mathbb{N}. \tag{6.12}$$

Remarques 6.2.6.

1. Puisque les premiers termes $u_0 = 0$, $u_1 = 1$, $v_0 = 2$ et $v_1 = P$ sont des entiers, alors les suites u_n et v_n sont des suites d'entiers.
2. Pour tout entier N :

$$u_n\left(P \pmod N, Q \pmod N\right) \equiv u_n(P,Q) \pmod N. \tag{6.13}$$

Démonstration. Ce résultat est trivial pour $n = 0$ et $n = 1$, et pour $n \geq 2$:

$$\begin{aligned} u_n(P,Q) \pmod N &\equiv \left(P \pmod N\right)\left(u_{n-1}(P,Q) \pmod N\right) - \\ &\quad \left(Q \pmod N\right)\left(u_{n-2}(P,Q) \pmod N\right) \text{ par (6.5)} \\ &\equiv u_n\left(P \pmod N, Q \pmod N\right). \end{aligned}$$

Donc, nous avons (6.13). De la même façon nous obtenons :

$$v_n\left(P \pmod N, Q \pmod N\right) \equiv v_n(P,Q) \pmod N \tag{6.14}$$

□

3. Les nombres de Lucas augmentent très rapidement, le tableau (6.1) présente les premiers nombres de Lucas pour $P = 3$ et $Q = 1$.

Les propriétés des suites de Lucas :

On peut trouver plusieurs relations entre les deux suites de Lucas u_n, v_n, P, Q et le discriminant D de l'équation (6.7),

Nous avons les relations suivantes, qui sont facile à démontrer en utilisant les définitions de u_n et v_n et les relations (6.9), (6.10), (6.11) et (6.12) :

$$v_{2n} = v_n^2 - 2Q^n \tag{6.15}$$

$$v_{2n-1} = v_n v_{n-1} - PQ^{n-1} \tag{6.16}$$

$$v_{2n+1} = Pv_n^2 - Qv_n v_{n-1} - PQ^n \tag{6.17}$$

$$v_n^2 = Du_n^2 + 4Q^n \tag{6.18}$$

$$2v_{n+m} = v_n v_m + Du_n Du_m \tag{6.19}$$

$$2Q^m v_{n-m} = v_n v_m - Du_n Du_m. \tag{6.20}$$

n	$v_n(3,1)$	$u_n(3,1)$
0	2	0
1	3	1
2	7	3
3	18	8
4	47	21
5	123	55
6	322	144
7	843	377
8	2207	987
9	5778	2584
10	15127	6765
11	39603	17711
12	103682	46368
13	271443	121393
14	710647	317811
.	.	.
.	.	.
.	.	.
24	10749957122	4807526976

TABLE 6.1: Exemple des premiers nombres de Lucas pour $P = 3$ et $Q = 1$.

6.2.3 L'algorithme de chiffrement monocast LUC :

Nous donnons les définitions de résidu quadratique modulo et le symbole de Legendre [50, 131], des concepts utilisés dans les propriétés cryptographiques de la suite $s(a)$ de Lucas utilisée dans nos travaux.

Définition 6.2.7. *Soit $p \in \mathbb{Z}$ un premier impair. On dit que $n \in \mathbb{Z}$ est* ***un résidu quadratique modulo*** *p si $n \pmod p$ est un carré dans $\mathbb{F}_p$, c'est-à-dire s'il existe $m \in \mathbb{Z}$ tel que $n \equiv m^2 \pmod p$.*

Définition 6.2.8. *Soit p un nombre premier $p \neq 2$ et $a \in \mathbb{Z}$.* ***Le symbole de Legendre*** *est définit par :*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & si\ a \equiv 0 \pmod p \\ +1 & si\ a\ est\ un\ carré\ non\ nul\ modulo\ p \\ -1 & si\ a\ n'est\ pas\ un\ carré\ non\ nul\ modulo\ p. \end{cases} \tag{6.21}$$

Si $\left(\frac{a}{p}\right) = +1$ on dit que a est un résidu quadratique modulo p.
Si $\left(\frac{a}{p}\right) = -1$ on dit que a n'est pas un résidu quadratique modulo p.

Propriétés 6.2.9. *Nous avons les propriétés suivantes qui facilitent le calcule de ce symbole :*

1. *Pour $a, b \in \mathbb{Z}$:*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \ \text{ et } \ \left(\frac{a}{p}\right) = 0 \ \text{ si et seulement si } PGCD(a,p) > 1.$$

2. *Critère d'Euler : Pour $a \in \mathbb{Z}$:*

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p.$$

3. *Pour tout $p \neq 2$:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \ \text{ et } \ \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

4. *Loi de réciprocité quadratique : Pour p, q impairs et distincts :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Exemple 6.2.10. *L'équation $x^2 = 219$ admet-elle une solution modulo 383 ?*

$$\begin{aligned}\left(\frac{219}{383}\right) &= \left(\frac{3}{383}\right)\left(\frac{73}{383}\right)\\ &= -\left(\frac{383}{3}\right)\left(\frac{383}{73}\right)\\ &= -1\left(\frac{-1}{3}\right)\left(\frac{18}{73}\right)\\ &= \left(\frac{2}{73}\right)\\ &= 1.\end{aligned}$$

La réponse est oui.

La structure de LUC est similaire à RSA. La donnée claire est chiffrée en blocs, chaque bloc à une valeur binaire inférieur à $N = pq$ (l'entier de RSA). Le chiffrement et le déchiffrement pour un bloc P de donnée clair et une donnée chiffrée C est comme suit [154, 155] :

$$\begin{aligned}&\text{Le chiffrement : } C \equiv v_e(P,1) \pmod N\\ &\text{Le déchiffrement : } M \equiv v_d(C,1) \pmod N.\end{aligned} \tag{6.22}$$

Alice et Bob doivent partager la même information N. La clé publique de Bob est (e, N), la clé privée de Bob est (d, N). Ce cryptosystème à clé publique doit satisfaire les conditions suivantes [151] :

1. Il est possible de calculer les valeurs de e, d et N tels que :

$$v_d\left(v_e(P,1) \pmod N, 1\right) \pmod N \equiv P \pmod N. \tag{6.23}$$

2. Il est facile de calculer $v_e(P,1) \pmod N$ et $v_d(C, 1 \pmod N))$ pour tout $P \leq N$.
3. Il est impossible de déterminer d à partir de e et N.
4. Il est infaisable de calculer P à partir de C, e et N.

Où le $PGCD$ est le Plus Grand Commun Diviseur. Le $PPCM$ est le Plus Petit Commun Multiple. $\left(\frac{\cdot}{p}\right)$ est le symbole de Legendre. Le lecteur pourra trouver la preuve complète du shéma de LUC dans le célèbre papier de P. Smith [154]

Exemple 6.2.11. ***Chiffrement LUC :***

1. Choisir deux nombres premiers $p = 1949$ et $q = 2089$.
2. $N = p \times q = 4071461$.
3. Choisir $e = 1103$, premier avec $1948 \times 1950 \times 2088 \times 2090$.

Algorithm 9: Le chiffrement à clé pulique LUC.

Génération des clés :

1 Choisir des grands nombres premiers p et q.

2 Calculer $N = p \times q$.

3 Choisir un entier e tel que $PGCD\left[((p-1)(q-1)(p+1)(q+1), e)\right] = 1$.

4 Calculer le discriminant $D = P^2 - 4$ (P la donnée claire).

5 Calculer $S(N) = PPCM\left[\left(p - \left(\frac{D}{p}\right)\right), \left(q - \left(\frac{D}{q}\right)\right)\right]$.

6 Calculer $d = e^{-1} \pmod{S(N)}$.
La clé publique : la paire (N, e).
La clé privée : la paire (N, d).

7 Chiffrement :

$$P < N \qquad C = v_e(P, 1) \pmod{N}.$$

8 Déchiffrement :

$$P = v_d(C, 1) \pmod{N}.$$

4. La donnée claire $P = 11111$.
5. Calculer le discriminant $D = P^2 - 4 = 11111^2 - 4 = 123454317$.
6. Calculer $S(N) = PPCM\left[(1949 + 1), (2089 + 1)\right] = 407550$.
7. Calculer $d = e^{-1} \pmod{407550} = 24017$.
   La clé publique : la paire $(N, e) = (4071461, 1103)$.
   La clé privée : la paire $(N, d) = (4071461, 24017)$.
8. **Chiffrement de P :** $C = v_{1103}(P, 1) \pmod{4071461} = 3975392$.
9. **Déchiffrement de C :** $P = v_{24017}(3975392, 1) \pmod{4071461} = 11111$.

6.3 Les résultats Principaux

Dans cette section, nous décrivons nos principaux résultats, il s'agit de deux applications des suites Lucas :

1. **Le schéma de chiffrement multi-récepteur de Lucas :** Un système de chiffrement à clé publique multi-destination basé sur le chiffrement LUC.
2. **L'échange de clé de Lucas Diffie-Hellman étendue à un groupe d'utilisateurs :** Un procédé d'échange de clés étendu à un groupe d'utilisateurs.

Avant de présenter notre approche nous donnons la définition de la suite de Lucas utilisée pendant nos travaux. Il s'agit d'un cas particulier des suites de Lucas présentées dans la section (6.2.2) page 89. Les propriétés cryptographique de cette suite seront également évoquées avec l'analyse du coût de calcul du k^{eme} terme s_k.

6.3.1 Notations et Définitions

Tout au long de cette section, nous utiliserons les notations et les définitions suivantes :

- p est un nombre premier.
- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini de de p éléments.
- $\mathbb{F}_p[X]$ l'anneau des polynômes à coefficients dans $\mathbb{F}_p$.
- $n = pq$ l'entier de RSA.
- $a \in \mathbb{Z}$ tel que $PGCD(n, a) = 1$.
- $f(X) = X^2 - aX + 1$ est un polynôme primitive sur $\mathbb{F}_p[X]$.
- $A = \mathbb{F}_p[X]/(f(X))$.
- α racine de $f(X)$ dans le corps de décomposition de $f(X)$.
- Puisque nous avons qu'une seule suite de Lucas, nous allons la noter $(s_n)_n$.

Définition 6.3.1. *Pour tout $x \in A$ nous définissons l'application linéaire l_x de $A = \mathbb{F}_p[X]/(f(X))$ par :*

$$\begin{array}{rccc} l_x : & A & \longrightarrow & A \\ & y & \longmapsto & l_x(y) = xy \end{array}$$

Nous définissons également trace de x $T(x)$ et la norme de x $N(x)$ dans A par :

$$\begin{array}{rccc} T : & A & \longrightarrow & A \\ & x & \longmapsto & T(x) = Tr(l_x), \end{array}$$

$$\begin{array}{rccc} N : & A & \longrightarrow & A \\ & x & \longmapsto & N(x) = det(l_x). \end{array}$$

Où $det(l_x)$ et $Tr(x)$ sont le déterminant et la trace de l_x respectivement.

Définition 6.3.2. *Nous définissons la suite $s(a)$ comme suit :*

$$k \in \mathbb{Z},\ s_k(a) = T(\alpha^k). \tag{6.24}$$

Puisque $f(\alpha) = 0$ et $Tr(l_x)$ est linéaire, il résulte :

$$s_{k+2}(a) = as_{k+1}(a) - s_k(a) \pmod{p}. \tag{6.25}$$

Donc, $s(a)$ est une suite linéaire du second ordre (suite de Lucas), appelée également la suite caractéristique générée par a.

Remarque 6.3.3. *Soit l_k l'application linéaire de A définie par :*

$$\begin{array}{rccc} l_k(x) : & A & \longrightarrow & A \\ & x & \longmapsto & l_k(x) = \alpha^k x \end{array}$$

et M_k sa matrice par rapport la base $(1, \alpha)$.
Alors $M_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $M_1 = \begin{pmatrix} 0 & -1 \\ 1 & \bar{a} \end{pmatrix}$ où $\bar{a} = a \pmod{p}$.

Ainsi, $s_0(a) \equiv 2 \pmod{p}$ et $s_1(a) \equiv a \pmod{p}$.

6.3.2 Les propriétés cryptographiques des suites de Lucas

Dans cette section les principales propriétés cryptographiques des suites de Lucas sont données. Le lecteur pourra consulter [151, 155] pour toutes les applications cryptographiques des suites de Lucas.

Lemme 6.3.4. *Pour tout entier k. Alors :*

$$\begin{cases} i) & s_k(a) \equiv \alpha^k + \alpha^{-k} \pmod{p}, \\ ii) & s_k(a) \equiv s_{-k}(a) \pmod{p}. \end{cases}$$

Démonstration. Soit K le corps de décomposition de $f(X)$.
Puisque $f(X)$ est le polynôme caractéristique de M_1, alors M_1 est diagonalisable, il existe une matrice inversible P dans $\mathcal{M}_2(K)$ et $x \in K$ telle que si : $T = \begin{pmatrix} \alpha & x \\ 0 & \alpha^{-1} \end{pmatrix}$ et k un entier.
Alors $M_1 = PTP^{-1}$, donc $M_k = PT^kP^{-1}$.

Où $T^k = \begin{pmatrix} \alpha^k & x_k \\ 0 & \alpha^{-k} \end{pmatrix}$ et $x_k \in K$.

Donc, nous avons $i)$ $s_k(a) = Tr(M_k) = \alpha^k + \alpha^{-k}$.
$ii)$ résultat de $i)$. □

Corollaire 6.3.5. *Pour tout entier k, si* $f_k(X) = X^2 - s_k(a)X + 1$.
Alors $f_k(X) = (X - \alpha^k)(X - \alpha^{-k})$

Démonstration. Puisque $s_k(a) = \alpha^k + \alpha^{-k}$ (Lemme (6.3.4)) et $\alpha^k\alpha^{-k} = 1$.
Donc α^k et α^{-k} sont les racines de $f_k(X) = X^2 - s_k(a)X + 1$, il résulte :

$$f_k(X) = (X - \alpha^k)(X - \alpha^{-k}).$$

□

Lemme 6.3.6. *Pour tout entiers k et e :*

$$s_e(s_k(a)) \equiv s_{ke}(a) \pmod{p}.$$

Démonstration. Du corollaire (6.3.5), les racine du polynôme $f_k(X)$ sont α^k et α^{-k}.
Donc :

$$\begin{aligned} s_e(s_k(a)) &= (\alpha^k)^e + (\alpha^{-k})^e \text{ (par le lemme 6.3.4)} \\ &= T(\alpha^{ke}) \\ &= s_{ke}(a). \end{aligned}$$

□

Lemme 6.3.7. *Si p ne divise pas* $(a^2 - 4)$, *alors* $\pi = p^2 - \epsilon_p$ *est la période.*
Où $\epsilon_p = \left(\dfrac{a^2 - 4}{p}\right)$ *est le symbole de Legendre.*

Démonstration. Puisque α est un élément de A de norme 1, alors α est un élément inversible de A.
Soit a^2-4 le discriminant de $f(X)$, nous distinguons trois cas :

(i) Si $\left(\frac{a^2-4}{p}\right)=0$, p divise a^2-4. Alors $a \equiv \pm 2 \pmod{p}$.
Si $a \equiv 2 \pmod{p}$, alors $s_k(a)=2$.
Si $a \equiv -2 \pmod{p}$, alors $s_{2k}(a)=2$ et $s_{2k+1}(a)=-2$.

(ii) Si $\left(\frac{a^2-4}{p}\right)=1$.
Alors le corps de décomposition de $f(X)$ est $\mathbb{F}_p$, et $A \simeq \mathbb{F}_p \times \mathbb{F}_p$.
Par conséquent, l'exposant du groupe multiplicatif $A^\star$ est $p-1$.
Donc, $\alpha^{p-1}=1$.

(iii) Si $\left(\frac{a^2-4}{p}\right)=-1$.
Alors $A \simeq \mathbb{F}_{p^2}$ et la norme $N(\alpha)=\alpha^{p+1}=1$.
Soit $x \in N$ la période de $s(a)$.
Alors $\alpha^x=1$, puisque $\left(\frac{a^2-4}{p}\right)=-1$, $\alpha \notin \mathbb{F}_p^\star$, alors $x \geq p+1$. Ainsi :

$$\begin{aligned} s_{p+1}(a) &\equiv \alpha^{p+1}+\alpha^{-(p+1)} \\ &\equiv N(\alpha)+N(\alpha^{-1}) \\ &= 2 \\ &= s_0(a) \pmod{p} \text{ et } \pi \text{ divise } p+1. \end{aligned}$$

□

Corollaire 6.3.8. *Pour tout entier e tel que $PGCD(e,\pi)=1$, la fonction :*

$$\begin{array}{rccc} Luc_e : & \mathbb{F}_p & \longrightarrow & \mathbb{F}_p \\ & a & \longmapsto & s_e(a) \end{array}$$

est une bijection.

Démonstration. Puisque $PGCD(e,\pi)=1$, alors nous pouvons utiliser l'algorithme euclidien étendu (section 3.6.4) pour calculer l'inverse d de e modulo π. Cela signifie qu'il existe un entier k tel que $de=1+k\pi$.

Par conséquent :

$$\begin{aligned} s_d(s_e(a)) &\equiv s_{de}(a) \text{ (par le lemme 6.3.6)} \\ &\equiv s_{1+k\pi}(a) \\ &\equiv s_1(a) \\ &\equiv a \pmod{p}. \end{aligned}$$

□

Lemme 6.3.9. *Soit $e \in \mathbb{N}$ tel que $PGCD(e,\pi)=1$ et soit $c=s_e(a)$.*
Alors p ne divise pas c^2-4 si et seulement si p ne divise pas a^2-4 et $\left(\frac{a^2-4}{p}\right)=\left(\frac{c^2-4}{p}\right)$.

Démonstration. Puisque $a \equiv s_d(c) \pmod{p}$, où d est l'inverse de e modulo π, il suffit de montrer que si $\left(\frac{a^2-4}{p}\right) = 1$, alors $\left(\frac{c^2-4}{p}\right) = 1$.

Supposons que $\left(\frac{a^2-4}{p}\right) = 1$, alors $\alpha \in \mathbb{F}_p$.

Ainsi, $\alpha^e \in \mathbb{F}_p$ et $f_c(X) = X^2 - cX + 1$ se divise en $\mathbb{F}_p[X]$;
$f_c(X) \equiv (X - \alpha^e)(X - \alpha^{-e}) \pmod{p}$. Donc, $\left(\frac{c^2-4}{p}\right) = 1$. □

6.3.3 Méthode et coût de calcul

Nous donnons ici l'algorithme de calcul du k^{me} terme de la suite $s(a)$ avec une analyse de coût de calcul, le lemme suivant sera utilisé dans la méthode de calcule de s_k.

Lemme 6.3.10. *Pour tout entier n, posons $s_n := s_n(a) \pmod{p}$. Alors :*

$$\begin{cases} i) & s_{2n} & \equiv & s_n^2 - 2, \\ ii) & s_{2n+1} & \equiv & s_n s_{n+1} - a. \end{cases}$$

Démonstration. Soient n et m deux entiers, par le Lemme 6.3.4 ous avons :

$$\begin{aligned} s_n s_m &\equiv (\alpha^n + \alpha^{-n})(\alpha^m + \alpha^{-m}) \pmod{p} \\ &\equiv (\alpha^{n+m} + \alpha^{-n-m}) + (\alpha^{n-m} + \alpha_2^{-n+m}) \pmod{p} \\ &\equiv s_{n+m} + s_{n-m} \pmod{p}. \end{aligned}$$

Donc,
$s_{n+m} \equiv s_n s_m - s_{n-m} \pmod{p}$.

En particulier, nous avons, i) et ii).

□

Méthode de calcul

Soit $k = 2^r m$, où m est un entier impair. Pour calculer s_k, d'abord nous calculons s_m, puis s_{2m} par le Lemme 6.3.10, nous avons :

$$\begin{aligned} s_{2m} &\equiv s_m^2 - 2 \\ s_{4m} &\equiv s_{2m}^2 - 2 \\ &\cdots\cdots \\ s_k &\equiv s_{2^{r-1}m}^2 - 2. \end{aligned}$$

Donc pour calculer s_k, nous avons besoin de r multiplications modulo p et nous avons besoin également de s_m.

Nous pouvons écrire m sous la forme : $m = \sum_{i=0}^{l-1} k_i 2^{l-1-i}$, pour tout $0 \leq i < l-1$, soit $f_{i+1} = 2f_i + k_{i+1}$ et $f_0 = k_0$. Alors $f_{l-1} = k$, pour $0 \leq i < l-1$ et supposons que, $s_{f_{i-1}}$ et $s_{f_{i-1}+1}$ est calculé. Alors :

$$\text{Si } k_i = 0, \text{ alors } \begin{cases} s_{f_i} & \equiv & s_{2f_{i-1}} s_{f_{i-1}}^2 - 2 \\ s_{f_i+1} & \equiv & s_{2f_{i-1}+1} \equiv s_{f_{i-1}}(a) s_{f_{i-1}+1} - a \end{cases}$$

$$\text{Si } k_i = 1, \text{ alors } \begin{cases} s_{f_i} & \equiv & s_{2f_{i-1}+1} \equiv s_{f_{i-1}} s_{f_{i-1}+1} - a \\ s_{f_i+1} & \equiv & s_{2(f_{i-1}+1)} \equiv s_{f_{i-1}+1}^2 - 2 \end{cases}$$

L'algorithme de calcul

Algorithm 10: L'algorithme de calcul.

1. Input : $k = 2^r \sum_{i=0}^{l-1} k_i 2^i$ et a, où $k_0 \neq 0$ et $k_{l-1} \neq 0$.
2. Output : s_k.
3. $s_0 = 2$, $s_1 = a$.
4. Pour i de 0 à $l-1$ faire :
5. Si $k_i = 0$ alors $s_1 = s_1 s_0 - a$, $s_0 = s_0^2 - 2$.
6. Sinon alors $s_0 = s_1 s_0 - a$, $s_1 = s_1^2 - 2$.
7. Fin si.
8. Fin pour.
9. $s = s_0$.
10. Pour i de 1 à r faire :
11. $s = s^2 - 2$.
12. Fin pour.
13. Retourner (s).

Coût de calcul

Cette méthode garantit que s_k peut être calculé avec le même coût de calcul que le k^{eme} puissance calculée dans RSA . Mais, dans le calcul de s_m, calculer deux nombres à chaque étape ne ralentit pas le calcul, mais il y a des optimisations dans le calcul qui signifie que la quantité totale de calcul est seulement la moitié du coût

nécessaire pour le système RSA. Par conséquent, pour calculer $s_k(a)$, le nombre total de multiplications modulo p est $log_2(k)$.

6.3.4 Notre approche : Schéma de chiffrement multi-récepteur

Dans cette section, nous proposons un schéma de chiffrement multi-récepteur basé sur les suites Lucas et le théorème des restes chinois. Notre schéma se compose de trois étapes : la génération des clés, le chiffrement et le déchiffrement.

1. **Génération des clés :** Supposons qu'il existe $r+1$ utilisateurs. Tout utilisateur sélectionne $s \leq r$ récepteurs autorisés $u_1, \cdots, u_s$, chaque utilisateur a une paire de clés publiques (n_i, e_i), où $n_i = p_i q_i$ c'est un entier RSA, e_i est premier avec $(p_i+1)(p_i-1)(q_i+1)(q_i-1)$ et $n_1, \cdots, n_r, n_{r+1}$ sont premiers entre eux.
2. **Le chiffrement :** L'expéditeur utilise tous les s clés publiques des récepteurs pour chiffrer le message, puis diffuse le texte chiffré à l'ensemble des s récepteurs.

   Supposons qu'il a besoin d'envoyer un message $0 < m < N$ aux s récepteurs légitimes, où N est le minimum des valeurs n_i. Il diffuse le message chiffrée m comme suit :

   (a) Pour chaque $i = 1, \ldots, s$, il calcule $c_i = s_{e_i}(m)$, $n_1, \cdots, n_s$ sont publiques et premiers entre eux.

   (b) Il utilise le Théorème des restes chinois (section (3.6.5)) pour calculer l'entier c tel que pour tout $i = 1, \ldots, s$,

   $$c \equiv c_i \pmod{n_i}. \tag{6.26}$$

   (c) Il diffuse le message chiffrée c aux s récepteurs.
3. **Le déchiffrement :** Quand un récepteur autorisé i reçoit le message chiffrée c, il calcule sa clé privée d_i puis il déchiffre le message chiffrée c comme suit :

   (a) Il calcule les valeurs de $c_i \equiv c \pmod{n_i}$, $\epsilon_{p_i} = \left(\frac{c_i^2 - 4}{p_i}\right)$ et $\epsilon_{q_i} = \left(\frac{c_i^2 - 4}{q_i}\right)$.

   (b) Il calcule sa clé privée d_i :

   $$\text{l'inverse de } e_i \text{ modulo } \pi = (p_i - \epsilon_{p_i})(q_i - \epsilon_{q_i}).$$

   (c) Enfin, il calcule le message déchiffré :

   $$m \equiv s_{d_i}(c_i) \pmod{n_i}. \tag{6.27}$$

Preuve du schéma

Démonstration.

La phase de chiffrement

Afin de calculer le le message chiffré c, pour tout $i = 1, \cdots, s$, l'expéditeur calcule $M_i = \prod_{j=1, j\neq i}^{s} n_j$, y_i l'inverse modulo n_i et $c = \sum_{i=1}^{s} c_i y_i M_i$.

Comme $y_i M_i \equiv 1 \pmod{n_i}$ et pour chaque $j \neq i$, $y_i M_i \equiv 0 \pmod{n_j}$ (puisque n_j divise M_i), pour chaque $i = 1, \ldots, s$,

$$c \equiv c_i \pmod{n_i}.$$

La phase de déchiffrement

Comme $c_i \equiv s_{e_i}(m) \pmod{n_i}$ et $PGCD(e, \pi) = 1$, $\left(\frac{c_i^2 - 4}{p}\right) = \left(\frac{m^2 - 4}{p}\right)$ et $\left(\frac{c_i^2 - 4}{q}\right) = \left(\frac{m^2 - 4}{q}\right)$.

Ainsi,

$$\begin{aligned} s_{d_i}(c_i) &\equiv s_{d_i}(s_{e_i}(m) \\ &\equiv s_{d_i e_i}(m)(\text{ par le Lemme 6.3.6}) \\ &\equiv m \pmod{n_i}. \end{aligned}$$

□

6.3.5 L'analyse de l'approche proposée

Dans cette section nous allons analyser la sécurité, du coût de calcul et de l'anonymat des récepteurs du schémas proposé. L'anonymat garantit que l'identité des récepteurs est protégé. Nous allons également comparer le coût de calcul de notre schéma avec le schéma de L. Harn, et al. [117].

La sécurité

Puisque notre cryptosystème multi-récepteur utilise le cryptosystème "LUC", la sécurité du système est équivalente au cryptosystème "LUC". Si Oscar veut déchiffrer le message chiffré c, il doit casser le cryptosystème LUC, qui est équivalent cryptographiquement à la sécurité de RSA [36, 154]. Donc, la sécurité de notre schéma est équivalente à la sécurité de RSA.

L'anonymat des récepteurs

Lorsqu'un expéditeur diffuse le message chiffré, puisqu'il utilise la clé publique commune $c_i = s_{e_i}(m)$, $n_1, \cdots, n_s$ pour le chiffrement, aucun utilisateur dans le groupe ne connait l'expéditeur du message, ce qui garantit l'anonymat du schéma proposé.

L'analyse computationnelle et comparaison

Nous allons comparer la performance du chiffrement "LUC" et le schéma L. Harn et al. [117] avec le schéma proposé. A partir du Tableau 6.2, on peut constater que le schéma proposé est plus efficace en terme de temps de calcul, la complexité est la moitié en comparant avec le schéma L. Harn et al. [117] .

	Le schéma de "LUC"	Le schéma de L. Harn, et al. [117]	Notre schéma
Expéditeur	$n/2 \times T_{E\_1024}$	$n \times T_{E\_1024}$	$n/2 \times T_{E\_1024}$
Récepteur	T_D	T_D	T_D
Nombre de cycles de transmission	n	1	1
Anonymat des récepteurs	Non	Oui	Oui

TABLE 6.2: Chiffrement multi-récepteur : comparaison des résultats avec d'autres schémas.

6.3.6 L'échange de clés de Lucas Diffie-Hellman étendue à un groupe d'utilisateurs

Le standard d'échange de clés Diffie-Hellman était le premier standard proposée en 1976 [186] (c.f. la section 3.6.6). Il y a eu des recherches pour l'étendre à un contexte de groupe. L'objectif de l'échange Diffie-Hellman est d'échanger une information secrète (une clé secrète par exemple) au sein d'un groupe mais on ne dispose pas de canal sécurisé. Plusieurs solutions ont été proposées dans la littérature, dont certaines restent seulement théoriques sans pouvoir les appliquer, la sécurité de certains autres reste à prouver (Voir par exemple [29, 75, 127, 128]). Dans cet article, une extension de l'échange de clés Diffie-Hellman basée sur des suites Lucas est proposée (voir la Figure 6.1).

Soit $n = pq$ un entier de RSA, a un entier tel que $f(X) = X^2 - aX + 1$ est un polynôme primitif modulo p et modulo q aussi.

Supposons que r utilisateurs $u_1, \cdots, u_r$, dont l'accès à une clé publique (n, a) et chacun a sa propre clé privée x_i, veulent se mettre d'accord sur une clé privée partagée. La construction de cette clé privée est comme suit :

La construction de la clé privée commune :

— Le premier utilisateur u_1 publie $y_1^{(1)} = s_{x_1}(a)$.

— Le second u_2, publie $(y_1^{(2)}, y_2^{(2)}, y_3^{(2)})$, où :

$$\begin{aligned} y_1^{(2)} =& s_{x_2}(a), \\ y_2^{(2)} =& s_{x_1}(a), \\ y_3^{(2)} =& s_{x_2}(y_1). \end{aligned} \tag{6.28}$$

La notation y_i^j signifie que cette quantité est publié par le j^{eme} utilisateur.

— Le troisième publie $(y_1^{(3)}, y_2^{(3)}, y_3^{(3)}, y_4^{(3)})$, où :

$$\begin{aligned} y_1^{(3)} =& s_{x_3}(y_1^2), \\ y_2^{(3)} =& s_{x_3}(y_2^2), \\ y_3^{(3)} =& y_3^2, \\ y_4^{(3)} =& s_{x_3}(y_3^2). \end{aligned} \tag{6.29}$$

— Une fois le i^{eme} utilisateur publie $(y_1^{(i)}, \cdots, y_{i+1}^{(i)})$.
Le $(i+1)^{th}$ publie $(y_1^{(i+1)}, \cdots, y_{i+2}^{(i+1)})$, où pour tout $j = 1, \cdots i$:

$$\begin{aligned} y_j^{(i+1)} =& s_{x_{i+1}}(y_j^{(i)}), \\ y_{i+1}^{(i+1)} =& y_{i+1}^{(i)}, \\ y_{i+2}^{(i+1)} =& s_{x_{i+1}}(y_{i+1}^{(i)}). \end{aligned} \tag{6.30}$$

— Enfin, le dernier utilisateur u_n publie $(y_1^{(n)}, \cdots, y_n^{(n)})$ et garde en privée la clé commune :

$$\begin{aligned} y =& y_{n+1}^{(n)} \\ =& s_{x_i}(y_i^{(n)}). \end{aligned} \tag{6.31}$$

— Chaque utilisateur u_i, $i = 1, \cdots n-1$ peut calculer la même clé privée : $y = s_{x_i}(y_i^{(n)})$ sans partager aucune information secrète.

La clé privée commune est $y = y_{n+1}^{(n)}$.

Démonstration.

$$\begin{aligned} y =& s_{x_n}(y_n^{(n-1)}) \\ =& s_{x_n}(s_{x_{n-1}}(...(s_{x_1}(a))...)) \\ =& s_{x_n x_{n-1} .... x_1}(a)(\text{ par le Lemme 6.3.6}). \end{aligned}$$

□

6.4 Conclusion

Dans cet article, nous avons introduit un nouveau système de chiffrement multi-récepteur qui fournit l'anonymat des récepteurs. Notre système est comparable avec les systèmes existants en termes de coût de calcul. La sécurité du schéma proposé est

égale à la sécurité du système de chiffrement basé sur les suites de Lucas "LUC". La comparaison avec d'autres résultats et l'analyse de la sécurité montrent clairement que la méthode proposée fournit l'anonymat des récepteurs et un temps de calcul acceptable.

Nous avons proposé également un protocole d'échange de clés sur un groupe d'utilisateurs basé sur les suites de Lucas.

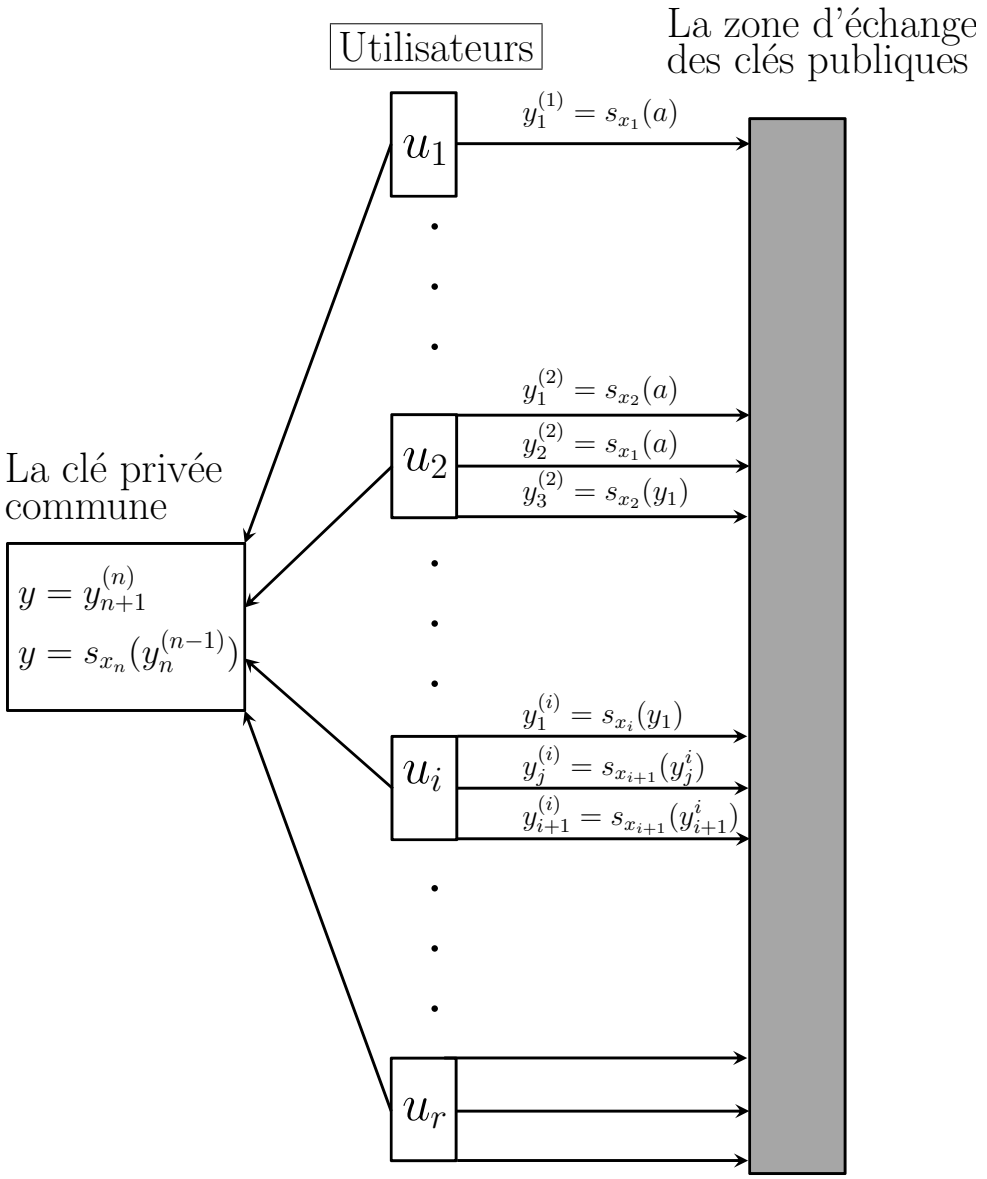


FIGURE 6.1: L'échange de clés de Lucas Diffie-Hellmane étendue à un groupe d'utilisateurs.

Chapitre 7

Conclusion et perspectives

Pour conclure cette thèse, un résumé des recherches effectuées est présenté dans ce chapitre. Les objectifs principaux de nos travaux décrits étaient :

1. Présenter un état de l'art des techniques de chiffrement existantes, leurs classifications, les méthodes de cryptanalyse les plus connues et les mesures couramment utilisées pour évaluer un cryptosystème.
2. Proposer des schémas de chiffrement et d'échanges sécurisés des images médicales, nous avons développé trois algorithmes pour faire face à des problèmes liés à la sécurité. Les méthodes proposées sont applicables dans le domaine de la sécurité des données et la production des logiciels qui traitent des données médicales sensibles et d'autres types de données confidentielles.

Dans le premier chapitre nous avons présenté une introduction générale de cette thèse, nous avons abordé les motivations de nos travaux, un bref historique et l'organisation de cette thèse. Ensuite nous avons discuté dans le chapitre 2 l'image numérique et l'imagerie médicale. Également dans ce chapitre, on a récapitulé également dans ce chapitre les techniques et les tests employés pour mesurer la robustesse d'un système de chiffrement. Le chapitre 3 traite les notions de sécurité et une présentation des deux branches de la cryptologie : la cryptographie et la cryptanalyse et les sujets en relation.

Nous avons proposé dans le Chapitre 4, un nouveau schéma de chiffrement partiel des images médicale, le chiffrement partiel est applicable dans plusieurs domaines tel que les images médicales, les plaques d'immatriculation d'automobile et la vidéo surveillance, dans ces domaines le chiffrement total n'est pas nécessaire. Le chiffrement partiel est moins couteux comparé avec le chiffrement total. Cette technique est basée sur la coloration de graphes, on construit à partir de l'image originale un graphe de couleurs, puis on sélectionne quelques couleurs en fonctions du pourcentage de chiffrement désiré. Enfin, on chiffre les pixels choisis par un algorithme symétrique. Les analyses montrent l'efficacité et la robustesse de cette méthode.

Le Chapitre 5, traite un nouveau algorithme de chiffrement, l'avantage majeur de cette méthode est l'exploitation de la puissance du chiffrement asymétrique et la vitesse des algorithmes symétriques. D'autre part, cette méthode supprime le partage de la clé secrète. Également, la clé secrète est générée aléatoirement, stockée et chiffrée, elle est différente pour chaque image, ce qui rend l'attaque par force brute très difficile. L'image est chiffrée par un algorithme symétrique. Ensuite, cette clé est chiffrée par un algorithme asymétrique. Le cryptogramme de clé chiffrée sera inséré dans l'image chiffrée en utilisant une technique stéganographique. Les résultats des tests montrent une bonne résistance contre les attaques les plus connues.

Dans le chapitre 6, nous avons introduit un nouveau schéma de chiffrement multi-récepteur, le chiffrement multi-récepteur permet à un expéditeur de transmettre une donnée chiffrée à un groupe d'utilisateurs autorisés, la personne hors de ce groupe ne peut déchiffrer la donnée. En plus, le système proposé garantit l'anonymat des utilisateurs, cette nouvelle approche multi-récepteur est basée sur les suites de Lucas. Nous avons comparé notre algorithme avec un système récent, les résultats d'analyses montrent que notre algorithme est plus performant au niveau sécurité et temps de traitement.

Parmi les évolutions de nos travaux, on peut citer en premier lieu, d'envisager d'intégrer d'autres méthodes d'optimisation dans le chiffrement sélectif. Également d'appliquer ces méthodes pour d'autres types de données, images couleurs, son et vidéos. Proposer des schémas de chiffrement multi-récepteur basés sur les courbes elliptiques, le chiffrement ElGamal et les codes correcteurs.

Bibliographie

[1] A. Anderson and E. Biham. Tiger : *A Fast New Hash Function.* In D. Gollmann, editor, Fast Software Encryption - FSE 1996, volume 1039 of Lecture Notes in Computer Science, pages 89-97. Springer-Verlag, (1996).

[2] A. Bosselaers and B .Preneel, editors. *Integrity Primitives for Secure Information Systems,* volume 1007 of Lecture Notes in Computer Science, chapter 3, pages 69-111. Springer, (1995).

[3] A. Fiat and M. Naor, *Broadcast encryption,* in Proceeding of Advances Cryptology - Crypto, LNCS 839, pp. 480-491, Springer-Verlag, California, USA, Aug. 1994.

[4] A. Gamst. *Some lower bounds for a class of frequency assignment problems.* IEEE Transactions of Vehicular Technology, 35 : 8-14, 1986.

[5] Aris Gkoulalas-Divanis ; Grigorios Loukides. "Medical Data Privacy Handbook." *Loukides. Springer International Publishing, Switzerland (2015). 832 pp., ISBN : 978-3-319-23633-9.*

[6] A. Hertz, D. Werra. *Using tabu search techniques for graph coloring.* Computing, 39(4) : 345-351, 1987.

[7] Ahmed, H. E. H., Kalash, H. M., & Allah, O. S. F. (2007). *An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption.* An International Journal of Computing and Informatics, 31(1), 121-129.

[8] Auguste Kerckhoffs. *La cryptologie militaire. Journal des sciences militaires.* IX ,janvier 5-83, et février 161-191 (1883).

[9] A. Kumar and M. K. Ghose, *Extended substitution-diffusion based image cipher using chaotic standard map,* Communications in Nonlinear Science and Numerical Simulation, vol. 16, pp. 372-382, 2011.

[10] A. Latham : *Steganography : JPHIDE and JPSEEK, 1999.* http ://linux01.gwdg.de/∼alatham/stego.html.

[11] A. Lim, F. Wang. *Robust graph coloring for uncertain supply chain management.* In Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS'05)- Track 3-Volume 03. IEEE Computer Society, 11(8) : 263-277, 2005.

[12] Amin, M., Allah, O. S. F., & Abd El-Latif, A. A. (2010). *A chaotic block cipher algorithm for image cryptosystems.* Communications in Nonlinear Science and Numerical Simulation, 15, 3484-3497.

[13] Ashtiyani, M., Birgani, P.M. and Hosseini, H.M., *Chaos-Based Medical Image Encryption Using Symmetric Cryptography*, Information and Communication Technologies : From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on IEEE, in Damascus, 2008, pp. : 1-5.

[14] A. M Alattar, G.I. Al-Regib, and S.A. Al-Semari, *Improved Selective Encryption Techniques for Secure Transmission of MPEG Video Bit-Streams.*, In ICIP 99, International Conference on Image Processing, IEEE, volume 4, pages 256-260, 1999.

[15] Moumen, A. & Sissaoui, H. (2017). *Images Encryption Method using Steganographic LSB Method, AES and RSA algorithm." . Nonlinear Engineering, 6(1), pp. 53-59. Retrieved 4 Apr. 2017, from doi :10.1515/nleng-2016-0010.*

[16] A. Mohamed, G. Zaibi, and A. Kachouri, *Implementation of rc5 and rc6 block ciphers on digital images,* in Systems, Signals and Devices (SSD), 2011 8th International Multi-Conference on. IEEE, 2011, pp. 1-6.

[17] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography.* CRC Press, (1996).

[18] A. Westfeld, A. Pfitzmann., *Attacks on Steganographic Systems*, 3rd International Workshop. Lecture Notes in Computer Science, Vol.1768. Springer-Verlag, Berlin Heidelberg New York (2000) 61-75.

[19] A. Said, *Measuring the Strength of Partial Encryption Scheme.* ICIP 2005, IEEE International Conference in Image Processing, Genova, vol. 2, pp. 1126-1129, Italy, 2005.

[20] A. Westfeld : *F5-a steganographic algorithm. In I.S. Moskowitz,* éditeur : Proc. Information Hiding, 4th International Workshop, IHW 2001, volume 2137 de Lecture Notes in Computer Science, pages 289-302, Pittsburgh, PA, USA, avril 2001. Springer. ISBN : 3-540-42733-3.

[21] A. Westfeld : *The steganographic algorithm F5.,* 1999. http ://www.rn.inf.tudresden.de/ $\sim$ westfeld/f5.html.

[22] Amigó, J.M. (2009). Chaos-Based Cryptography. *In : Intelligent Computing Based on Chaos, Springer, ISBN 978-3-540-95971-7, pp. 291-313, Berlin.*

[23] Abdelkader Moumen, Mohamed Bouye and Hocine Sissaoui. *New secure partial encryption method for medical images using graph coloring problem.* Nonlinear Dynamics, 2015, Volume 82, Number 3, Page 1475.

[24] B. Kaliski. *The MD2 Message-Digest Algorithm.* RFC 1319 (Informational), (1992). http ://www.ietf.org/rfc/rfc1319.txt.

[25] B. Newman. *Secrets of German Espionage.* Robert Hale Ltd, London, 1940.

[26] B. M. Hennelly and J. T. Sheridan, *Image encryption based on the fractional Fourier transform,* Proc. SPIE, vol. 5202, pp. 76-87, 2003.

[27] B. Schneier,*Applied Cryptography,* Second Edition, John Wiley and Sons, New York, (1996).

[28] B. Pfitzmann : *Information hiding terminology.* In Proceedings of the Workshop on Information Hiding, numt'ero 1174, pages 347-350, Cambridge, England, mai 1996. Springer Verlag.

[29] Chin Chen Chang, Tzong Chen Wu, and C.P. Chen. *The Design Of A Conference Key Distribution System.* In Advances in Cryptology -AUSCRYPT'92, Lecture Notes in Computer Science, pages 467-474. Springer- Verlag, Berlin Germany, December 1992.

[30] C. I. Fan, L. Huang, and P. Ho, *Anonymous multi-receiver identity-based encryption,* IEEE Transations on Computers, vol. 59, no. 9, pp. 1239-1249, Sep. 2010.

[31] C. Fontaine : *Contribution à la recherche de fonctions booléennes hautement non linéaires, et au marquage d'images en vue de la protection des droits d'auteur.* Thèse de doctorat, Université Paris VI, novembre 1998.

[32] C. Cachin : *An information-theoretic model for steganography.*In D. Aucsmith, t'editeur : Proc. Information Hiding, 2nd International Workshop, volume 1525 de Lecture Notes in Computer Science, pages 306-318, Portland, Oregon, USA, avril 1998. Springer.

[33] C. Cachin : *Digital steganography.* In H.C.A. van Tilborg, t'editeur : Encyclopedia of Cryptography and Security. Springer, 2005. ISBN : 978-0-387-23473-1.

[34] Cherif Moumen, Malek Benslama and Mekhilef Saad, *Cryptography of the Medical Images*, PIERS Proceedings, Kuala Lumpur, MALAYSIA, 2012, pp. : 42-48.

[35] C. Shannon, *Communication theory of secrecy systems,* Bell system technical journal, vol. 28, no. 4, pp. 656-715, 1949.

[36] Chi-Sung Laih, Fu-Kuan Tu, Wen-Chun Tai, *On the security of the Lucas function,* Information Processing Letters 53(1995), pp 243-247.

[37] Calcote.S, "Developing a secure healthcare information network on the Internet," *Healthcare Financial Manage., vol. 51, no. 1, Jan. 1997, pp. 68.*

[38] C.C. Chang, M.S. Hwang, and T-S Chen. *A new encryption algorithm for image cryptosystems. The Journal of Systems and Software.,* 58 :83-91, 2001.

[39] C.M. Wang, N.I. Wu, C.S. Tsai and M.S. Hwang, *A high quality steganography method with pixel-value differencing and modulus function*, J. Syst. Softw. 81, 150-158, (2008).

[40] D. Bleichenbacherl, W. Bosma, and K. Lenstra, *Some Remarks on Lucas-Based Cryptosystems,* Advances in Cryptology - CRYPT0 '95, LNCS 963, pp. 386-396, 1995.

[41] *Digital Imaging and Communications in Medicine, http ://medical.nema.org/.*

[42] D. Brélaz. *New methods to color the vertices of a graph.* Communications of the ACM, 22(4) : 251-256, 1979.

[43] Don Coppersmith. *The Data Encryption Standard (DES) and its strength against attacks.* IBM J. Res. Dev., 38(3) :243-250, May 1994.

[44] D. Jones. *Applications of splay trees to data compression,*. Commun. ACM, 31(8) : 996-1007,(1988).

[45] D. E. Newton, *Encyclopedia of Cryptology,* ABC-CLIO Inc , California, USA, 1997.

[46] D. Jones. *Applications of splay trees to data compression.* Commun. ACM, pages 996-1007,(Aug 1988).

[47] David Kahn, *La guerre des codes secrets.* InterEditions, (1980).

[48] David Kahn, *The Codebreakers.* Macmillan Publishing Company, New York, (1967).

[49] Daniel Salles, *Éducation à l'image et aux médias : la liberté de la presse*, Centre de Ressources en éducation aux médias CREM, mars 2005.

[50] D. Stinson, *Cryptography : Theory and Practice,* (2nd) Chapman & Hall / CRC Boca Raton, USA, (2002).

[51] D. Wagner. *The boomerang attack.* In L. Knudsen, editor, Fast Software Encryption'99, volume 1636 of Lecture Notes in Computer Science, pages 156-170. Springer-Verlag, 1999.

[52] D. de Werra. *An introduction to timetabling.* European Journal of Operational Research, 19(2) :151-162, 1985.

[53] DAVOINE F., PATEUX S., *"Tatouage de documents audiovisuels numériques."* HERMES, Lavoisier, Vuibert, Paris, 2004.

[54] Donald E. Knuth, *The Art of Computer Programming,* vol. 2 : Seminumerical Algorithms, 3e éd., Addison-Wesley, Boston, 1998.

[55] D. H. Lehmer, (1930), *An extended theory of Lucas functions,* Annals of Mathematics (2), Vol. 31, pp. 419-48.

[56] D. Bleichenbacher, B. Kaliski, and J. Staddou. *Recent Results on PKCS : RSA Encryption Standard.*, *RSA Laboratories Bulletin, 24 June 1998.*

[57] D.W. Bender, N.M. Gruhl and A. Lu, *Techniques for data hiding, IBM Syst.* J. 35, 313-316, (1996).

[58] Eli Biham and Adi Shamir. *Differential Cryptanalysis of DES-like Cryptosystems.* Journal of Cryptology, 4(1) :3-72, 1991.

[59] Eli Biham and Adi Shamir. *Differential Cryptanalysis of the Full 16-Round DES.* In Ernest F. Brickell, editor, Advances in Cryptology - CRYPTO'92, volume 740 of Lecture Notes in Computer Science, pages 487-496. Springer, August 1993.

[60] E. Biham and V. Furman. *Impossible differential on 8-round MARS' core.* In AES Candidate Conference, pages 186-194, 2000.

[61] E. Thambiraja. G. Ramesh. Dr. R. Umarani. *A Survey on Various Most Common Encryption Techniques.* International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 7, (July 2012).

[62] E. Ott, Chaos in Dynamical Systems (*Cambridge University Page, Cambridge, 2002).*

[63] F. Y. Shih et S. Y.T. Wu. *"Combinational image watermarking in the spatial and frequency domains."* Pattern Recognition, 36 :969-975, 2003.

[64] F. E. A. Lucas, *Théorie des fonctions numériques simplement périodiques, American Journal Mathematics,* Vol. 1, pp. 184-240 and 289-321, (1878).

[65] F. Cayre, C. Fontaine, T. Furon. *"Watermarking Security : Theory and Practice,"* IEEE Transactions on Signal Processing, Volume 53, Number 10, pp 3976-3987 (Oct 2005).

[66] F. Raynal, F. Petitcolas et C. Fontaine : *L'art de dissimuler les informations.* Pour la Science, été 2002. Dossier "L'art du secret".

[67] Federal Information Processing Standards : AES, *Announcing the Advanced Encryption Standard.* Federal Information Processing Standards Publication, (2001).

[68] F. T. Leighton. *A graph coloring algorithm for large scheduling problems.* Journal of Research of the National Bureau of Standards, 84(6) : 489-506, 1979.

[69] G. H. Chiou and W. T. Chen, *Secure broadcasting using the secure lock.* IEEE Transations on Software Engineering, vol. 15, no. 8, pp. 929-934, Aug. 1989.

[70] G.A. Sathishkumar , K.Bhoopathy bagan. N.Sriraam, *Image Encryption based on Diffusion and Multiple Chaotic Maps*, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011.

[71] G. Saporta : *Probabilité, Analyse des Données et Statistiques.* Technip, 1990.

[72] G. Kipper : *Investigator's guide to steganography.* Information Security. Auerbach, 2004. ISBN : 0-8493-2433-5.

[73] Gardner, M. *"Trapdoor Ciphers" and "Trapdoor Ciphers II." Chs. 13-14 in Penrose Tiles and Trapdoor Ciphers... and the Return of Dr. Matrix, reissue ed. New York : W. H. Freeman, pp. 183-204, 1989.*

[74] G. J. Simmons., *The prisoners problem and the subliminal channel*, in Advances in Cryptology, pp. 51-67, Plenum Press, New York, NY, USA, 1984.

[75] Hugh Harney, Carl Muckenhirn, and Thomas Rivers. *Group Key Management Protocol (GKMP) Architecture.* INTERNET-DRAFT, September 1994.

[76] H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini, *Dynamic threshold cryptosystems : a new scheme in group oriented cryptography,* in Proceeding of Pragocrypt'96 : the 1st International conference on the Theory and Applications of Cryptology, pp. 370-379, Prague, Czech Republic, Sep. 1996.

[77] H. CHENG and X. LI, *Partial Encryption of Compressed Images and Videos.* IEEE Transactions on Signal Processing, 48(8) :2439-2451, (2000).

[78] H. Feistel, *Cryptography and computer privacy,* Scientific American, 228 (1973) 5, 15-23.

[79] *Health Level Seven, https ://www.hl7.org/implement/standards/.*

[80] H. Elkamchouchi and M. A. Makar, *Measuring encryption quality of Bitmap images encrypted with Rijndael and KAMKAR block ciphers,* in Proceedings Twenty second National Radio Science Conference (NRSC 2005), pp. C11, Cairo, Egypt, Mar. 15, 17, 2005.

[81] Hans Dobbertin. *Cryptanalysis of MD4.* In Dieter Gollmann, editor, Fast Software Encryption - FSE'96, volume 1039 of Lecture Notes in Computer Science, pages 53-69. Springer, February 1996.

[82] H. Nien, S. Changchien, S. Wu, and C. Huang, *A new pixel-chaoticshuffle method for image encryption,* in Control, Automation, Robotics and Vision, 2008. ICARCV 2008. 10th International Conference on. IEEE, 2008, pp. 883-887.

[83] HINDEL R. : " Implementation of the DICOM 3.0 Standard - A Pragmatic Handbook " , *Oak Book (IL) : Robert Hindel, Radiological Society of North America, 1994, 118p.*

[84] I. Elashry, O. Allah, A. Abbas, S. El-Rabaie, and F. El-Samie, *Homomorphic image encryption,* Journal of Electronic Imaging, vol. 18, p.033002, 2009.

[85] I. Ziedan, M. Fouad, and D. H. Salem, *Application of Data encryption standard to bitmap and JPEG images,* in Proceedings Twentieth National Radio Science Conference (NRSC 2003), pp. C16, Egypt, Mar. 2003.

[86] *Integrating the Healthcare Enterprise, http ://www.ihe.net/.*

[87] I. Ismail, M. Amin, and H. Diab, *A digital image encryption algorithm based a composition of two chaotic logistic maps,* International Journal of Network Security, vol. 11, no. 1, pp. 1-10, 2010.

[88] JTC 1 / SC 27. *Information Technology - Security Techniques - Hash-functions - Part 4 : Hash-functions using modular arithmetic.* ISO/IEC 10118-4 :1994, (1998).

[89] JTC 1 / SC 27. *Information Technology - Security Techniques - Hash-functions - Part 3 : Dedicated hash-functions.* ISO/IEC 10118-3 : (2004, 2004).

[90] J. M. A. G. Millrioux and J. Daafouz, *Connection between chaotic and conventional cryptography,* IEEE Transactions on circuits and systems, 55(2008), 1695-1703.

[91] Jolfaei, A. & Mirghadri, A, *A New Approach to Measure Quality of Image Encryption*, International Journal of Computer and Network Security, 2(8), PP 38-44, 2010.

[92] J.-M. Rodrigues, W. Puech, and A.G. Bors, *A Selective Encryption for Heterogenous Color JPEG Images Based on VLC and AES Stream Cipher.* CGIV'06, Leeds, UK, 2006.

[93] J. Wilkins. *Mercury : or the Secret and Swift Messanger : Shewing, How a Man May With Privivacy and Speed Communicate His Thoughts to a Frind at Any Distance.* Rich Baldwin, London, 1694.

[94] J. Daemen and V. Rijmen. *The Design of Rijndael.* SpringerVerlag New York, Inc. Secaucus, NJ, USA, (2002).

[95] J. Stern, *La science du secret. Sciences.* Odile Jacob. (1998), 1-9.

[96] J. Fridrich and P. Lisonek , *Grid coloring in steganography*, *IEEE Transactions on Information Theory,* 53 (4) : 1547-1549, (2007).

[97] Jawad Ahmad and Fawad Ahmed. *Efficiency Analysis and Security Evaluation of Image Encryption Schemes* International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol :12 No :04.

[98] J. Fridrich, M. Goljan and R. Du., *Detecting LSB steganography in color and gray-scale images.*, IEEE MultiMedia, 8(4) :22-28, 2001.

[99] Johann BARBIER., *Analyse de canaux de communication dans un contexte non coopératif -Application aux codes correcteurs d'erreurs - et à la stéganalyse.*, Thèse de Doctorat présentée à L'école Supérieure et d'Application des Transmissions., soutenue le 28 novembre 2007.

[100] J. Fridrich, M. Goljan et R. Du., *Attacking the OutGuess.*, Proc. of the ACM Workshop on Multimedia and Security 2002.

[101] John Viega, (en) *Practical Random Number Generation in Software*, in Proc. 19th Annual Computer Security Applications Conference, Dec. 2003.

[102] J. Barbier, E. Filiol et K. Mayoura : *Universal detection of JPEG steganography.* Journal of Multimedia, 2(2) :1-9, avril 2007. ISSN : 1796-2048.

[103] J.C. Judge : *Steganography : Past, Present and Future.* SANS, 2001.

[104] J.A. Reeds : *Solved : The ciphers in book III of Trithemius's Steganographia.* Cryptologia, (22) :291-319, octobre 1998.

[105] J. Cohen and M. Fisher, *A robust and verifiable cryptographically secure election scheme. In Symposium on Foundations of Computer Science. IEEE. (1985). 2.*

[106] J. Fridrich, M. Goljan et R. Du : *Reliable detection of LSB steganography in grayscale and color images.* In Proc. ACM Workshop on Multimedia and Security, pages 27-30, Ottawa, Canada, octobre 2001.

[107] K. Chen and T.V. Ranmabadran, *Near-Lossless Compression of Medical Images Through Entropy Coded DPCM.* IEEE Transactions on Medical Imaging, 3(3) :538-548, 1994.

[108] L. Ghislaine, *Introduction à la cryptologie.* Edition HSC (2001).

[109] L. Kocarev, *Chaos-Based Cryptography : A Brief Overview,* IEEE Circ. Syst. Mag., Vol. 1, No. 3, pp. 6 21, (2001).

[110] L. R. Knudsen. *Truncated and higher order differentials.* In B. Preneel, editor, Fast Software Encryption'94, volume 1008 of Lecture Notes in Computer Science, pages 196-211. Springer- Verlag, 1994.

[111] L. R. Knudsen and T. A. Berson. *Truncated differentials of SAFER.* In D. Gollmann, editor, Fast Software Encryption'96, volume 1039 of Lecture Notes in Computer Science, pages 15-26. Springer-Verlag, 1996.

[112] Li, S. J., Chen, G. R., & Zheng, X. (2004). *Chaos-based encryption for digital images and videos.* In : Multimedia Security Handbook, Chapter 4.

[113] L houssain El Fadil and Abdelkader Moumen. *"Anonymous Multi-Receiver Public Key Encryption Based on Lucas Sequences." Accpeted 21/10/2016. Applied Mathematical Sciences.*

[114] Luby, M. *Pseudorandomness and Cryptographic Applications. Princeton, NJ : Princeton University Press, 1996.*

[115] Louwerse.K, *The electronic patient record : The management of access - Case study : Leiden University Hospital,* Int. J. Med. Inform., vol. 49, no. 1, Mar. 1998, pp. 39-44.

[116] L. El Fadil, *A Public-Key Cryptosystem Based on Lucas Sequences,* Palestine Journal of Mathematics Vol. 1(2) (2012) 148-152.

[117] L. HARN, C.- C. CHANG, and H.-L. WU, *An Anonymous Multi-Receiver Encryption Based on RSA*, Journal of Network Security, Vol.15, No.4, PP.307-312, July 2013.

[118] Lian, S. (2009). *Multimedia content encryption : Techniques and applications.* London : Taylor & Francis Group, LLC.

[119] M. Gamache, A. Hertz, J. O. Ouellet. *A graph coloring model for a feasibility problem in monthly crew scheduling with preferential bidding.* Computers Operations Research, 34(8) : 2384-2395, 2007.

[120] M. Van Droogenbroeck, *Partial Encryption of Images for Real-time Applications.* Fourth IEEE Benelux Signal Processing, Hilvarenbeek, The Netherlands, pages 11-15, April 2004.

[121] Mitsuru Matsui. *The First Experimental Cryptanalysis of the Data Encryption Standard.* In Yvo Desmedt, editor, Advances in Cryptology - CRYPTO'94, volume 839 of Lecture Notes in Computer Science, pages 1-11. Springer, August 1994.

[122] Mao, Y. B., Chen, G. R., & Lian, S. G. (2004). *A symmetric image encryption scheme based on 3D chaotic cat maps.* Chaos, Solitons and Fractals, 21, 749-761.

[123] M. Allen, G. Kumaran, T. Liu. *A combined algorithm for graph-coloring in register allocation.* In D. S. Johnson, A. Mehrotra, M. Trick (eds.), Proceedings

of the Computational Symposium on Graph Coloring and its Generalizations, pages 100-111, Ithaca, New York, USA, 2002.

[124] M.R. Garey, D.S. Johnson. *Computers and intractability : A guide to the theory of NPcompleteness.* W.H. Freeman and Company, New York, Nantes, France, 1979.

[125] Meyer, J. and Gadegast, F., *Security Mechanisms for Multimedia Data with the Example MPEG-1 Video,* Project Description of SECMPEG, Technical University of Berlin, Germany, (May 1995).

[126] M. Van Droogenbroeck and R. Benedett, *Techniques for a selective encryption of uncompressed and compressed images,* in ACIVS Advanced Concepts for Intelligent Vision Systems, Ghent, Belgium, (September 2002), pp. 90-97.

[127] M. Steiner, G. Tsudik and M. Waidner, *Diffie-Hellman Key Disrtribution Extended to Group Communication,* Proceding of the 3rd ACM conference on computer and communications security, March 14-16 (1996), new Delhi.

[128] M. Burmester and Y. Desmedt. *A Secure And Efficient Conference Key Distribution System.* In I.B. Damgard, editor, Advances in Cryptology, EUROCRYPT'94, Lecture Notes in Computer Science. Springer-Verlag, Berlin Germany, 1994.

[129] M. Bellare, A. Boldyreva, and S. Micali, *Public-key encryption in a multi-user setting : security proofs and improvements,* in Proceeding of Advances Cryptology - Eurocrypt 2000, LNCS 1807, pp.259-274, Springer-Verlag, Bruges, Belgium, May 2000.

[130] M. El-lskandarani, S. Darwish, and S. Abuguba, *A robust and secure scheme for image transmission over wireless channels,* in Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference on. IEEE, 2008, pp. 51-55.

[131] Michel Demazure. *Cours d'Algèbre-Primalité, Divisibilité, Codes,* volume 1 of Nouvelle Bibliothèque mathématique. Cassini, 1997.

[132] M. Chapman : *Hiding the Hidden : A Software System for Concealing Ciphertext in Innocuous Text.* Th'ese de doctorat, The University of Wisconsin-Milwaukee, mai 1997.

[133] M. Fouquet, *Anneau d'endomorphismes et cardinalité des courbes elliptiques : aspects algorithmiques. PhD thesis, Ecole Polytechnique. Dec, (2001). 2.*

[134] McCurley K.S., *The Discrete Logarithm Problem,* Cryptology and Computational Number Theory, volume 42, pages 49-74, American Mathematical Society, 1990

[135] Munch.H, U. Englemann, A. Schroter and H.P. Meinzer, "The integration of medical images with the patient record and their web based distribution", *Journal. Acad. Radiol. ,vol.11, no.6, 2004, pp. 661-668.*

[136] NEMA : " NEMA Standards : Digital Imaging & Communications in Medicine " , *Rosslyn (Virginia) : National Electrical Manufacturers Association, NEMA Standards Publication, N° PS 3.5-1996, 1996, 77p.*

[137] N. Bourbakis and C. Alexopoulos. *Picture data encryption using scan patterns.* Pattern Recognition, 25(6) :567-581, (1992).

[138] National Bureau of Standards, *Data Encryption Standard,"* FIPS Publication 46, (1977).

[139] *National Institute of Standards and Technology. Secure Hash Standard.* FIPS Publication 180, (1993).

[140] N. El-Fishawy and O. Zaid, *Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms,* International Journal of Network Security, vol. 5, no. 3, pp. 241-251, 2007.

[141] N. Barnier, P. Brisset. *Graph coloring for air traffic flow management.* In CPAIOR'02 : Fourth International Workshop on Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimisation Problems, pages 133-147. Le Croisic, France, 2002.

[142] N.F. Johnson, Z. Duric et S. Jajodia : *Information Hinding - Steganography and watermarking - Attacks and countermeasures.* Adavances in Information Security. Kluwer Academic. ISBN : 0-7923-7204-2.

[143] N. Provos et P. Honeyman : *Detecting steganographic content on the internet.* In Proc. ISOC NDSS'02, San Diego, CA, USA, février 2002.

[144] N.F. Johnson et S. Jajodia : *Exploring steganography : Seeing the unseen.* IEEE Computer, 31(2) :26-34, 1998.

[145] N. Koblitz, *Elliptic Curve Cryptosystems. Mathematics of Computation. 48, 203-209 (1987). 2, 6, 21, 37.*

[146] N. Provos., *Universal steganography*, août 1998. http ://wwww.outguess.org/.

[147] P. Kocher, J. Jaffe, and B. Jun. *Differential power analysis.* In M. J. Wiener, editor, Advances in Cryptology-CRYPTO'99, volume 1666 of Lecture Notes in Computer Science, pages 388-397. Springer-Verlag, 1999.

[148] P. Shanmugam1, C.Loganathan, *INVOLUTORY MATRIX IN VISUAL CRYPTOGRAPHY*, IJRRAS, 2011, Vol 6, Issue4, pp. : 424-428.

[149] Pommer, A. and Uhl, A., *Selective Encryption of Wavelet-Packet Encoded Image Data,* to appear in ACM Multimedia Systems Journal, Special Issue on Multimedia Security in 2003.

[150] Podesser, M., Schmidt, H.-P. and Uhl, A., *Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments,* 5th Nordic Signal Processing Symposium, on board Hurtigruten, Norway, October 4-7, (2002).

[151] P. Ribenboim, *The Little Book of Big Primes,* Springer-Verlag, 1991.

[152] PIVA A., BARNI M., BARTOLINI F., DE ROSA A., *"Data Hiding Technologies for Digital Radiography"*, IEEE Vision, Image and Signal Processing, vol. 152, nř5, p. 604- 610, 2005.

[153] P. WAYNER., *Disappearing cryptography - Information Hiding : steganography and watermarking*, Morgan Kaufmann, 2002. ISBN : 1-55860-769-2

[154] P. Smith and M. J. J. Lennon, *LUC : A new public key system.* In Proc. of the Ninth IFIP Int. Symp. on Computer Security, p. 103-117, 1993.

[155] P. Smith. *LUC Public Key System : A secure Alternative to RSA.* Dr. Dobb's Journal, January 1993.

[156] R. L. Rivest, A. Shamir, and L. Adleman. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* Communications of the ACM, 21 :120-126, (1978).

[157] R. Rivest. *The MD4 Message-Digest Algorithm.* RFC 1320 (Informational), (1992). http ://www.ietf.org/rfc/rfc1320.txt.

[158] R. Chandramouli, *M. Kharrazi et N.D. Memon : Image steganography and steganalysis : Concepts and practice.* In T. Kalker, I. J. Cox et Y.M. Ro, ťediteurs : Proc. Digital Watermarking, Second International Workshop, IWDW 2003, volume 2939 de Lecture Notes in Computer Science, pages 35-49, Seoul, Korea, octobre 2003. Springer. ISBN : 3-540-21061-X.

[159] R. Chandramouli et N.D. Memon : *Steganography capacity : A steganalysis perspective.* In Proc. SPIE, Security and Watermarking of Multimedia Contents V, volume 5020, pages 173-177, Santa Clara, CA, USA, janvier 2003.

[160] R. Chandramouli : *Mathematical theory for steganalysis.* In Proc. SPIE Security and Watermarking of Multimedia Contents IV, 2002.

[161] Robinson.G.P, H. D. Tagare, J. S. Duncan, and C. C. Jaffe, "Medical image collection indexing : Shape - based retrieval using KD-trees," *Comput. Med. Imag. Graph., vol. 20, no. 4, 1996, .pp. 209-217.*

[162] Rafael C. Gonzalez, Richard E. Woods, *Digital Image Processing, 2nd edition,* Addison-Wesley, 1993.

[163] R. Dorne, J.K. Hao. In : Voss, s., martello, s., osman, i.h., roucairol, c.(eds.), *tabu search for graph coloring, t-colorings and set t-colorings metaheuristics.* Advances and Trends in Local Search Paradigms for Optimization. Kluwer, 117 : 77-92, 1998.

[164] R. Norcen,M. Podesser, A. Pommer, H.P. Schmidt, and A. Uhl. *Confidential storage and transmission of medical image data. Computers in Biology and Medicine,.* 33 :277-292, 2003.

[165] S. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, *A new modified version of advanced encryption standard based algorithm for image encryption,* in Electronics and Information Engineering (ICEIE), 2010 International Conference On, vol. 1. IEEE, 2010, pp. V1-141.

[166] Somdip Dey, *SD-AEI : An Advanced Encryption Technique For Images*, IEEE 2012, Second International Conference on Digital Information Processing and Communications (ICDIPC2012), Lithuania, pp. 68-73.

[167] S. Lian, J. Sun and Z. Wang. *Security analysis of a chaos based image encryption algorithm,* Physica A : Statistical and Theoretical Physics, vol. 351, Issues 2-4, 15 June 2005, pp. 645-661.

[168] Simon Singh, *Histoire des codes secrets. De l'Égypte des pharaons à l'ordinateur quantique*, Jean-Claude Lattès, (1999).

[169] S. Li, X. Mou and Y. Cai, *Pseudo-Random Bit Generator Based on Couple Chaotic Systems and Its Applications in Stream Cipher Cryptography,* Springer-Verlag, Berlin LNCS, Vol. 2247, pp. 316 329, (2001).

[170] S. Mukhopadhyay, M. Mitra, S. Banerjee, edited by S. Banerjee, *Chaos Synchronization and Cryptography for Secure Communications : Applications for Encryption (IGI Global Publishers, USA, 2010), ISBN : 1615207376, p. 476.*

[171] S. M. Douiri and S. Elbernoussi, *New Heuristic for the Sum Coloring Problem*, Applied Mathematical Sciences,. 5(63), 3121-3129, 2011.

[172] Spanos, G. A. and Maples, T. B., *Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-time Video,* Proceedings of 4th International Conference on Computer Communications and Networks, 20-23, (1995).

[173] S. Berkovits, *How to broadcast a secret,* in Proceeding of Advances Cryptology - Eurocrypt'91, LNCS 547, pp. 535-541, Springer-Verlag, Brighton, UK, Apr.1991.

[174] S. M. Douiri, M.B. O. Medeni, S. Elbernoussi1, E. Souidi. *A New Steganographic Method For Grayscale Image Using Graph Coloring Problem. Applied Mathematical Sciences.* 7, No. 2, 521-527 (2013).

[175] S. Katzenbeisser et F.A.P. Petitcolas : *Information Hiding. Techniques for steganography and digital watermarking.* Computer Science. Artech House. ISBN : 1-5853-035-4.

[176] S. C. Pohlig and M. E. Hellman, *An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance. IEEE Transactions on Information Theory. IT-24(1), 106-110, january (1978).*

[177] T. Paraskevi, N. Klimis, K. Stefanos. *Security of Human Video Objects by Incorporating a Chaos-Based Feedback Cryptographic Scheme,* ACM Multimedia '04, October, 10- 16, 2004, New York, NY USA.

[178] T. Baritaud, H. Gilbert, and M. Girault. *F.F.T. hasing is not collision-free.* In R.A. Rueppel, editor, Advances in Cryptology - Proceedings of EUROCRYPT 1992, volume 658 of Lecture Notes in Computer Science, pages 35-44. Springer-Verlag, (1992).

[179] T. Berger and P. Loidreau. *Weak keys in McEliece public-key cryptosystem.* IEEE Transactions on Information Theory, 47(3) :1207-1212, (March 2001).

[180] Tagare.H.G, C. C. Jaffe, and J. Dunkan, "Medical image databases : A content-based retrieval approach," *Journal of Am. Med. Inform. Assoc., vol. 4, no. 3, May 1997, pp. 184-198.*

[181] T. Elgamal, *A public key cryptosystem and a signature scheme based on discrete logarithms.* IEEE Transactions on Information Theory, v.31 n.4, p.469-472, July 1985.

[182] US Federal Rules of Evidence 1001, 1002, and 1003. *Federal Rules of Evidence* (LII 2006 ed.)

[183] Vinay pandey , Angad Singh, Manish Shrivastava, *Medical Image Protection by Using Cryptography Data-Hiding and Steganography*, International Journal of Emerging Technology and Advanced Engineering , 2012, Volume 2, Issue 1, pp. : 106-109.

[184] V. Miller, *Use of elliptic curves in cryptography in Advances in cryptography-CRYPTO 85. Lecture Notes In Computer Science Springer-Verlag. vol 218, 417-426 (1989). 2, 6.*

[185] V. Shoup, *Lower Bounds for Discrete Logarithms and Related Problems. In Eurocrypt -97, LNCS. 1233,Springer-Verlag , 256-266 (1997). 2, 37.*

[186] W. Diffie and M. E. Hellman, *New directions in cryptography,* IEEE Trans. Inform. Theory, vol. IT-22, (1976), pp. 644-654.

[187] W. Puech and J.M. Rodrigues. *A New Crypto-Watermarking Method for Medical Images Safe Transfer.* In Proc. 12th European Signal Processing Conference (EUSIPCO'04), pages 1481-1484, Vienna, Austria, (2004).

[188] W. Puech, J.M. Rodrigues and J.E Develay-Morice. *Safe Transfer of Medical Images by Conjoined Coding : Selective Encryption by AES Using the Stream Cipher Mode OFB and JPEG Compression.* Traitement du signal (TS), numéro spécial "Traitement du signal appliqué à la cancérologie", vol. 23, n^o 3-4, pp. 201-211, (2006).

[189] William Puech, Jose Marconi Rodrigues. *Crypto-Compression of Medical Images by Selective Encryption of DCT,* EUSIPCO'05 : European Signal Processing Conference, Sep 2005, Antalya (Turkey).

[190] W. Stallings, *Cryptography and Network Security,* 3rd edition, Prentice Hall, (2003).

[191] Wolfram, S. (1985). *Cryptography with cellular automata. In : Advances in Cryptology- Crypto'85, Lectures Notes in Computer Science, Vol. 218, pp.429-432, Springer- Verlag, Berlin.*

[192] Xiaoyun Wang and Hongbo Yu. *How to Break MD5 and Other Hash Functions.* In Ronald Cramer, editor, Advances in Cryptology - EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science, pages 19-35. Springer, May 2005.

[193] Xiaoyun Wang, Hongbo Yu, and Yiqun Lisa Yin. *Efficient Collision Search Attacks on SHA-0.* In Victor Shoup, editor, Advances in Cryptology - CRYPTO 2005, volume 3621 of Lecture Notes in Computer Science, pages 1-16. Springer, August 2005.

[194] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. *Finding Collisions in the Full SHA-1.* In Victor Shoup, editor, Advances in Cryptology - CRYPTO 2005, volume 3621 of Lecture Notes in Computer Science, pages 17-36. Springer, August 2005.

[195] X. Shu-Jiang, W. Ying-Long, W. Ji-Zhi, and T. Min, *A novel image encryption scheme based on chaotic maps,* in Signal Processing, 2008. ICSP 2008. 9th International Conference on. IEEE, 2008, pp. 1014-1018.

[196] Xuehu Yan, et al, *A New Assessment Measure of Shadow Image Quality Based on Error Diffusion Techniques*, Journal of Information Hiding and Multimedia Signal Processing, Volume 4, Number 2, April 2013.

[197] X. Du, Y. Wang, J. Ge, and Y. M. Wang, *An ID-based broadcast encryption scheme for key distribution,* IEEE Transations Broadcast, vol. 51, no. 2, pp. 264-266, June 2005.

[198] Yen, J. C., & Guo, J. I. (2000). *A new chaotic key-based design for image encryption and decryption.* In Proceedings of IEEE International Conference on Circuits and Systems (Vol. 4, pp. 49-52).

[199] Y. Mao and G. Chen, *Chaos-based image encryption,* Handbook of Geometric Computing, pp. 231-265, 2005.

[200] Y. Matias and A. Shamir. *A video scrambling technique based on space filing curves.* In CRYPTO '87, pages 398-417, (1988).

[201] Yue Wu, Joseph P. Noonan and Sos Agaian *NPCR and UACI Randomness Tests for Image Encryption*, Journal of Selected Areas in Telecommunications (JSAT), 2011,pp : 31-38.

[202] Z. Han, W. Feng, L. Hui, L. Da Hai, and L. Chou, *A new image encryption algorithm based on chaos system,* in Robotics, Intelligent Systems and Signal Processing, 2003. Proceedings. 2003 IEEE International Conference on, vol. 2. IEEE, 2003, pp. 778-782.

[203] Ziedan, I. E., Fouad, M. M., & Salem, D. H. (2003). *A pplication of data encryption standard to bitmap and JPEG images.* In Proceedings of 12th National Radio Science Conference (NRSC2003) (pp. C16/1-C16/8).