**République Algérienne Démocratique et Populaire**

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Dr YAHIA FARES de Médéa



Faculté des Sciences et de la Technologie

Département du Génie électrique et de l'Informatique

**Mémoire de fin d'études**

**Pour l'obtention du diplôme de Master en Génie électrique**

**OPTION : télécommunication**

## THÈME :

# Cryptage chaotique pour la sécurisation de l'information : application au texte et à l'image

**Présenté Par :**

**HAMIOUDA Bachir**

**TOUAHRI Oussama**

**Proposé et dirigé par :**

**Mr. LAIDI Kamal**

**Promotion 2011/2012**

# *Remerciement*

*Le premier merci à ALLAH qui nous a donné la volenté et le courage pour la réalisation de ce Modeste travaille.*

*Nous tenons tout d'abord à adresser nos plus sincères et profonds remerciements à mr laidi kamel qui a proposé ce travail et qui nous avons encadré, épaulé et supporté pendant tout la durée de ce travail et nous le remercions aussi de nous avoir apporté la rigueur scientifique nécessaire au bon déroulement de ce mémoire et de nous avoir fait partager son vaste expérience dans le domaine de cryptographie.*

*Je remercie MR Birane, MR Boucherit et MR Regai pour avoir accepté d'examiner ce travail.*

*Un grand merci à nos parents qui nous ont toujours soutenus, aidé et remonté le moral quand c'était nécessaire.*

*Aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire, merci.*

*Enfin, nous adressons nos plus sincères remerciements à tous nos proches et amis, qui nous ont toujours soutenue et encouragée au cours de la réalisation de ce mémoire.*

*Merci à tous et à toutes.*

# *Dédicaces*

*Je dédie ce modeste travail à mes cher parent qui mon toujours soutenu et encouragé, Que ce travail soit une petit récompense pour leurs efforts et confiance. Merci maman merci papa*

*Je dédie aussi ce travail à mes petites sœurs NASSIMA, RIHANA, KATR ENNADA et MILAD*

*A ma grande mère, mes tantes SAIDA, NACERA, HADDA*

*A tous mes amis les deux MOHAMED, TEDJ EDDINE, REDHWANE, YOUCEF, AMIN, ABD ENNOUR, NACER, HAMZA ET TOUT l'équipe de l'union générale des étudiants algériens et l'équipe de Qnet…. Qui mon toujours soutenu et aider.*

*A mon promoteur Mr. LAIDI KAMEL qui m'aidé dans tous me recherche dans ce thème et dans tous mes années des études, merci MR.*

*OUSSAMA.*

# *Dédicaces*

*Je dédie ce modeste travail :*

*A mes très chers parents qui m'ont permis de réussir dans mes études, et mes frères.*

*A tous ceux qui m'ont aidé durant mes études.*

*Et a tous mes amis YOUCEF, MOHAMED, HAMZA, FODIL….*

*BACHIR.*

# TABLE DES MATIÈRES

**Table des matières** .....

**Liste des figures**.....

**Introduction générale**.....01

## Chapitre 1 : Introduction à la cryptographie

1.1 Introduction ..... 03

1.2 Notions de cryptologie..... 03

1.2.1 Cryptographie..... 03

1.2.2 Cryptanalyse..... 04

1.3 Historique..... 05

1.4 Techniques de cryptographie classique..... 06

1.4.1 Système de César..... 06

1.4.2 Système de Vigenère..... 07

1.4.3 Système de Playfair..... 09

1.4.4 Système ADFG(V) X.....09

1.4.5 Machines à rotors.....10

1.5 Techniques de cryptographie modernes.....12

1.5.1 Chiffrement symétrique.....12

1.5.1.1 Crypto systèmes par flots.....12

1.5.1.2 Crypto systèmes par blocs.....13

1.5.1.2.1 DES (Data Encryptions Standard) ..... 14

1.5.1.2.2 AES (Advanced Encryptions Standard) ..... 15

1.5.2 Chiffrements asymétriques.....15

1.5.2.1 Chiffrement RSA (1978) .....16

1.5.2.2 Chiffrement d'ElGamal (1985) .....18

1.5.2.3 D'autres chiffrements asymétriques.....18

1.6 Avantages et inconvénients des chiffrements symétriques et asymétriques.....19
1.7 Sécurité et attaques de systèmes actuels.....19
1.7.1 L'attaque en force (ou Brute force attack, Exhaustive keysearchattack) .....20
1.7.2 L'attaque à l'aide de l'analyse statistique (ou Statistical analysesattack) .....20
1.7.3 L'attaque à l'aide de textes chiffrés seulement (ou Ciphertext-onlyattack) .....21
1.7.4 L'attaque à l'aide de textes clairs (ou Known-plaintextattack) .....21
1.7.5 L'attaque à l'aide de textes clairs choisis (ou Chosen-plaintextattack) .....21
1.7.6 L'attaque d'une tierce personne (ou Man-in-the-middle attack ) .....21
1.7.7 L'attaque à l'aide du temps d'opération (ou Timing Attack ) ..... 21
1.7.8 Attaque des crypto systèmes RSA.....21
1.7.9 Attaques des crypto systèmes DES.....24
1.8 Conclusion.....25

# Chapitre 02 : Cryptographie chaotique

2.1 Introduction .....26
2.2 Généralités sur les systèmes chaotiques ..... 27
2.2.1 Propriétés des systèmes chaotiques ..... 28
2.2.2 Les caractéristiques des systèmes chaotiques..... 29
2.2.3 Synchronisation de chaos..... 30
2.2.4 Avantage de chaos..... 31
2.2.5 Les domaines d'application..... 32
2.3 La cryptographie chaotique.....33
2.3.1 Générateur pseudo-aléatoire.....33
2.3.2 Principe de cryptage chaotique.....33
2.3.3 Types de cryptographie chaotique.....34
2.3.3.1 Chiffrement analogique.....35
2.3.3.2 Chiffrement numérique.....38
2.3.4 Application de la cryptographie chaotique.....39
2.4 Récurrences chaotique.....40
2.5 Conclusion.....43

# Chapitre 03 : Méthode de Baptista : application et résultats

3.1 Introduction ……..……44
3.2 Explication de la méthode ……...44
3.3 Organigramme de la méthode de Baptista …….53
3.4 Application de la méthode sous ‘MATLAB’ ……...54
3.4.1 Interface du programme de cryptage et du décryptage d’un texte…….54
3.4.2 Cryptage et décryptage d’un texte pour différentes valeurs de ŋ …….55
3.4.3 Cryptage et décryptage d’un texte pour différentes valeurs de la clef b ……..60
3.4.4 Cryptage et décryptage d’un texte pour différentes valeurs de X0 ……...64
3.4.5 Interfaces des programmes de cryptage/décryptage d’une image ……..67
3.4.6 Cryptage et décryptage d’une image pour différentes valeurs de ŋ ……...68
3.4.7 L’effet de l’augmentation de la valeur de ŋ sur le cryptage et le décryptage d’une image ……..……70
3.4.8 Cryptage et décryptage d’une image pour différentes valeurs de la clef b …….….71
3.4.9 Cryptage et décryptage d’une image pour différentes valeurs de condition initiale..74
3.5 Conclusion ……..77
Conclusion Générale ……..78
Bibliographie……

# LISTE DES FIGURES

Fig.1.1 Exemple de cryptage par le système de Vigenère.....08

Fig.1.2 Cryptage par le système ADFG(V)X.....10

Fig.1.3 Le cryptage en utilisant la machine à rotors.....11

Fig.1.4 Exemple de chiffrement à masque jetable.....13

Fig.1.5 Attaque de crypto système RSA.....23

Fig.2.1 Générateur Pseudo-Aléatoire « générateur des séquences chaotiques » .....33

Fig.2.2 Le principe de cryptage par des séquences chaotiques.....34

Fig.2.3 système à masquage additif.....35

Fig.2.4 Système de cryptage par commutation.....36

Fig.2.5 Système de cryptage par modulation..... 37

Fig.2.6 Attracteur de Hénon pour a=1,4 et b=0,3.....40

Fig.2.7 Récurrence de Lozi.....41

Fig.2.8 Comportement chaotique de la carte logistique.....42

Fig.2.9 Diagramme de bifurcation de la carte logistique.....43

Fig.3.1 Représentation schématique explique comment un attracteur est devisé comme sous intervalle. Chacun de taille $\varepsilon = (X_{max} - X_{min})/S$.....45

Fig.3.2 Densité invariante naturelle de l'équation (3.1) dans l'intervalle .....47

Fig.3.3 Distribution de fréquence d'un texte chiffré.....51

Fig.3.4 Organigramme de la méthode de Baptista.....53

Fig. 3.5 Interface du programme de cryptage du texte.....54

Fig.3.6 Interface du programme de décryptage d'un texte.....55

Fig.3.7 Cryptage de la phrase ''souris à la vie et elle te sourira'', ŋ =0.....56

Fig.3.8 Décryptage du texte chiffré de la phrase ''souris à la vie et elle te sourira'', ŋ =0.....56

Fig.3.9 Cryptage de la phrase ''souris à la vie et elle te sourira'', ŋ =0.2.....57

Fig.3.10 Décryptage du texte chiffré de la phrase ''souris à la vie et elle te sourira'' ŋ =0.2.....57

Fig.3.11 **C**ryptage de la phrase ''souris à la vie et elle te sourira'', ŋ =0.6.....58

Fig.3.12 Décryptage du texte chiffré de la phrase ''souris à la vie et elle te sourira'', ŋ =0.6……58

Fig.3.13 Cryptage de la phrase ''souris à la vie et elle te sourira'', ŋ =0.95.....59

Fig.3.14 Décryptage du texte chiffré de la phrase ''souris à la vie et elle te sourira'', ŋ =0.95.....59

Fig.3.15 Cryptage de la phrase ''souris à la vie et elle te sourira'', b=3.8.....60

Fig.3.16 Décryptage du texte chiffré de la phrase ''souris à la vie et elle te sourira'', b=3.8.....61

Fig.3.17 Décryptage du texte chiffré de la phrase ''souris à la vie et elle te sourira'', b=3.8001……..61

Fig.3.18 Cryptage de la phrase ''souris à la vie et elle te sourira'', b=3.9.....62

Fig.3.19 Décryptage du texte chiffré de la phrase ''souris à la vie et elle te sourira'',

b=3.9.....62

Fig.3.20 Décryptage du texte chiffré de la phrase ''souris à la vie et elle te sourira'', *b*=3.9001……..63

Fig.3.21 Cryptage de la phrase ''souris à la vie et elle te sourira'', $X_0$=0.25..... 64

Fig.3.22 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, X0=0.25.....64

Fig.3.23 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, $X_0$=0.250001.....65

Fig.3.24 Cryptage de la phrase ‘’souris à la vie et elle te sourira’’, $X_0$=0.8.....65

Fig.3.25 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, $X_0$=0.8.....66

Fig.3.26 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, $X_0$=0.800001.....66

Fig.3.27 Interface du programme de cryptage d’une image.....67

Fig.3.28 Interface du programme de décryptage d’une image.....68

Fig.3.29 Cryptage d’une image avec ŋ=0.....68

Fig.3.30 Décryptage d’une image crypté ŋ=0.....69

Fig.3.31 Cryptage d’une image avec ŋ=0.7.....69

Fig.3.32 Décryptage d’une image avec ŋ=0.7.....69

Fig.3.33 Décryptage d’une image avec ŋ=0.95.....70

Fig.3.34 L’influence de ŋ sur une image décrypté .....70

Fig.3.35 Image décrypté bruité à cause de ŋ.....70

Fig.3.36 Cryptage d’une image avec, b=3.78.....71

Fig.3.37 Décryptage d’une image crypté, b=3.78.....71

Fig.3.38 Décryptage d’une image crypté, $b$=3.780001.....72

Fig.3.39 Cryptage d’une image avec, $b$=3.99.....72

Fig.3.40 Décryptage d’une image crypté, b=3.99.....73

Fig.3.41 Décryptage d’une image crypté, b=3.990001.....73

Fig.3.42 Cryptage d'une image avec, $X_0$=0.2 .....74

Fig.3.43 Décryptage d'une image crypté, $X_0$=0.2.....74

Fig.3.44 Décryptage d'une image crypté, $X_0$=0.20001.....75

Fig.3.45 Cryptage d'une image avec, $X_0$=0.85.....75

Fig.3.46 Décryptage d'une image crypté, $X_0$=0.85.....76

Fig.3.47 Décryptage d'une image crypté, $X_0$=0.850001.....……..76

# LISTE DES TABLEAUX

**Tableau 1.1** un exemple de substitution ……...….……07

**Tableau 1.2** cryptage par le système de Vigenère …….……08

**Tableau 1.3** numérotation des alphabets …….……..…17

**Tableau 1.4** codes du mot (BONJOUR) …….……17

**Tableau 1.5** chiffrement des codes du mot (bonjour) ……...17

**Tableau 1.6** déchiffrement de mot bonjour chiffré ……18

**Tableau 1.7** le temps de calcul des Yi ……....23

**ملخص**

**إن الهدف الرئيسي من هاته المذكرة هو دراسة إحدى طرق تشفير المعلومات و التي ادخلت في سنة 1998 من طرف الباحث M.S.BAPTISTA، حيث أن هاته الطريقة هي إحدى أحدث و أأمن الطرق التي يمكن إستعمالها في تشفير و إرسال المعلومات و بطريقة عملية ، و لا يمكن لأي كان أن يسرق المعلومات المشفرة بأية طريقة كانت لو لم يكن يعرف كل المعطيات التي استعملت في التشفير أي أنه من غير الممكن قرصنة تشفير هاته الطريقة.**

**Résumé**

**Le but de ce mémoire est l'étude d'une méthode de cryptage d'informations. Cette méthode a été introduite en 1998 par le chercheur M.S.BAPTISTA. Elle est l'une des méthodes les plus nouvelles et plus sécurisées que l'on peut utiliser dans le cryptage et dans la transmission des informations. Il est impossible à quelqu'un de voler ou de pirater les informations s'il ne connait pas les données complètes utilisées par cette méthode de cryptage. Donc c'est impossible de pirater ou de casser le cryptage quand on utilise cette méthode.**

**Abstract**

**A survey of information encrypting method has been provided in this work. This method was introduced in 1998 by the researcher M.S.BAPTISTA. Which is one of the newest and secure methods that can be used in information encryption and transmission. And it is impossible to someone to steal or hack information when he doesn't know the full used encryption data. Hence, it is impossible to hack the encryption when using this method for encryption.**

# 1. Introduction général

La cryptographie joue un rôle important dans la sécurité et la fiabilité des systèmes de transmission de données, surtout avec le développement du commerce électronique, les utilisateurs ont besoin d'authentifier et protéger des données sensibles dans leur ordinateurs et de garantir la confidentialité des transactions sur des réseaux publics tels que l'Internet. En général, un ‘’crypto système’’ doit considérer plusieurs aspects, tels que l'intégrité des données, l'authentification, l'autorisation, confidentialité, et bien d'autres.

Les techniques de cryptographie classique sont basées sur la théorie des nombres et en particulier sur la décomposition d'un entier en éléments simples. Nous pouvons aussi citer les deux algorithmes bien connus : DES, RSA. Néanmoins, avec la révolution de l'informatique, ces algorithmes proposés ne sont pas assez sécurisés. En effet, ils sont basés sur le fait que nous ne possédons pas actuellement de calculateurs capables de décomposer tout entier en éléments simples et que nous n'avons pas un algorithme qui nous donne tous les nombres premiers. Pour ces raisons, plusieurs chercheurs essayent de mettre en œuvre d'autres crypto systèmes Durant ces dernières décennies, la théorie des systèmes non linéaires a été appliquée à la cryptographie afin d'augmenter le degré de sécurité. Notamment, après le travail de Pecora et Carroll, des applications du chaos ont attiré beaucoup d'attention. Grace aux propriétés naturelles des systèmes chaotiques, telles que leurs Sensibilité aux conditions initiales et le fait qu'ils évoluent dans un large bande de fréquence, les systèmes chaotiques sont de bons candidats pour la cryptographie. De nombreux schémas sont proposés afin d'appliquer les systèmes chaotiques dans le domaine de la cryptographie.

Dans 1998, M.S Baptista a trouvé une méthode de cryptographie qui est basé sur le chaos, et qui est très sensible au condition initiale et au clef de cryptage est aussi elle est plus sécurisé par rapport des anciens méthodes puisque elle est très difficile de prévoir les résultat de cryptage à cause de quelques paramètres dans cette méthode de cryptage, et la casse de cette méthode est impossible pour un personne qui ne sait pas les valeurs exactes de paramètres de cryptage ou quel qu’un qui a une valeur approximative de ces paramètres puisque elle est très sensible à la variation de ces paramètres.

Dans ce cadre et pour voir l’intérêt du cryptage chaotique entre notre travail ; qui consiste à appliquer la méthode de Baptista pour le cryptage et le décryptage de texte et image.

Notre travail est organisé comme suit : après une introduction générale au domaine, le premier chapitre donne un état de l'art sur le cryptage et son histoire.

Le deuxième chapitre est consacré aux notions générales du cryptage chaotique et son intérêt pour la sécurisation des informations.

Le troisième chapitre est une application de la méthode de Baptista en utilisant MATLAB comme moyen de programmation.

Enfin, nous résumons les résultats obtenus et leur intérêt par une conclusion générale.

## 1.1 Introduction

La cryptographie, ou art de chiffrer, coder les messages, est devenue aujourd'hui une science à part entière. Au croisement des mathématiques, de l'informatique, et parfois même de la physique, elle permet ce dont les civilisations ont besoin depuis qu'elles existent : le maintien du secret. Pour éviter une guerre, protéger un peuple, il est parfois nécessaire de cacher des choses.

Issu du grec Cryptos (caché ou secret) et graphie (écriture), la cryptographie désigne la science de l'écriture secrète. Le service de base fourni par la cryptographie est la capacité de transmettre une information entre deux correspondants sans que celle-ci ne soit accessible à des personnes tierces.

Lorsque les informations sont de nature critique et nécessitent plus de protection que celle procurée par d'autres mécanismes, on peut avoir recours à la cryptographie ou chiffrement pour renforcer la confidentialité des données et le contrôle d'accès à ces données.

Un système cryptographique permet de transformer un message intelligible ou message en clair en un message chiffré incompréhensible ou cryptogramme Ce procédé est désigné sous le terme de chiffrement ou "cryptage ". La procédure de chiffrement utilise un algorithme et une clé de chiffrement.

La cryptographie étant un sujet très vaste, ce document se focalisera essentiellement sur l'une des méthodes de chiffrement dites modernes, c'est le cryptage chaotique.

## 1.2 Notions de cryptologie

### 1.2.1 Cryptographie

Le cryptage est un processus qui permet d'assurer la sécurité des informations personnelles et confidentielles. Il s'agit d'un procédé par lequel des segments de données sont mélangés mathématiquement à l'aide d'un mot de passe. Le processus de cryptage rend les données illisibles, à moins qu'elles ne soient décryptées ou jusqu'à ce qu'elles le soient.

Le cryptage des données peut constituer une mesure efficace de protection pour la gestion des informations personnelles du personnel ou des élèves. Les employées et employés des conseils scolaires devraient comprendre que le cryptage des données ne remplace pas d'autres mesures de protection des informations telles que le contrôle de l'accès, l'authentification ou l'autorisation; que le cryptage des données devrait être utilisé conjointement avec ces autres contrôles; et que la mise en œuvre du cryptage des données devrait être proportionnelle aux besoins en matière de protection des données.

### 1.2.2 Cryptanalyse

La cryptanalyse des algorithmes est essentielle pour trouver les failles des algorithmes. Faire la cryptanalyse d'un algorithme de chiffrement, c'est étudier sa sécurité en tentant de résoudre (casser) les fonctions cryptographiques qui le composent à l'aide d'attaques. Il est donc avantageux pour un algorithme d'être complètement publié (code source) dans le but que des cryptographes étudient sa sécurité

Dans cet ordre d'idées, il existe plusieurs attaques qui sont souvent utilisées et qui ont été répertoriées

D'abord il est important de connaître les vulnérabilités des systèmes cryptographiques. Souvent, les attaques fructueuses sur un système de chiffrement ne touchent aucunement les algorithmes de chiffrement en cause. Il peut s'agir notamment de l'exploitation d'une erreur de conception, d'une erreur de réalisation ou d'une erreur d'installation

#### 1.2.2.1 Liste des types de vulnérabilités

· Vulnérabilités des architectures cryptologiques.

· Vulnérabilités des réalisations.

· Vulnérabilités liées aux mots de passe.

· Vulnérabilités du matériel.

· Vulnérabilités des modèles de la confiance.

· Vulnérabilités des utilisateurs.

· Vulnérabilités de la reprise après incident.

· Vulnérabilités cryptographiques.

## 1.3 Historique [PAL 06] [PIE 12]

L'histoire de la cryptographie a été pendant longtemps l'histoire des codes secrets et depuis l'Antiquité, ils ont décidé du sort des hommes et des nations. En effet, jusqu'aux années 1970, l'unique objectif de la cryptographie était de construire des systèmes de chiffrement. Les crypto systèmes sauvèrent les Grecs des Perses, accompagnèrent César dans ses conquêtes, firent arrêter et décapiter Marie Stuart, décidèrent Wilson à rejoindre les Alliés et permirent d'épargner des milliers de vies pendant la Seconde Guerre mondiale.

L'invention de la radio a donné un nouvel élan à la cryptographie, car il est devenu encore plus facile d'intercepter une communication longue distance. La Seconde Guerre mondiale a été profondément affectée par l'utilisation de la cryptographie et le cassage des systèmes cryptographiques utilisés pour les communications radio. Il est intéressant de voir que les premières machines calculatoires conçues et construites par les Britanniques pour casser le système de chiffrement allemand, Enigma, sont les premiers exemples réels d'ordinateurs, si bien que l'on peut dire que la cryptographie est à l'origine de l'informatique.

La révolution d'Internet et l'utilisation de plus en plus massive d'informations sous forme numérique facilitent les communications et rendent de ce fait plus fragiles les informations que l'on détient. En effet, les réseaux « ouverts » créent des brèches de sécurité car il est plus aisé pour un adversaire d'accéder aux informations. De même, le remplacement de l'Homme par des machines rend les relations beaucoup plus anonymes alors qu'en même temps, l'accès aux données demande des moyens d'authentification forts. De plus, la dématérialisation des documents change les moyens de preuve juridique : les signatures numériques doivent remplir certaines exigences que nous ne connaissions pas avec les signatures manuscrites. Ainsi, la révolution numérique des communications et de l'information a ouvert de nombreux champs d'investigation à la cryptographie, différents du seul besoin de confidentialité, de sorte que celle-ci a envahi notre vie quotidienne : carte à puce, transaction bancaire, Internet, téléphone cellulaire, télévision à péage...

Dans le même temps, la cryptologie est devenue une science. La cryptologie, la science du secret d'après son étymologie grecque, comprend d'une part la cryptographie, art de la conception de systèmes sécurisés, et d'autre part la

cryptanalyse, art du cassage des systèmes. Par abus de langage, nous emploierons souvent le terme cryptographie à la place de cryptologie. Les différentes techniques employées, mélangeant mathématiques classiques du XVIIIe siècle et informatique théorique, lui confèrent aujourd'hui une place à part parmi les sciences. Depuis les années 1970, on a assisté à une explosion de la recherche en cryptographie. Beaucoup de systèmes ont été proposés, et beaucoup ont été détruits.

Notre compréhension de la notion subtile de « sécurité cryptographique » a constamment progressé et, de nos jours, les crypto systèmes sont prouvés sûrs (sous certaines hypothèses plausibles). Les relations fascinantes entre la cryptographie, la théorie de la complexité et la théorie algorithmique des nombres ont petit à petit enrichi ces trois domaines de recherche.

## 1.4 Techniques de cryptographie classique [PAL 06] [PIE 12] [DAN 03] [DAN 96]

Contrairement à ce que l'on peut penser, la cryptographie n'est pas seulement une technique moderne, ni un produit de l'ère informatique. En effet de tout temps, les hommes ont ressenti le besoin de cacher des informations confidentielles. Bien évidemment depuis ses débuts la cryptographie a grandement évolué. Au cours des siècles, de nombreux systèmes de chiffrage ont été inventés, tous de plus en plus perfectionnés, et il est vrai que l'informatique y a beaucoup contribué. Mais au commencement les algorithmes étaient loin d'être aussi complexes et astucieux qu'à notre époque. La majeure partie des méthodes d'antan reposait sur deux principes fondamentaux : la substitution (remplacer certaines lettres par d'autres) et la transposition (permuter des lettres du message afin de le brouiller).

### 1.4.1 Système de César [SAN 04] [DAN 96]

L'un des systèmes les plus anciens et les plus simples est le codage par substitution mono alphabétique (ou alphabets désordonnés). Il consiste à remplacer chaque lettre par une lettre différente. Il existe donc grâce à ces techniques 26 façons de coder un message, ce qui fait que ce système a été longtemps utilisé par les armées pendant l'antiquité. Ce procédé très fiable à l'époque est tout de même problématique car il nécessite que les interlocuteurs se souviennent tous deux de

la clef. De plus, il est évident que la sûreté de ce codage est quasi nulle et qu'il pourrait être déchiffré par n'importe quelle personne qui y mettrait le temps nécessaire.

**Tableau 1.1** un exemple de substitution.

| Texte clair | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Texte codé | W | X | E | H | Y | Z | T | K | C | P | J | I | U | A | D | G | L | Q | M | N | R | S | F | V | B | O |

La méthode la plus ancienne admise par l'histoire (par substitution alphabétique) est le non moins connu code de César, consistant en un décalage simple de lettres. Par substitution si l'on remplace le A par le C, alors le B devient D, le D un F, etc.… César utilisait ce code simple pour transmettre via un message des consignes à ces généraux d'armées sans qu'il puisse être exploité par un quelconque ennemi dans le cas où le message serait intercepté.

Malheureusement il n'y a que 26 façons différentes de chiffrer à l'aide de ce code ce qui en fait un code très peu sûr. Mais ce qui est d'autant plus insolite, c'est le fait que ce code de « César » est encore utilisé de nos jours sur Internet avec le (rotation de 13 lettres) qui consiste à cacher des messages afin qu'ils ne soient pas lus involontairement, comme par exemple s'ils dévoilent le dénouement d'un film ou encore qui donne la réponse à une devinette.

### 1.4.2 Système de Vigenère [SAN 04] [DAN 96]

Un autre système de cryptographie des plus anciens est cette fois-ci, la substitution poly alphabétique, qui utilise plusieurs alphabets décalés pour crypter un message.

L'algorithme de substitution poly alphabétique le plus connu est le chiffre de Vigenère, mis au point par Blaise de Vigenère en 1586, qui fut utilisé pendant plus de 3 siècles. Son chiffre consiste à utiliser le chiffre de César, mais en changeant le décalage à chaque fois. Il utilise alors un carré composé de 26 alphabets alignés, décalés de colonne en colonne d'un caractère. Il place également au-dessus de ce carré, un alphabet pour la clef et à sa gauche un autre alphabet pour le texte à coder. Il suffit alors, pour chiffrer un message, de choisir un mot de

longueur quelconque, de l'écrire sous le message à coder (de façon répétée s'il le faut) et de regarder dans le tableau l'intersection de la lettre à coder et de la lettre de la clef.

Pour mieux comprendre le fonctionnement du Carré de Vigenère nous vous proposons cet exemple :

Supposons que nous voulons coder le texte « CARRE DE VIGENERE » avec la clef « MALICE ». On commence par écrire la clef sous le texte à coder :

**Tableau 1.2** cryptage par le système de Vigenère

| C | A | R | R | E | D | E | V | I | G | E | N | E | R | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M | A | L | I | C | E | M | A | L | I | C | E | M | A | L |

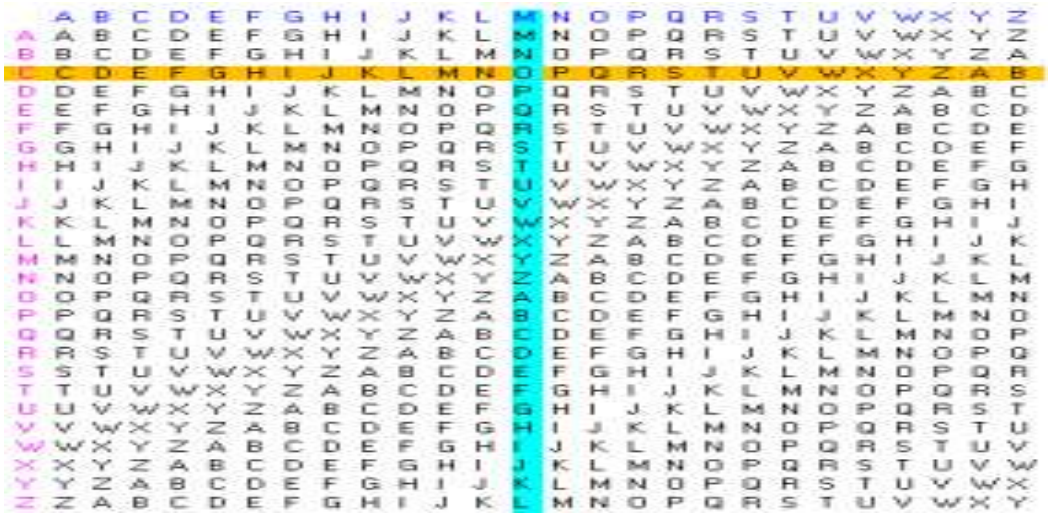


Fig1.1 : exemple de cryptage par le système de Vigenère.

Pour coder la lettre C, la clef est donnée par la lettre M. On regarde dans le tableau l'intersection de la ligne donnée par le C, et de la colonne donnée par le M. On trouve O. Puis on continue, jusqu'à ce qu'on ait fini de chiffrer notre texte. En chiffrant le texte « Carre de Vigenère », on obtient donc le texte « OAUZG HG VTOGRQRP ».

Cet algorithme de cryptographie ainsi que celui de César sont les premiers des algorithmes à clef privée.

### 1.4.3 Système de Playfair [DAN 03] [SAN04]

Il existe d'autres systèmes presque aussi anciens basés également sur des techniques par substitution mais moins connus que ceux vus précédemment. Il s'agit des systèmes par substitution de poly grammes. En effet au lieu de substituer des caractères, on substitue par exemple des diagrammes (des groupes de lettres le plus souvent). Le système de « Playfair » inventé par Sir Charles Wheatstone, popularisé par L.Playfair utilise ce stratagème au moyen d'une table. Cet algorithme remplace chaque paire de lettre du texte en clair par une autre paire. Il utilise pour cela une table (matrice) carrée de coté 5, construite à partir d'une clef, qui contient toutes les lettres de l'alphabet hormis une (souvent le J par similitude avec le I).

Chaque couple de lettre donne les coordonnées d'un rectangle dans la matrice. On remplace donc ce couple par les lettres formant les deux autres coins du rectangle . Si les deux lettres du couple sont sur la même ligne, on prend les deux lettres suivantes. Si elles sont sur la même colonne, on prend les 2 lettres du dessous. Si les 2 lettres sont identiques, on intercale entre elles une lettre convenue à l'avance (X ou Y).

Malheureusement, ce chiffre ingénieux ne fut pas utilisé souvent en raison du fait qu'il se déchiffre aisément en regardant quel couple de lettres apparaît le plus souvent dans le texte chiffré, et en supposant qu'ils représentent le couple de lettres le plus courant.

### 1.4.4 Système ADFG(V) X [SAN04]

Mais même si la cryptographie était beaucoup utilisée de tout temps, jusqu'au début du XXe siècle, elle gardait une importance mineure, et les méthodes utilisées étaient bien souvent rudimentaires. Avec la 1e guerre mondiale, la cryptographie subit un véritable « boum ». La communication entre état-major et les troupes se fait par radio et il faut donc empêcher les ennemis de comprendre les messages s'ils sont interceptés. C'est là que la cryptographie intervient, permettant à l'armée française de stopper de nombreuses offensives allemandes. Le chiffre ADFGVX en est un exemple concret. En effet ce code était utilisé par l'armée allemande depuis mars 1918 et malgré leurs efforts et leur talent, l'équipe française de cryptographie n'arrivaient pas à le déchiffrer. Pour réaliser ce code, qui mélange transpositions et substitutions, il faut ranger les 26 lettres de l'alphabet ainsi que les 10 chiffres dans un tableau de 6 cases sur 6. Au-dessus et à côté de ce tableau est ajouté le fameux mot

ADFGVX. Chacune des lettres du texte en clair est remplacée par le couple de lettres qui correspond à sa ligne et sa colonne.

Le 2 juin 1918, l'équipe de cryptographie perce à jour ce système et déchiffre un message allemand ordonnant une attaque éclair près de Compiègne. Les troupes françaises s'y massent, permettant de stopper l'ennemi.

| | A | D | F | G | V | X |
|---|---|---|---|---|---|---|
| A | Q | Y | A | L | S | E |
| D | Z | X | R | C | H | 0 |
| F | F | O | 4 | M | 8 | 7 |
| G | 3 | I | T | G | U | K |
| V | P | D | 6 | 2 | N | G |
| X | 1 | 5 | J | 9 | W | B |

Fig. 1.2 : cryptage par le système ADFG(V)X

### 1.4.5 Machines à rotors

Très vite après la première guerre, on s'est rendu compte que si l'on souhaitait diffuser beaucoup de documents chiffrés rapidement, et pouvoir changer de clef de chiffrement facilement, il fallait fabriquer des machines à chiffrer et à déchiffrer. Les machines utilisées à ces fins sont les machines à rotors (dont la plus célèbre était la machine ENIGMA à 3 rotors inventée dans les années 30). Cette machine électrique est composée d'un clavier alphabétique, d'un écran lumineux et de trois rotors. Le système est simple : l'utilisateur tape une lettre sur le clavier et le texte chiffré apparaît alors sur l'écran. A chaque frappe sur le clavier, le premier rotor tournait d'une unité puis à la fin d'un tour complet décalait le deuxième rotor d'une unité et ainsi de suite. On positionnait initialement les rotors comme on voulait, ce qui définissait ainsi la clef (FAC par exemple).

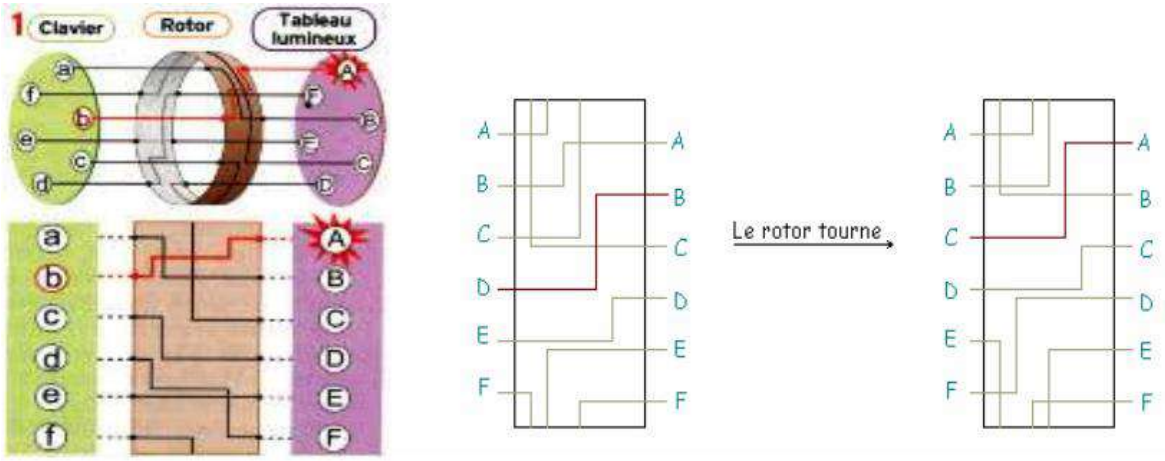



Fig. 1.3 : le cryptage en utilisant la machine à rotors

Grâce à cette machine un texte pouvait être codé d'un million de façons différentes. La frappe au clavier d'une lettre en allumait une autre sur l'écran de manière symétrique (si A donnait C alors C donnait A). Ainsi pour chiffrer un message, une fois la clef fixée, il suffisait de le taper sur la machine et pour le déchiffrer de mettre les rotors dans la même position initiale et de taper le message chiffré. Chaque message commençait par la donnée de la clef choisie par l'opérateur, qu'il cryptait elle aussi selon une liste de clef changeant tous les jours. La machine ENIGMA a été utilisée pendant toute la seconde guerre mondiale par l'armée allemande qui croyait en son inviolabilité. Une équipe de mathématiciens (spécialisée en cryptanalyse, art de déchiffrer des messages) anglais dirigée par A. Turing finit par la décrypter.

On voit donc ici que la cryptographie est une technique de guerre à part entière et qu'elle joue un vrai rôle dans l'ère moderne. En effet on se rend compte qu'en l'espace de quelques années, la cryptographie et la cryptanalyse sont passées de simples techniques désuètes, à véritables sciences. Cette progression des techniques et algorithmes de cryptage ne s'est pas faite toute seule et c'est totalement à cause des attaques incessantes, visant à « casser » les techniques adverses, que l'on a pu assister à un tel bond.

## 1.5 Techniques de cryptographie modernes [PIE 12] [HER 01]

### 1.5.1 Chiffrement symétrique [PIE 12]

Le chiffrement symétrique utilise la même clef pour chiffrer et déchiffrer un message. La connaissance de cette clef est cruciale pour la confidentialité des informations échangées. Les algorithmes de chiffrement symétrique sont souvent basés sur des techniques de substitutions et de transpositions .Cela offre un moyen rapide et efficace pour chiffrer un message. Nous présentons trois méthodes de chiffrement : Le chiffrement de Vernam, le DES et l'AES que sont devisés sur 2 catégories de crypto système, crypto système par flot (vernam) et crypto système par bloc (DES, AES).

#### 1.5.1.1 Crypto systèmes par flots

Dans un crypto système par flots, le cryptage des messages se fait caractère par caractère ou bit à bit, au moyen de substitutions de type César générées aléatoirement : la taille de la clef est donc égale à la taille du message. L'exemple le plus illustratif de ce principe est le chiffre de Vernam. Cet algorithme est aussi appelé « One Time Pad » (masque jetable), c'est à dire que la clef n'est utilisée qu'une seule fois.

##### 1.5.1.1.1 Le chiffrement parfait (chiffrement de Vernam) [CED 10]

Il s'agit du « chiffrement à masque jetable » (One-time Pad) inventé par le Major J. Mauborgne et G. Vernam en 1917. Un masque jetable est une suite de bits aléatoires aussi longue que le message à chiffrer. Cette suite est un secret connu uniquement des deux participants et ne peut être utilisée qu'une seule fois. Le message original est codé sous forme de bits, pour le chiffrer, nous comparons chaque bit du masque et du message. S'ils sont égaux, nous écrivons 1 sinon 0 dans le message chiffré, ceci revient à effectuer une addition bit à bit modulo 2. Connaissant le masque, il est alors facile de reconstituer le message original .Illustrons cette technique en additionnant modulo 26 les lettres de l'alphabet au lieu d'utiliser l'addition bit à bit modulo 2. Imaginons que nous souhaitons chiffrer une autre fameuse citation de Jules César, prononcée lorsqu'il franchit le Rubicon : « ALEA JACTA EST ». Nous utilisons comme masque jetable, une phrase connue à l'avance par les deux participants. Prenons la phrase de Jules César déchiffrée précédemment « VENI VIDI

VICI ». La figure 1.1 montre comment cette phrase est chiffrée en « WQSJ FJGCW NVC ».

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *A* | *L* | *E* | *A* | *J* | *A* | *C* | *T* | *A* | *E* | *S* | *T* |
| | 1 | 12 | 5 | 1 | 10 | 1 | 3 | 20 | 1 | 5 | 19 | 20 |
| + | *V* | *E* | *N* | *I* | *V* | *I* | *D* | *I* | *V* | *I* | *C* | *I* |
| | 22 | 5 | 14 | 9 | 22 | 9 | 4 | 9 | 22 | 9 | 3 | 9 |
| = | *W* | *Q* | *S* | *J* | *F* | *J* | *G* | *C* | *W* | *N* | *V* | *C* |
| | 23 | 17 | 19 | 10 | 6 | 10 | 7 | 3 | 23 | 14 | 22 | 3 |

Fig. 1.4 Exemple de chiffrement à masque jetable.

Malheureusement, le chiffrement à masque jetable présente quelques inconvénients lors de sa mise en pratique car le masque doit être :

– aussi long que le message à chiffrer.

– utilisé une seule fois.

– généré de manière aléatoire pour éviter qu'il ne soit deviné.

– échangé de manière sûre entre les participants.

Sans connaître le masque il est prouvé sous ces conditions qu'il est impossible de retrouver le message original. Le chiffrement à masque jetable est un chiffrement parfait i.e. sans la clef le message est indéchiffrable. Comme l'a fort bien souligné Steve Bellovin: « As a practical Person, I've observed that one-time pads are theoretically unbreakable, but practically very weak. By contrast, conventionnel ciphers are theoretically breakable, but practically strong. » : Le chiffrement à masque jetable est inviolable en théorie mais inutilisable en pratique. Il faut donc se tourner vers d'autres méthodes de chiffrement.

### 1.5.1.2 Crypto systèmes par blocs

La deuxième classe de crypto systèmes utilisée aujourd'hui est celle des crypto systèmes par blocs. Dans ce mode de cryptage, le texte en clair est fractionné en blocs de même longueur à l'aide d'une clef unique. Les algorithmes de chiffrement par blocs sont en général construits sur un modèle itératif. Ce modèle emploie une fonction

F qui prend en paramètres une clef k et un message de n bits. F est répétée un certain nombre de fois, on parle de ronde. A chaque ronde, la clef k utilisée est changée et le message que l'on chiffre est le résultat de l'itération précédente.

$$C_1 = F(k_1, M)$$

$$C_2 = F(k_2, C_1) \qquad (1.1)$$

....

$$C_r = F(k_r, C_{r-1})$$

Emetteur et destinataire se partagent une clé K secrète. L'algorithme qui engendre les clefs $k_i$ à partir de K se nomme l'algorithme de cadencement des clefs.

La fonction F doit être inversible, ce qui veut dire qu'il faut pour toute clef k et message M pouvoir recalculer M à partir de F (k', M), sinon le déchiffrement est impossible et on ne dispose pas d'un algorithme utilisable. C'est-à-dire qu'il existe une fonction G vérifiant G (k, F (k, M)) = M et que F est une permutation. La sécurité d'un algorithme de chiffrement par blocs réside principalement dans la conception de l'algorithme de cadencement des clefs et la robustesse de la fonction F. Si l'algorithme de cadencement est mal élaboré, les ki peuvent être déductibles les unes des autres. La fonction F doit donc être difficile à inverser sans connaître la clef k ayant servie dans le calcul de C = F (k, M). En d'autres termes, connaissant seulement C, F et G, on ne doit pouvoir retrouver le message M seulement en effectuant une recherche exhaustive de la clef.

Les caractéristiques de ces systèmes sont en général liées à leur très forte sensibilité à la dépendance inter-symboles, ainsi qu'à leur mécanisme de propagation d'erreurs. Toute erreur commise sur un bloc de texte clair ou chiffré peut perturber gravement le chiffrement/déchiffrement de ses voisins.

#### 1.5.1.2.1 DES (Data Encryptions Standard)

Le 23 Novembre 1976, le NIST (National Institute of Standards and Technologies) adopte le standard de chiffrement DES. Ce chiffrement conçu par IBM sous le nom de LUCIFER a été choisi par la NIST après quelques petites modifications. Ce chiffrement symétrique permet de chiffrer des messages de 64 bits avec une clef k de 56 bits. Pour chiffrer un texte, il faut d'abord le découper en blocs de 64

bits puis appliquer le chiffrement sur chacun des blocs. Ce procédé est un mode de chiffrement par blocs. Nous donnons ci-dessous une idée simple et intuitive du fonctionnement du DES (pour plus de détails consulter le livre de B. Scheiner « Applied Cryptography ». Ce chiffrement est constitué de 16 enchaînements successifs d'opérations de transposition, de substitution et de chiffrement de Vernam. Les avancées matérielles en informatique permettent aujourd'hui, en un temps raisonnable de « casser » un message chiffré avec DES par « force brute», i.e. en testant toutes les clefs possibles grâce à une énumération exhaustive. En 1998, la NIST lança un appel d'offres pour choisir, l' « Advanced Encryptions Standard » (AES), le successeur du DES, devenu trop sensible aux attaques par recherches exhaustives.

#### 1.5.1.2.2 AES (Advanced Encryptions Standard)

Le standard de chiffrement AES fut adopté en 2000 par le NIST en emplacement du DES. Le NIST nomma AES cet algorithme symétrique de Rijndael, conçu par Vincent Rijmen et Joan Daemen. Ce chiffrement est constitué de substitutions, de décalages, de « ou exclusif » et de multiplications dans un corps fini de polynômes fixés ; ces opérations sont élémentaires, simples et rapides à calculer. Il permet de crypter des blocs de 128, 192 ou 256 bits en utilisant des clefs symétriques de 128, 192 ou 256 bits. Le choix de la taille de la clef et de la taille des blocs sont indépendants, il y a donc au total 9 combinaisons possibles. Ceci laisse une plus grande flexibilité à l'utilisateur d'AES en fonction du niveau de sécurité et de la vitesse de calcul désirés.

### 1.5.2 Chiffrements asymétriques

Un chiffrement asymétrique utilise une clef de chiffrement différente de celle de déchiffrement. La clef de chiffrement est souvent connue de tous les agents, elle est appelée clef publique et permet de construire un message chiffré. Cependant seuls les participants connaissant la clef de déchiffrement, appelée clef privée, peuvent déchiffrer les messages. Les chiffrements asymétriques sont la plupart du temps basés sur l'existence de fonctions mathématiques dites à sens unique ou sens unique avec trappe. Une fonction à sens unique est une fonction mathématique facilement calculable mais dont la réciproque est, en pratique, impossible à calculer car trop coûteuse. Par exemple, le produit de deux grands nombres premiers est une opération mathématique simple, mais trouver à partir de ce produit les deux nombres premiers est un problème

connu difficile. Ce problème est appelé problème de factorisation. Les fonctions à sens unique avec trappe sont, elles aussi, facilement calculables mais leur réciproque est difficile à effectuer sauf pour les personnes qui connaissent une information secrète : la trappe. Ainsi, la factorisation en produit de deux nombres premiers est une fonction à sens unique avec trappe : si nous connaissons un des deux nombres premiers, il devient alors aisé par une simple division de retrouver le second nombre premier. Nous illustrons ci-dessous ces méthodes de chiffrement. D'abord nous décrivons le chiffrement RSA, certainement le plus connu et le plus utilisé des chiffrements asymétriques, ensuite nous présentons le chiffrement asymétrique probabiliste d'ElGamal.

#### 1.5.2.1 Chiffrement RSA (1978)

L'algorithme le plus célèbre d'algorithme à clef publique a été inventé en 1977 par Ron Rivest, Adi Shamir et Len Adleman, à la suite de la publication de l'idée d'une cryptographie à clef publique par Diffie et Hellman. Il fut appelé RSA, des initiales de ces inventeurs.

RSA est basé sur la difficulté de factoriser un grand nombre en produit de deux grands facteurs premiers. L'algorithme fonctionne de la manière suivante : Imaginons que Bob souhaite recevoir d'Alice des messages en utilisant RSA.

**Génération des clefs**

a. p et q, deux grands nombres premiers sont générés au hasard grâce à un algorithme de test de primalité probabiliste, avec n = pq.

b. Un nombre entier e premier avec (p-1)(q-1) est choisi. Deux nombres sont premiers entre eux s'ils n'ont pas d'autre facteur commun que 1.

c. L'entier d est l'entier de l'intervalle [2, (p-1)(q-1)[ tel que ed soit congrue à 1modulo (p-1)(q-1), c'est-à-dire tel que ed-1 soit un multiple de (p-1)(q-1).

**Distribution des clefs**

Le couple (n, e) constitue la clef publique de Bob. Il la rend disponible à Alice en lui envoyant ou en la mettant dans un annuaire. Le couple (n, d) constitue quant à lui sa clef privée.

**Chiffrement du message**

Pour crypter le message Alice représente le message sous la forme d'un ou plusieurs entiers M compris entre 0 et n-1. Elle calcule

$$C = M^e \bmod n \qquad (1.2)$$

Grâce à la clef publique (n, e) de Bob et envoie C à Bob.

**Déchiffrement du message**

Bob reçoit C et calcule grâce à sa clef privée Cd mod n. Il obtient ainsi le message initial M.

**Exemple**

Bob choisit p = 17 et q = 19, n = p x q = 323 et e = 5. Sa clef privée est alors d=173 car 173 x 5 = 1 (mod (16 x 18))

Supposons qu'Alice veuille lui envoyer le message « BONJOUR » en se servant du tableau suivant pour transformer les lettres en nombre :

**Tableau 1.3** numérotation des alphabets

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

Cela donne :

**Tableau 1.4** codes du mot (BONJOUR)

| B | O | N | J | O | U | R |
|---|---|---|---|---|---|---|
| 2 | 15 | 14 | 10 | 15 | 21 | 18 |

Après avoir chiffré en remplaçant chaque nombre b par ($b^e$ mod n) on obtient :

**Tableau 1.5** chiffrement des codes du mot (bonjour)

| 32 | 2 | 29 | 193 | 2 | 89 | 18 |
|---|---|---|---|---|---|---|

Qu'Alice envoie à Bob.

Bob réalise pour chaque nombre b du message $b^d$ mod n pour trouver :

**Tableau 1.6** déchiffrement de mot bonjour chiffré

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 15 | 14 | 10 | 15 | 21 | 18 |
| B | O | N | J | O | U | R |

Qui est bien le message initial.

RSA est basé sur la difficulté de factoriser n. En effet celui qui arrive à factoriser n peut retrouver facilement la clef secrète de Bob connaissant seulement sa clef publique. C'est pourquoi dans la pratique la taille des clefs est au minimum de 512 bits.

### 1.5.2.2 Chiffrement d'ElGamal (1985)

En 1985, ElGamal invente une technique de chiffrement asymétrique probabiliste i.e. un même message m peut avoir plusieurs chiffres différents. Cette fois le problème difficile utilisé est le logarithme discret, provenant de la théorie des nombres, i.e. à partir de ga mod p il est difficile de retrouver a, où ga mod p dénote g à la puissance a modulo p. Pour utiliser le chiffrement d'ElGamal, il faut d'abord choisir un grand nombre premier p et un générateur g du groupe multiplicatif dans Z/pZ. La clef privée est un nombre entier aléatoire $\chi$ tel que $1 \leq \chi \leq p - 2$. La clef publique est constituée de p, g et $h = g\chi \bmod p$. Par ce chiffrement, un message m chiffré est représenté par un couple de nombres (a, b). Pour coder un message, choisissons aléatoirement un nombre r tel que $1 \leq r \leq p - 2$ et calculons le couple de nombres (a, b) tel que :

$$\{M\}(P, g, h) = (gr \bmod p, mhr \bmod p) = (a, b) \quad (1.3)$$

Nous retrouvons le message m à partir du chiffré (a, b) = {m}(p,g,h), connaissant $\chi$, en calculant :

$$m = b / a\chi \bmod p \quad (1.4)$$

### 1.5.2.3 D'autres chiffrements asymétriques

Il existe de nombreuses méthodes de chiffrements asymétriques. Elles sont souvent rattachées à un problème mathématique difficile, comme le chiffrement de Rabin, inventé

en 1979, qui est basé sur le problème difficile des racines carrées dans un corps fini. Citons une dernière méthode de chiffrement qui repose sur un problème difficile beaucoup plus complexe. Il s'agit de l'usage des courbes elliptiques en cryptographie proposé en 1985 par Miller (pour une approche générale des courbes elliptiques.

## 1.6 Avantages et inconvénients des chiffrements symétriques et asymétriques

Nous comparons ces deux types de chiffrements qui sont complémentaires et omniprésents dans les protocoles cryptographiques modernes.

Le chiffrement symétrique est plus rapide à calculer et utilise des clefs de tailles plus petites qu'un chiffrement asymétrique. De plus, il est basé des fonctions mathématiques simples et donc facilement implémentables au niveau matériel. Par contre, pour chaque communication avec chaque participant, une clef déférente est nécessaire. Il faut donc gérer la distribution d'un grand nombre de clefs, sachant que la divulgation de la clef serait catastrophique pour la sécurité de la communication.

Un chiffrement asymétrique permet de signer facilement un message, alors qu'un chiffrement symétrique ne peut le faire. La distribution des clefs publiques est très simple à gérer avec ce genre de chiffrement. De plus, cette méthode de chiffrement utilise des clefs de grandes tailles et nécessite un temps de calcul plus long et plus de ressources que lors d'un chiffrement symétrique, ceci à cause de la complexité des opérations à effectuer.

## 1.7 Sécurité et attaques de systèmes actuels [ASD 08]

Bien évidemment, la qualité la plus importante que doit posséder un crypto système est la sécurité, c'est-à-dire qu'il doit pouvoir résister à quelconque attaque qui aurait pour but de le casser et dans extraire le texte en clair original. Bien évidemment la bête noire de la cryptographie est la cryptanalyse, mais l'on se rend vite compte que sans ces multiples attaques ennemies, la cryptographie n'aurait bien évidemment jamais autant progressé et serait restée au même stade que celle de César.

De nos jours, comme de tous temps, un système de chiffrement repose donc sur son inviolabilité. C'est pour cela que pour des systèmes aussi utilisés que RSA, DES ou SSL, la cryptanalyse de ces algorithmes est essentielle pour en trouver les failles. A l'aide de simulations (attaques), on effectue alors la cryptanalyse des algorithmes de chiffrement

: on étudie sa sécurité en tentant de casser les fonctions cryptographiques qui le composent. Il est donc préférable pour un algorithme d'être diffusé (code source) pour que des cryptographes puissent mettre à l'épreuve sa sécurité.

Dans le cas des systèmes vus auparavant et bien d'autres, il semble évident que la cryptanalyse a bien aidée à renforcer leur sécurité, mais celle-ci n'en est pas pour autant devenue parfaite. En effet leur quasi invulnérabilité cède parfois devant certaines attaques.

En fait, les attaques sur un système de chiffrement ne touchent souvent pas les algorithmes de chiffrement en cause. Il peut s'agir la plupart du temps de l'exploitation d'une erreur de conception, d'une erreur de réalisation ou d'une erreur d'installation.

On peut distinguer deux types réels d'attaque. Premièrement les attaques passives ont pour but d'intercepter un message et d'exploiter les informations contenues dans celui-ci. Cette attaque ne modifie en rien les informations interceptées ou de manières imperceptibles. Le deuxième type d'attaques est les attaques actives qui visent à ralentir, dégrader ou même empêcher la communication, d'envoyer des informations parasites dans le but de saturer des systèmes, de modifier les informations afin de tromper le destinataire ou de faire carrément disparaître ces informations.

Les types d'attaques employés le plus couramment sont nombreux et diffèrent selon le type du système (symétrique, asymétrique, etc…).

Nous vous présentons ici une liste des types d'attaques sur les algorithmes :

### 1.7.1 L'attaque en force (ou Brute force attack, Exhaustive key search attack)

Le cryptographe essaie toutes les combinaisons de clefs possibles jusqu'à l'obtention du texte clair. Avec des ordinateurs de plus en plus performants et des méthodes de calculs distribués, l'attaque en force restera toujours un moyen de casser des systèmes de chiffrement.

### 1.7.2 L'attaque à l'aide de l'analyse statistique (ou Statistical analyses attack)

Le cryptographe possède des informations sur les statistiques du message clair (fréquences des lettres ou des séquences de lettres). Les systèmes tels que ceux par substitution ne résistent pas à une telle attaque.

### 1.7.3 L'attaque à l'aide de textes chiffrés seulement (ou Ciphertext-only attack)

Le cryptographe dispose de messages chiffrés par l'algorithme et fait des hypothèses sur le texte clair (présence d'expressions, de mots, le sens du message, format ASCII etc.). Il peut grâce à cela soit retrouvé les textes en clair, soit retrouver la clef.

### 1.7.4 L'attaque à l'aide de textes clairs (ou Known-plaintext attack)

Le cryptographe dispose des messages ou parties de message clairs et de leur version chiffrée. Le but du cryptographe est alors de retrouver la clef. Ce type d'attaque est très répandu.

### 1.7.5 L'attaque à l'aide de textes clairs choisis (ou Chosen-plaintext attack)

Le cryptographe dispose des messages clairs et de leur version chiffrée. Il a aussi la possibilité de tester des messages et d'obtenir le résultat chiffré. Les chiffrements asymétriques sont notamment vulnérables à cette attaque.

### 1.7.6 L'attaque d'une tierce personne (ou Man-in-the-middle attack )

Cette attaque plus communément appelée l'attaque de «l'homme du milieu» intervient dans une transaction entre deux personnes (groupes…). Une troisième personne s'interpose de manière transparente entre les deux et termine la transaction normalement en captant les messages et en transmettant d'autres messages. Il peut donc ainsi intercepter et même modifier les messages envoyés sans que les deux entités s'en aperçoivent. Cette attaque peut être évitée avec les signatures digitales.

### 1.7.7 L'attaque à l'aide du temps d'opération (ou Timing Attack )

Cette méthode est basée sur la mesure du temps nécessaire pour effectuer des chiffrements ou des déchiffrements. Ainsi cette étude permet de mieux cibler la longueur de la clef utilisée et a donc pour but de limiter grandement le domaine des clefs à explorer pour une cryptanalyse classique.

### 1.7.8 Attaques des crypto systèmes RSA

RSA est probablement une méthode de chiffrement assez sûre: il y a très certainement plus de risques liés à une mauvaise utilisation qu'à une attaque, mais les risques issus de cette dernière ne sont pourtant pas nuls. Nous rappelons que par exemple lors d'une

attaque d'un système de type RSA, l'objectif d'un attaquant n'est pas forcément de retrouver la clef privée associée à la clef publique. Le plus souvent l'attaquant cherche seulement à retrouver le message clair à partir d'un message chiffré ou même seulement un bit ou une partie du message.

Bien que RSA soit un des crypto systèmes les plus sûrs de nos jours, il n'en demeure malheureusement pas moins vulnérable à certaines attaques comme l'attaque de «l'homme du milieu» ou la Timing attaque. L'attaque de « l'homme du milieu » peut être employée de façon évidente pour casser cet algorithme. Supposons dans notre cas qu'Edgar soit un espion et qu'il veuille intercepter les conversations entre Alice et Bob. Il suffit alors à Edgar de choisir une clef privée b et une clef publique qui convient (a, n) qu'il envoie à Alice en lui faisant croire que ce sont les nouvelles clefs de Bob. Notre espion peut alors lorsqu'il intercepte les messages d'Alice, les déchiffrer et les comprendre. Il lui reste donc à s'assurer que Bob ne se rende compte de rien en rechiffrant les messages d'Alice avec l'ancienne clef publique de Bob qui reçoit le message comme si aucune opération n'avait été effectuée dessus. S'il le veut il peut effectuer la même opération en sens inverse, pour récupérer les messages que Bob envoie à Alice. Pour contrer cette attaque, il est très important pour Alice et Bob de toujours s'assurer que personne ne tente de modifier leurs messages en effectuant plusieurs vérifications. Pour cela, les méthodes les plus utilisées sont celles d'authentification et de signature que nous expliquerons plus en détail dans un chapitre ultérieure. Ces méthodes permettent de s'assurer que le document reçu n'a pas été modifié en cours de route, et qu'il provient bien de l'expéditeur initial.

De plus on a vu que le principe de base de RSA était la décomposition d'un nombre n'en produit de 2 nombres entiers p et q. Une attaque assez évidente serait de tenter de trouver la factorisation de n. Cependant les plus puissants algorithmes existants ne peuvent effectuer cette factorisation que pour des entiers inférieurs à 155 chiffres (soit une clef de 512 bits). Il est donc évident que la sécurité du RSA repose sur la difficulté de factoriser de grands entiers car il est simple, pour garantir une grande sécurité, de choisir de plus grandes clefs (par exemple de 1024 ou 2048 bits). Malheureusement on ne peut pas affirmer que cette simple protection suffise, car la constante amélioration des ordinateurs et des algorithmes de factorisation permettront peut-être plus tôt que prévu de casser RSA.

Enfin, il existe un nouveau type d'attaque qui semble plus percutante et plus novatrice que les autres, la Timing attaque. En effet comme nous l'avons vu, le fonctionnement de RSA est basé sur la fonction $b^e$ mod n servant à déchiffrer le texte y codé reçu. L'entier n est rendu publique et le texte y a pu être intercepté par un attaquant qui aura alors pour but de trouver la clef secrète e. Pour chaque message y que reçoit la victime, elle devra donc calculer $b^e$ mod n. Il est alors facile pour l'attaquant d'enregistrer les messages reçus par la cible et de mesurer le temps mis pour répondre à chaque message codé y.

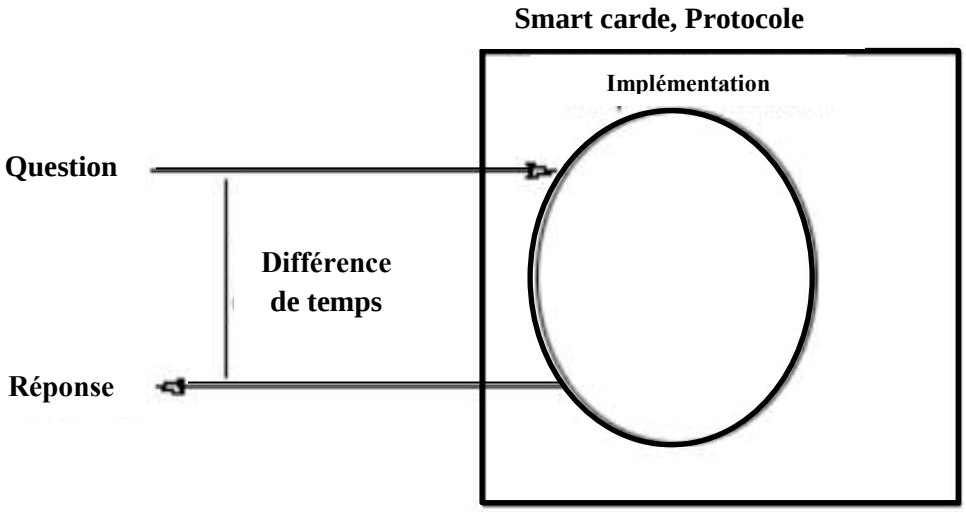



Fig. 1.5 : attaque de crypto système RSA

L'attaquant peut ensuite recueillir les temps de calcul pour un grand nombre de messages et dresser un tableau associant un message avec le temps de décryptage associé (voir tableau ci-dessous).

**Tableau 1.7** le temps de calcul des Yi

| Y1 | Y2 | Y3 | … | Yi | … | Yn |
|---|---|---|---|---|---|---|
| 137 ms | 154 ms | 132 ms | … | 170 ms | … | 147 ms |

Ainsi en dressant cette liste de mesure et en l'exploitant, l'on peut restreindre de beaucoup l'intervalle dans lequel on recherche la clef, car il est évident que pour des clefs d'une telle longueur, il faut explorer une immensité de cas différents. Cependant cette attaque n'est pas infaillible, car il est sûr que RSA ne serait pas encore si utilisé de nos jours si une attaque avait d'aussi grandes chances de « casser » à chaque tentative

ce système. La solution assez évidente pour parer ce genre d'attaque est de choisir un nouvel exposant x pour chaque opération, l'attaque ne fonctionne donc plus.

De nombreuses attaques maintenant assez répandues fonctionnent contre le crypto système RSA, mais la grande sécurité de ce système permet d'y remédier. C'est pour cela que comme nous l'avons dit précédemment les failles de RSA pourraient plutôt provenir de la manière de l'utiliser et non de ces failles de sécurités en elle-même. RSA en demeure un des systèmes les plus sûrs de nos jours.

### 1.7.9 Attaques des crypto systèmes DES

Le DES l'un des crypto systèmes les plus connus à clefs privées, n'est tout autant que RSA pas invulnérables à toutes les attaques qu'il peut subir régulièrement. En effet de nombreuses attaques sont déjà arrivées par le passé à venir à bout des algorithmes qui composent le DES, malgré le fait qu'il était considéré comme l 'un des moyens de chiffrement les plus sûrs. Mais les attaques incessantes qu'il subissait, ont eu raison de DES et ont montré au grand jour ses faiblesses.

L'attaque qui fonctionne le mieux sur DES est l'attaque en force qui consiste, comme nous l'avons vu, à essayer d'appliquer toutes les combinaisons de clefs envisageables sur le texte chiffré, jusqu'à obtenir le texte en clair. Cette méthode semble assez « primaire », mais elle a pourtant permis en 1999 à l'aide d'un grand nombre d'ordinateurs travaillant simultanément de casser le DES en seulement 22 heures. Ceci dit l'attaque de type force brute ne se révèle pas tout le temps aussi fructueuse que cela, et il faut dans certains cas plusieurs mois voire plusieurs années pour passer toutes les clefs.

Les attaques par force brute ne sont pas les seuls à fonctionner contre DES. Les attaques à l'aide du texte clair fonctionnent également comme contre beaucoup de crypto systèmes actuels. Cette attaque consiste en une « cryptanalyse linéaire», c'est à dire que l'attaquant essai de modéliser sous forme d'approximation linéaire les algorithmes conduisant aux textes chiffrés. Avec un grand nombre de textes clairs et de textes chiffrés, on peut obtenir certains bits de la clef. Cette attaque est actuellement l'une des plus performantes, puisqu'elle ne nécessite que 243 couples de textes (clairs et chiffrés). Grâce à une telle cryptanalyse une clef DES a été trouvée en seulement 50 jours avec l'aide d'une douzaine de machines.

## 1.8 Conclusion

Les cryptographes n'ont cessé de redoubler d'ingéniosité, faisant se succéder des dizaines de systèmes de chiffrement plus recherchés les uns que les autres. Se livrant bataille pour la gloire ou l'argent, ils n'ont cessé de faire évoluer cette science qu'est la cryptographie. Avec d'abord une mécanisation (notamment la machine Enigma), puis grâce à l'avènement des ordinateurs, et avec eux une puissance de calcul surpassant de loin le niveau humain, la cryptographie a su trouver son chemin dans les dédales du progrès.

...Progrès qui ne s'arrête jamais ! Déjà maintenant, d'autres voies, encore obscures, se dessinent :

- Les ordinateurs quantiques : ils procureraient une puissance de calcul colossale, et une sécurité infaillible ! Cependant, la théorie est là, mais la mise en œuvre semble très difficile... pour l'instant :)
- la cryptographie multi variable quadratique : des multiples équations faisant intervenir jusqu'à 120 variables
- Le chaos chiffrant : "noyer" le message dans un signal chaotique et, connaissant les caractéristiques du signal, le retrouver.
- Des méthodes fondées sur les courbes elliptiques .

## 2.1 Introduction.

L'augmentation considérable des débits des télécommunications réalisée ces dernières années tant dans les transmissions numériques qu'analogiques, a rendu les méthodes usuelles de cryptage vulnérables. En effet, ces dernières reposant sur un algorithme de calcul deviennent de plus en plus fragile face à la montée en puissance des calculateurs, car, si leur rapidité de calcul est très efficace pour chiffrer ou déchiffrer l'information, elle l'est aussi pour la cryptanalyse (la «science» du cassage des codes ou «clés») puisqu'un très bon moyen de casser un code peut se réduire selon les cas à chercher toutes les combinaisons. De plus, l'annonce des capacités de calcul très prometteuses (et colossales) de l'ordinateur quantique ainsi que la constante avancée de la théorie des nombres font apercevoir la chute brutale du cryptage algorithmique. Deux alternatives très prometteuses ont alors été développées: la cryptographie quantique et la cryptographie chaotique.

La sécurisation de la chaîne de transmission devient de plus en plus nécessaire avec l'évolution des communications en termes de nombre d'utilisateur et nature d'information à transmettre. Durant ces années, des nouvelles méthodes qui utilisent le chaos dans les systèmes de transmission sont développées, ces méthodes ont poussé les recherches vers l'amélioration de la qualité de l'information reçue ainsi que la robustesse des algorithmes qui traitent cette information transmise. Pour cela, actuellement tout système de télécommunication performant nécessite un système de cryptage robuste afin de se protéger envers les attaques possible.

La cryptographie de chaos (chaotique) a été réalisé au début des années 90 et est résultat et émergeant hors des études sur la théorie de chaos.

Les différentes possibilités d'utiliser les signaux chaotiques en cryptographie s'articulent aujourd'hui autour de deux directions principales de travail : l'utilisation de chaos pour crypter les messages à transmettre et l'utilisation de chaos pour l'échange d'un secret commun servant de clé de communication entre interlocuteurs autorisés. Ces deux directions sont indépendantes et compatibles entre elles : elles peuvent donc être réunies au sein d'un même système final. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information. La récupération de l'information chiffrée nécessitera la synchronisation de l'émetteur et de récepteur.

## 2.2 Généralités sur les systèmes chaotiques [TAL 10] [CAR 11]

Le terme "chaos" définit un état particulier d'un système dont le comportement n'est pas attendu de se produire, est très sensible aux conditions initiales, est imprédictible à long terme. caractérisé par une confusion de tous les éléments et par l'absence de l'ordre.

Les origines de la notion du chaos qui a commencé avec **Isaac Newton** (1642 - 1727), et un siècle après Isaac Newton, **Pierre Simon Laplace** (1749 - 1827), reposait sur le fait que l'univers serait régi par des lois immuables et qu'il serait possible de connaître l'avenir et le passé à partir du simple présent. Laplace écrivait ceci : « nous devons donc envisager l'état présent de l'univers comme l'effet de son état antérieur, et comme la cause de ce qui va suivre ». Un écossais du nom de **James Clerk Maxwell** (1831 - 1879) dans son livre intitulé « Matter and Motion », il réfute l'idée Laplacienne selon laquelle « les mêmes conditions produisent toujours les mêmes effets ».

Le premier découvreur du chaos est physicien français **Henri Poincaré** (1854 - 1912). Il découvrit la notion de sensibilité aux conditions initiales à travers le problème de l'interaction de trois corps célestes (1890). Il s'agit tout simplement de considérer trois corps comme l'ensemble « Terre, Lune, Soleil ». Plutôt que d'étudier le mouvement de ces astres, il cherche à déterminer l'ensemble des mouvements susceptibles d'être reproduits par le système. En effet, l'étude de l'interaction de deux corps peut être facilement menée par les lois de Newton, mais la considération d'un troisième corps implique des comportements complexes s'apparentant au hasard. La sensibilité aux conditions initiales est l'une des caractéristiques du chaos. Elle correspond au fait que de petites causes entraînent de grands effets. Plus tard**,** dans les années 1960, **Edward Lorenz (**1917 - 2008), physicien météorologue de son état, travaillait au Massachusetts Institute of Technology (M.I.T), a travaillé sur un projet visant à simuler les conditions météorologiques sur un ordinateur. Il a choisi plus de 10 équations non linéaires sur la vitesse du fluide du stress circulatoire pour calculer les valeurs. Un jour, il a accidentellement trébuché sur l'effet papillon dans le processus de simulation. L'effet papillon reflète la façon dont les changements sur la petite place peuvent influencer les choses sur la grande échelle. Le battement d'ailes d'un papillon, engendrerait une tempête. Il est l'exemple classique du chaos, où de petits changements peuvent entraîner des changements importants. En 1963, **Edward Lorenz** organisa 3 équations simples appelées

les équations de Lorenz. Le chaos a trouvé de nombreuses applications dans les domaines tant physique que biologique, chimique ou économique, par exemple.

### 2.2.1 Propriétés des systèmes chaotiques. [CAR 11] [CHA 09] [GOU 10]

Les systèmes qui sont fondamentalement non-linéaires et présentant un comportement apparemment aléatoire pour certaine plage de valeurs des paramètres du système sont appelés chaotiques. Toutefois, les solutions ou les trajectoires du système resté borné dans l'espace des phases. Cet état instable a une forte dépendance sur les valeurs des paramètres et sur la façon dont le système commence.

Les propriétés suivantes caractérisent la dynamique chaotique

- Dynamique déterministe et aspect pseudo aléatoire : Un processus déterministe peut causer un comportement pseudo aléatoire.

- Sensibilité aux conditions initiales : Une petite déviation dans l'entrée peut causer un grand changement au rendement. et on peut dire que de très petits changements sur l'état initial peuvent mener à des comportements radicalement différents dans son état final.

- Ergodicité : Le rendement a la même distribution pour n'importe quelle entrée (chaque trajectoire tend à une distribution invariable qui est indépendante de conditions initiales). L'ergodicité est que la propriété dans laquelle une trajectoire dans l'espace des phases est arbitrairement proche de ses états antérieurs. Une trajectoire d'un système chaotique dans ses errances évolutionnistes satisfait également cette propriété. Il reflète essentiellement que le système est éventuellement limité à un objet spatial, un ensemble de points appelé un attracteur. La densité de ces points est invariante dans le temps et cette propriété est essentielle à la cryptographie.

- Complexité de structure et complexité d'algorithme : Un processus simple a une complexité très élevée.

- l'imprévisibilité: en raison de la sensibilité aux conditions initiales.

### 2.2.2 Les caractéristiques des systèmes chaotiques [CAR 11] [CHA 09]

Quelques caractéristiques qui permettent de comprendre les points marquants d'un système chaotique.

- ***Les attracteurs:***

Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires des points de l'espace des phases, c'est à dire une situation ou un ensemble de situations vers lesquelles évoluent un système, quelles que soient ses conditions initiales.

Le bassin d'attraction d'un attracteur est l'ensemble des points de l'espace des phases qui donnent une trajectoire évoluant vers l'attracteur considéré. Il existe deux types d'attracteurs: les attracteurs réguliers et les attracteurs étranges ou chaotiques.

- **Les Attracteurs réguliers :** Les attracteurs réguliers caractérisent l'évolution de systèmes non chaotiques, et peuvent être de trois sortes :

- **un point fixe :** un point fixe est un point vers lequel un système évolue, comme les états finals d'un caillou en chute, ou l'eau dans un verre.
- **un cycle limite :** un cycle de limite est une orbite périodique du système qui est isolé. Les exemples incluent les oscillations d'une horloge de pendule, et le battement de cœur tout en se reposant.
- **un tore:** Il peut y avoir plus d'une fréquence dans la trajectoire périodique du système par l'état d'un cycle limité. Si deux de ces fréquences forment une fraction irrationnelle, la trajectoire n'est plus clôturée, et le cycle de limite devient un tore limité.

- **Les attracteur étranges :** Le mot "attracteur étrange" a été inventé par **David Ruelle** et **Floris Takens** en 1971. Les attracteurs étranges sont des caractéristiques de l'évolution des systèmes chaotiques ; au bout d'un certain temps, tous les points de l'espace des phases (et appartenant au bassin d'attraction de l'attracteur) donnent des trajectoires qui tendent à former l'attracteur étrange**.** Un attracteur étrange est une surface repliée plusieurs fois sur elle-même. Ainsi, deux points très proches au départ (conditions initiales) peuvent se retrouver à deux extrémités opposées de l'attracteur. Cela traduit le comportement divergent des phénomènes chaotiques.

- **Spectre de puissance :** l'analyse de **Fourier** permet de caractériser les fréquences d'un signal de l'évolution temporelle d'une des variables du système. Celle-ci donnera le spectre de fréquences composant le signal chaotique.
- **Exposants de Lyapunov :** Certains systèmes dynamiques (systèmes qui décrivent dans l'espace un état qui évolue dans le temps) sont très sensibles aux petites variations de leur condition initiale. Ces variations peuvent rapidement prendre d'énormes proportions. Le mathématicien **Alexander Lyapunov** s'est penché sur ce phénomène et a développé une quantité permettant de mesurer la vitesse à laquelle ces petites variations peuvent s'amplifier. sont des coefficients qui permettent de mesurer la sensibilité aux conditions initiales d'une série temporelle.
- **Bifurcation :** La bifurcation est l'étude de la variation des solutions d'un problème non linéaire c'est à dire la variation de la stabilité en fonction des variations des paramètres. C'est donc un changement qualitatif dans le comportement dynamique à la suite d'une petite variation dans les paramètres du système.

### 2.2.3 Synchronisation de chaos [ALS 06] [JMA 09] [BOS 10]

- Le rôle de la synchronisation est d'essayer à estimer certains des états du système dynamique ou parfois des entrées inconnues. À ce jour, différentes formes de synchronisation ont été explorées. Parmi ces formes on trouve les méthodes à synchronisation complète (SC), les méthodes à synchronisation généralisée (SG) et les méthodes à synchronisation de phase (SP).

Dans la synchronisation complète (la synchronisation identique), nous avons une coïncidence complète entre les variables d'états des deux systèmes synchronisés. Les méthodes à synchronisation complète sont typiquement associées avec la synchronisation des systèmes identiques. D'autres exemples de synchronisation complète utilisent un schéma à rétroaction et sont décrits comme étant bidirectionnels, car les deux systèmes sont à la fois source et destination.

Les méthodes à synchronisation généralisée se manifestent par une relation fonctionnelle entre deux systèmes chaotiques couplés. Ces méthodes sont considérées comme une généralisation des méthodes à synchronisation complète pour synchroniser des systèmes chaotiques typiquement différents.

Dans la synchronisation de phase, la phase entre deux oscillateurs chaotiques est verrouillée, ou, plus généralement, une définition particulière adéquate d'une représentation de la phase de deux systèmes chaotiques est verrouillée. Ces méthodes peuvent être utilisées avec des systèmes identiques ou pas.

Dans tous les cas de figure, une attention particulière doit être donnée au choix de couplage. Il est possible de coupler les systèmes chaotiques dans un sens (couplage unidirectionnel) ou dans les deux sens (couplage bidirectionnel).

- Dans le cas d'un couplage unidirectionnel, l'énergie est transférée d'un système à l'autre, à l'aide d'un élément de couplage fonctionnant dans un seul sens.
- Dans le couplage bidirectionnel, l'élément de couplage permet l'échange de l'énergie dans les deux sens.

### 2.2.4 Avantages du chaos [HAM 11]

En première approche, les systèmes chaotiques sont des systèmes dynamiques qui évoluent dans une région bornée, qui possèdent une infinité de trajectoires non périodiques denses. Ils sont très sensibles aux conditions initiales: deux conditions initiales très proches conduisent à deux trajectoires qui s'éloignent rapidement l'une de l'autre. Les propriétés nous permettent théoriquement de générer un nombre infini de signaux chaotiques non corrélés d'un même système en utilisant différentes valeurs initiales. Ceci peut être employé pour générer des séries de nombres pseudo-aléatoires. Cette série est très utile dans certains crypto systèmes traditionnels ou dans le protocole de TCP/IP. Une autre application de cette propriété est de produire des séquences chaotiques pour remplacer les séquences étalées conventionnelles utilisées dans les systèmes de spectre étalé par séquence directe. Ensuite, il est à noter qu'en raison de leur propriété aléatoire, les signaux chaotiques ont des fonctions d'autocorrélation très étroites et des spectres de puissance à large bande proche du bruit blanc. Ainsi, la corrélation croisée de signaux chaotiques a une valeur très petite. Puisque le système chaotique a une trajectoire non périodique et est sensible aux conditions et aux paramètres initiaux, logiquement il peut aussi être employé pour crypter des messages.

Dans les systèmes de transmission conventionnels, des signaux sinusoïdaux sont employés comme signaux porteurs, ce qui offre une efficacité excellente dans une large bande. Cependant, la puissance transmise est concentrée dans une bande étroite, entraînant une densité spectrale de puissance élevée. Les problèmes principaux avec cette caractéristique sont: l'atténuation élevée dans une bande de fréquence étroite ce qui peut mener à la perte de synchronisation, des niveaux élevés d'interférence avec d'autres utilisateurs du réseau, les possibilités élevées d'interception, etc. Au contraire, les signaux chaotiques sont habituellement identifiés comme du bruit et ont des bandes larges, ainsi ils peuvent être utilisés pour étaler l'information originale à bande étroite. Ainsi, en utilisant les signaux chaotiques pour crypter l'information, les signaux résultants sont des signaux de spectre écarté ayant une bande plus grande et des densités spectrales de puissance inférieures à des solutions usuelles.

### 2.2.5 Domaines d'application. [STA 11]

La théorie du chaos s'applique aux systèmes dynamiques. Parmi ces systèmes, on retrouve :

_ Des systèmes dynamiques courants (calcul de trajectoires : d'un élément mobile, d'une planète, etc.).
_ L'évolution des populations.
_ Des automates cellulaires.
_ La météorologie.
_ L'astrophysique.
_ La stabilité du système solaire.
_ La biochimie moléculaire.
_ La cryptographie.

## 2.3 La cryptographie chaotique.

### 2.3.1 Générateur Pseudo-Aléatoire. [STA 11] [AHM 07]

Un générateur pseudo-aléatoire de symboles (GPA) "générateur des séquences chaotiques "est un automate à nombre fini d'états. A partir de la donnée d'un nombre fini de symboles, que l'on appelle graine, il produit une suite potentiellement illimitée des symboles qui a l'apparence d'une suite aléatoire.

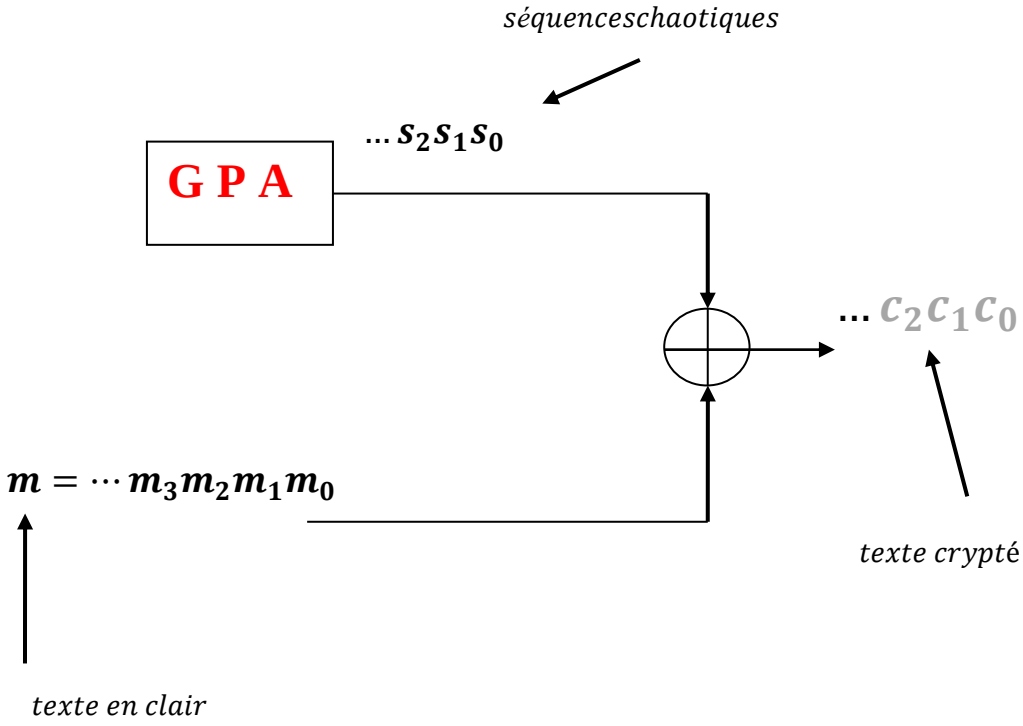



Fig. 2.1 Générateur Pseudo-Aléatoire des séquences chaotiques

### 2.3.2 Principe de cryptage chaotique [JGZ 11] [RBK 07] [LID 05]

La structure du système de cryptage Chaos est le plus étroitement à la séquence de la théorie de la cryptographie traditionnelle. Le chiffrement d'un message par le chaos s'effectue en superposant à l'information initiale un signal chaotique. Nous envoyons par la suite le message noyé dans le chaos à un récepteur qui connaît les caractéristiques du générateur de chaos. Le message est couramment appelé « **texte en clair** », le processus de transformation du message visant à le rendre incompréhensible par l'intrus s'appelle le **chiffrement ou encryption « Séquences chaotiques »**. Le résultat de ce processus de

chiffrement est appelé « **texte chiffré (ou cryptogramme)** ». Le processus de reconstruction du texte en clair à partir du texte chiffré est **le décryptage ou déchiffrement.** La figure ci-dessous montre le principe de cryptage et de décryptage à base des séquences chaotiques.

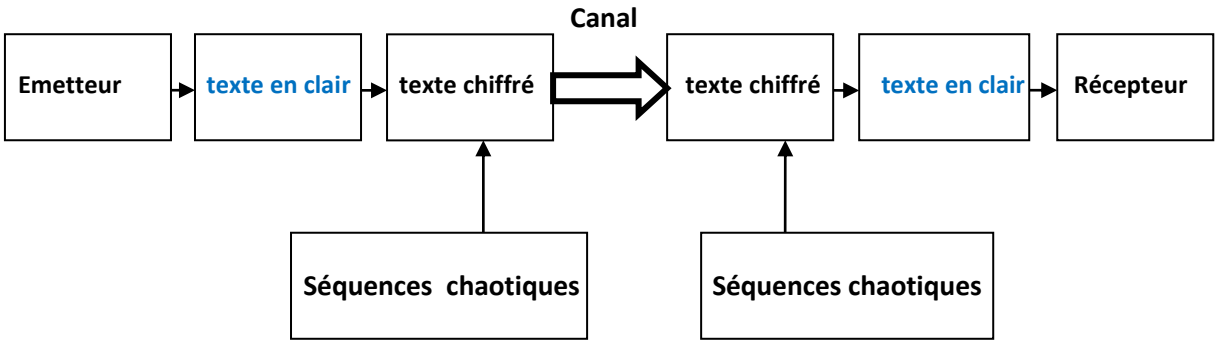



Fig.2.2 Principe de cryptage des séquences chaotiques.

Les caractéristiques de cryptage des séquences chaotiques:

- Avoir une très bonne aléatoire, il est semblable au bruit et il est difficile à déchiffrer.
- Il a grand espace clé; système Chaos de multiples paramètres.
- Pour le système, le chaos est difficile d'être reconstruite, les séquences chaotiques sont également difficiles à reconstituer; Il est donc difficile à déchiffrer.
- Il est commode de produire des séquences chaotiques; Comparé au registre à décalage à rétroaction non linéaire, il a une plus grande flexibilité.

### 2.3.3 Types de la cryptographie chaotique [CAR 11] [CHA 09] [ALS 06] [LAH 07]

En général, les crypto systèmes chaotiques peuvent être divisés en deux types, analogiques et numériques. Les crypto systèmes chaotiques analogiques sont des régimes de communication sécurisés conçus pour les canaux bruyants, basés sur la technique de synchronisation du chaos. Les crypto systèmes chaotiques numériques sont conçus pour les ordinateurs numériques, où une ou plusieurs cartes chaotiques sont mises en œuvre dans la précision de calcul finie pour chiffrer le message en clair de plusieurs manières.

### 2.3.3.1 Chiffrement analogique.

- **Cryptage par addition :**

Cette méthode appelée« masquage chaotique » s'applique aussi bien à des signaux analogiques que numériques. L'émetteur est un système chaotique autonome dont le signal de sortie $y(t)$ est ajouté au signal du message $m(t)$, cette technique consiste à camoufler le signal utile en l'additionnant à un signal chaotique. La somme de deux signaux est transmise au récepteur à travers c'un canal de transmission public. Le récepteur est constitué d'un système chaotique identique à l'émetteur et un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction. L'information est alors récupérée on soustrayant la sortie de récepteur avec celle de l'émetteur. Notons que dans cette méthode, l'attracteur étrange du système chaotique n'est pas modifié par le message. L'inconvénient de cette méthode est qu'afin de garantir la synchronisation, le message doit être inférieur à la sortie de l'émetteur. Or, en présence d'un bruit de canal d'une puissance proche de celle du message, il devient difficile de détecter l'information. De plus, cette méthode reste sensible aux attaques extérieures et l'usage du canal de transmission est inefficace du point de vue de l'énergie transmise par rapport à la qualité d'information fournie. Le schéma représentant cette méthode est donné par la figure suivante.

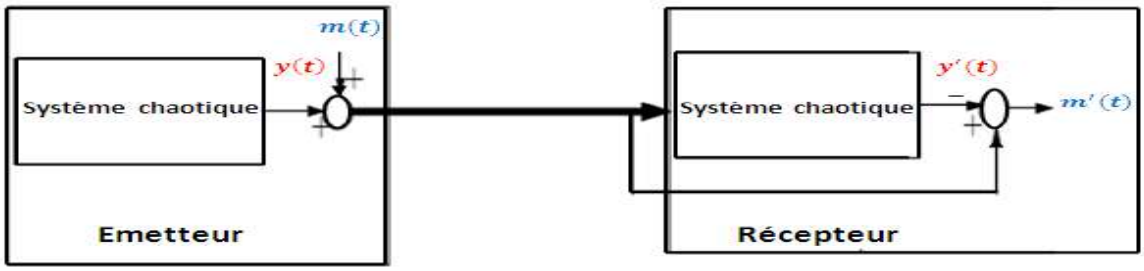



Fig.2.3 Système à masquage aditif

$$m'(t) = y'(t) - y(t) \tag{2.1}$$

Cette méthode présente les avantages et les inconvénients suivants :

Les avantages :

- Conception simple.

-Applicable à tous types de signaux.

Les inconvénients :

-Sécurité faible.

-Forte sensibilité au bruit.

-Energie perdue dans le cryptage.

- **Cryptage par commutation :**

Un autre schéma de transmission chaotique de données est la communication chaotique. Cette méthode est utilisée pour transmettre un message binaire, une opération de commutation est employée selon la valeur du message binaire : Si sa valeur est"0", le système chaotique $f(t)$ est choisi et le signal de sortie est transmis, sinon la sortie du système chaotique$g(t)$ est transmis. Dans ce sens, le message binaire commute l'émetteur entre deux attracteurs étranges correspondants à deux systèmes chaotiques.

Le récepteur est constitué de deux systèmes chaotiques identiques à ceux de l'émetteur. Pour chaque valeur du message, l'un des deux systèmes se synchronise avec l'émetteur et un bloc de comparaison permet de relever la valeur du message notée « $m'(t)$».

Du coté du récepteur, il y a deux systèmes chaotiques $f'(t)$ et $g'(t)$ qui correspondent respectivement à$f(t)$ et $g(t)$. Supposons que le canal est parfait, et que le signal transmis est"0", alors le sous système $f'$se synchronisera avec le système chaotique$f$ , mais le sous système $g'$ ne pourra pas être synchronise. Selon les erreurs de synchronisation de $(f'(t)\ ;f(t))$ et $(g'(t)\ ;f(t))$, le signal peut être récupéré avec succès. Cette méthode est présentée par la figure suivante.

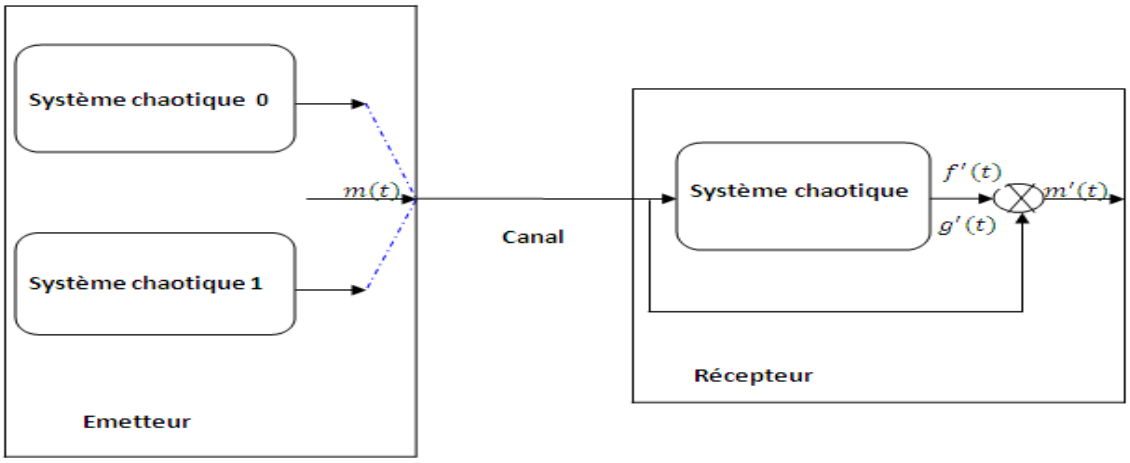



Fig.2.4 Système de cryptage par commutation

Cette méthode présente deux inconvenants :

- La vitesse de transmission est limité par la vitesse d'évolution du système d'un attracteur à un autre.

- Le changement de paramètre est une modification radicale qui entraîne de fortes variations dans les propriétés statistiques de signal. Donc, la sécurité de la communication est fortement comprise.

➢ **Cryptage par modulation**

Cette technique utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique, utilise le message pour modifier directement l'attracteur étrange du système chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la trajectoire de changer continûment d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique "normal". Cependant, la façon d'injecter le message et donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur.

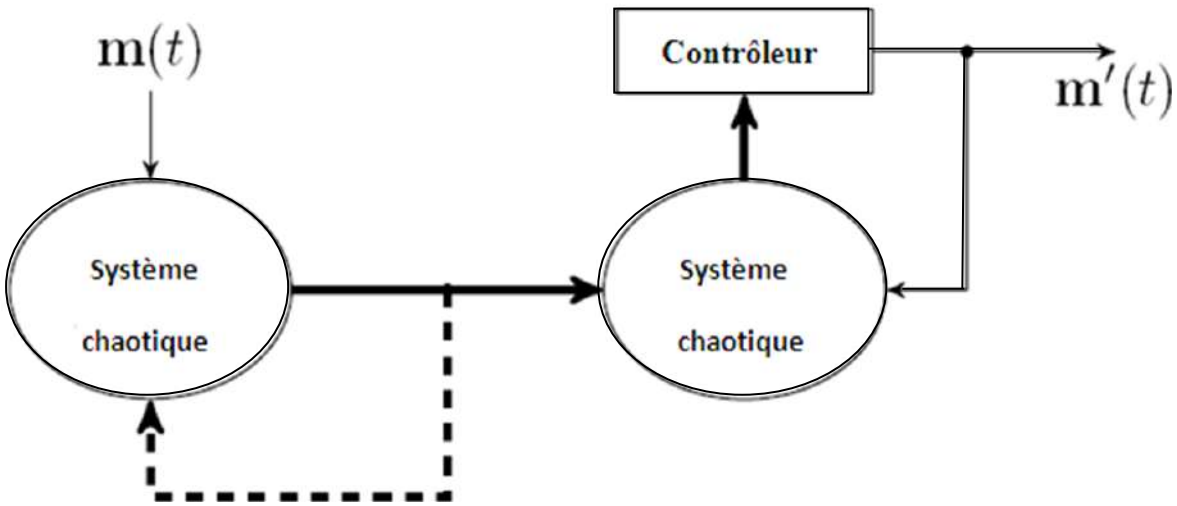



Fig. 2.5 Système de cryptage par modulation

### 2.3.3.2 Chiffrement numérique.

- **Chiffrements par flot**

Les noyaux les plus connus de chiffrements à flots chaotiques sont PRNG-s chaotiques, qui utilisent des flux principaux de masquer les textes en clairs. Deux algorithmes principaux génèrent des nombres pseudo-aléatoires chaotiques sont: (1) extraire des bits binaires provenant des orbites chaotiques, (2) divisant l'intervalle de chaotique en n parties et l'étiquetage de chaque partie en un nombre compris entre 0 ~ n-1, puis générer nombre pseudo-aléatoire par qui font partie de l'orbite chaotique po arrive. PRNG-s ont un défaut fatal qui est quand il est utilisé dans les chiffres numériques chaotiques ne peuvent pas produire un nombre réellement aléatoire, parce que l'ordinateur ne peut pas fournir une précision infinie pour exécuter des orbites chaotiques.

- **Chiffrements par ploc**

T. Habutsu et al, proposé un chiffrement par bloc chaotique en 1991, qui ont utilisé la carte tente d'inclinaison avec des itérations en arrière pour le chiffrement et en avant pour le déchiffrement. De nombreuses modifications ont été proposées pour développer le niveau de sécurité, la plupart de ces méthodes changer la carte chaotique par d'autres ou la carte chaotique de 2-D.

- **Chiffrement à clé publique**

L'idée de cryptographie à clé publique a été introduite par Diffie et Hellman en 1976. Plus tard, Rivest, Shamir et Adlemann, à proposer le bien-connu crypto système RSA. Chiffrement à clé publique appartient à chiffrement asymétrique, il est un type spécial de la cryptographie. Les premiers chiffrements chaotiques à clé publique sont développés dans les années 90. Kocarev et Tesav proposé un algorithme de chiffrement à clé publique basé sur les cartes de Chebyshev en 2003. R Tenny et Al proposé une méthode de chiffrement qui a utilisé la distribution dynamiques non-linéaires pour cryptage par clé publique.

- **Chiffrements basées sur la recherche**

E. Alvarez et al, proposé une approche de cryptage chaotique en 2001. L'approche est basée sur l'itération de la carte chaotique et divise le flux arbitraire long dans un nombre 3-triple transmet alors au récepteur. MS Baptista a proposé un système

de cryptographie en 1998 basé sur la propriété d'Ergodicité des systèmes chaotiques, la visite éventuelle de la trajectoire à toutes les partitions dans l'espace des phases que le nombre d'itérations se développe, et de crypter chaque caractère du message avec le nombre.

### 2.3.4 Application de la cryptographie chaotique [BOS 10]

Ces dernières années, en raison de fréquents débit d'images numériques à travers le monde sur les médias de transmission, il est devenu indispensable pour les protéger des fuites. De nombreuses applications comme les bases de données images militaire, de la vidéoconférence confidentielles, systèmes d'imagerie médicale, la télévision par câble, ligne d'albums photos personnels, etc. exigent des systèmes de sécurité robuste, rapide et fiable pour stocker et transmettre des images numériques. Les exigences à remplir les besoins de sécurité des images numérique sont conduit à la mise au point des bonnes techniques de cryptage. Au cours de la dernière décennie, de nombreux algorithmes de chiffrement ont été proposés dans la littérature fondée sur des principes différents. Parmi eux, « le chaos »des techniques de cryptage basées sur le chaos, afin de fournir une bonne combinaison de vitesse, de haute sécurité, la complexité, les frais généraux raisonnables de calcul et de puissance de calcul, etc.

Les images numériques ont certaines caractéristiques telles que : la redondance des données (Data), une forte corrélation entre les pixels adjacents, sont moins sensibles par rapport aux données de texte soit un tout petit changement dans l'attribut d'un pixel de l'image ne dégrade pas considérablement la qualité de l'image et la capacité de données en vrac, etc. En conséquence, les chiffres traditionnels comme AES, DES, RSA, etc. ne sont pas adaptés pour le cryptage des images en temps réel que ces chiffres nécessitent un temps de calcul et de grande puissance de calcul élevé. Pour le chiffrement des images en temps réel les chiffres préférables sont seulement ceux qui prennent moins de temps et d'en même temps sans compromettre la sécurité. Un schéma de chiffrement qui tourne très lentement, même peut être un degré plus haut de fonctionnalités de sécurité serait de peu d'utilité pratique pour les processus en temps réel.

## 2.4 Récurrences chaotiques [CHA 09] [BOS 10] [AHM 07]

La théorie du chaos a été développée pour une longue période. Un grand nombre de système de chaos avait été mis au point; par exemple, Carte Tente, Carte Tente d'Obliquité et la Carte Logistique, etc. De nombreux chercheurs ont convenu le système chaotique doit avoir la fonction suivante bornée, non linéaire, non-périodique et sensible aux petites perturbations. Le chaos peut surgir simplement en réitérant des fonctions mathématiques. Plusieurs fonctions simples existent dans la littérature.

- **Carte de Hénon (Récurrence de Hénon):**

La récurrence de Hénon [1976], de deux dimensions. Il est l'un des exemples les plus étudiés des systèmes dynamiques qui présentent un comportement chaotique . La carte de Hénon, prend un point ($x_n, y_n$) dans le plan et le fait correspondre à un nouveau point.

$$\begin{cases} x_{n+1} = y_n + 1 - ax_n^2 \\ y_{n+1} = bx_n \end{cases} \quad (2.2)$$

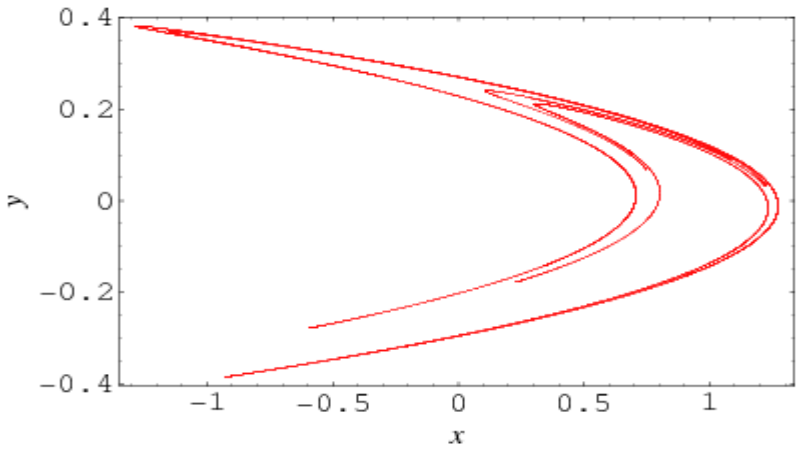



Fig.2.6 Attracteur de Hénon pour a = 1,4 et b = 0,3

- **Carte de Lozi (Récurrence de Lozi):**

Une carte bidimensionnelle similaire à la carte de Hénon mais avec le terme $-ax_n^2$ remplacépar$-a|x_n|$. Elle est donnée par les équations :

$$\begin{cases} x_{n+1} = y_n + 1 - a|x_n| \\ y_{n+1} = bx_n \end{cases} \quad (2.3)$$

L'attracteur étrange illustré ci-dessous résulte de a = 1,4 et b = 0,3

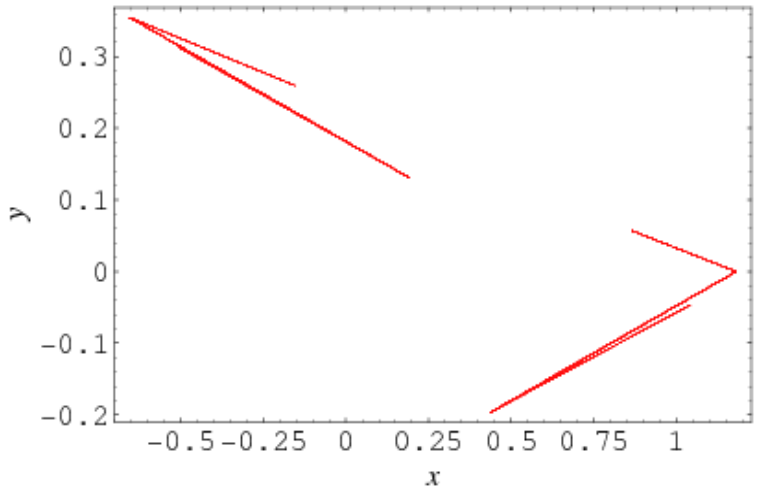



Fig.2.7 récurrence de lozi

- **Carte de Bogdanov (Récurrence de Bogdanov):**

Carte bidimensionnelle qui est conjugué à l' carte de Hénon dans sa limite non dissipative. Elle est donnée par :

$$\begin{cases} x' = x + y' \\ y' = y + \epsilon y + kx(x-1) + \mu xy \end{cases} \quad (2.4)$$

- **Carte Tente :**

Un linéaire par morceaux, à une dimension carte sur l'intervalle [0,1] présentant chaotiques et donnée par.

$$x_{n+1} = \mu(1 - 2|x_n - 0.5|) \quad (2.5)$$

- **carte standard (**carte standard de Chirikov**):**

Catre à deux dimensions définie par :

$$\begin{cases} x_{n+1} = x_x + k \sin y_n \\ y_{n+1} = y_n + x_{n+1} \end{cases} \quad (2.6)$$

$x_x$et$y_n$ sont prise modulo$2\pi$.

- **Cercle Carte :**

La carte est un cercle unidimensionnel qui mappe un cercle sur lui-même.

Définie par :

$$x_{n+1} = x_n + a - \frac{k}{2\pi}\sin(2\pi x_n) \quad (2.7)$$

La carte cercle présente un comportement tout à fait inattendue.

- **Carte logistique :**

Carte unidimensionnelle, elle est un exemple simple de suite dont la récurrence n'est pas linéaire, souvent citée comme exemple de la complexité pouvant surgir de simple relation non linéaire. Cette carte fut popularisée par le biologiste RobertMay en 1976.La carte logistique est l'une des fonctions plus simples chaos utile pour des applications de cryptographie.

Avec l'équation de récurrence :

$$x_{n+1} = bx_n * (1 - x_n) \quad (2.8)$$

La carte logistique calculée en utilisant une procédure graphique connue comme "Orbite des itérations de la fonction $x_{n+1}$ ".

Le diagramme en face montre le comportement chaotique de la carte logistique.

Où $0<b<4$ et $x_n \in [0,1]$.

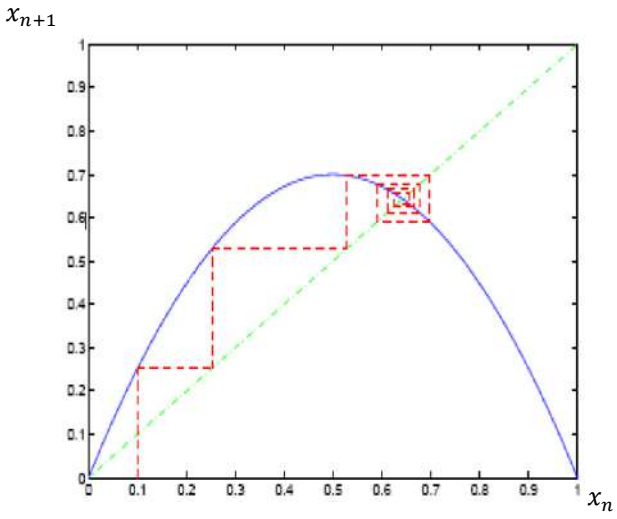



Fig.2.8 comportement chaotique de la carte logistique

Dans la recherche des systèmes chaotique, il souligne que le travail de la carte logistique est à l'état chaotique quand $3.57 \leq b \leq 4$. En d'autres termes, cela signifie que la séquence générée à partir de l'état initial sera non périodique, la dépendance n'est pas convergente et sensible de sa valeur à l'état initial.

- $0 \leq b \leq 1$ : tous les points attirent vers 0.
- $1 \leq b \leq 3$ : tous les points se stabiliseront sur la valeur $\frac{b-1}{b}$ quelle que soit $x_0$.
- $3 < b < 3.57$ :les points oscilleront entre deux valeurs, puis entre quatre puis 8, 16, 32…etc.
- $b = 3.57$ : le chaos s'installe. Aucune oscillation n'est encore visible et de légères variations des conditions initiales conduisent à des résultats radicalement différents.
- $4 \leq b$: la carte quitte l'intervalle [0,1] et diverge presque pour toutes les valeurs initiales.

.

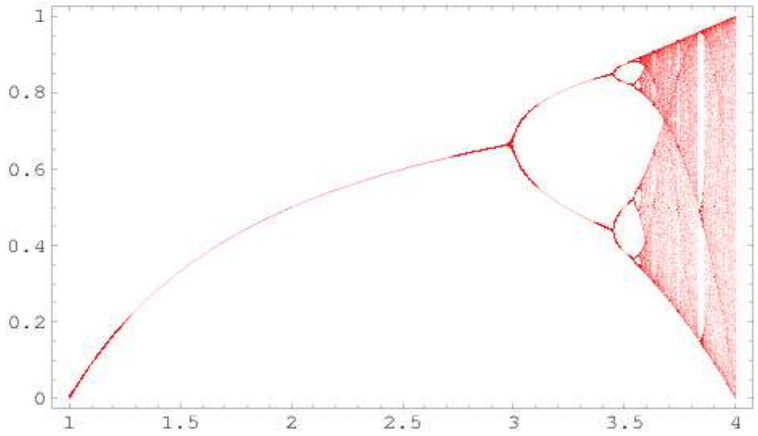



Fig.2.9 Diagramme de bifurcation

La figure ci-dessus représente un diagramme de bifurcation de la carte logistique obtenu en traçant en fonction de $b$ une série de valeurs pour $x_n$ obtenus en commençant avec une valeur aléatoire $x_0$, itérer plusieurs fois.

## 2.5 Conclusion.

La cryptographie basée sur la théorie du chaos est développée rapidement au cours de ces dernières années. Aujourd'hui la plupart des recherches se concentrent sur l'utilisation du chaos dans des crypto systèmes en vue d'apporter une amélioration (temps de chiffrement, sécurité) par rapport aux méthodes standards de la cryptographie (DES, DEA, AES), ceci grâce aux caractéristiques des signaux chaotiques tels que : bonnes propriétés cryptographiques, reproductibilité à l'identique et l'hyper sensibilité aux clef secret.

## 3.1 Introduction

**Les oscillations chaotiques** [BAP 98]

Les oscillations déterministes appelées chaos sont utilisées pour être traitées comme des phénomènes stochastiques et imprévisibles, de nos jours ce comportement stochastique de type chaotique qui présente des oscillations caractérisé par un large spectre de fréquences est utilisé pour masquer des informations, afin de transmettre des messages en toute sécurité.

Une première application se présente pour transmettre des signaux utilisant le chaos qui est proposé par Pecora et Caroll, d'après eux deux circuits chaotiques similaires peuvent avoir leurs trajectoires synchronisés, après que le message à envoyer est masqué dans un des signaux chaotiques, et pendant la transmission ce message est extrait en utilisant un circuit synchronisé, le plus souvent par le récepteur.

Une autre idée pour la transmission d'un message, utilisant le chaos, venu de la réalisation dans laquelle le chaos peut être contrôlé par l'utilisation de petites perturbations, l'émetteur envoie un signal chaotique contrôlé qui encode un message binaire. Le récepteur trouve qu'un 0 ou 1 ''chiffre binaire'' est en cours de transmission , l'émetteur envoie un petit paramètre de perturbation et le récepteur doit l'appliquer sur un système chaotique, afin de cibler la trajectoire dans une certaine région dans l'espace de phase, le message est récupéré en supposant que cette région est associé avec quelques unités d'alphabets, l'émetteur envoie un feed-back de correction d'orbite , le récepteur doit l'appliquer sur la trajectoire du système chaotique pour que cette trajectoire atteint un certain e-voisinage d'un point dans un intervalle de temps préétablie

L'information est récupérée donc par le récepteur en supposant que certaine unité de l'alphabet est associée à la fois à l'heure d'arrivée et le voisinage de $\varepsilon$ atteint.

## 3.2 Explication de la méthode [YEA 10] [BAP 98]

Dans cette méthode, le message à transmettre est un texte composé de certains alphabets, ainsi que des portions ($\varepsilon$-intervalles) de l'attracteur avec des unités de l'alphabet sont associées. Toutefois, le message chiffré à transmettre, le texte chiffré, est obtenu à partir d'un texte, texte en claire, mais pas avec l'utilisation des systèmes chaotiques synchrones

ni de contrôle des techniques ciblées, mais plutôt en tirant parti d'une propriété typique d'un système chaotique : l'ergodicité.

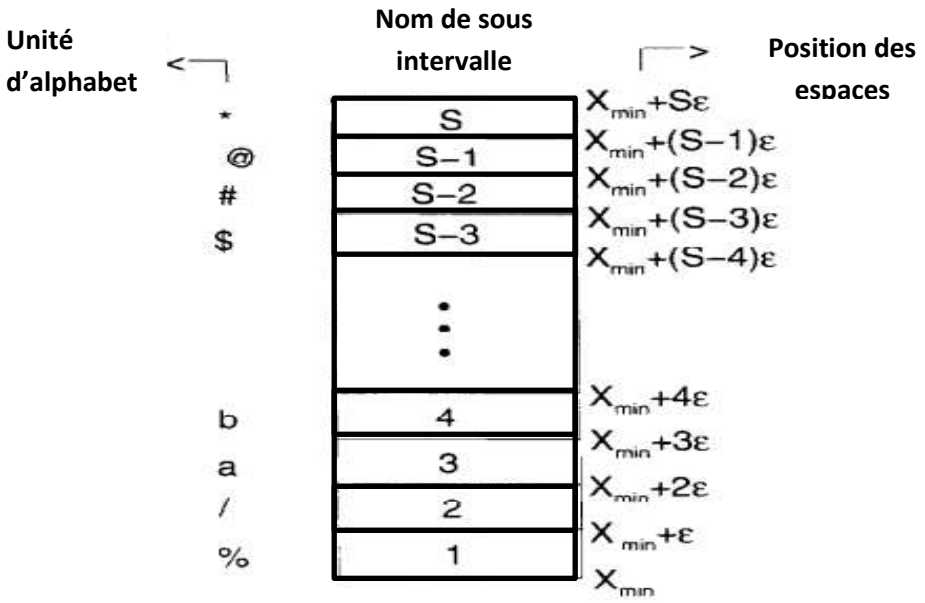



Fig 3.1 représentation schématique explique comment un attracteur est dévisé comme sous intervalles. Chacun de taille $\varepsilon = (X_{max} - X_{min})/S$.

En utilisant la carte logistique simple à une dimension

$$X_{n+1} = b.X_n(1 - X_n) \tag{3.1}$$

Quand $X_n \in [0, 1]$, pour un paramètre de contrôle $b$ réglé afin de donner à l'équation (3.1) un comportement chaotique, nous pouvons crypter rapidement et de façon secrète des informations pour des futurs transmissions. Supposons que le cryptage de certains caractères est le nombre des itérations de l'équation précédente pour rendre son trajectoire, en démarrant d'une condition initiale $X_0$, atteindre l'intervalle $\varepsilon$ associé avec ce caractère.

Dans la figure 3.1, une représentation schématique de la méthode de l'association des S-unités d'alphabets avec les S-intervalles est montrée. Chaque intervalle ou site est une gamme de $[X_{min} + (S - 1).\varepsilon, X_{min} + S.\varepsilon]$, où dans ce cas $S = 256, \varepsilon = [X_{max} - X_{min}]/S$, $et$ $[X_{max} - X_{min}]$ est une partie de l'attracteur. Le nombre des itérations (le texte chiffré) est utilisé avec les clefs secrètes: les S associations entre les S $\varepsilon$-intervalles et les S-unités de certains caractères, la première condition initiale $X_0$, et le

paramètre de contrôle $b$ (dans ce cas S+2 clefs secrètes sont utilisés), permettant au récepteur de décrypter le texte chiffré (récupérer les caractères originaux) par itération de l'équation (3.1) autant de fois indiqué par le texte chiffré. La position du point final, par rapport à S intervalles de $\varepsilon$ indique le caractère original au récepteur. Dans le paragraphe précèdent, nous nous sommes référés a $X_0$ comme condition initiale, parce que chaque fois que nous cryptons un texte en claire (par exemple le mot ''hi'' est un texte claire en 2 unités), une nouvelle condition initiale est considérée, si C1 est le texte chiffré de la première unité de texte en claire, pour crypter la deuxième unité dans ce texte, en utilisant comme condition initiale :

$$X_0' = F^{c_1}(X_0) \tag{3.2}$$

Où $F^{c1}$ est l'itération $N^0$ $C_1$ de l'équation (3.1).

Si C2 est le texte chiffré de la $2^{ème}$ unité dans le texte à chiffrer, la condition initiale pour crypter une troisième unité est :

$$X_0'' = F^{c_2}(X'_0) \tag{3.3}$$

Cette règle est donc carrément appliquée pour le reste des caractères d'un texte en claire. La condition initiale est commutée pour permettre aux différentes unités de texte en claire d'avoir la même unité du texte chiffré. Grace à cette astuce cette méthode de cryptographie n'est pas de la classe des transformations 'un par un', qui est très fréquente dans la méthode cryptographique habituelle.

Notons que $X_0''$ peut être obtenu par :

$$F^{C_1+C_2}(X_0) \tag{3.4}$$

Cependant nous préférons de ne pas utiliser cette dernière notation, parce que nous voulons souligner que, indépendamment de la condition initiale, l'unité de texte chiffrée $C_n$ est un nombre que ne peut pas dépasser 65532, d'ailleurs de cette condition, les unités de texte chiffré dépendent aussi des deux paramètres, un temps de transit $N_0$ et un coefficient ŋ qu'on va le définir dans le prochain paragraphe.

Concernant la taille de la trajectoire utilisée dans ce travail, certains points concernant l'ergodicité doivent être revus.

A cause de l'ergodicité, un nombre infinie de trajectoires à partir de n'importe quel $X_0$, avec des tailles différentes atteignent le même intervalle $\varepsilon$. En conséquence, une seule unité dans un texte en claire peut être cryptée avec un nombre infini de trajectoires. Cependant, ce n'est pas pratique de travailler avec un grand nombre de possibilités et ce n'est pas nécessaire.

La raison pour laquelle nous pouvons considérer une taille minimum de trajectoires, dont la taille représente une unité de texte en claire crypté, repose sur l'existence d'une densité naturelle invariant pour des attracteurs chaotiques. Cette densité invariante est la distribution de l'espace des trajectoires de taille infinie. En plus, à cause de l'ergodicité, presque toutes les conditions initiales, quand ils sont réitérées, génèrent un attracteur avec la même densité invariante naturelle.

Comme les systèmes chaotiques sont ergodiques, presque n'importe quelle condition initiale, lorsque elle est réitérée par un tel système, atteindra n'importe quel intervalle $\varepsilon$ plusieurs fois, à condition que cet intervalle appartient à l'attracteur. Concernant la fréquence, chaque partie de l'attracteur est visitée dépendamment de cette densité.

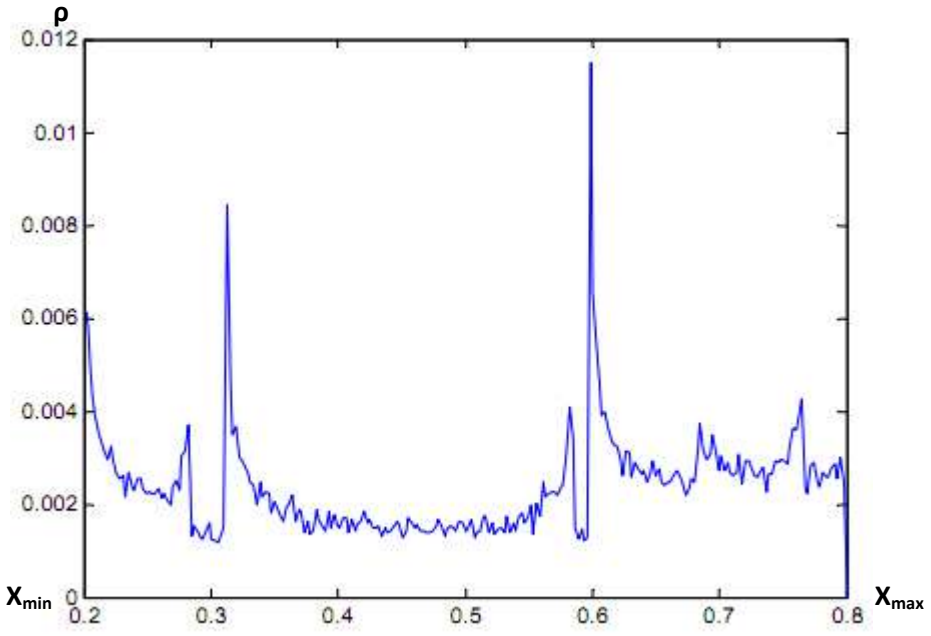



Fig.3.2 Densité invariante naturelle de l'équation (3.1) dans l'intervalle [0.2, 0.8], obtenue à partir d'une trajectoire de taille N=65536. Le paramètre de contrôle b=3.78, et la condition initiale $X_0$=0.43203152000000

Pour calculer la densité naturelle invariante, mais pas par une méthode analytique, il faut tenir compte qu'une trajectoire de taille N-itération, démarre à partir d'un certains $X_0$, et

pour vérifier sa distribution dans de nombreux intervalles $\varepsilon$ on devise l'attracteur. Des trajectoires qui ne dépassent pas une taille de 65532 itérations ont été choisis, de telle sorte qu'un nombre $C_{n,}$ qui est une unité d'un texte chiffrée est calculé rapidement et envoyé au récepteur en utilisant une transmission d'un nombre entier d'un seul octet. La densité invariante naturelle de l'équation (3.1) pour b=3.78, est obtenue pour une trajectoire des composantes $X_n = X_0, X_1, \ldots, X_N$ pour N=65536 , montrée dans l'intervalle $[X_{\min} - X_{\max}] \rightarrow [0.2 , 0.8]$ divisé par les 256 sites qu'on peut les voir dans la figure 3.2 , ainsi dans cette figure la largeur de l'intervalle $\varepsilon$ , $\varepsilon$ = 0.002343750, désigné par deux lignes parallèles, et il a un minimum de distribution de densité sur l'attracteur , ρ= 0,0011 , ça signifie que pour le trajectoire considéré 76 point ce situe dans cet intervalle , en outre par le fait que différentes conditions initiales conduisent à la même densité invariante , des trajectoires de tailles 65536 itérations à partir de n'importe quelle condition initiale (à l'intérieur de l'attracteur) vont vers une intervalle $\varepsilon$ au moins 76 fois approximativement , si b=3.78 .

Même si la clef b est différente, ça entraînerait une distribution de densité naturelle différente, on peut la trouver dans le cas d'un régime chaotique, un grand nombre d'intervalles $\varepsilon$ , avec une densité non nulle pour une trajectoire de taille 65532 itérations, en générale, pour tous les systèmes chaotiques, un seul $\varepsilon$ -intervalle est trouvé avec une densité non nulle si

$$\varepsilon = \alpha N^{-1/D_0} \qquad (3.5)$$

Où $\alpha$ dépend de système dynamique.

On va limiter la trajectoire pour obtenir une taille moins de 65532 itérations, mais aussi en ne considérant pas la première itération (le temps de transit $N_0$). Ces trajectoires (à partir de $X_0$) qui vont vers l'intervalle indiqué dans la figure 2 ont des tailles différentes. Supposons que cette intervalle est celui associé à la lettre ''a'', par définition on va représenter la taille de ces trajectoires par $n_i^a$ (i=1, 2,3,……) avec $n^a_{i+1} > n_i^a$ et $n_1^a > N_0$, avec $N_0$ est le temps de transit choisis pour être $N_0$=250 et $n_i^a$ sont les caractères qui sont éventuellement chiffrés (obtenues à partir de certain $X_0$) du caractère ''a'' que l'on peut envoyer au récepteur.

Après le temps transitoire, nous ne pouvons pas avoir une trajectoire qui rend tout intervalle $\varepsilon$ d'au moins 76 fois, pour b=3.78. Toutefois, quand $N_0$ est très faible , notre choix est encore grand, la raison de ce temps de transit est parce que si quelqu'un sait toute

les clefs S, correspondants à des S associations entre les S-unités de certains alphabets et les S intervalles $\varepsilon$ , mais il n'a pas une connaissance complète soit de la première condition initiale $X_0$ ou b , (la connaissance complète signifie que nous supposons que l'on sait ces clefs avec la précision numérique utilisée est de 16 chiffres de précision) il n'est pas capable de casser notre méthode de cryptographie, dès que l'équation (3.1) appliquée utilisant des clefs qui ont une valeur de $10^{-6}$, qui est très différente des vrais valeurs de (b et $X_0$) conduit à des trajectoires différents au bout de 256 itérations en raison de la sensibilité des systèmes qui ont des conditions chaotiques, cela nécessite une certitude de 16 chiffres, dans les deux clefs b et $X_0$ et nécessite aussi une méthode d'essai d'erreur pour essayer de casser notre méthode de cryptographie, (si ceux-ci sont les seules clefs inconnues ) dans un grand nombre de $10^{16}*10^{16}$ tentatives .

Jusqu'à ici, on a limité l'unité de texte chiffré $C_n$, pour qu'il sera supérieur de $N_0$ et inférieur à 65532, mais nous avons de nombreuses options de $C_n$ (plusieurs de ces options, dépendent de la densité de distribution), parmi ceux-ci, l'émetteur va choisir une pour la transmettre au récepteur, la méthode que l'metteur choisit pour envoyer $C_n$ dépends de coefficients ŋ , un nombre que connait seulement l'émetteur. Si ŋ=0, le message à envoyer. $C_n$ est le nombre $n_1$, le nombre minimal d'itérations nécessaire pour faire une trajectoire (en partant d'un certain $X_0$ et accéder au site associé au caractère), à condition que $n_1 > N_0$. Si ŋ≠0, ( pour n'importe quelle nombre $n_1 > N_0$), le trajectoire se tombe sur le site que l'on désire, l'émetteur obtient un nombre k à partir du générateur aléatoire (une distribution normale dans l'intervalle [0,1]), et il teste si K> ŋ ou non. Si oui, $n_i$ est considéré comme le nombre d'itérations nécessaire pour atteindre la trajectoire de ce site, autrement, l'émetteur maintient l'itération de l'équation (3.1) jusqu'à ce que cette dernière condition est satisfaite.

Nous allons maintenant crypter un message en utilisant dans l'équation (3.1) une clef b=3.8, en va diviser l'intervalle (limité par $[X_{\min} = 0.2, X_{\max} = 0.8])$ $en\ S = 256$ sous intervalles, pour $\varepsilon$ =0.00234375. L'association entre les sous intervalles et le code ASCII des alphabets, qui est produit par l'utilisation de fonction de MATLAB 'caractére'-0, dont le code ASCII de la lettre 'a' est 97.

Pour b=3.8 en va vérifier que les trajectoires de taille = 65532 itérations, vont vers l'un des 256 sous intervalles au moins 60 fois et il n'y a aucun sous intervalle qui a une densité nulle.

Le temps de transit qui est égale à 250 itérations est également adapté pour b=3.8. En effet, la largeur b est le minimum que peut être $N_0$ pour que l'équation (3.1) soit chaotique. Dans la première application de la méthode, le coefficient ŋ=0, et $N_0$=250 sont à considérer. Supposons que le message qu'on va crypter est le mot 'hi', la première condition initiale est $X_0$=0.23232300000000, et la clef b=3.8, la lettre 'h' est associé au site (sous intervalle) numéro 104 qui représente l'intervalle [0.44140625000000, 0.44375000000000] et la lettre 'i' est associé au site (sous intervalle) numéro 105 qui représente l'intervalle [0.44375000000000, 0.44609375000000].
Pour chiffrer le mot 'hi', un seul texte chiffré ($C_1$ $C_2$) est possible qui est égale à 1713 364 la première unité de texte chiffré est 1713 est obtenue par l'itérations de l'équation (3.1) jusqu'à atteindre le sous intervalle numéro 104 , à condition que le nombre d'itérations $n_1^h > N_0$, et pour obtenir la deuxième unité de texte chiffré, on va remettre la condition initiale à $X_0' = X_{1713}$ , et on va itérer l'équation (3.1) jusqu'à où sa trajectoire atteint le sous intervalle numéro 105 à condition que le nombre minimum d'itérations $n^i_1 > N_0$.

Ces numéros sont envoyés vers le récepteur qui peut récupérer le message crypté en vérifiant que le nombre d'itérations de l'équation (3.1) est égale 1713, avec $X_0$=0.23232300000000, le point obtenu est égale à $X_{1713}$=0.44160905447136, qui a une location dans le sous intervalle 104, qui représente la lettre 'h'. Le récepteur va remettre sa condition initiale à $X_0'$=0.44160905447136 et il va itérer cette nouvelle condition initiale 364 fois pour qu'on obtient $X_{364}$=0.44486572362642 qui est dans l'intervalle 105, lié avec la lettre 'i'.
Nous voyons clairement que le prochain bloc de texte chiffré dépend de l'unité actuelle de texte chiffré et cette dernière dépend de l'unité précédente, comme les systèmes chaotiques dépendent des conditions initiales. Cette dépendance peut être comprise quand on réinitialise la condition initiale, comme dans l'exemple précèdent $X_0' = X_{1713}$. Nous voyons que les itérations dans l'équation (3.1), utilisant la nouvelle condition initiale, le point $X_{364}$ atteint le sous intervalle numéro 105. Toutefois, pour toute condition initiale légèrement différente, on ne peut pas garantir qu'après 364 itérations la trajectoire va vers le sous intervalle numéro 105. Une conséquence de cette situation est que la distribution de fréquences des unités d'un texte chiffré ne dépend que du système chaotique utilisé pour crypter le texte en clair, et non pas de type de la langue du texte en clair.

Pour ŋ=0, un chiffrement de plus du mot 'hi', sans changement des clefs b et $X_0$ donne toujours le même cryptage. Ce chiffrement est un des chiffrements qui arrivent en

introduisant le coefficient ŋ. D'autre part , si nous supposons que ŋ=0.7, sans changer les clefs b et la condition initiale $X_0$, le texte chiffré du mot 'hi' peut être soit 2471 1352 ou 6581 15763, En fait, ce simple mot à deux lettres pourrait être chiffré à au moins 602 façons (méthodes), sans changement de l'une des clefs.

Si nous envisageons de changer la première condition initiale à chaque fois que nous transmettons ces mêmes deux lettres du mot, par exemple en faisant $X_0$=X', donc les nombres des textes chiffrés peuvent dépasser $10^{16}*60^2$. Un autre avantage de coefficient ŋ est la propriété de l'aplatissement de la distribution de fréquence d'un long texte chiffré (ou plusieurs textes chiffrés concaténer). Cet effet d'aplatissement est très important, puisque la distribution d'un générique chiffré créé en utilisant cette méthode ne dépends pas de type de lange (anglais, français, Germanie,……) ou des textes crées aléatoirement, ni sur la condition initiale, et ne dépends pas de la clef secrète b. Ainsi, afin de ne pas laisser toute oreille indiscrète savoir une valeur approximative de b en faisant une analyse de la distribution de fréquences, nous devons travailler avec le coefficient ŋ. Pour montrer l'efficacité de coefficient ŋ, la méthode de cryptographie (en utilisant b=3.8, et $X_0$=0.65476546500000) est appliquée sur un texte en anglais composé de 28000 caractères, après la création de texte chiffré, pour ŋ=0, et $N_0$=250, l'analyse de sa distribution en fréquence est montrée dans la figure 3.3

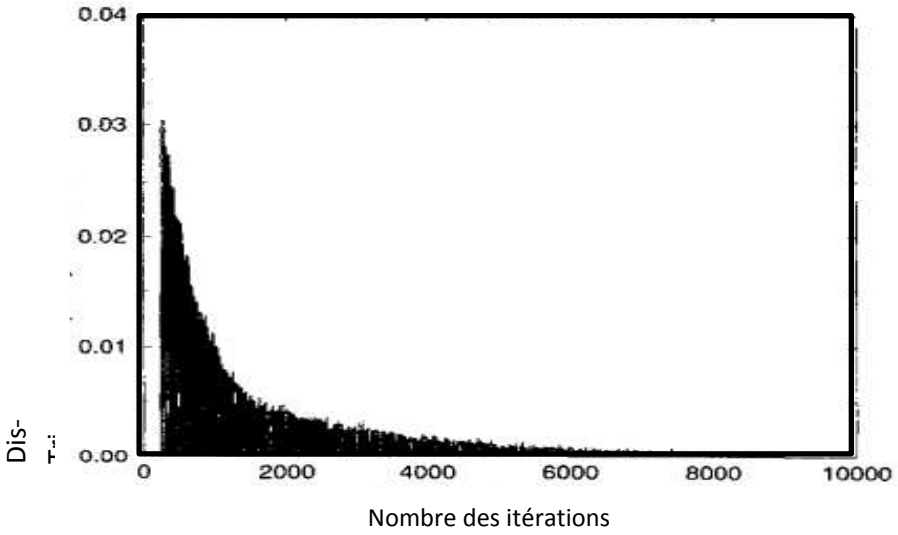



Fig.3.3 Distribution de fréquences d'un texte chiffré obtenu en utilisant une méthode de cryptographie avec (b=3.8, et la première condition initiale X0=0.65476546500000) dans un texte en anglais de 28000 lettres, les barres noires correspondent à un coefficient ŋ=0, et les barres gris pour ŋ=0.7

Pour les barres sombres noires, nous voyons qu'il y a un comportement de décroissance de type exponentielle et cette forme a une pente qui est en fonction de la clef b. Quand nous réappliquons la méthode sur le même texte, en utilisant ŋ=0.7, nous voyons que la distribution de fréquences, indiquée par les barres grises, a été aplatie.

En fait, le plus grand ŋ donne l'aplatissement de la distribution de fréquence du texte chiffré. Cependant, la plus grande valeur de ŋ donne le plus grand nombre d'itérations nécessaires pour diriger la trajectoire vers le site désiré. Nous ne voulons pas dépasser ce nombre 65532. Pour atteindre cette exigence, des coefficients ŋ<0.99 ont été choisis.

On montre que l'unité de texte chiffré est transmise au récepteur en utilisant uniquement une transmission d'un octet entier, qui est un avantage de la méthode par rapport aux méthodes précédentes qui utilisaient le chaos pour transmettre des informations. Un autre élément favorable de travailler avec des nombres entiers, c'est que sa transmission est le bruit robuste, et nous n'envoyons pas aussi du message avec le signal chaotique, ce qui permettrait à un espion de reconstruire la dynamique du système qui génère le signal chaotique et ainsi identifier le message. Les systèmes haute-dimensionnelles dont la dynamique de reconstruction pourrait être difficile, ne sont plus nécessaires. Ainsi, la simple équation d'une seule dimension peut être utilisée pour la cryptographie.

Une amélioration de la sécurité, souvent utilisée dans la cryptographie serre de faire une commutation périodique des clefs. Chaque fois qu'un changement des clefs doit être fait, aucun calcul difficile est requis pour un cryptage rapide, mais seulement une vérification d'un sous intervalle s'il a une densité non nulle pour les trajectoires de taille de 65532 itérations.

Dans les autres méthodes, tous les calculs de ciblage doivent être effectués à nouveau avant de commencer l'envoi des messages. D'autre part, au lieu de changer les clefs, nous pouvons modifier le coefficient ŋ. Un travail effectué par l'émetteur seulement. Cette méthode est basée sur des expériences numériques, ainsi elle pourrait être dépendante de la machine. Toutefois, pour rejeter cet inconvénient. Par exemple le point $X_n$=0.3682129812675678, avant ses itérations aurait sa valeur coupée à la précision de quatorzième chiffres, $X_n$ = 0.36821298I2675600. La méthode en utilisant ce seuil a été appliqué avec succès étant considéré que le récepteur dispose d'une machine différente de celle de l'émetteur.

Si un autre alphabet plus complexe est nécessaire, soit dans les 65523-unités alphabétiques, toujours en considérons qu'un octet de sous intervalle associés égale à 256, chaque unité de texte en clair (dans ces 65523 unités d'alphabets) pourrait être associé à deux des 256 sites, puisque tout entier représenté par deux octets qui sont inférieur ou égal à 65523 peuvent être devisée par deux nombres entiers chacun des deux a un octet.

## 3.3 Organigramme de la méthode de Baptista

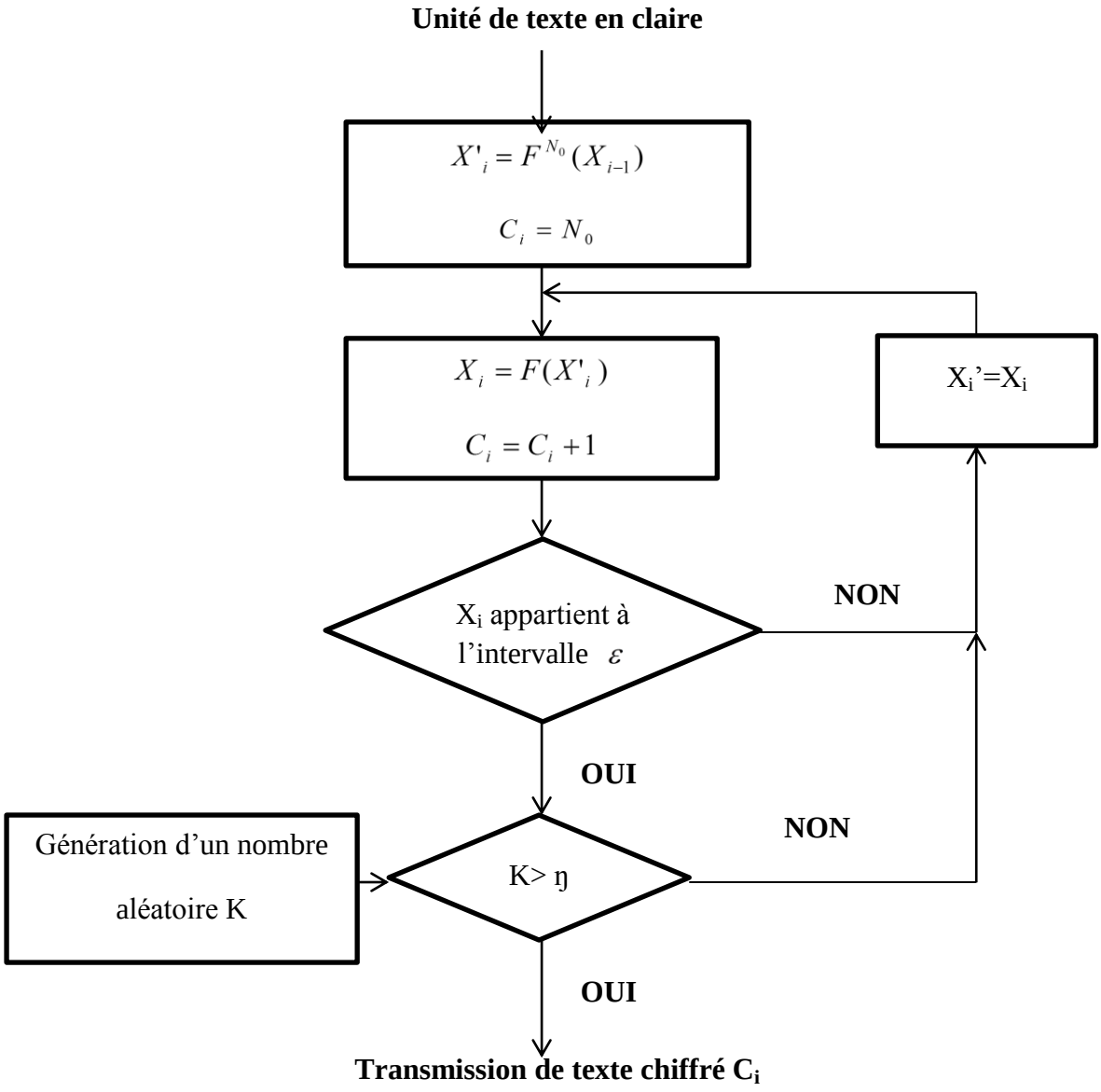



Fig.3.4 Organigramme de la méthode de Baptista

## 3.4 Application de la méthode sous 'MATLAB'

### 3.4.1 Interface du programme de cryptage et du décryptage d'un texte

#### a. Cryptage

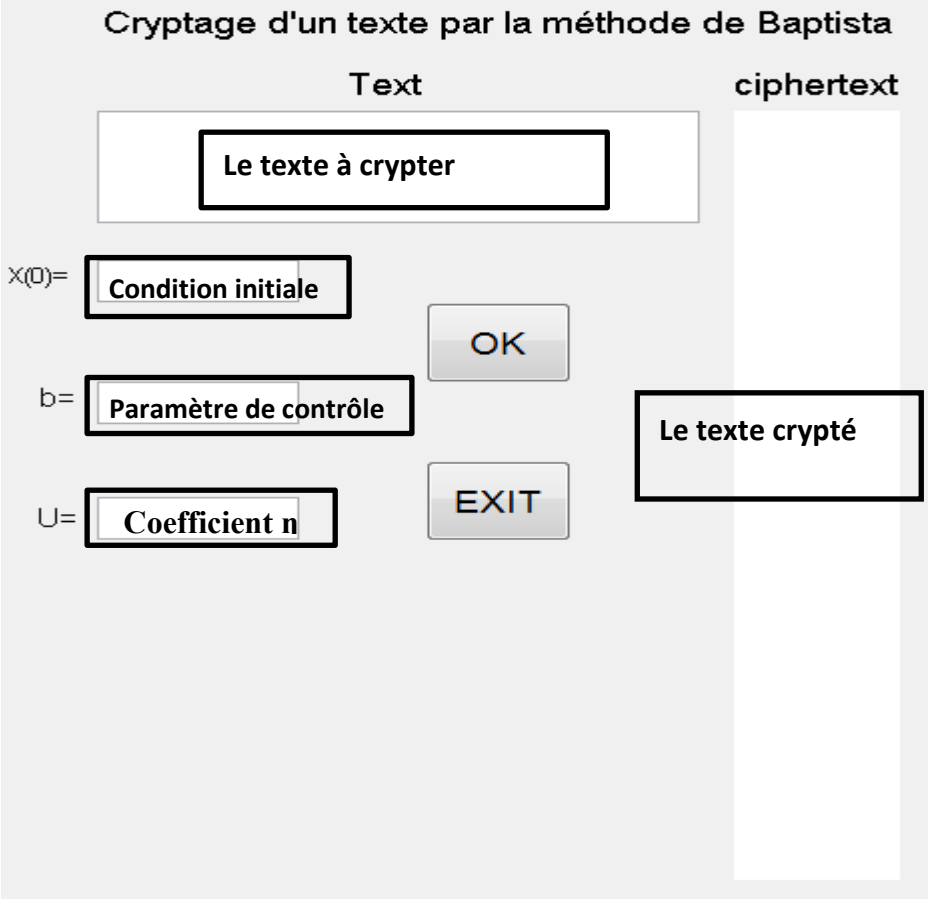



Fig. 3.5 Interface du programme de cryptage du texte

Ce programme est un programme de cryptage d'un texte. Comme il est mentionné dans le schéma ci-dessus, nous écrivons le texte à crypter dans la zone (text) et on donne la condition initiale avec la valeur de coefficient ŋ et la clef b. Le programme va calculer le texte crypté et donnera le résultat dans la zone (ciphertext).

**b. Décryptage**




Fig. 3.6 Interface du programme de décryptage d'un texte

Comme il est mentionné dans la figure (3.6) on donne la valeur de texte chiffré (ciphertext) au programme avec la valeur de la condition initiale $X_0$ et la clef b utilisés dans le cryptage , le programme décryptera ce texte crypté pour avoir comme résultat le texte en claire (originale), ce dernier sera affiché dans la zone (text).

### 3.4.2 Cryptage et décryptage d'un texte pour différentes valeurs de ŋ

On va exécuter le programme de cryptage et du décryptage du texte avec différentes valeurs de ŋ et nous allons analyser les résultats qui sont mentionnés dans les figures ci-dessous avec les paramètres de cryptages suivants :

- La première condition initiale $X_0$=0.2323.

- Le paramètre de contrôle b=3.8.

a. ŋ =0

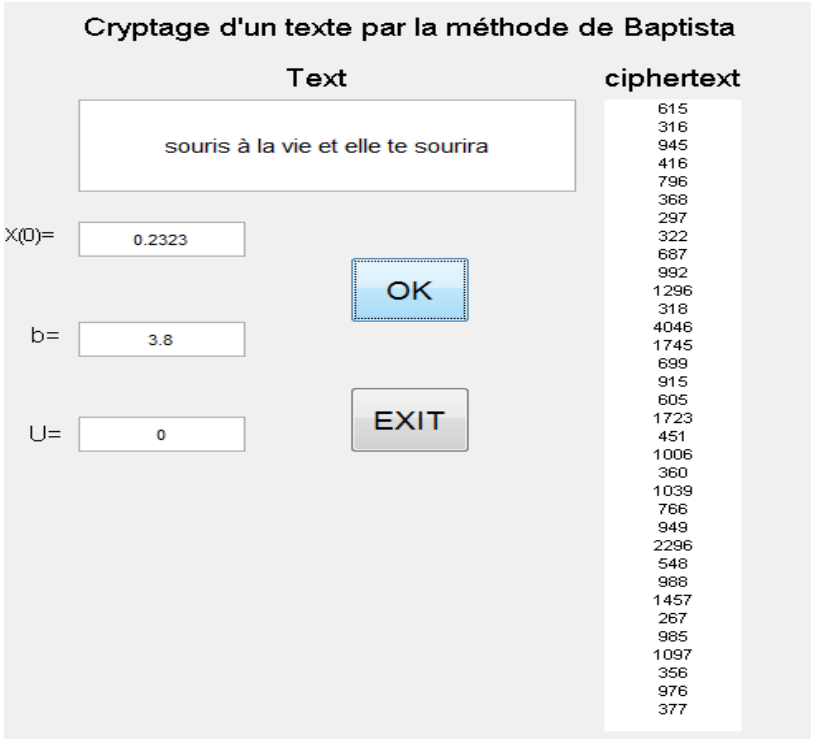



Fig. 3.7 Cryptage de la phrase ‘’souris à la vie et elle te sourira’’, ŋ =0

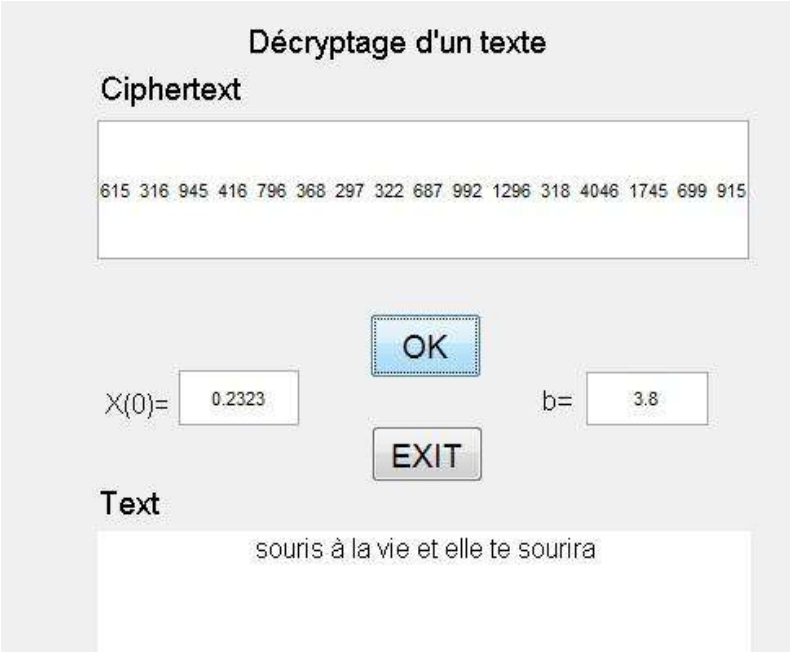



Fig. 3.8 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, ŋ =0

b. ŋ =0.2

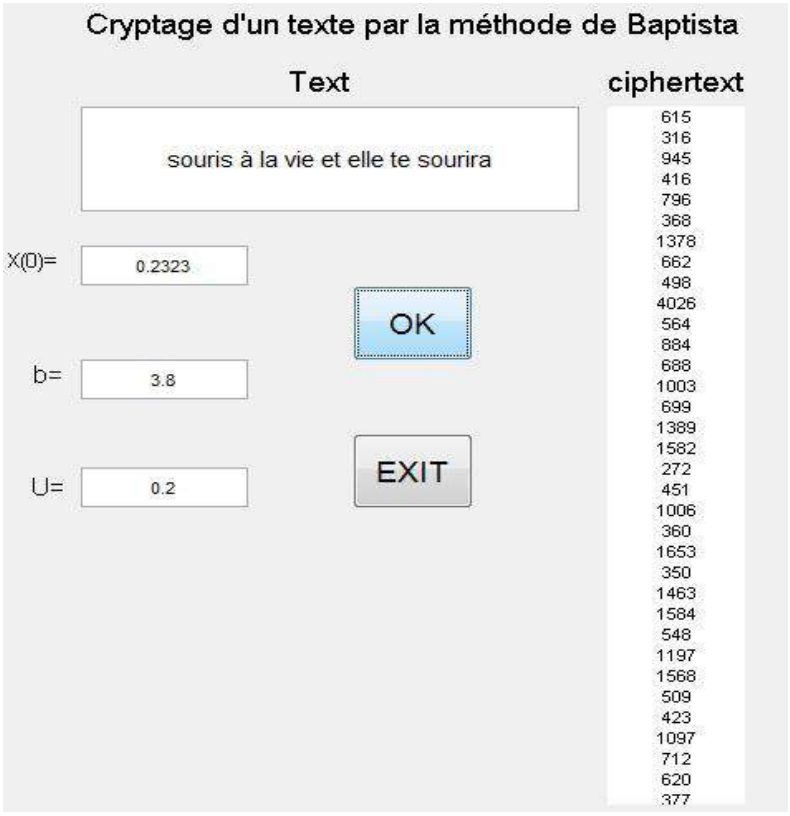



Fig. 3.9 Cryptage de la phrase ‘’souris à la vie et elle te sourira’’, ŋ =0.2




Fig. 3.10 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, ŋ =0.2

c. ŋ =0.6

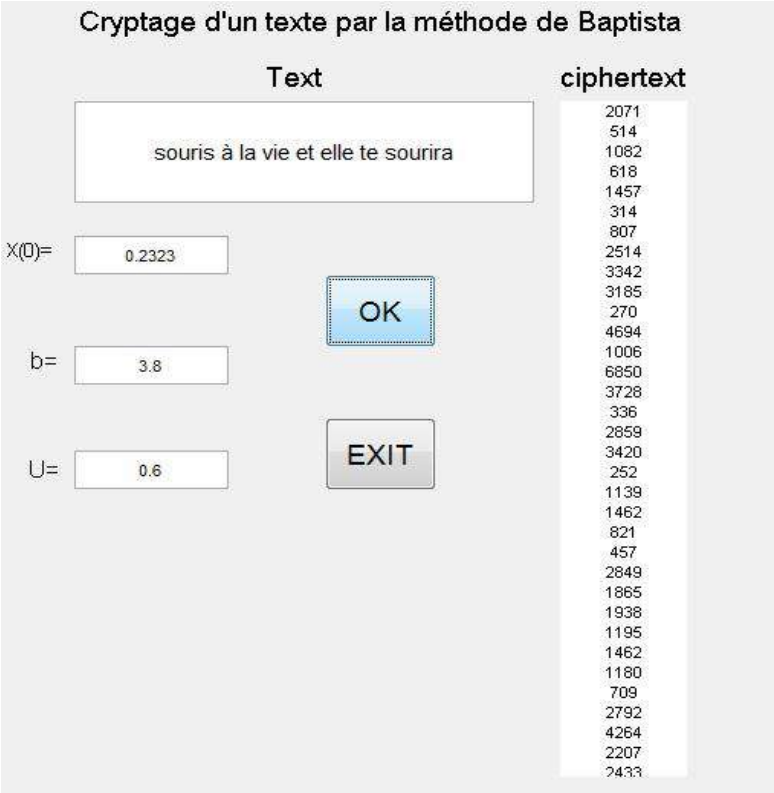



Fig. 3.11 **C**ryptage de la phrase ‘’souris à la vie et elle te sourira’’, ŋ =0.6




Fig. 3.12 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, ŋ =0.6

d. ŋ =0.95




Fig.3.13 Cryptage de la phrase ‘’souris à la vie et elle te sourira’’, ŋ =0.95

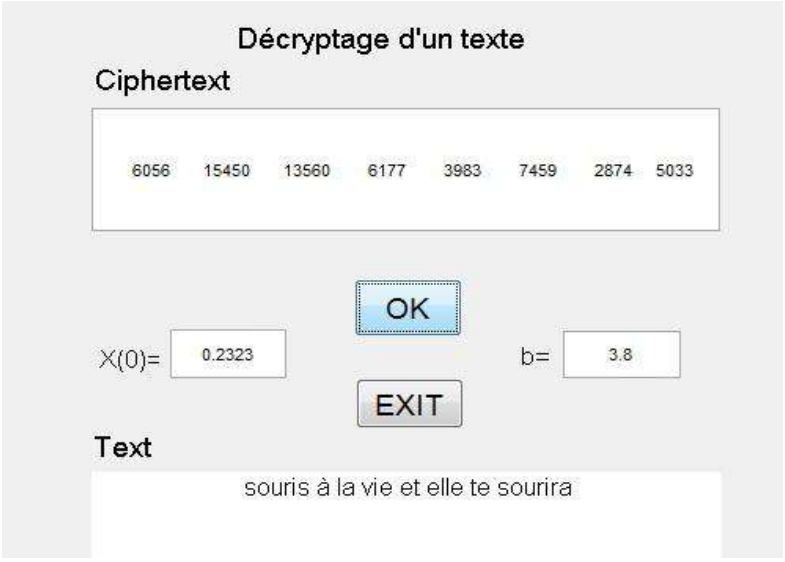



Fig.3.14 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, ŋ =0.95

D’après les résultats d’exécution nous remarquons que pour différents exécutions du programme de cryptage du texte avec les mêmes paramètres ($X_0$, b) et pour ŋ=0 on trouve le même résultat toujours, puisque la variable aléatoire k qui est compris entre [0,1] est toujours supérieur à la valeur de ŋ donc le plus petit nombre d’itérations nécessaire pour que la trajectoire atteint l’intervalle $\varepsilon$ voulue est la valeur du texte chiffré , et pour un

coefficient ŋ >0 nous remarquons que nous avons des valeurs de textes chiffrés qui sont changés avec le changement du coefficient ŋ , puisque chaque fois qu'on augmente la valeur de coefficient ŋ nous obtenons une diminution de probabilité pour que la variable aléatoire K est supérieur à ŋ et l'équation de la carte logistique atteigne l'intervalle $\varepsilon$ voulue en même temps, c'est pour ça que nous avons trouvé toujours des valeur de texte chiffré qui augmente avec l'augmentation du coefficient ŋ.

### 3.4.3 Cryptage et décryptage d'un texte pour différentes valeurs de la clef b

a. b=3.8

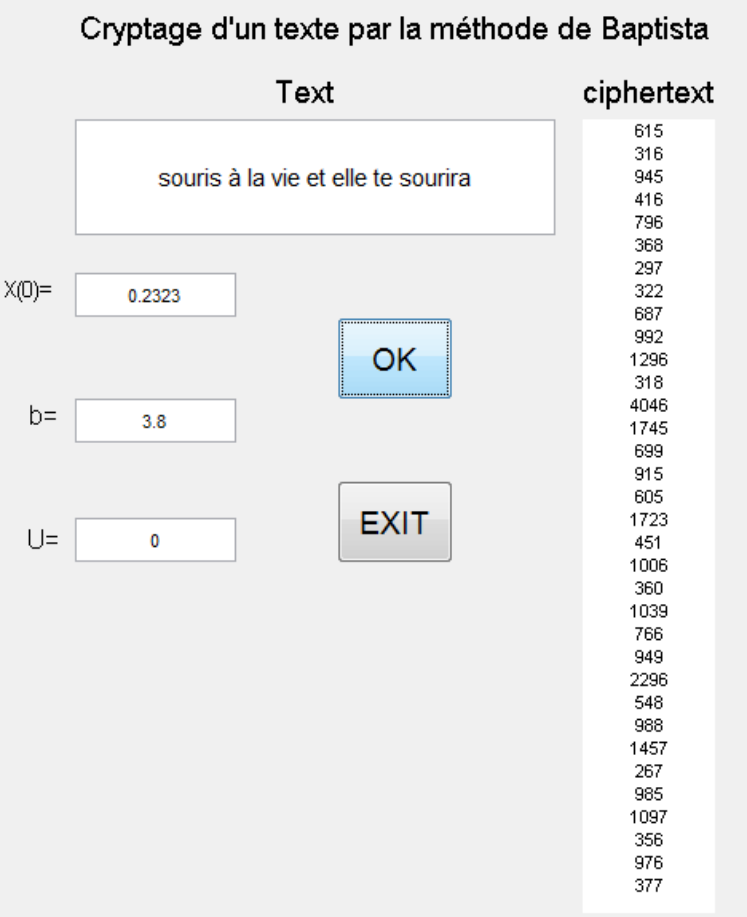



Fig.3.15 Cryptage de la phrase ''souris à la vie et elle te sourira'', b=3.8

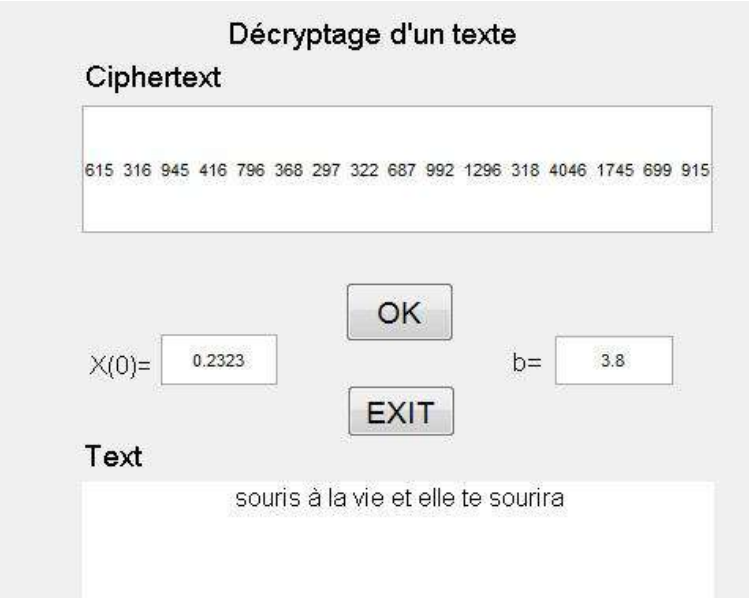



Fig.3.16 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, b=3.8

**Décryptage du texte avec une très petite variation dans la clef b.**

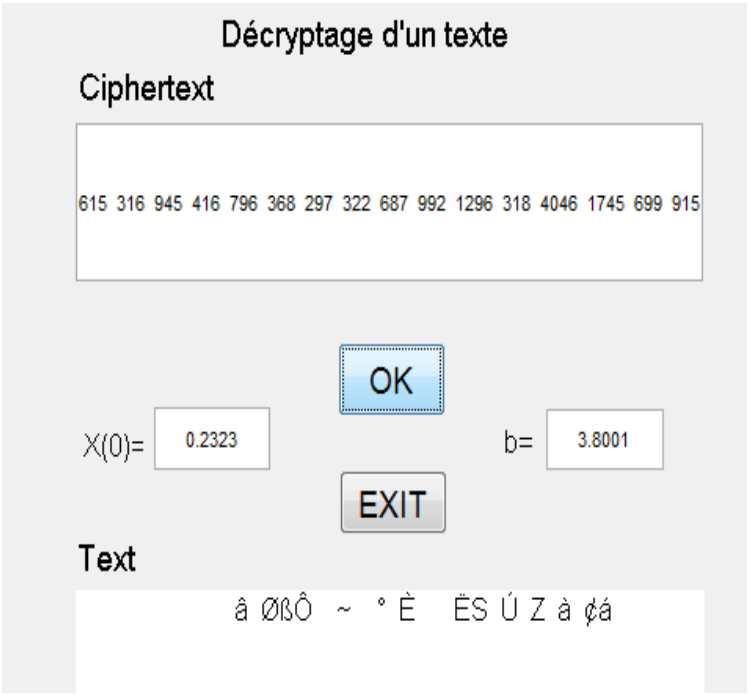



Fig.3.17 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, b=3.8001

b. b=3.9




Fig.3.18 Cryptage de la phrase ‘’souris à la vie et elle te sourira’’, b=3.9

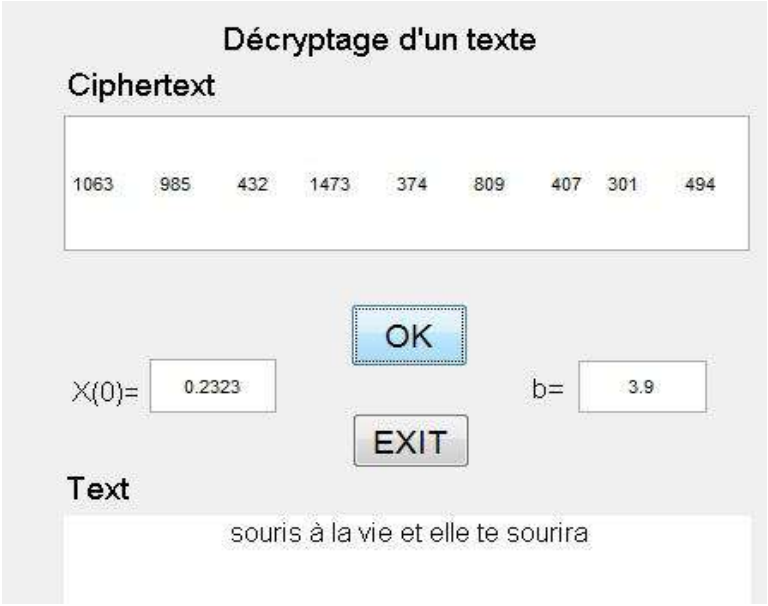



Fig.3.19 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, b=3.9

**Décryptage du texte avec une très petite variation dans la clef b.**

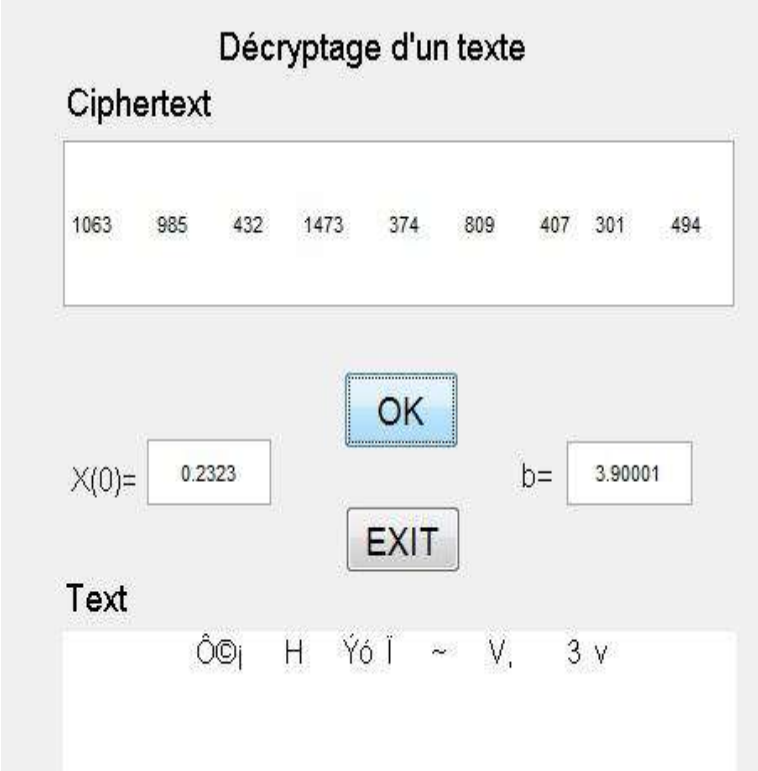



Fig.3.20 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, $b$=3.9001

D’après le résultat, nous trouvons des valeurs différentes de textes chiffrés qui sont varié avec la variation de la clef de cryptage, et une très petite variation du paramètre de contrôle b nous donne un changement totale du message décrypté. Donc ce paramètre de contrôle influe sur la trajectoire de l’équation de la carte logistique mais conduira toujours au même intervalle $\varepsilon$ désiré. Donc tous les textes chiffrés pour les différents valeurs de b sont juste, et aussi nous trouvons que cette méthode est très sensible à la variation du paramètre de contrôle b.

### 3.4.4 Cryptage et décryptage d'un texte pour différentes valeurs de $X_0$

a. $X_0$=0.25

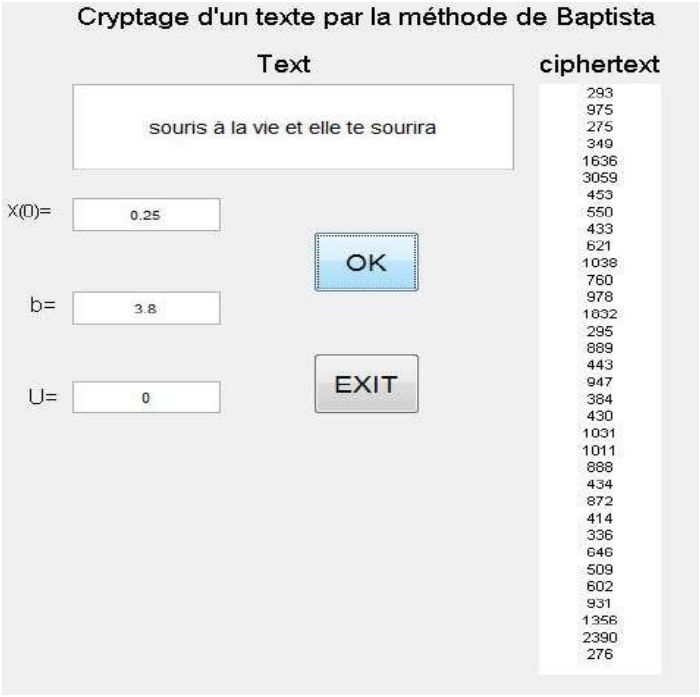



Fig.3.21 Cryptage de la phrase ''souris à la vie et elle te sourira'', $X_0$=0.25




Fig.3.22 Décryptage du texte chiffré de la phrase ''souris à la vie et elle te sourira'', $X_0$=0.25

**Décryptage du texte avec une petite variation dans la condition initiale** $X_0$

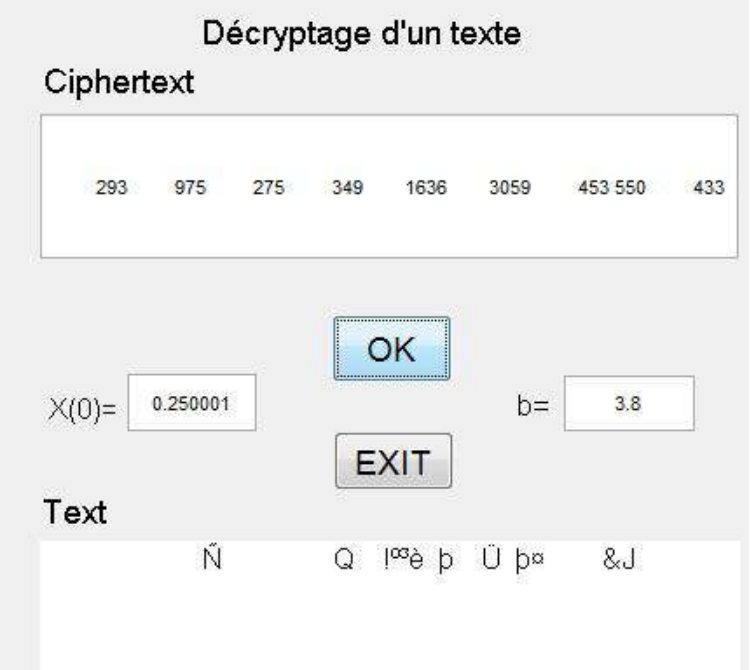



Fig.3.23 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, $X_0$=0.250001

b. $X_0$=0.8

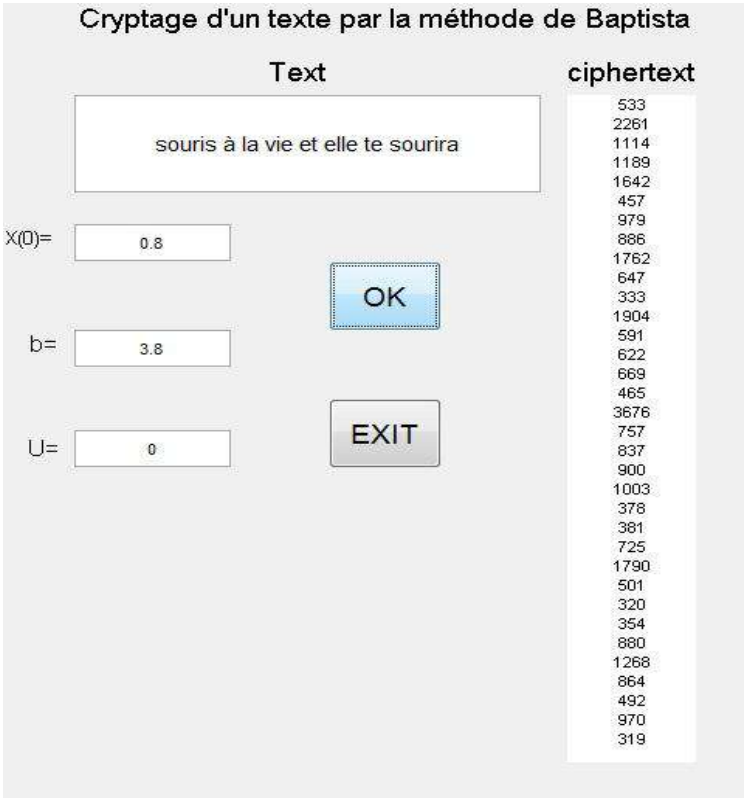



Fig.3.24 Cryptage de la phrase ‘’souris à la vie et elle te sourira’’, $X_0$=0.8




Fig.3.25 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’$X_0$=0.8

**Décryptage du texte avec une petite variation dans la condition initiale $X_0$**




Fig.3.26 Décryptage du texte chiffré de la phrase ‘’souris à la vie et elle te sourira’’, $X_0$=0.800001

D’après le résultat, nous trouvons des valeurs différentes de textes chiffrés qui sont varié avec la variation de la condition initiale, et une très petite variation de cette condition nous donne un changement total du message décrypté. Donc ce condition $X_0$ influe sur la

trajectoire de l'équation de la carte logistique mais conduira toujours au même intervalle $\varepsilon$ désiré. Donc tous les textes chiffrés pour les différentes valeurs de $X_0$ sont juste, et aussi nous trouvons que cette méthode est très sensible à la variation de la première condition initiale.

### 3.4.5 Interfaces des programmes de cryptage/décryptage d'une image

#### a. Cryptage

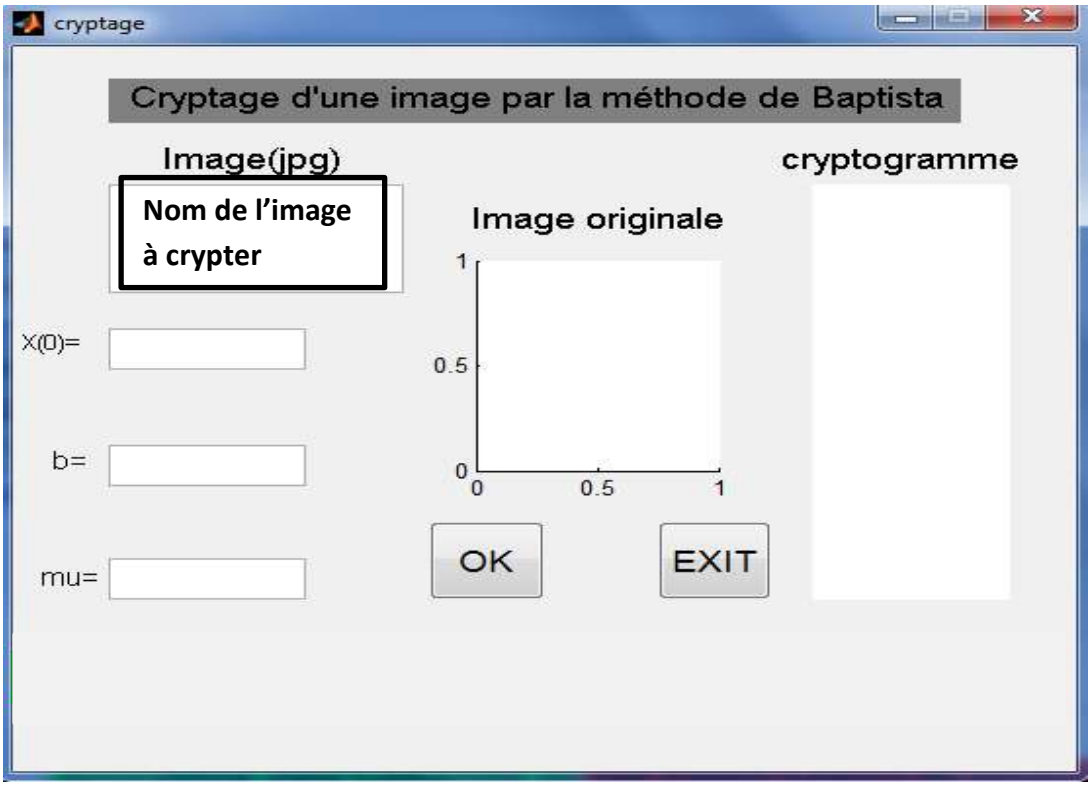



Fig.3.27 Interface du programme de cryptage d'une image

Dans le programme de cryptage d'image on donne au programme le nom de l'image extension (JPG) dans la zone (image(JPG)) avec la première condition initiale ($X_0$) el la clef de cryptage (b) avec le coefficient ŋ, puis le programme va afficher l'image originale dans la zone (image originale) et le cryptage de cette image dans la zone (cryptogramme).

**b. Décryptage**

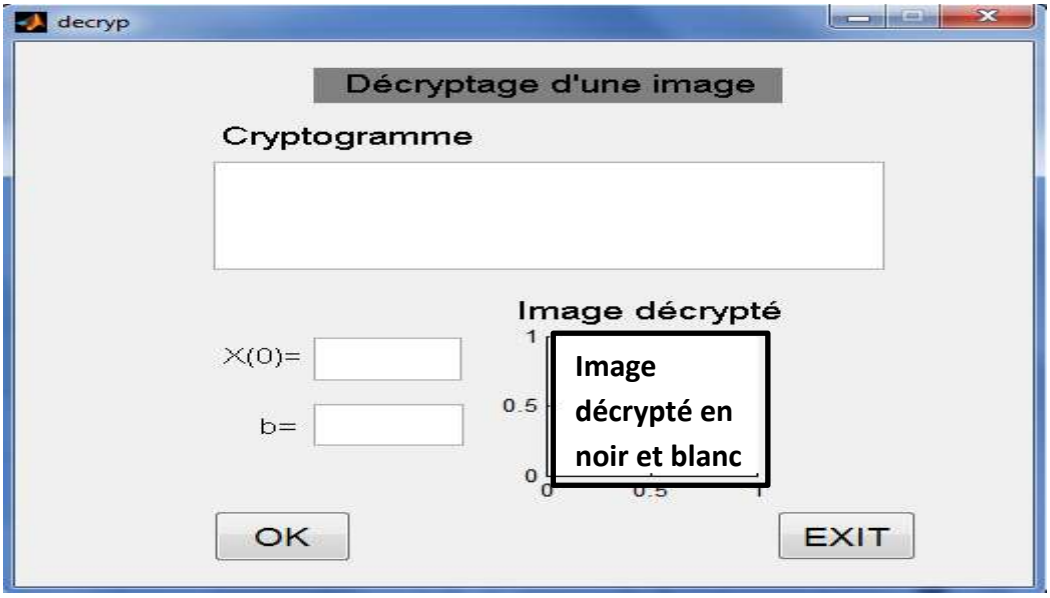



Fig.3.28 Interface du programme de décryptage d'une image

La figure précédente représente le menu du décryptage d'une image crypté. On donne au programme les valeurs du cryptogramme puis les valeurs de ($X_0$ et B) après en clic sur OK le programme va trouver l'image originale en noir et blanc et il va l'afficher dans la zone (image décrypté).

### 3.4.6 Cryptage et décryptage d'une image pour différentes valeurs de ŋ

a. ŋ=0

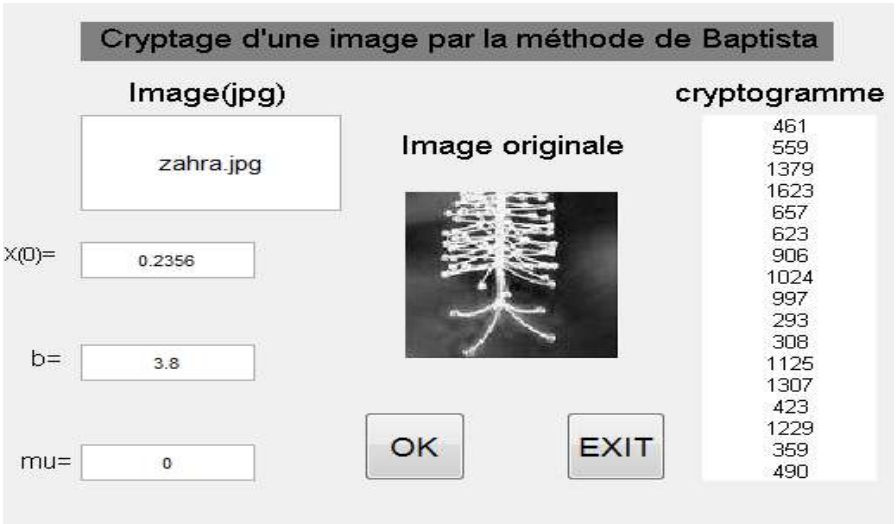



Fig.3.29 Cryptage d'une image avec ŋ=0

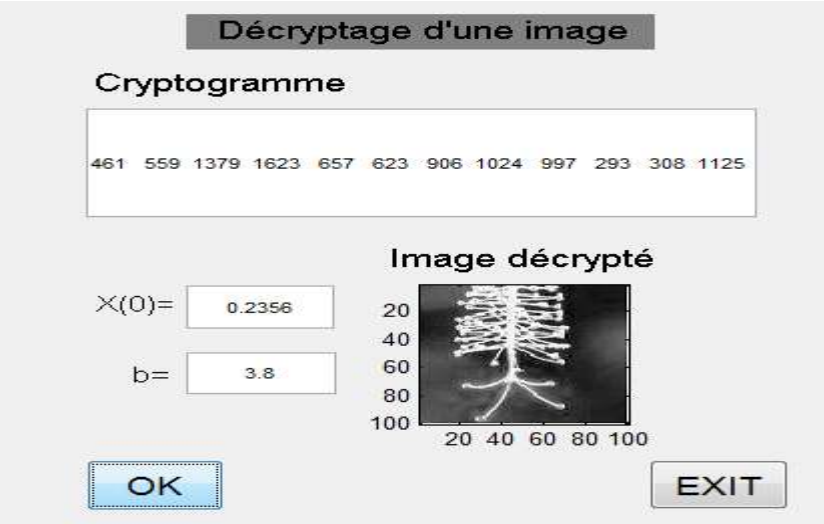



Fig.3.30 Décryptage d'une image crypté ŋ=0

b. ŋ=0.7

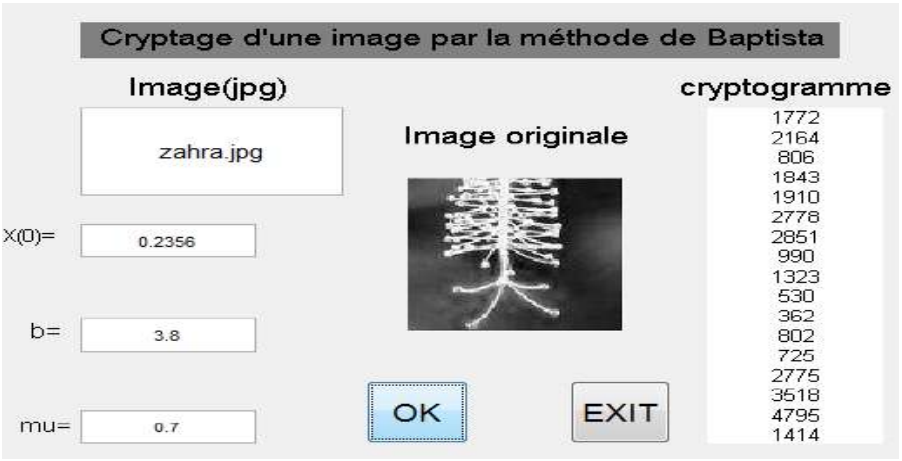



Fig.3.31 Cryptage d'une image avec ŋ=0.7

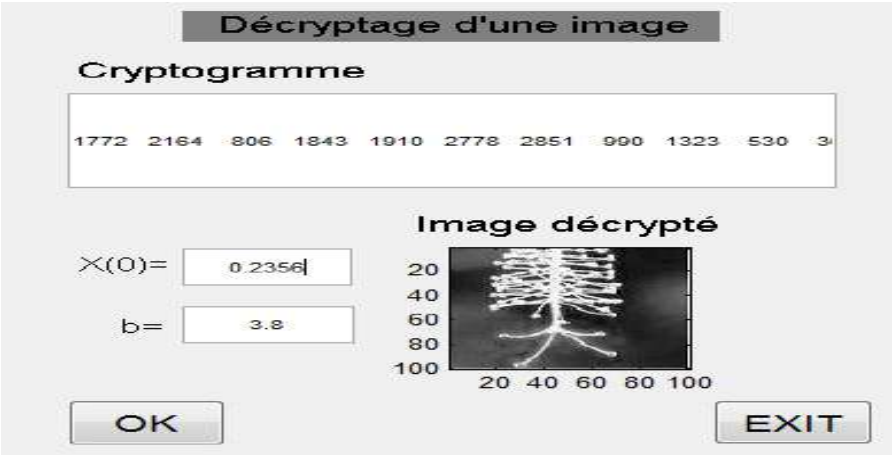



Fig.3.32 Décryptage d'une image avec ŋ=0.7

D'après les résultats, Pour les mêmes paramètres utilisés dans le cryptage, nous obtenons la même image utilisée dans le cryptage. Nous trouvons que la valeur du texte chiffré augmente avec l'augmentation de la valeur du coefficient ŋ et nous remarquons un temps d'exécution plus grand. Ceci à cause de ŋ, lorsque ŋ augmente nous obtenons une diminution de probabilité pour que la variable aléatoire généré k soit supérieur à ŋ, donc l'équation (3.1) atteint l'intervalle voulu.

### 3.4.7 L'effet de l'augmentation de la valeur de ŋ sur le cryptage et le décryptage d'une image :

on va crypter l'image précédente puis la décrypter pour une valeur de coefficient ŋ grande (par exemple ŋ=0.95, 0.97, 0.99) :

#### a. Décryptage d'une image avec une valeur de ŋ =0.95

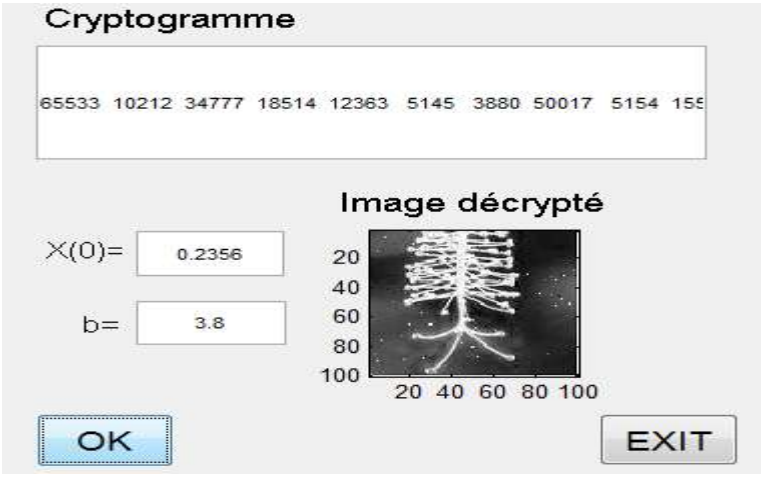



Fig.3.33 Décryptage d'une image avec ŋ=0.95

#### b. Décryptage d'une image avec une valeur de ŋ = 0.97 et 0.99 :

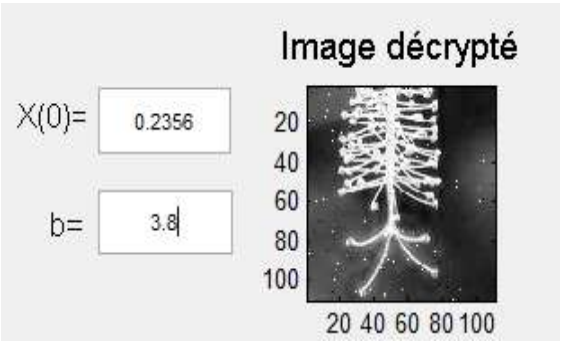



Fig.3.34 Image décryptée, ŋ=0.97

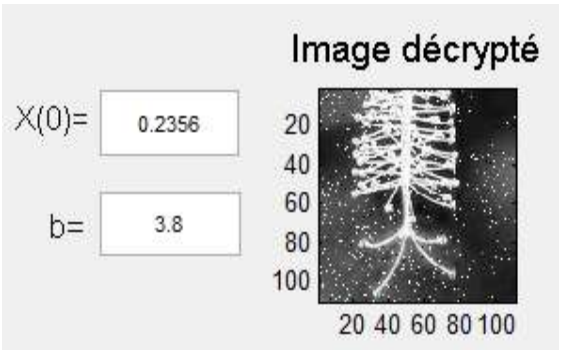



Fig.3.35 Image décryptée, ŋ=0.99

D'après les résultats du cryptage et du décryptage de l'image pour les grandes valeurs de ŋ, on observe des grandes valeurs pour l'image chiffré, et certaines valeur sont égaux au nombre maximum des itérations permises (65532). Dans le décryptage on observe des points grilles (bruit) sur l'image décryptée. Donc la détermination de la valeur de coefficient ŋ a une influence sur la qualité de décryptage de l'image, et la cause des points grilles, c'est que lors de l'opération de décryptage des chiffres de l'image cryptée qui égale à (65532). Le programme fait le maximum de nombre d'itérations mais sans atteindre l'intervalle associé. Donc nous obtenons quelques points décryptés erronés dans l'image, c'est la cause de ces points grilles.

### 3.4.8 Cryptage et décryptage d'une image pour différentes valeurs de la clef b

a. b=3.78

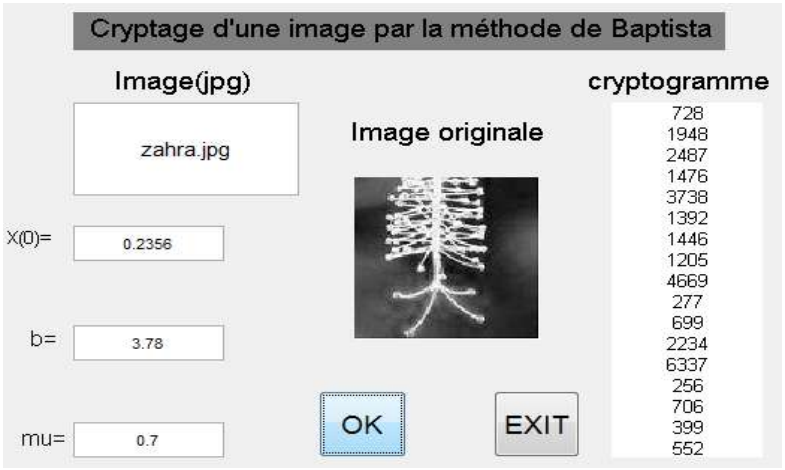



Fig.3.36 Cryptage d'une image avec, b=3.78

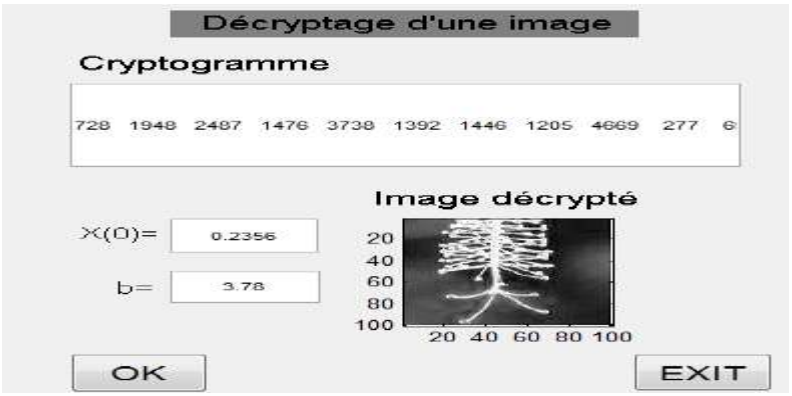



Fig.3.37 Décryptage d'une image cryptée, b=3.78

Décryptage avec une petite variation du paramètre de contrôle *b*.

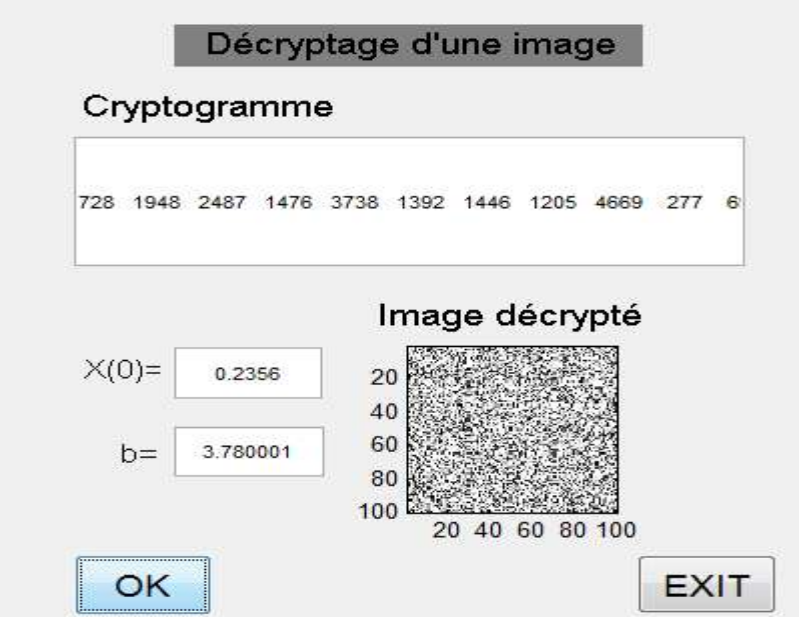



Fig.3.38 Décryptage d'une image cryptée, *b*=3.780001

b. cryptage pour *b*=3.99

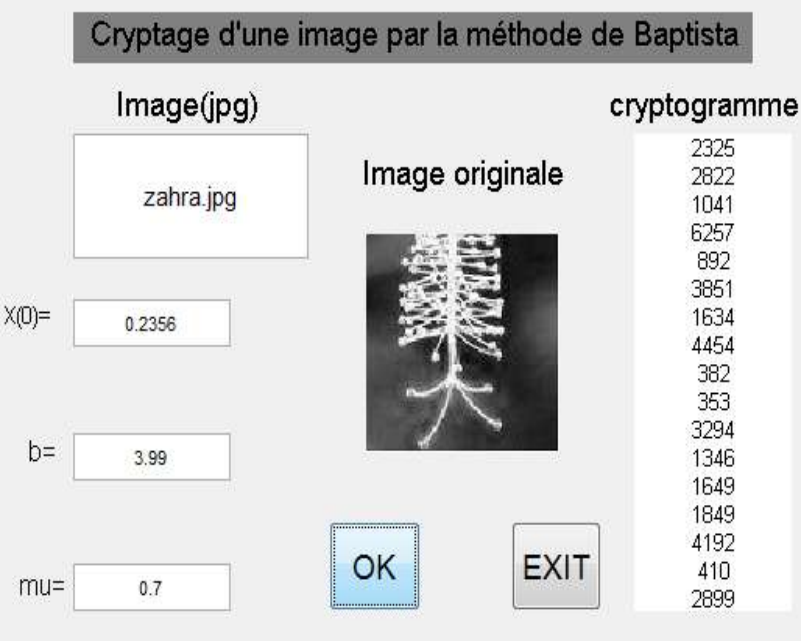



Fig.3.39 Cryptage d'une image avec, *b*=3.99

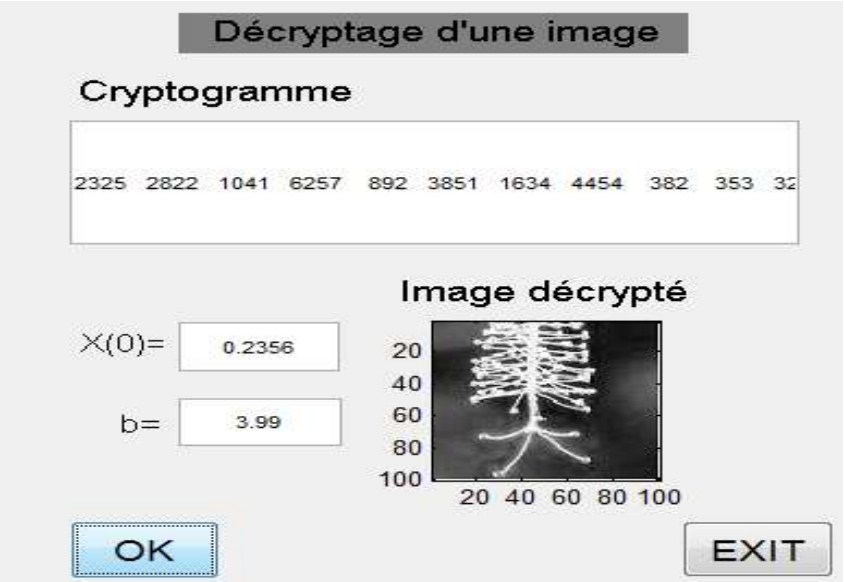



Fig.3.40 Décryptage d'une image cryptée, b=3.99

Décryptage avec une petite variation du b.

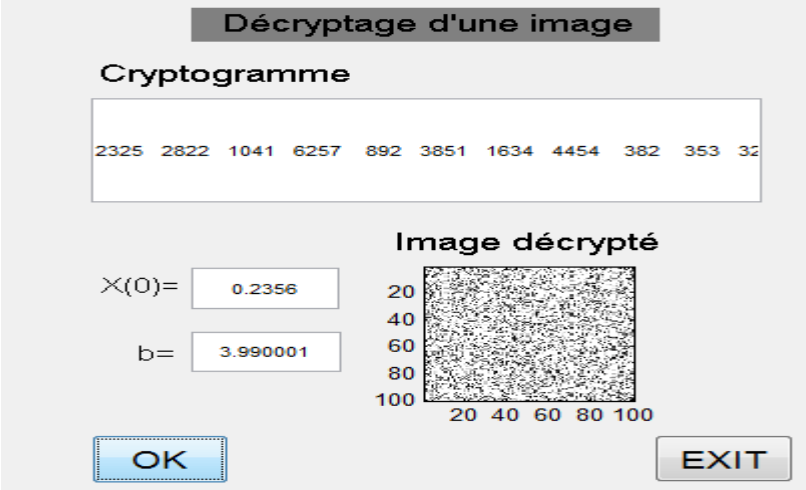



Fig.3.41 Décryptage d'une image cryptée, b=3.990001

D'après le résultat, nous trouvons des valeurs différentes pour les images chiffrées qui varient avec la variation de la clef de cryptage b. Une très petite variation du paramètre de contrôle b nous donne un changement total dans l'image décryptée. Donc, aussi pour les images, ce paramètre de contrôle influe sur la trajectoire de l'équation de la carte logistique mais conduira toujours au même intervalle $\varepsilon$ désiré. Donc toutes les valeurs des chiffres

des images cryptées pour les différentes valeurs de b sont justes. Aussi, nous trouvons que cette méthode est très sensible à la variation du paramètre de contrôle b.

### 3.4.9 Cryptage et décryptage d'une image pour différentes valeurs de condition initiale $X_0$ :

a. $X_0$=0.2

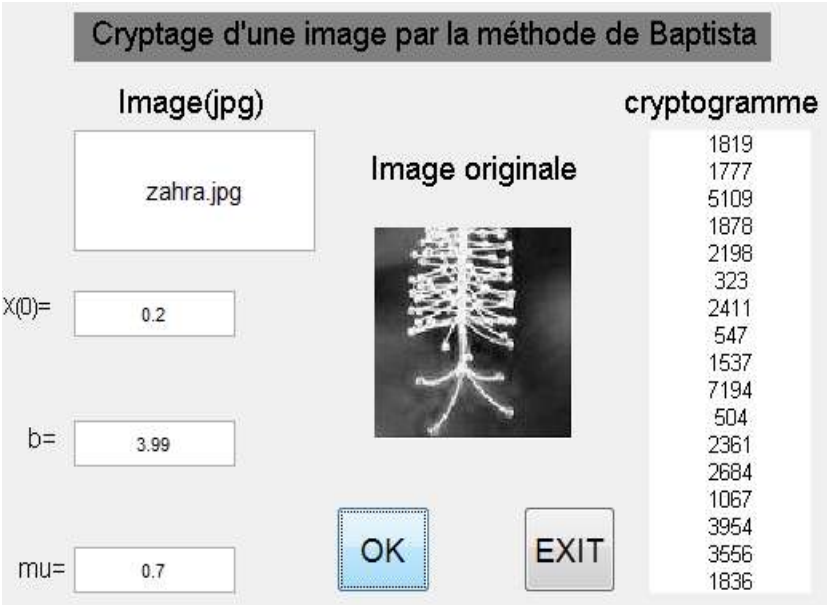



Fig.3.42 Cryptage d'une image avec, $X_0$=0.2

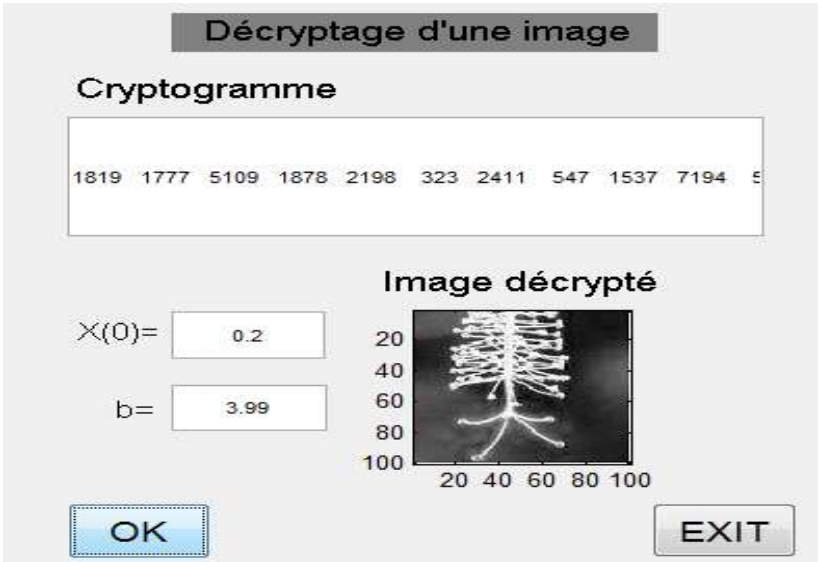



Fig.3.43 Décryptage d'une image cryptée, $X_0$=0.2

Décryptage pour une petite variation de condition initiale $X_0$.

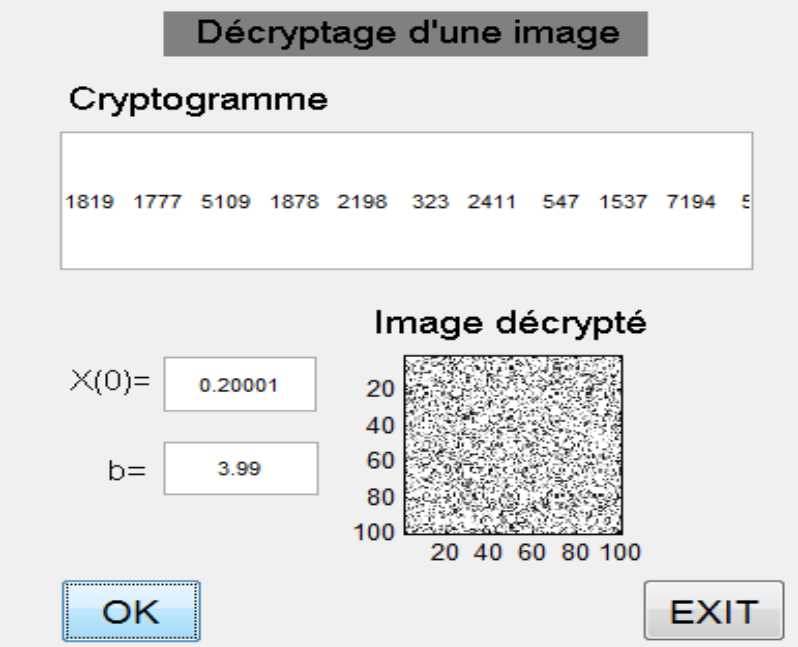



Fig.3.44 Décryptage d'une image cryptée, $X_0$=0.20001

b. $X_0$=0.85

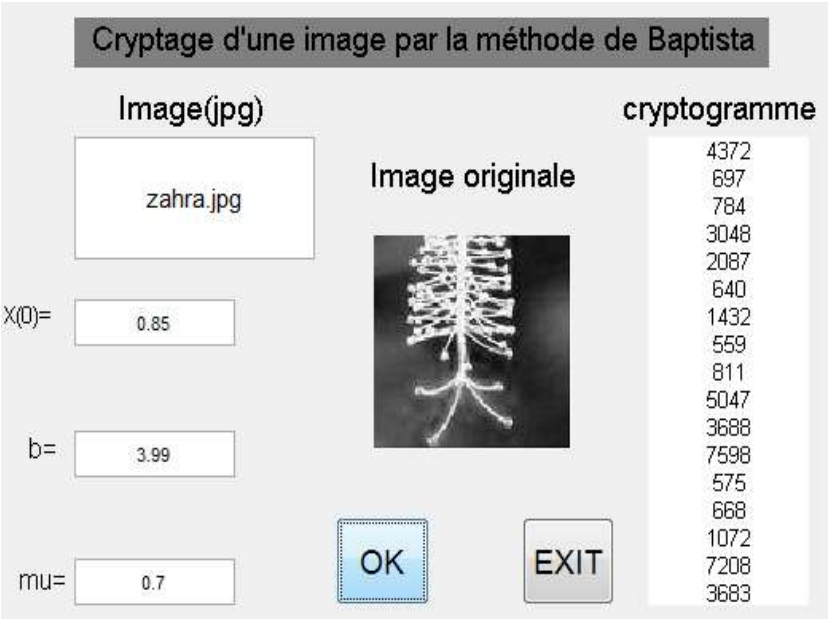



Fig.3.45 Cryptage d'une image avec, $X_0$=0.85

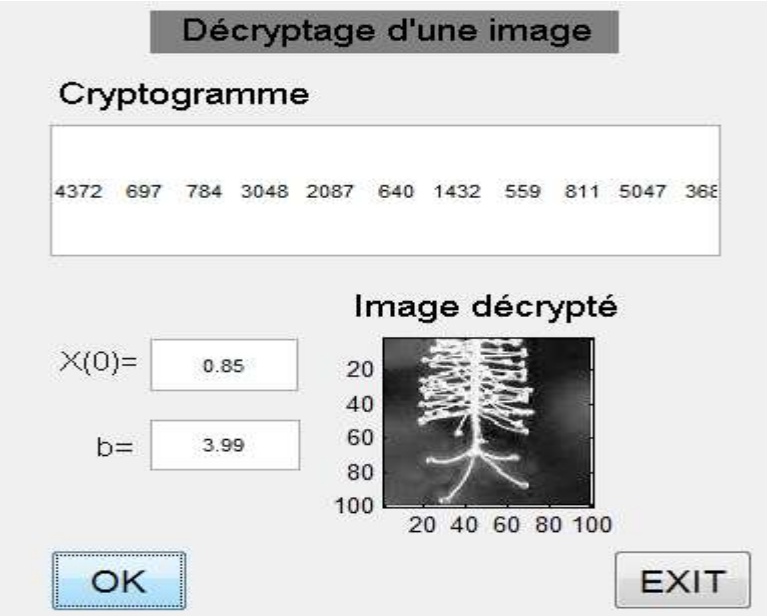



Fig.3.46 Décryptage d'une image cryptée, $X_0$=0.85

Décryptage pour une petite variation de condition initiale $X_0$ :

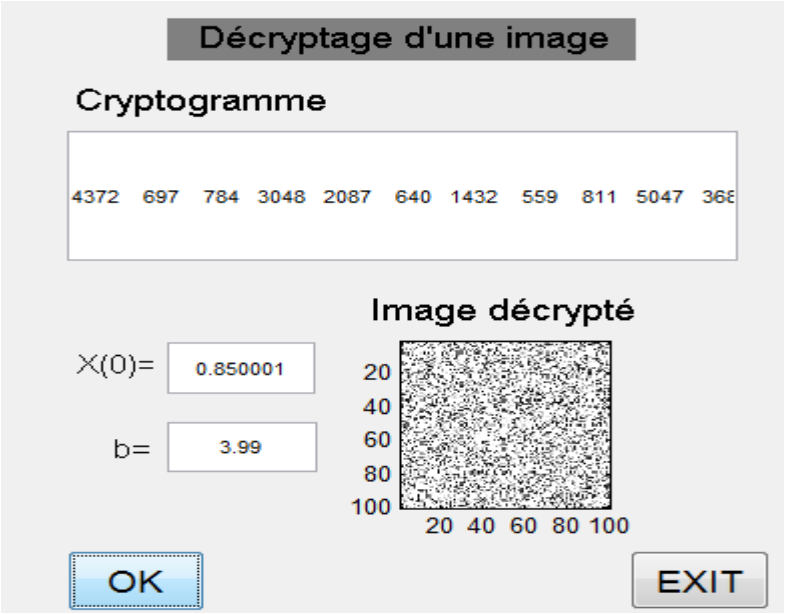



Fig.3.47 Décryptage d'une image cryptée, $X_0$=0.850001

D'après le résultat, nous trouvons des valeurs différentes pour les images chiffrées qui varient avec la variation de la première condition initiale$X_0$. Une très petite variation du paramètre de condition initiale $X_0$ nous donne un changement total dans l'image décryptée. Donc, aussi pour les images, ce paramètre de contrôle influe sur la trajectoire de l'équation

de la carte logistique mais conduira toujours au même intervalle $\varepsilon$ désiré. Donc toutes les valeurs des chiffres des images cryptées pour les différentes valeurs de $X_0$ sont justes. Aussi, nous trouvons que cette méthode est très sensible à la variation de la première condition initiale $X_0$.

## 3.5 Conclusion

Dans ce chapitre, nous avons effectué une étude et une implémentation de la méthode de baptista : après l'exécution du programme de cryptage de texte en clair et l'image qui porte le nom ''zahra.jpg'', nous parvenons à récupérer le texte et l'image qui sont exactement identiques aux originaux. Et pour des paramètres de cryptage ($X_0$ et $b$) légèrement différentes par rapport aux celles utilisés dans le cryptage nous obtenons un changement total dans le texte ou l'image décrypté. Donc Un « pirate » voulant s'attaquer le chiffrement du message, ne pourra pas reconstituer correctement le message crypté, puisqu'il ne connaît pas les conditions initiales exactes qui ont été utilisées lors de la transmission. Il lui sera alors difficile de s'affranchir de ce « bruit » mélangé au message avant la transmission , puis nous arrivons à étudier l'effet de coefficient ŋ et nous avons vu les valeurs de ce coefficient qui influe sur la qualité de cryptage et de décryptage d'un texte ou d'une image soit en cryptage ou en décryptage, on a trouvé que ce coefficient a un grand rôle dans la sécurité du cryptage puisqu'il diminue la probabilité qu'une autre personne peut prévoir la résultat de texte chiffré. Et d'autre part les grandes valeurs de coefficient ŋ peuvent avoir une influence sur la possibilité de décryptage correcte d'un texte, ou une influence sur la qualité de l'image décrypté et ce dernier a aussi une influence sur le temps d'exécution des opérations, en cryptage ou en décryptage, puisque la probabilité que l'équation de la carte logistique (à une dimension) de la méthode de baptista atteint l'intervalle $\varepsilon$ désiré et que la variable aléatoire généré K soit supérieur au coefficient ŋ en même temps est faible. c'est pour cela que la boucle s'exécute plusieurs fois donc ça nous donne des valeurs de texte chiffré plus grande et parfois le maximum de nombres d'itérations (65532) donc ça prend plus de temps d'exécution nécessaire dans le cryptage ou le décryptage.

# 4. Conclusion Générale

La cryptographie reste encore le seul moyen pour assurer la sécurité des correspondances. Étroitement liée à l'effort de guerre, elle n'a pas cessé de se développer depuis ses origines antiques.

Les Anciens avaient déjà perçu dans cette technique quelque peu ésotérique le meilleur moyen de garantir la confidentialité de leurs missives. Ils l'ont développée d'une façon simple mais efficace, l'adaptant aux divers besoins.

Leurs innovations nous ont été transmises soit par le concepteur lui-même (César) soit par des historiens qui en admiraient l'ingéniosité. La qualité de ces méthodes a suscité l'intérêt des crypto-logues ultérieurs qui employèrent ces techniques en introduisant leurs propres inventions. Dans ce travaille, nous avons étudié une méthode de cryptographie c'est la cryptographie chaotique

Nous avons étudié une méthode de cryptographie qui est la cryptographie chaotique. Une application de cryptographie chaotique numérique est apparue en 1998, c'est la méthode de Baptisa qui est basée sur une équation de carte logistique d'une seule dimension. Nous avons implémenté le programme de cryptage et de décryptage des textes et des images sous MATLAB, et nous avons démontré que cette méthode de cryptage est très sensible au conditions initiales ce qui augmente la sécurité de cryptage puisque une très petite variation dans les paramètres de cryptages (condition initiale ou clef de cryptage) a une très large influence sur le message crypté et ça va produire des erreurs dans le message décrypté, donc un pirate ne peut rien faire sur le message chiffré sans savoir la valeur exacte de la condition initiale et de la clef de cryptage , et aussi nous avons trouvé que la condition initiale change à chaque nouveau caractère. Donc tous le cryptage et le décryptage est lié à la première condition initiale, et nous avons démontré qu'il y a des conditions pour définir les paramètres de cryptage sinon le cryptage ne sera pas chaotique ou ça va avoir une influence sur le massage décrypté et il va produire des erreurs dans les textes ou des bruits dans les images.

# BIBLIOGRAPHIES

[AHM 07] ALI-PACHA.A, HADJ-SAID. N, M'HAMED.A"Chaos Crypto-Système basé sur l'Attracteur de Hénon-Lozi",2007.

[ALS 06] Gonzalo Alvarez and Shujun Li"Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems" , International Journal of Bifurcation and Chaos 2006.

[BAP 98] M.S. Baptista "Cryptography with chaos"Physics Letters, January 1998.

[BOS 10] Birkhäuser Boston"Chaos Control and Synchronization",a part of Springer Science+Business Media 2010.

[CAR 11] Pellicer-Lostao Carmen and López-Ruiz Ricardo"Notions of Chaotic Cryptography: Sketch of a Chaos Based Cryptosystem",University of Zaragoza, Spain 2011.

[CED 10] Cédric Lauradoux ''une introduction à la cryptographie '' 2010

[CHA 09] Cheng-Ta Chao"A high security Baptista-type cryptosystem using cascaded chaotic maps",National Cheng Kung University 2009.

[DAN 96] Dany-jack mercier "Cryptographie classique et cryptographie publique à clé révélée'' Université des antilles et de la Guyane France 1996

[DAN 03] Dany-jack mercier ''cryptographie classique'' (IUFM) de guadeloupe France 2003

[GOU 10] Goumidi Djamal Eddine"Fonction logistique et standard chaotique pour le chiffrement des images satellitaires", Université Mentouri de Constantine 2010.

[HAM 11] HAMICHE Hamid "Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données" THÈSE DE DOCTORAT 2011.

[HER 01] HERVE SHAUER ‘’Introduction à la cryptographie’’ laboratoire Ghislaine France 2001.

[JGZ 11] Yong-Xian Jin, Yi-Sheng Guan, and Lin Zheng “An Image Encryption Algorithm Based on Chaos“, Springer-Verlag Berlin Heidelberg 2011.

[JMA 09] Josie Maria Amigo“Chaos-Based Cryptography“,Springer-Verlag Berlin Heidelberg 2009.

[LAH 07] Shujun Li , Gonzalo Alvarez, Zhong Liand Wolfgang A. Halang“Analog Chaos-based Secure Communications and Cryptanalysis“,2007.

[LID 05] Q.V. Lawande B. R. Ivan and S. D. Dhodapkar“CHAOS BASED CRYPTOGRAPHY : A NEW APPROACH TO SECURE COMMUNICATIONS“,2005.

[PAL 06] Pascal Lafourcade ‘’ Vérification de protocoles cryptographiques en présencede théories équationnelles. ‘’Thèse de doctorat école normale supérieur de cachan septembre 2006

[PIE 12] pierre-alain FOUQUE ‘’dossier techniques d’ingénieurs (cryptographie appliqué)’’ Laboratoire de cryptographie de la direction centrale de la Sécurité des systèmes d'information(DCSSI) France

[RBK 07] Nada REBHI, Mohamed Amine BEN FARAH, Abdennaceur KACHOURI & Mounir SAMET “ Analyse De Sécurité d’une Nouvelle Méthode De Cryptage Chaotique“ 4th International Conference: Sciences of Electronic, TUNISIE 2007.

[RIN 09] Cristian-Iulian RINCU“CHAOS-BASED CRYPTOGRAPHY. A POSSIBLE SOLUTION FOR INFORMATION SECURITY“,2009.

[SAN04] Sandrine Julia ‘’ techniques de cryptographie ‘’ France 2004

[STA 11] Lhomer Stanislas“Générateurs pseudo-aléatoires Chaotiques“

[TAL10] TALBI Ibtissem “Systèmes dynamiques non linéaires et phénomènes de chaos“,Université Mentouri de Constantine 2010.

[TTA 04] Roy Tenny, Lev S. Tsimring, Henry D.I. Abarbanel “Security of Chaos-Based Communication and Encryption“,2004.

[YEA 10] Hippolyte Sienpégnou YEO, Sharif ALWI “Cryptage Chaotique à l'Aide d'une Application Unidimensionnelle “ , Université de Tlemcen 2010.