Université Abou Bekr Belkaid جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

pour l'obtention du diplôme de Master en Informatique

Option: *Réseau et Système Distribuer (R.S.D)*

Thème

Génération et distribution des clés Cryptographique a partir des signaux ECG

Réalisé par :

- BENGHORZI Amel

Présenté le 26Juin 2016 devant le jury composé de MM.

- *BENAMAR.A* — *Président*
- *MANA.M* — *(Encadreur*
- *BENAISSA.M* — *Examinateur*
- *BENZIANE.M* — *Examinateur*

Année universitaire : 2015-2016

REMERCIEMENTS :

eJ remercie ALLAH le tout puissant de nous avoir donné le courage et la volonté de mener à terme le présent travail.

eJ présente sem remerciements les plus sincères à notre promoteur **Mr. Mana Med,** pour leur disponibilité et leur encadrement, ainsi que pour leur soutien tout au long de l'année. C'est grâce à eux que nous avons pu mener à bien ce travail. Qu'ils trouvent ici le témoignage de notre reconnaissance.

eJ remercie s'adressent aux membres du *Jury* qui nous font l'honneur de participer à la soutenance.

J aimersia également remercier tous nos amis et collègues de leur soutien et aide et qui nous ont donné la force pour continuer.

sem remerciements vont aussi à tous ceux qui ont contribué de prés ou de loin à la concrétisation de ce travail. Qu'ils trouvent tous ici l'expression de notre gratitude et notre parfaite considération.

Table des matières

Université Abou Bekr Belkaid جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Génération et distribution des clés Cryptographique a partir des signaux ECG

Réalisé par :

- BENGHORZI Amel

Présenté le 26Juin 2016 devant le jury composé de MM.

- *BENAMAR.A* — *Président*
- *MANA.M* — *(Encadreur*
- *BENAISSA.M* — *Examinateur*
- *BENZIANE.M* — *Examinateur*

Année universitaire : 2015-2016

REMERCIEMENTS :

eJ remercie ALLAH le tout puissant de nous avoir donné le courage et la volonté de mener à terme le présent travail.

eJ présente sem remerciements les plus sincères à notre promoteur **Mr. Mana Med,** pour leur disponibilité et leur encadrement, ainsi que pour leur soutien tout au long de l'année. C'est grâce à eux que nous avons pu mener à bien ce travail. Qu'ils trouvent ici le témoignage de notre reconnaissance.

eJ remercie s'adressent aux membres du *Jury* qui nous font l'honneur de participer à la soutenance.

J aimersia également remercier tous nos amis et collègues de leur soutien et aide et qui nous ont donné la force pour continuer.

sem remerciements vont aussi à tous ceux qui ont contribué de prés ou de loin à la concrétisation de ce travail. Qu'ils trouvent tous ici l'expression de notre gratitude et notre parfaite considération.

Table des matières

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

TABLE DES MATIÈRES

Introduction générale

Introduction générale

Ces dernières années ont été marquées par l'explosion des systèmes de communication, qui ont permis le développement des échanges électroniques, tant dans le domaine industriel et bancaire que dans celui du commerce en ligne et récemment celui des relations entre les citoyens et les administrations. Si, jusqu'à présent, l'ouverture et l'interopérabilité des réseaux et systèmes, ainsi que leurs performances, ont été privilégiées aux dépens de la sécurité, on assiste maintenant à une prise de conscience des problèmes par les acteurs de ces nouveaux réseaux.

Récemment, des études ont été menés sur la possibilité d'utilisation de la biométrie dans le domaine cryptographique. L'idée consiste à générer les clés cryptographiques à partir des données biométriques. Par définition la biométrie est une technique visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et d'un seul individu. On distingue les caractéristiques biométriques invariant dans le temps tels que l'empreint digital, l'iris, l'ADN,... et ceux variant dans le temps tel que l'ECG, PPG,...

Le choix de tel caractéristique biométrique dépend du domaine d'application et du niveau de sécurité qu'on souhaite.

Dans notre projet, on vise à générer des clés cryptographiques à partir des signaux ECG. Un signal ECG se caractérise par l'aspect aléatoire (propriété importante en cryptographie) car il est variable dans le temps; deux clés générés du même signal ECG à deux instants différents ne seront pas identiques. Parmi les domaines d'application nécessitants ce mécanisme de génération de clé, on peut citer le contrôle des patients à distance.

Pour la réalisation de notre projet, nous avons suivi le plan suivant:

En premier lieu, nous avons présenté le signal ECG; ensuite nous avons abordé les méthodes de chiffrement modernes. Le troisième point a été consacré à la présentation des codes auto-correcteurs d'erreurs, et notamment les codes Reed Solomon. Et dernier chapitre, nous avons présenté notre schéma de génération de clés cryptographiques à partir des signaux ECG.

Chapitre 1

CHAPITRE 1 : ELECTRO CARDIOGRAPHIQUE (ECG)

1. Introduction

L'ECG est l'enregistrement de l'activité électrique du cœur en fonction du temps.
Les tissus de l'organisme étant conducteurs, cet enregistrement

1. Introduction

L'ECG est l'enregistrement de l'activité électrique du cœur en fonction du temps. Les tissus de l'organisme étant conducteurs, cet enregistrement est réalisé grâce à des électrodes cutanées placées en des points déterminés permettant de définir des dérivations conventionnelles.

L'activité électrique cardiaque normale prend naissance dans le nœud sinusal puis se propage selon un cheminement déterminé : nœud sinusal, myocarde auriculaire, nœud auriculo-ventriculaire d'Aschoff-Tawara, faisceau de His et ses branches gauche et droite , réseau sous-endocarditique de Purkinje , myocarde ventriculaire .
Ainsi se succèdent sur le tracé ECG la dépolarisation auriculaire (onde P), la dépolarisation ventriculaire (complexe QRS), puis la repolarisation ventriculaire (onde T, onde U). [11]

2. Définitions :

L'électrocardiogramme enregistre les variations des potentiels électriques entre 2 points éloignés, à la surface du corps (*E.C.G.* ou *E.K.G.*) : elles sont dues à la dépolarisation-repolarisation du muscle cardiaque (dérivations indirectes) selon une séquence déterminée par l'organisation fonctionnelle du tissu nodal. Dans les conditions normales, le départ de l'activation provient du "pace-maker" atrial (nœud sino-atrial). La propagation de l'activation se ralentit à l'approche du nœud atrio-ventriculaire (ce qui est essentiel à la succession normale de la contraction atriale puis ventriculaire dans des conditions permettant un remplissage ventriculaire efficace). Elle s'accélère ensuite dans le faisceau de His et ses ramifications.

Le tracé obtenu n'est pas fondamentalement différent de l'enregistrement de l'activité électrique cardiaque au moyen d'électrodes directement appliquées sur le cœur (dérivations directes) puisque le corps est un milieu conducteur. Les potentiels recueillis sont seulement plus faibles.

Par contre, ce tracé global diffère considérablement de celui obtenu à l'aide d'une micro-électrode implantée dans une cellule myocardique et qu'on désigne parfois par l'expression : "électrogramme cardiaque" ou enregistrement unitaire, pour bien le différencier de l'électrocardiogramme proprement dit. [8]

3. Principe de l'électrocardiographie

L'électrocardiographie consiste à explorer l'activité électrique du cœur en enregistrant des électrocardiogrammes, graphes traduisant les différences de potentiel électrique dans différents points du corps en fonction du temps. L'activation des fibres musculaires cardiaques peut se diviser en deux temps :
Une phase de dépolarisation, une autre de repolarisation.

La phase de dépolarisation est très brusque, c'est en quelque sorte la phase principale ; la repolarisation a pour rôle de rétablir les charges aux valeurs initiales. Les différences de potentiel induites ne sont que de l'ordre de quelques millivolts mais elles sont suffisamment importantes pour pouvoir être détectées dans le corps humain qui forme un milieu conducteur assez homogène. Il en résulte que plusieurs électrodes placées en des points différents du corps ne perçoivent pas le même courant électrique. [7]

Le principe de l'enregistrement moderne est, à peu de chose près, celui qui fut proposé par Einthoven : grâce à deux électrodes collées à la surface de la peau, on enregistre la différence de potentiel entre deux points diamétralement opposés par rapport au cœur, ce signal étant directement corrélé au déplacement de l'impulsion électrique dans les fibres du muscle cardiaque.

L'activité électrique instantanée peut être définie par un vecteur orienté suivant la différence de potentiel présente dans le cœur, et de module proportionnel à celle-ci. Le couple d'électrodes enregistre à chaque instant l'amplitude de la projection de ce vecteur suivant leur axe : ainsi, lorsque le vecteur électrique est orienté de l'électrode - à l'électrode +, on observe sur l'enregistreur une déflexion positive, et lorsque le vecteur est orienté en sens inverse, la déflexion est négative. [6]

Le vecteur de dépolarisation est nul (point rouge), le tracé est donc plat (a). Une stimulation extérieure du côté gauche induit une perte de charge de ce côté ; l'impulsion électrique se propage alors de gauche à droite. Le vecteur de dépolarisation associé (flèche rouge) est orienté de l'électrode négative vers l'électrode positive : l'enregistrement présente donc une déflexion positive (b) qui est maximale lorsque la dépolarisation a atteint le milieu de la cellule. La fin de la dépolarisation se traduit par une pente descendante(c), car le vecteur est toujours orienté dans le même sens mais son amplitude diminue. Une fois la cellule dépolarisée, le tracé est plat (d). La repolarisation

de la cellule se traduit par un vecteur électrique orienté dans le sens opposé au précédent le tracé présent donc, dans un premier temps, une déflexion négative (e) pour ensuite redevenir plat (f). [Hurst, 1990] [6]

Comme le montre l'image suivante :

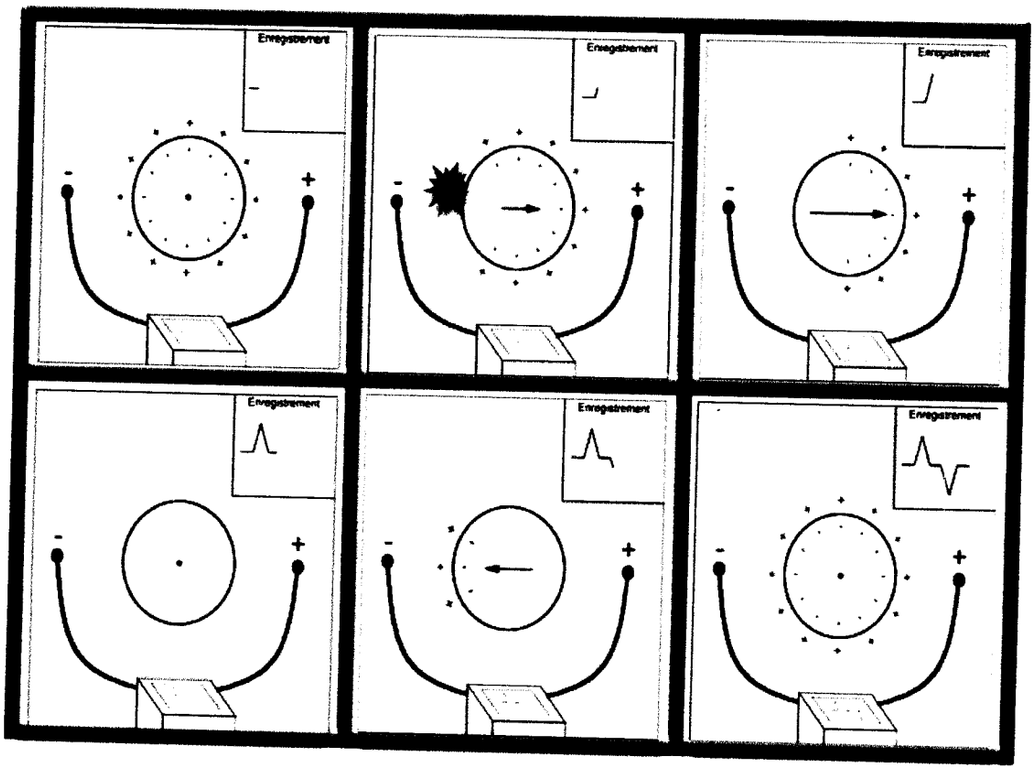


Figure 1.1 Dépolarisation-repolarisation et l'enregistrement ECG [10]

4. Signification des phénomènes électriques de l'ECG

L'activation électrique du myocarde nait au niveau du nœud sinusal (nœud de Keith et Flack) Qui représente le générateur naturel d'impulsion électrique. L'impulsion formé au niveau du nœud sinusal est transmise à la musculature auriculaire (conduction sino-trial = conduction SA) et se propage dans un premier temps dans l'oreillette (conduction intra-atrial = dépolarisation auriculaire).

L'excitation électrique atteint ensuite par le nœud auriculo-ventriculaire (nœud d'Aschoff -Tawara) et le tronc du faisceau de His, les ventricules (conduction auriculo-ventriculaire = conduction AV). La dépolarisation des ventricules résulte de la transmission de l'impulsion électrique par les deux branches intraventiculaire du

faisceau de His et le réseau de Purkinje (conduction intraventriculaire = dépolarisation ventriculaire)

Le système spécifique du myocarde comprend le nœud auriculo-ventriculaire, le tronc du His

La branche de conduction droite et la branche de conduction gauche, qui se divise en hémibranche antérieur et extérieur gauches.

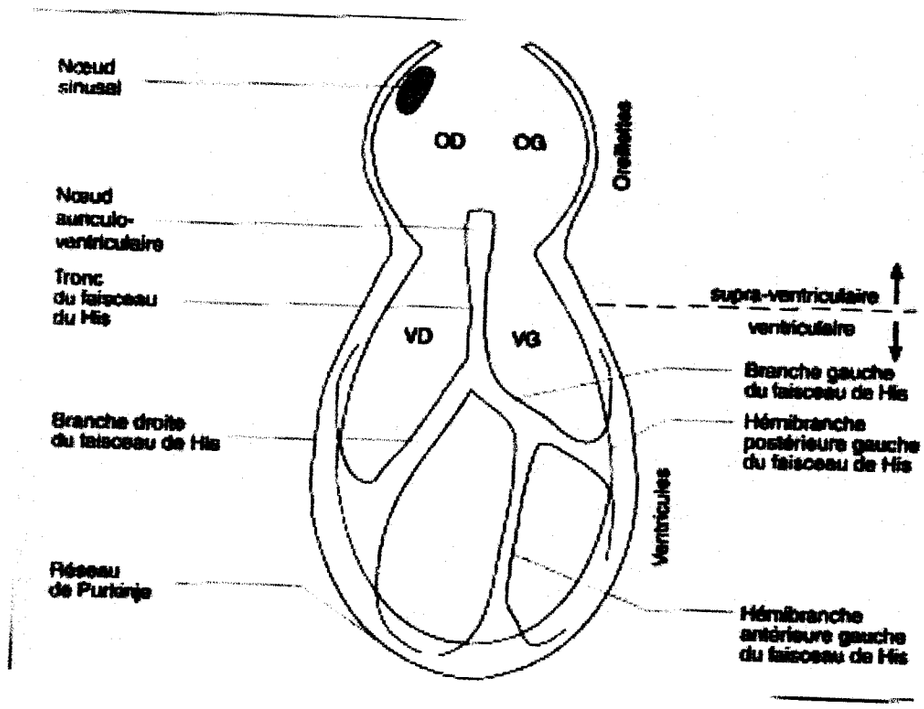


Figure 1.2 Représentation de la naissance de l'impulsion électrique et sa conduction [9]

Pendant que la dépolarisation se propage au niveau des ventricules, la repolarisation se fait au niveau des oreillettes (repolarisation atrial). La propagation complète de la dépolarisation au niveau ventriculaire est elle aussi suivie par une repolarisation (repolarisation ventriculaire).

Toute la succession de ces phénomènes électriques au niveau du myocarde, de la dépolarisation à la repolarisation est représentée sur l'électrocardiogramme.

Remarque :

La repolarisation de l'oreillette elle est masquée par la dépolarisation ventriculaire.

Les phénomènes électriques de la dépolarisation et de la repolarisation peuvent regrouper en ondes et segments. [9]

5. L'Acquisition du signal ECG :

5.1. Les dérivations :

L'électrocardiogramme de surface est obtenu par des électrodes appliquée sur la peau, où des électrodes a polarité opposée représentent des dérivations bipolaires.

Une électrode positive et un point de référence déterminent une dérivation unipolaire.

L'amplitude des différentes ondes résulte de la grandeur de la différence de potentiel recueillie dans la direction du vecteur des différentes dérivations.

L'électrocardiogramme standard comporte 12 dérivations :6 dérivation périphériques (DI , DII ,DIII, aVR, aVL, aVF) et 6 dérivations précordiales (V1-V6).

Les dérivations frontales comportent les dérivations d'Einthoven DI, DII, DIII (dérivations standard bipolaires des membres) et les dérivations de Goldberger aVR, aVL, aVF (dérivations unipolaires des membres).

Les dérivations des membres sont des projections des phénomènes électriques du myocarde dans le plan frontal.

5.1.1 Dérivations des membres (dérivations Frontales):

Bipolaires :

- **D1** : Bras gauche (+) et bras droit (-)
- **D2** : Jambe gauche (+) et bras droit (-)
- **D3** : Jambe gauche (+) et bras gauche (-)

Unipolaires :

aVR ; **aVL** ; **aVF** se sont des dérivations unipolaires et correspondent au membre avec lequel elles sont connectées soit respectivement le bras droit, le bras gauche, et la jambe gauche. C'est la théorie de Wilson et Golberger, où l'électrode exploratrice positive correspond au membre appliqué. Le voltage est alors amplifié (d'où le préfixe a) pour obtenir un tracé de même amplitude D1,D2,D3.

- **VR** Bras droit (+) et borne centrale de Wilson (-).

- VL Bras gauche (+) et borne centrale de Wilson (-).
- VF : Jambe gauche (+) et borne centrale de Wilson (-).[9] [11]

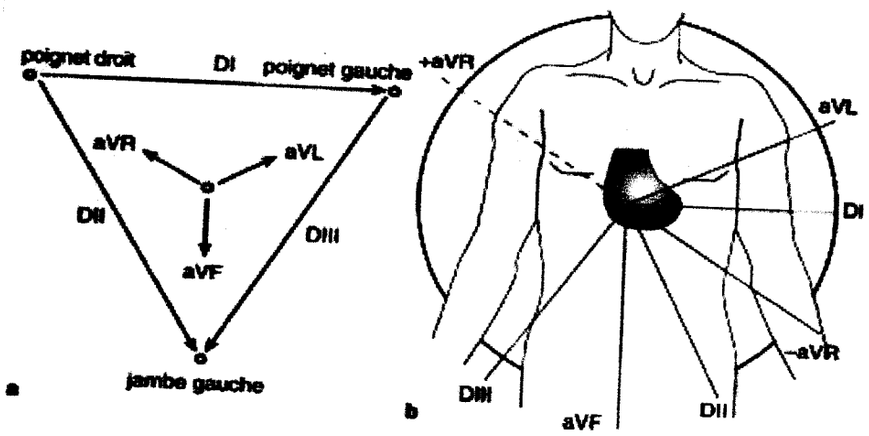


Figure 1.3 Représentation des dérivations frontales (des membres) [9]

5.1.2 Dérivations précordiales (Dérivations horizontales):

La borne centrale de Wilson est le potentiel stable obtenu en reliant par des résistances les 3 électrodes des membres.

Les dérivations précordiales sont aussi, d'un point de vue électro-physiologique, des dérivations unipolaires

- V1 : 4e espace intercostal - bord droit du sternum (+) ; et borne centrale de Wilson (-).
- V2 : 4e espace intercostal - bord gauche du sternum (+) ; et borne centrale de Wilson (-).
- V3 : A équidistance de V2 et de V4.
- V4 : 5e espace intercostal-ligne verticale passant par le mamelon (ou ligne verticale médio-claviculaire) (+) et borne centrale de Wilson (-).
- V5 : 5e espace intercostal à équidistance de V4 et de V6 (+) et borne centrale de Wilson (-).
- V6 : 5e espace intercostal - ligne médio-axillaire (+) et borne centrale de Wilson (-).

Il peut être utile d'ajouter :

- V7, voire V8 et V9 : sur la même « horizontale » que V4, respectivement sur la ligne axillaire postérieure, sous la pointe de l'omoplate, au bord gauche du rachis
- V3R, V4R : symétriques, à droite de V3-V4
- VE (épigastrique) : pointe de la xiphoïde.

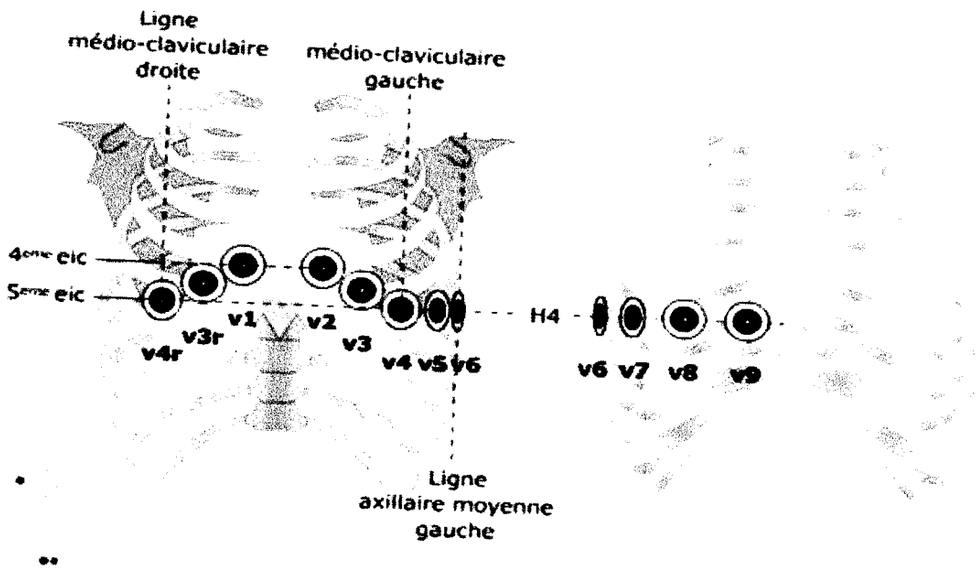


Figure 1.4 Disposition des électrodes d'E.C.G. précordiale [9]

6. Electrocardiogramme d'Holter

Le Holter est un appareil portable développé par le biophysicien Norman Holter en 1961, cet appareil destiné à enregistrer les signaux cardiaques à travers des électrodes sur la surface thoracique en continu sur une période de 24 heures ces enregistrements sont mémorisés sur support numérique (mémoire flash …) ou sur une bande magnétique analogique.

Ce type d'enregistrement permet d'analyser l'évolution dynamique de l'électrocardiogramme.

En effet l'activité électrique cardiaque n'est pas parfaitement stationnaire et l'analyse dynamique des changements du signal électrique du cœur a ouvert une nouvelle approche pour l'évolution des risques d'arythmie cardiaque.

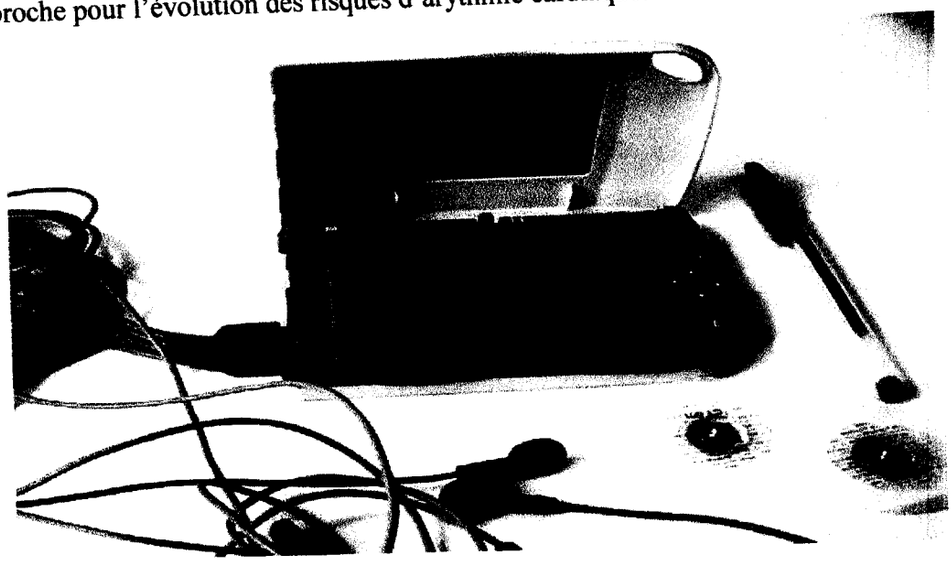


Figure 1.5 électrocardiogramme d'Holter

7. Tracé de l'Electrocardiogramme

Le tracé comprend une onde P, un complexe QRS, une onde T :

7.1 Onde P

L'onde p représente la dépolarisation auriculaire. Les caractéristiques d'une dépolarisation auriculaire normale sont une onde p positive, arrondie, lisse, convexe, d'une durée de 0,05s à 0,10s

Son amplitude est inférieure à 2,5 mm

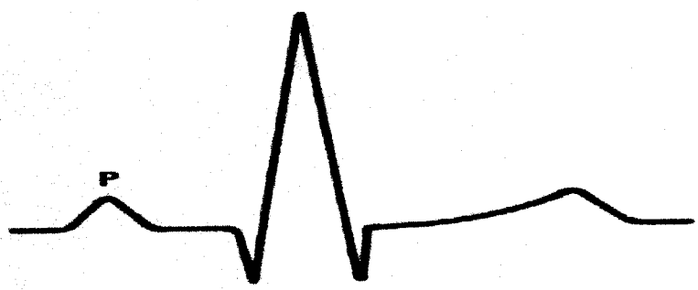


Figure 1.6 Représentation graphique de l'onde P [10]

7.2 Espace PR

C'est un segment isoélectrique qui correspond au temps qui s'écoule pendant la propagation de la dépolarisation partie du nœud sino-atrial et diffusant à travers les atrials jusque vers les ventricules :

Sa durée normale est de 120 à 200 millisecondes, selon l'âge et la fréquence cardiaque : si sa durée est > 200 ms, cela indique un trouble de la conduction entre l'atrium et le ventricule ; si sa durée est <120 ms, c'est que le ventricule se contracte avant d'en avoir reçu l'ordre à partir du nœud sino-atrial : ce n'est plus un rythme sinusal.

7.3Complexe QRS

Le complexe QRS représente la dépolarisation ventriculaire (propagation intra-ventriculaire de la stimulation électrique) il se situe directement après l'onde P dans un tracé normal.

Ce complexe QRS comprend les trois ondes Q, R et S :

7.3.1 Morphologie du complexe QRS

Elle est variable selon les dérivations. Elle reflète les différentes phases de l'activation du myocarde ventriculaire, activation qui peut être décomposée en trois vecteurs principaux, successifs.

• un vecteur septal, de faible amplitude, surtout orienté à droite. Il se dirige vers V1 et V2, où il détermine une petite onde r et fuit D1, aVL, V5, V6, où il donne une petite onde q ;

• un vecteur pariétal, de grande amplitude. La nette prépondérance de la masse ventriculaire gauche explique la direction vers la gauche et en bas de ce vecteur. Il détermine une positivité importante (onde R) en D1, D2, D3 et en précordiales gauches (V4, V5, V6) et une négativité importante (onde S) en V1 et aVR ;

• un vecteur basal, de faibles amplitudes, orientées un peu à droite et en haut. Il en résulte une négativité terminale (inconstante) en D3, V5, V6.

Chez le sujet normal : il faut retenir l'absence d'onde q en précordiales droites, celle-ci n'apparaissant que dans les précordiales gauches, où elle doit rester fine (<0,04s) et peu

profonde. L'onde R croît de V1 à V5, où elle est habituellement maximale, à V6. La dérivation où l'onde R a une amplitude égale à celle de l'onde S est appelée zone de transition, et se situe généralement en V3-V4.

Dans les dérivations frontales, la morphologie est beaucoup plus variable, selon l'axe électrique.

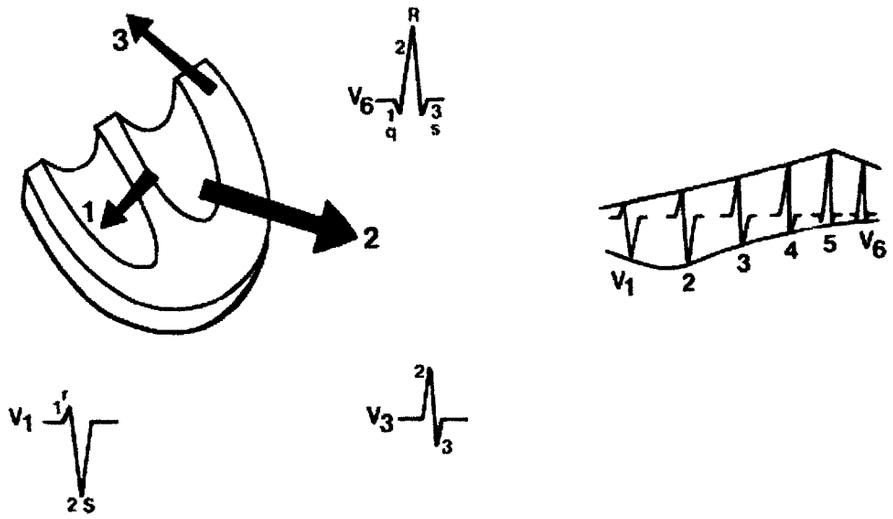


Figure 1.7 la représentation des différentes ondes QRS [10]

7.4 Espace ST

Le segment ST représente la phase initiale de la repolarisation ventriculaire. La transition entre l'onde S (ou fin de R) et le segment ST est appelé point J. le segment ST se situ sur la ligne de base dans les conditions normales ; dans ces cas normales le segment ST ne doit pas dévier de plus 1mm au dessus ou en dessous de la ligne de base (ligne isoélectrique).

7.5Onde T

L'onde T représente la phase finale de la repolarisation ventriculaire, cette phase elle est rapide et efficace. L'onde T elle est généralement asymétrique, arrondie, lisse et positive

Elle est positive dans le cas normal dans toutes les dérivations à l'exclusion d'aVR.

7.6 L'espace QT

Cet espace englobe les deux phases dépolarisation plus repolarisation ventriculaire. Il se commence dés le début des complexe QRS et se termine a la fin de l'onde T.

Le QT est fréquence dépendant, car au cours d'une accélération du rythme cardiaque, dépolarisation et repolarisation sont plus rapides, afin d'augmenter leur efficacité propre

7.7Onde U

Elle est positive et suit l'onde T. Elle est toujours peu ample et mal discernable. Elle est parfois absente. [9] [10]

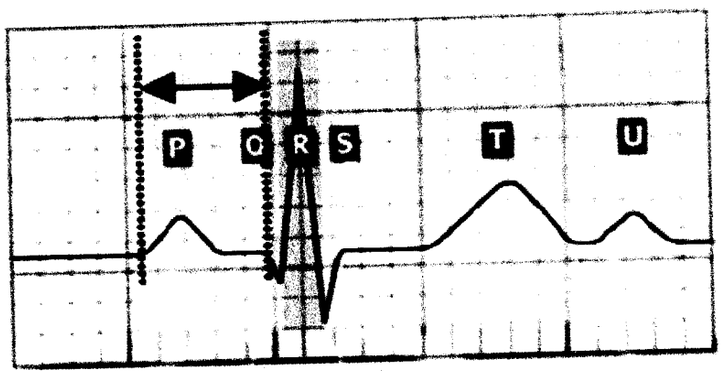


Figure 1.8 Représentation des différentes ondes du signal ECG [9]

Type d'onde	Origine	Amplitude (mV)	Durée (S)
L'onde P	Dépolarisation articulaire	<=0.20	P-R : 0.12-0.22
L'onde R	Repolarisation et dépolarisation ventriculaire	1.60	0.07-0.1
L'onde T	Repolarisation des ventricules	0.1-0.5	Q-T : 0.35-0.44
Intervalle ST	Contraction ventriculaire		S-T : 0.015-0.5
L'onde U	Repolarisation lente de système inerventriculaire.	<0.1	T-U : 0.2

Tableau1.1 tableau des paramètres d'un signal ECG en cas normal.

8. Caractéristiques d'un signal ECG

Le signal ECG a des caractéristiques spécifiques souhaitables pour les système de sécurité. En effet des signaux exacts d'ECG ne sont pas nécessaire, il suffit d'enregistrer seulement des intervalles entre R-R, référencés par la séquence IPI (InterPulse Interval).

8.1. Variation dans le temps

A ce point, il est important de faire la distinction entre les biométrie de temps variable et invariables. Par exemple, la biométrie des empreintes digitales ou des iris ne dépendent pas du temps de mesure, elle est donc basée sur un enregistrement invariable dans le temps.

Par contre, la biométrie basée sur l'ECG est à temps variable car l'ECG varie dans le temps selon l'état dans laquelle se trouve l'individu.

Une meilleur clé cryptographique à besoin d'un niveau important d'aspect aléatoire, et les clés dérivées des signaux aléatoire (à temps variable) permettent d'avoir une sécurité très élevée, tel qu'un intrus ne peut pas prévoir la clé. C'est particulièrement le cas pour l'ECG, puisqu'il est variable dans le temps en changeant avec les diverses activités physiologiques des individus.

8.2. Le temps de synchronisation et la récupération de clé

Pour exposer la fiabilité de la regénération précise au niveau des dispositifs, nous considérons les signaux de la figure 1.9

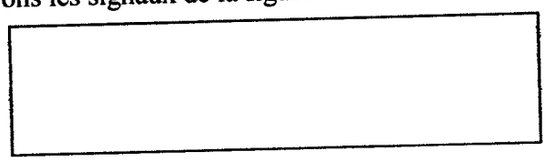


Figure1.9 signaux ECG récupérés à trois emplacements différents.

[biometric methods for secure communications in body sensor networks]D.Hatzinakos,F.M.Bui

Il suffit de se concentrer sur les complexes QRS, en particulier l'onde R, qui représente habituellement les crêtes les plus élevés dans un signal ECG.

Les trois signaux différents sont mesurés simultanément à partir de trois emplacements différents d'électrode, où l'on remarque la forme défirente des complexe QRS pour chaque signal, mais des séquences IPI identiques pour les trois signaux, moyennant une synchronisation appropriée.

Physiologiquement, cette constatation est réelle car trois signaux sont des représentations du même phénomène cardiovasculaire provenant du même cœur, même si les mesures sont prises à des endrois différents du corps.

Par conséquent, afin de récupérer des séquences IPI identiques, la synchronisation s'avère une condition principale à satisfaire.

Ainsi, le système peut imposer le renouvèlement des clés aussi fréquemment que nécessaire pour satisfaire la demande de sécurité élevée de l'application envisagée .

9. Conclusion

Il est très important de connaitre les circonstances dans lesquelles l'électrocardiographie donne des renseignements utiles et celles dans lesquelles elle n'en donne pas, pour cela on a distingué deux domaines où l'électrocardiographie s'est montrée utile et parfois même indispensable :

- Les troubles du rythme : ce groupe d'affections perturbe l'intervalle existant normalement entre la contraction des oreillettes et celle des ventricules.
- Les altérations de la forme de l'électrocardiogramme : ce groupe d'affections perturbe la façon dont les oreillettes et surtout les ventricules se comporte envers la processus d'excitation.

Pour une appréciation valable de l'électrocardiogramme, il est nécessaire de recourir a un enregistrement sur papier calibré de 6 dérivations des membres et de 6 dérivations précordiales.

L'enregistrement standard d'un électrocardiogramme permet la mesure des intervalles de temps (en s ou ms) et d'intensité (en v ou mv) des segments de l'ECG.

Chaque dérivation ECG représente un téritoire spécifique du myocarde :

- ✓ Dérivations inférieures : DII, DIII et aVF
- ✓ Dérivation antérieures : V1-V4
- ✓ Dérivations latérales : DI, aVL, V5,V6. [9]

Chapitre2

1. Introduction

Dû au développement gourmand des systèmes informatiques et réseaux de télécommunication, les besoins en matière de sécurité sont grandissants.D'autre part les entreprises, sont informatisées, et nécessitent une infrastructure sécurisée pour garantir la confidentialité de ses transactions.

La figure suivante présente les niveaux de sécurité selon les différentes portées de l'information.

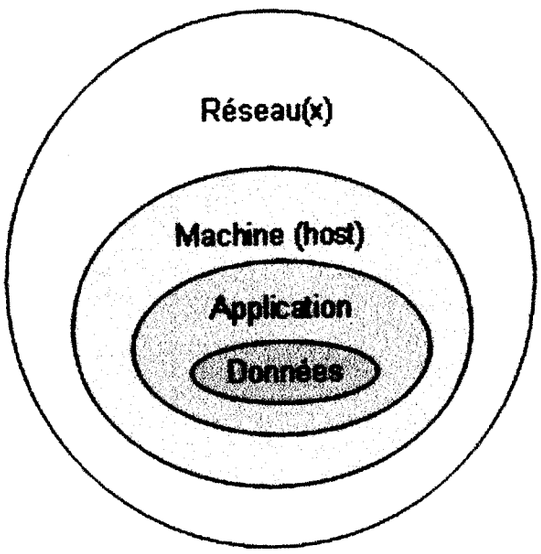


Figure2.1la sécurité à plusieurs niveaux (portée de l'information) [6]

2. Définitions

- Le chiffrement est la transformation d'une information intelligible en une information qui ne pourra pas être comprise par des personnes qui ne seraient pas autorisées à lire cette information.
- L'objectif fondamental de la cryptographie est de permettre à plusieurs personnes de communiquer entre eux à travers un canal de transmission sans qu'aucun opposant ne puisse comprendre ce qu'ils ont échangé.
- L'information qu'une personne X souhaite transmettre à une autre personne Y est appelée texte clair. Elle peut êtresous plusieurs formes (texte, donnée numérique, …).
- Le processus de transformation d'un message M pour le rendre incompréhensible (intelligible) est appelé chiffrement. Le texte chiffré est appelé cryptogramme.
- Le processus inverse c.-à-d.la construction du message clair à partir du message chiffré est appelédéchiffrement.[2]

3. Aspects techniques de chiffrement

Depuis des siècles, de nombreuses méthodes de chiffrement ont été développées pour se protéger de la curiosité et de la malveillance de ses ennemis. On se contente de ne décrire que les méthodes modernes.

Les méthodes de chiffrement modernes se subdivisent en deux grandes classes :

- Méthodes de chiffrement symétrique (chiffrement à clé privé)
- Méthodes de chiffrement asymétrique (chiffrement à clé publique) [9].

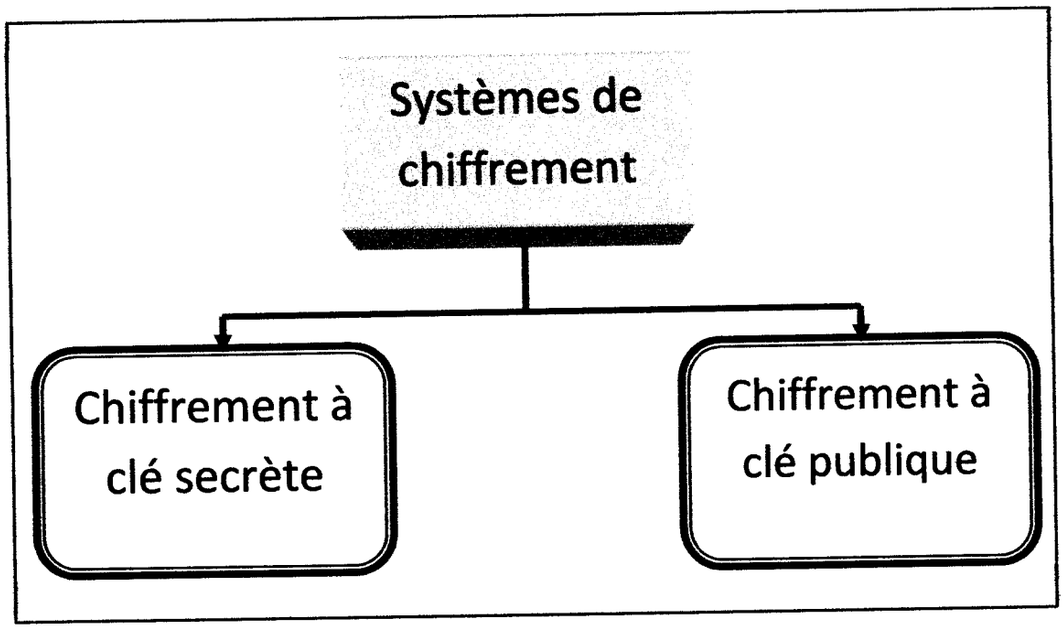


Figure2.3 Principales techniques en cryptographie [9]

3.1 Chiffrement symétrique

Le chiffrement symétrique appelé aussi système à clé secrète ou privé. Une même cléest utilisée pour le chiffrement et le déchiffrement, d'où l'obligation que celle-ci reste confidentielle, sous peine de rendre le système inefficient. [8]

3.1.1 Principe général

Ce type de chiffrement repose sur le partage d'une même clé secrète *k*entre les interlocuteurs. Cette clé sert à chiffrer et déchiffrer les messages échangés.

L'émetteur transmet cette clé k au récepteur à travers un canal de communication d'une façon confidentiel (généralement un canal de communication privé), à ce qu'aucun opposant ne puisse l'intercepter.[6]

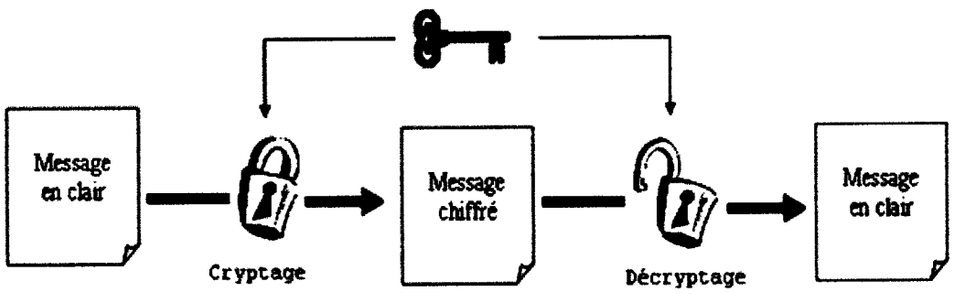


Figure2.4 Représentation du Chiffrement symétrique

Ce type de chiffrement possède plusieurs inconvénients :

- Si la clé secrète est compromise par un opposant, alors tout le système sera compromis.
- Il est très difficile d'implémenter une architecture qui permet une transmission confidentielle des clés secrètes.
- Si une clé différente est utilisée pour chaque paire différents d'utilisateurs des réseaux, le nombre de clés est très important et rend difficile la gestion de celles-ci.

3.1.2 Exemples d'algorithmes de chiffrement symétrique

a. DES (*Data Encryptions S*tandard)

Le DES (standard de chiffrement de données) est un standard depuis les années 70.

Le DES ne chiffre pas les données à la volée quand les caractères arrivent, mais il découpe le texte clair en blocs de 64 bits. Cet algorithme est simple car il combine que des permutations et des substitutions. La clé dans le DESsert à chiffrer et déchiffrer le message à la fois. Elle est de taille de 56bits.

La clé est utilisée pour générer 16 autres clés de 48bits utilisées dans les 16 itérations du DES. [11]

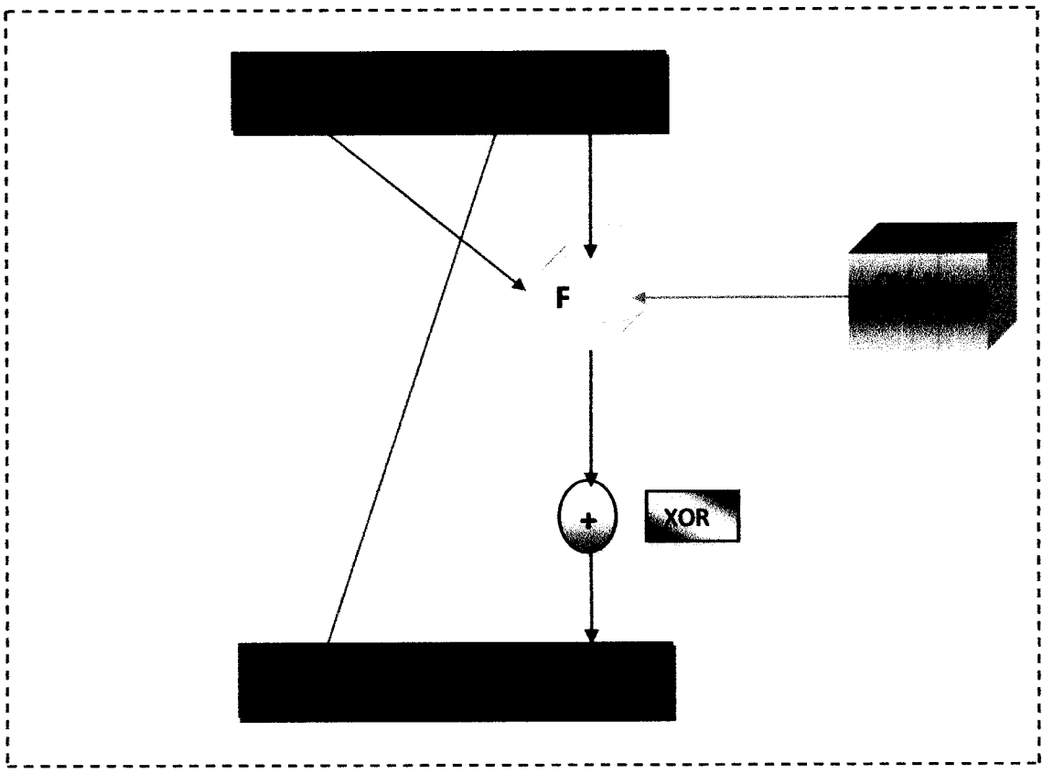


Figure 2.5 Un tour de L'Algorithme DES [11]

La fonction F :

$f: \{0, 1\}^{32} \times \{0, 1\}^{48} \longrightarrow \{0, 1\}^{32}$

$R_{i-1} \quad K_i \longrightarrow f(R_{i-1}K_i)$

C'est une fonction qui se compose de:

Une augmentation E de $Ri-1$ pour en faire un bloc de 48 octets, c'est-à-dire que $E(Ri-1)$ est composé de tous les bits de $Ri-1$, 16 d'entre eux apparaissant deux fois;

On calcule $E(Ri-1)$ Ki, et on le découpe en 8 sous-chaînes de 6 bits.

Chacune des sous-chaînes de 6 bits est transformée par une fonction non linéairefixée en une sous-chaîne de 4 bits.[13]

Les sous-chaînes de 4 bits sont réordonnées suivant une permutation fixée.

b. Triple DES

C'est un algorithme de chiffrement symétrique enchaînant trois applications de l'algorithme DES « d'où l'appellation 3DES » sur un bloc de 64bits en utilisant deux ou trois clés DES différentes. [9]

Le mode d'usage standard est de l'utiliser en mode EDE (Encryptions Décryptions Encryptions).

Le 3DES est formellement écrit par : $C = E^{k3}{}_{DES}\left[D^{k2}{}_{DES}\left(E^{k1}{}_{DES}\left[M \right] \right) \right]$

c. AES (*A*dvanced *E*ncryption *S*tandard)

AES le standard de chiffrement avancé destiné à remplacer le DES qui est devenu trop faible avec la progressionde la puissance des ordinateurs.

Présentation

L'AES a été retenu par le NIST (National Institue of Standard and Technologie) comme un nouveau standard de chiffrement, il est plus puissant et plus sûr que le DES. Il chiffre les blocs de 128bits avec clés varies entre 128, 192 ou 256 bits.[16]

L'AES est un chiffrement itératif effectue plusieurs tours (itérations) d'une même composition de transformation. Le nombre de tours n=10 pour une clé de 128bits et n=14 pour une clé de 256bits. [11]

Avantage

- Plus performant que le DES.
- Plusieurs longueurs de clés et de bloc sont possibles.
- une grande rapidité de traitement (facilité de calcul).
- Flexibilité d'implémentation : adapter à plusieurs plateformes et applications.

- Simplicité : le design de l'AES est relativement simple. [9]

3.2Chiffrement asymétrique

Ce type de chiffrement est appelé aussi système de chiffrement à clé publique. Une bi-clé est utilisée pour le chiffrement et le déchiffrement. Une clé sert au chiffrement et l'autre sert au déchiffrement.

3.2.1 Principe générale

Les algorithmes de chiffrement asymétrique exigent deux clés indépendantes.Donc le destinataire d'un message possède ux clés (bi-clé) l'une privé (secrète) et l'autre publique.

Les données sont chiffrées par la clé publique du destinataire.Le déchiffrement est réaliséà travers la clé secrète correspondante. Cette clé peut être conservée sur une carte à puce ou sur un token USB … [6]

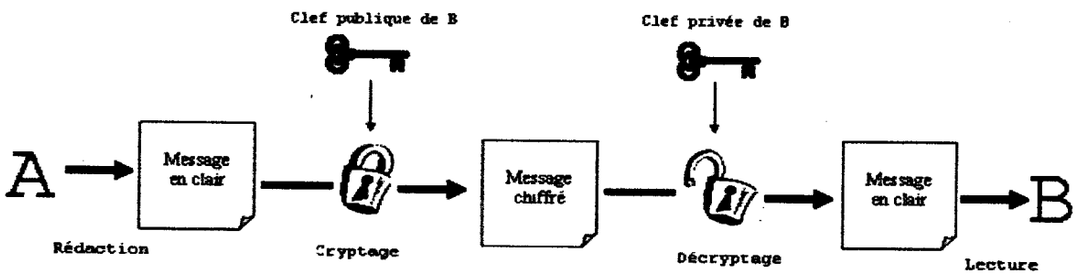


Figure 2.6 Représentation du chiffrement asymétrique

3.2.2 Exemples d'algorithmes de chiffrement asymétrique

a. RSA (RivestShamir Adleman)

Cet algorithme est inventé par Rivest, Shamir et Adleman en 1978. C'est l'algorithme à clé publique le plus commode qui existe. Il est basé sur le calcul exponentiel. Sa sécurité repose sur la factorisation unidirectionnelle suivante, le calcul du produit de deux nombres premiers est aisé. La factorisation d'un nombre en ses deux facteurs premiers est très complexe.[9]

RSA est aujourd'hui utilisé dans une large variété de produits (téléphones, réseaux internet,…), de logiciels de différentes marques (Microsoft, Sun, …) et enfin dans les télécommunications.

Algorithme RSA

- ✓ Détermination des clés :
  - déterminer deux nombres premiers entre eux p et q.
  - calculer $n = p * q$
  - calculer $\Phi(n) = (p-1) * (q-1)$. [2]
  - Choisir un entier e premier (e soit très grand), la clé publique est donc (e, n)
  - Choisir un entier d tel que : $e * d = 1 \bmod (\Phi(n))$, la clé privée sera donc (d, n)[2]
- ✓ Fonction E d'encodage :

le processus de chiffrement est donné par la formule suivante:

$$E_k(M) = M^e \bmod (n)$$

- ✓ Fonction D décodage :

La formule de déchiffrement est la suivante:

$$D_{k'}(E_k(M)) = E_k(M)^d \bmod (n)\ [1]$$

Avantage

- IL est impossible de déduire la clé privé de la clé publique.
- Il n'y a pas un transfert d'un secret (clé) contrairement au chiffrement symétrique.

- Il suffit de connaître la clé publique du correspondant pour lui envoyer un message chiffré, c'est pour ça le nombre de clés nécessaire est réduit. [9]

3.3 Fonction d'Hachage

3.3.1 Définition

Une fonction de hachage H est une application facilement calculable qui transforme une chaîne binaire de taille quelconque « t » en une chaîne binaire de taille fixe « n » ; appelé empreinte de hachage (résumé, ou condensé)

Les propriétés de base d'une fonction de hachage sont la compression et la facilité de calcul.

Pour un usage informatique en cryptographie, une fonction d'hachage doit satisfaire les propriétés suivantes :

- Résistance au calcul de préimage :

Pour tout $y \in h(\{0,1\}^*)$, il doit être calculatoirement difficile de trouver $x \in \{0,1\}^*$ Tel que $h(x) = y$.

- Résistance au calcul de second préimage : étant donné x {0,1}*, il doit être calculatoirement difficile de trouver $x' \neq x$ tel que $h(x) = h(x')$.

Une Fonction de Hachage à sens unique (One – Way – Hash – Function) est une fonction qui satisfait les propriétés de résistance à la préimage et à la seconde préimage. [8]

3.3.2 Utilité d'Hachage

Le but d'un condensé est simple, représenter des données de façon certaine tout en réduisant la taille utile qui sera réellement chiffrée. Prenons l'exemple de la cryptographie asymétrique; tout le monde admet qu'elle est très sure, fiable et durable. Néanmoins, sa complexité (calcul sur des nombres premiers de plusieurs centaines de chiffres par exemple) entraine une inévitable lourdeur d'emploi (charge CPU, etc.). On évite donc de l'utiliser pour de grandes masses de données ou pour des chiffrements de flux.[15]

Par contre imaginez que vous souhaitiez envoyer un fichier par mail, mais que ce fichier est de taille importante. Vous souhaitez de plus rassurer le destinataire sur la provenance de ce fichier (vous) et sur son contenu. Plutôt que de chiffrer votre fichier directement avec votre clé privée, vous aller hacher votre fichier et chiffrer le condensé obtenu avec votre clé privée. Vous enverrez ensuite votre fichier original ainsi que le condensé chiffré (la signature) à votre destinataire. [9]

Celui-ci va, lors de la réception, hacher d'une part le fichier reçu et d'autre part déchiffrer le condensé reçu (au moyen de votre clé publique).

S'il n'y a pas égalité entre les deux résultats, cela signifiera:

- soit que la signature n'est plus la vôtre, donc que quelqu'un a intercepté le fichier (pour le modifier ou le remplacer, etc.)
- soit que le fichier n'est plus le même que l'original (mais la signature n'a pas été remplacée); dans ce cas, la hachage ne peut plus donner le même condensé ce qui conduit au rejet lors du test de comparaison.

Dans les deux cas, ni l'intégrité ni l'authentification du fichier n'ont été vérifiées. Il ne faut donc pas faire confiance au fichier.[14]

Nous voyons comment dans ce cas simple, l'utilisation d'une fonction de hachage permet de s'assurer de l'intégrité des données et indirectement de les authentifier. Il existe bien sûr de nombreuses autres applications pour les fonctions de hachage, comme les MACs (message authentication code), certificats, etc.

3.4 Signaturenumérique et certificat électronique

Les signatures électroniques sont les outils techniquesqui peuvent être utilisés entre des internautes qui se connaissent a priori (ou dont les données ne sont pas importantes) alors que le certificat numérique est la confiancequi permet des échanges entre des internautes qui ne se verront jamais ou dont les données ont de la valeur.[14]

3.4.1 Signature numérique

Depuis longtemps des signatures manuscrites sont utilisées pour prouver l'identité de leur auteur.

Une signature électronique doit garantir deux propriétés : elle doit identifier le signataire du document, et garantir que le document n'a pas été altéré depuis l'apposition de la signature. Pour cela, les caractéristiques suivantes doivent être respectées :

- une signature est authentique. L'identité du signataire doit pouvoir être retrouvée de manière certaine.
- Une signature ne peut être falsifiée (imitée), quelqu'un d'autre ne peut se faire passer pour un autre.
- Une signature n'est pas réutilisable. Elle fait partie du document. Elle n'est pas déplaçable sur d'autre document.
- Un document signé est inaltérable. Le document signé ne peut plus être modifié.
- Une signature ne peut pas être reniée.

Dans les signatures on utilise généralement les cryptosystèmes à clé publique et les fonctions d'hachage à sens unique.

En pratique ce n'est pas le document à transmettre qui est directement signé, mais son empreinte.

C'est la clé privé d'Alice qui est utilisé pour générer la signature d'un document (à partir de son empreinte). On garantit ainsi que seul Alice a pu signer le document ; et on vérifie la validité de la signature grâce à la clé publique d'Alice qui tous le monde peut la connaître.[17]

3.4.2 Certificat électronique

Les certificats électroniques sont utilisés principalement pour assurer l'authentification. Donc le problème a été comment assurer que la clé publique que notre correspondant nous a communiqué est bien celle de la personne physique ou morale qu'il prétend être ?

Le certificat est en quelque sorte une carte d'identité numérique. Pour en obtenir un, il faut s'adresser à une autorité de certification (CertificateAuthority, ou CA).

« Un certificat est un document numérique qui contient toutes les coordonnées d'un interlocuteur utiles pour communiquer avec d'autre, ainsi que sa clé publique ». [14]

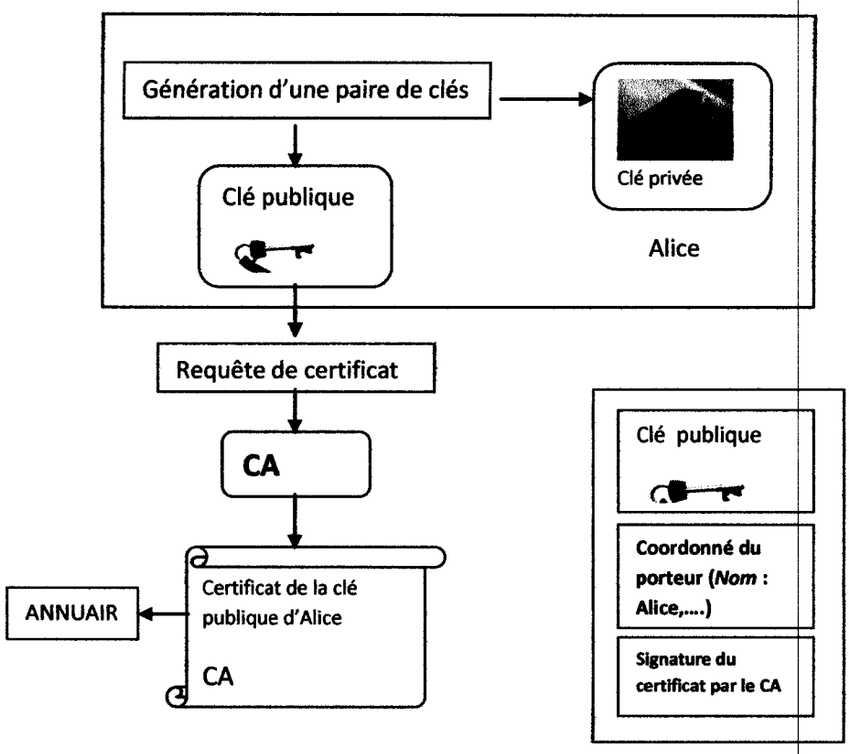


Figure 2.7 Principe de la création des certificats. [7]

Un certificat peut se présenter sous forme physique (carte à puce ou clé USB), ou sous forme logicielle (fichier). Les informations qu'il contient sont séparées en deux parties :

- Le certificat lui-même :
  - L'identité du détenteur du certificat (DN, adresse email, ...).
  - L'identité de l'émetteur du certificat (le CA).
  - Les limites de validité du certificat dans le temps.
  - La clé publique du détenteur, ainsi que l'algorithme de cryptage utilisé.
- La signature de certificat : il s'agit du condensat (hash) de la première partie du certificat, encrypté avec la clé privée du CA. Pour vérifier la validité de ce certificat, il suffit de décrypter sa signature avec la clé publique du CA, et de le comparer avec le condensat de la première partie, que l'on aura calculé auparavant.

3.5 Infrastructure à clé publique (PKI)

3.5.1 Définition

PKI (Public Key Infrastructure) est un système de gestion des clefs publiques qui permet de gérer des listes importantes de clefs publiques. Une PKI est donc un ensemble de technologies, organisations, procédures et pratiques qui supportent l'implémentation et l'exploitation de certificats basés sur la cryptographie à clé publique. [8]

3.5.2 Architecture d'une PKI

Dans une infrastructure à clé publique, pour obtenir un certificat numérique, l'utilisateur fait une demande auprès de l'autorité d'enregistrement. Ce dernier génère un couple de clé (clé publique, clé privée), envoie la clé privée au client, applique une procédure et des critères définis par l'autorité de certification qui certifie la clé publique et appose sa signature sur le certificat, parfois fabriquépar un opérateur de certification.[8][9]

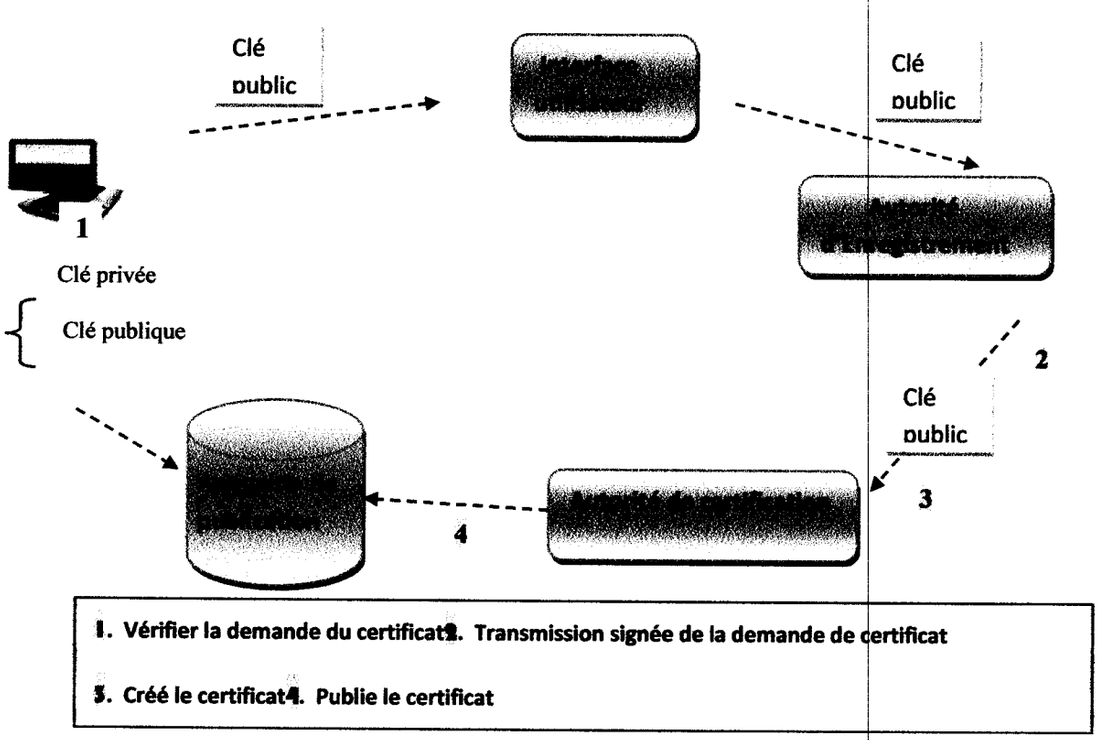


Figure2.8 Architecture d'infrastructure PKI [13]

4 Conclusion

Dans cette partie, nous avons abordé les standards de chiffrement modernes qui se classent en deux groupes, chiffrement symétrique et chiffrement asymétrique. Le DES est un exemple de standard de chiffrement moderne symétrique, mais actuellement ce standard est devenu obsolète. Des nouveaux standards sont mis en place afin de remplacer DES et répondre aux besoins contemporains.

RSA, présente un bon standard de chiffrement moderne asymétrique car il a résisté à toutes les attaques. Sa résistance est liée fortement au problème de la factorisation de grands nombres premiers.

La cryptographie asymétrique ou appelée encore cryptographie à clé publique nécessite une bonne gestion de clé; pour cela une structure appelée la PKI s'est construite pour jouer le rôle. Une PKI est une infrastructure à la fois technique et administrative. Le domaine des PKI est intéressant, il est possible de les utiliser pour des applications tels que mail chiffré, web sécurisé VPN.

Les deux standards de chiffrement (symétrique/asymétrique) sont utilisés conjointement. Les systèmes asymétriques sont utilisés pour transporter les clés secrètes, car les processus de chiffrement/déchiffrement dans les systèmes symétriques sont plus rapides que ceux dans les systèmes asymétriques.

Le chapitre suivant sera consacré à la présentation des codes auto correcteur d'erreur et notamment les codes de Reed Solomon.

Chapitre3

CHAPITRE3: LE CODE AUTO CORRECTEUR D'ERREUR REED SOLOMON

1. Introduction

Les techniques numériques sont à nos portes, leur utilisation s'étend et touche les domaines du son, de la vidéo et des données. Il n'y a plus de supports dédiés, l'acheminement du son, de la vidéo et des données en général se fait en empruntant des médiums divers (câble, hertzien, RTC, satellite, . . .). Ces médias pouvant être considérés comme imparfaits, cela peut entraîner une modification du message émis. L'imprévisibilité du message émis par la source impose alors au récepteur l'utilisation de techniques lui permettant de vérifier à la fois l'exactitude et la certitude de l'information reçue. Afin de diminuer le taux d'erreurs dans le message, des symbolessont rajoutés au message suivant une loi connue à la fois de l'émetteur et du récepteur. Deux types de techniques existent (figure 3.1):

- une technique qui détermine uniquement si le message reçu est entaché d'erreurs. On parle alors de codes détecteurs d'erreurs. Comme il n'y a que détection des erreurs, cela entraîne une retransmission du code reçu faux détecté comme tel.
- Une technique qui permet de détecter et corriger (dans une certaine mesure) les erreurs présentes dans le message. On parle de codes détecteurs correcteurs d'erreurs.[25]

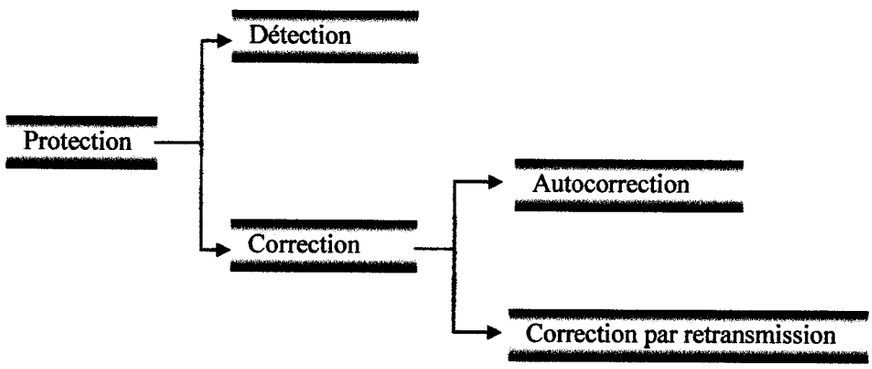


Figure 3.1 Schéma de protection contre les erreurs[28]

2. Principe des codes auto correcteurs d'erreurs

Le principe consiste à:

- Choisir un alphabet fini F de cardinal q et on représente l'information comme une suite d'éléments de F.
- Découper la suite obtenue en blocs de longueur fixe k.
- Un message m sera un bloc de longueur k:

$$m := (m_1 \dots m_k) \in F^k$$

L'ensemble F^kest l'espace des messages. Le nombre maximum de messages différents possiblesest égal à q^k. On peut aussi supposer que l'espace des messages est un sous-ensemble M de F^k; dans ce cas le nombre maximum de messages différents possibles est égal à $|M|$.

Si on transmet le message m par le canal de transmission et si ce message arrive à destination avec des erreurs, le récepteur ne pourra pas le restituer correctement.

- ✓ Donc,nécessité d' encoder le message avant de le transmettre.
- La phase d'encodage consiste à rajouter une redondance au message à envoyer.

Le processus d'encodage est une application injective E

$E: F^k \rightarrow F^n$

$m = (m_1 \dots m_k) \rightarrow c = (c_1 \dots c_n)$;

- ✓ On transmet c (et non m) via le canal de transmission.[26]

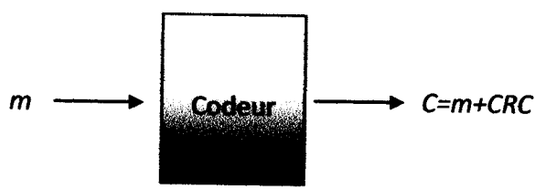


Figure3.2 Phase d'encodage[26]

- La phase de décodage consiste à restituer le message original *m* du message.[29]

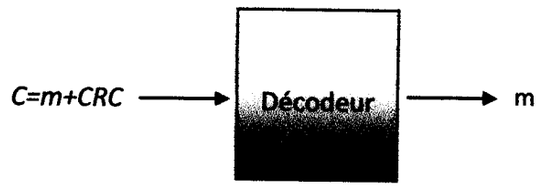


Figure3.3 Phase de décodage [26]

3. Types de codes

3.1 code en bloc

Un code (k, n)transforme tout bloc initial de *k* bits d'information en un bloc codé de *n* bits.

Le code introduit une redondance puisque n >= k. Le code est systématiquesi les *k* premiers bits du bloc codé sont égaux aux bits du bloc initial. Alors les *r* (r=n-k) derniers bits forment un champ de contrôle d'erreur. Le rendementd'un code (k, n) est : R = k/n

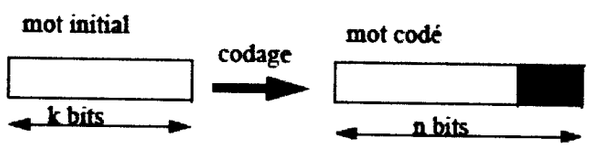


Figure3.4 Schéma du codage[18]

On appelle mot du code, la suite de *n* bits obtenue après un codage (k, n). Le nombre *n* de bits qui composent un mot du code est appelé la longueur du code. La dimension*k* étant la longueur initiale des mots.[26]

3.1.1 Code linéaire

Faire correspondre a chaque mot d'information un mot de code, par une fonction linéaire, facilite la construction du code aussi bien que le contrôle des messages reçus. Les codes linéaires sont des codes par blocs construits a l'aide d'une telle fonction.

a. Définition

Tout codage revient a définir une application f de B^k dans B^n, appelée fonction de code, évidemment injective, puisqu'un mot de code ne peut être l'image que d'un seul mot d'information.

Un code défini par une fonction de codage linéaire de B^k dans B^n est appelé linéaire.

- ✓ n est la longueur du code
- ✓ k est sa dimension comme sous-espace vectoriel de Bn.

Un code linéaire se notera en indiquant ces deux paramètres : $C_{n,k}$. [24]

b. Matrice génératrice

Soit C un code linéaire, une matrice génératrice de C est une matrice dont les lignes forment une base de C. Une matrice génératrice G est donc de taille k×n et de rang k.

Si m est un vecteur ligne de F_2^k, le produit m.G est un mot de code C et l'application m⟶m.G est un isomorphisme de F_2^ksur C. Si la matrice G est de la forme (I_k,P), on dit que le codage est systématique, les k premiers bits du mot de code portent l'information et les n-k suivants forment la redondance.

c. Matrice de contrôle

Soit C un code linéaire, une matrice de contrôle de C est la matrice d'un système d'équation linéaire dont les espace de solution est C. Autrement dit, une matrice de contrôle H est de taille (n-k)×n et de rang n-k.

$C = \{x \in F_2^n ; H^t \times x = 0\}$.[27]

4. Le code de Reed-Solomon

Le code de Reed-Solomon est un code de détection et de correction des erreurs. Il est un code en bloc, linéaire et cyclique.

Le code RS traite des mots (messages) de champs de Galois.

4.1 Champs de Galois (GF)

Les « champs de Galois » font partie d'une branche particulière des mathématiques qui modélise les fonctions du monde numérique. Ils sont très utilisés dans la cryptographie ainsi que pour la reconstruction des données.

Il y a deux types de champs, les champs finis et les champs infinis. Les « champs de Galois » finis sont des ensembles d'éléments fermés sur eux-mêmes. L'addition et la multiplication de deux éléments du champ donnent toujours un élément du champ fini.

4.2 Eléments des champs de Galois

Un champ de Galois consiste en un ensemble de nombres, ces nombres sont constitués à l'aide de l'élément base α comme suit :

$0, 1, \alpha, \alpha_2, \alpha_3 \ldots \alpha^{N-1}$

En prenant $N = 2^m - 1$, on forme un ensemble de 2^méléments. Le champ est alors noté$GF(2^m)$.[19]

$GF(2^m)$ est formé à partir du champ de base $GF(2)$ et contiendra des multiples deséléments simples de $GF(2)$.

En additionnant les puissances de α, chaque élément du champ peut être représenté parune expression polynomiale du type :

$$\alpha_{m-1}x^{m-2} + \alpha_{m-2}x^{m-2} + \ldots + \alpha x + \alpha_0$$

Sur les « champs de Galois », on peut effectuer toutes les opérations de base. L'additiondans un champ fini $GF(2)$ correspond à faire une addition modulo 2, donc l'addition detous les éléments d'un « champ de Galois » dérivés du champ de base sera

une additionmodulo 2 (XOR). La soustraction effectuera la même opération qu'une addition, c'est-à-dire,la fonction logique « XOR ».

La multiplication et la division seront des opérations modulo « grandeur du champ », doncmod (2^m-1).[29]

4.3 Opérations dans les champs de Galois

4.3.1 Addition dans les champs de Galois

Considérons le tableau ci-dessous dans lequel' on fait l'addition binaire entreles deux éléments A et B du $GF(2)$:

A	B	Reste	Résultat
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	0

Tableau 3.1 Addition dans $GF(2)$

En négligeant le reste dans le résultat final de l'addition, on constate que la somme entredeux éléments dans un $GF(2)$ donne une addition modulo 2, c'est-à-dire, une fonction logique « XOR ». Comme $GF(2)$ est le champ de base, cette relation sera valable pourtous leschamps dérivés, c'est-à-dire, pour $GF(2^m)$.

4.3.2 Soustraction dans le champ de Galois

Considérons le tableau suivant dans lequel on fait la soustraction binaire entre les deux éléments A et B :

A	B	Emprunte	Résultat
0	0	0	0
0	1	1	1
1	0	0	1
1	1	0	0

Tableau 3.2 Soustraction dans *GF* (2)

On constate que la soustraction dans GF (2) effectue la même opération que l'additiondans le même champ, c'est-à-dire une opération logique « XOR ».[29]

4.4 Construction d'un champ de Galois

Les champs de Galois sont construits à partir d'un polynôme primitif. Tous les élémentsnon nuls du champ peuvent être construits en utilisant l'élément α comme racine dupolynôme primitif. Chaque *GF*a peut être plusieurs polynômes primitifs $p(x)$, mais dansle tableau ci-dessous, on mentionne seulement les polynômes ayant le moinsd'éléments.

m	$P(X)$	m	$P(X)$
3	$1+X+X^3$	14	$1+X+X^6+X^{10}+X^{14}$
4	$1+X+X^4$	15	$1+X+X^{15}$
5	$1+X^2+X^5$	16	$1+X+X^3+X^{12}+X^{16}$
6	$1+X+X^6$	17	$1+X^3+X^{17}$
7	$1+X^3+X^7$	18	$1+X^7+X^{18}$
8	$1+X^2+X^3+X^4+X^8$	19	$1+X+X^2+X^5+X^{19}$
9	$1+X^4+X^9$	20	$1+X^3+X^{20}$
10	$1+X^3+X^{10}$	21	$1+X^2+X^{21}$
11	$1+X^2+X^{11}$	22	$1+X+X^{22}$
12	$1+X+X^4+X^6+X^{12}$	23	$1+X^5+X^{23}$
13	$1+X+X^3+X^4+X^{13}$	24	$1+X+X^2+X^7+X^{24}$

Tableau 3.3 polynômes primitifs dans $GF(2^m)$

Exemple de construction d'un GF(2^4)

On veut construire tous les éléments du *GF* (24) à partir du polynôme primitif :

$$p(x) = x^4 + x + 1$$

L'élément α est racine du polynôme primitif,donc:

$$p(\alpha) = \alpha^4 + \alpha + 1$$

$$\alpha^4 = \alpha + 1$$

Maintenant, il suffit de multiplier l'élément α par α à chaque étape et réduire par rapportà $\alpha^4 = \alpha + 1$ pour obtenir le champ complet. On aura besoin de 13 multiplications pourcompléter le champ.

Les éléments d'un « champ de Galois » de GF(2^4) sont :

Elements	Formes polynomiales	Formes binaires	Formes decimales
0	0	0000	0
1	1	0001	1
α	α	0010	2
α^2	α^2	0100	4
α^3	α^3	1000	8
α^4	$\alpha+1$	0011	3
α^5	$\alpha^2+\alpha$	0110	6
α^6	$\alpha^3+\alpha^2$	1100	12
α^7	$\alpha^3+\alpha+1$	1011	11
α^8	α^2+1	0101	5
α^9	$\alpha^3+\alpha$	1010	10
α^{10}	$\alpha^2+\alpha+1$	0111	7
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110	14
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111	15
α^{13}	$\alpha^3+\alpha^2+1$	1101	13
α^{14}	α^3+1	1001	9

Tableau 3.4 les éléments de GF(2^4)

4.6 Technique de codage de Reed Solomon

Considérons un code de Reed-Solomon avec ses symboles dans $GF(2^k)$, où k est le nombre de bits par symbole.

L'équation clé définissant le codage systématique de Reed – Solomon(n,k) est :

$c(x) = i(x)\, x^{n-k} + [\, i(x)\, x^{n-k}]$ modulo $g(x)$

$r(x) = [i(x)\, x^{n-k}]$ modulo $g(x)$

Avec:

c(x) :polynôme du mot-code, degré $n-1$

i(x) :polynôme d'information, degré $k-1$

r(x) : polynôme de contrôle, degré $n-k-1$

g(x) : polynôme générateur, degré $n-k$

Le codage systématique signifie que l'information est codée dans le degré élevé du mot-codeet que les symboles de contrôle sont introduits après les mots d'information.

Une autre méthode de codage consiste à multiplier le polynôme d'information par la matrice génératrice.Cette dernière est générée à partir du polynôme générateur de la façon suivante:[29][24]

Soit $g(x) = g_{n-k}\, x^{n-k} + \ldots g_1 x + g_0$

$$G = \begin{pmatrix} g_{n-k} \ldots\ldots\ldots\ldots g_1\ g_0\ 0 \ldots\ldots\ldots 0 \\ 0\ g_{n-k} \ldots\ldots\ldots\ldots g_1\ g_0\ 0 \ldots\ldots 0 \\ \vdots \\ 0 \ldots\ldots\ldots\ldots g_{n-k} \ldots\ldots g_1\ g_0 \end{pmatrix}$$

Exemple:

Prenons le message : x = { 1 , 2 , 3} dans un code de Reed Solomon RS(7,3)

La longueur du code N égal 7 , la longueur du message à transmit K égal 3 donc la longueur de la redondance sera (N – K) égal à 7-3 = 4.Le polynôme générateur associé est:

$$p(x) = x^4 + 3x^3 + x^2 + 2x + 3$$

La matrice génératrice Gsera donc construite à partir du polynôme générateur :

$$G = \begin{matrix} 1 & 3 & 12 & 3 & 00 \\ 0 & 1 & 31 & 2 & 30 \\ 0 & 0 & 13 & 1 & 23 \end{matrix}$$

Par élimination de gausse, on transforme la matrice G en une matrice composée de deux matrices I et L avec:

I= matrice identité de dimension K* K

L = matrice de dimension (N - K) * K

$$G' = \begin{matrix} 1 & 0 & 0 & 6 & 1 & 6 & 7 \\ 0 & 1 & 0 & 4 & 1 & 5 & 5 \\ 0 & 0 & 1 & 3 & 1 & 2 & 3 \end{matrix}$$

Le codage de l'information est obtenu par multiplication du message avec la matrice G'.

$$y = x * G' = 1,2,3 * \begin{matrix} 1 & 0 & 0 & 6 & 1 & 6 & 7 \\ 0 & 1 & 0 & 4 & 1 & 5 & 5 \\ 0 & 0 & 1 & 3 & 1 & 2 & 3 \end{matrix}$$

y est le mot code à envoyer, y= {1, 2, 3, 0, 0, 1, 3}

On remarque quele mot code y est composédu message x = {1,2,3} et de la redondance {0,0,1,3}.

4.7 Technique du décodage

L'idée de base du décodeur de Reed – Solomon est de détecter une séquence erronée avec peu de termes, qui sommée aux données reçues, donne lieu à un mot-code valable.

Plusieurs étapes sont nécessaires pour le décodage de ces codes :

Calcul du syndrome

Calcul des polynômes de localisation des erreurs et de d'amplitude

Calcul des racines et évaluation des deux polynômes

Sommation du polynôme constitué et du polynôme reçu pour reconstituer l'information de départ sans erreur.[25]

Le schéma de décodage est montré dans la figure ci-dessous :

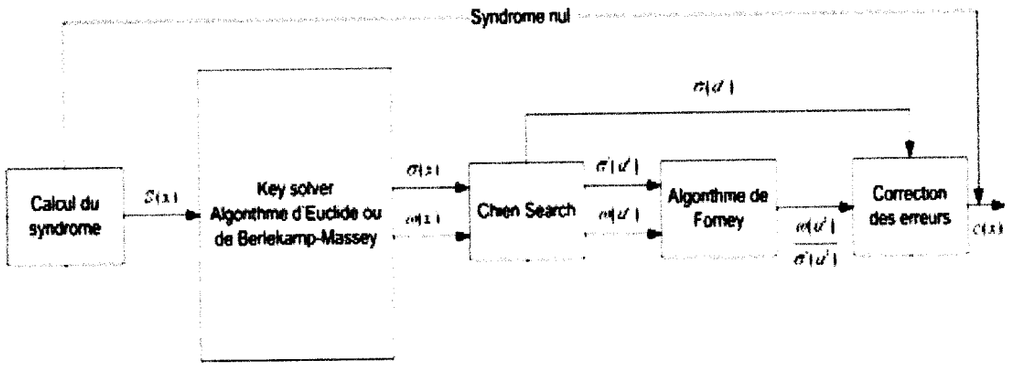


Figure 3.6schéma du décodage

Avec :

r (x) : mot-code reçu

S (x) : syndrome calculé

ω (x) : polynôme d'amplitude des erreurs

ω (α i) : polynôme d'amplitude des erreurs évalué pour tous les éléments dans GF (2^m)

σ (x) : polynôme de localisation des erreurs

σ (α i): polynôme de localisation des erreurs évalué pour tous les éléments dans GF (2^m)

$\sigma'(\alpha$ i) : dérivée du polynôme de localisation des erreurs évalué pour tous les éléments compris dans GF (2^m)

ω (α i)/ σ '(α i) : division entre le polynôme d'amplitude et la dérivée du polynôme de localisation des erreurs

c (x) : mot-code reconstitué[29]

4.7.1 Euclide :

a. Généralité du théorème d'Euclide :

L'algorithme d'Euclide est un algorithme récursif qui permet de trouver le plus grand diviseur commun de deux polynômes r0 (x) et r1 (x) dans le « champ de Galois » GF (q).

Il existe deux polynômes a (x) et b(x) en GF (q) tels que :

$$PGCD\ (r0\ (x), r1\ (x)) = a(x)\ r0\ (x) + b(x)\ r1\ (x)$$

Avec :

a(x) et b(x) peuvent être calculés selon l'algorithme d'Euclide.

En donnant deux polynômes non nuls r0 (x) et r1(x) en GF(q), l'algorithme d'Euclide fonctionne de la façon suivante :

$deg(r1(x)) \leq deg(r0(x))$

$a0(x) = 1, b0(x) = 0$

$a1(x) = 0, b1(x) = 1$

Pour i ≥ 2, on calcule le quotient qi (x) et le polynôme restant ri(x), la division est effectuée sur ri-2(x) et ri-1(x).

$$ri\text{-}2(x) = qi\ (x)\ ri\text{-}1(x) + ri(x)$$

Avec :

$$0 \leq \deg(ri(x)) < \deg(ri\text{-}1(x))$$

$$ai(x) = ai\text{-}2(x) - qi(x)\ ai\text{-}1(x)$$

$$bi(x) = bi\text{-}2(x) - qi(x)\ bi\text{-}1(x)$$

Les calculs se terminent lorsque deg (ri) = 0, le dernier polynôme non nul indique le plus grand diviseur commun. [24]

b. Correction d'erreurs avec Euclide

Le polynôme de localisation des erreurs est défini comme :

$$\sigma\ (x) = \prod_{k-1}^{v}(1 - \alpha^{ik}x)$$

$$= \sigma vxv + \sigma v\text{-}1xv\text{-}1 + \ldots + \sigma 1x + 1$$

Le polynôme d'amplitude des erreurs se calculera de la suivant façon :

$$\omega(x) = S(x)\ \sigma(x)$$

Avec :

σ (x) : polynôme de localisation des erreurs, inconnu à ce stade

ω (x) : polynôme d'amplitude, inconnu à ce stade

S (x) : polynôme syndrome, connu

Comme on connait seulement 2t symboles du polynôme du syndrome (x0... x2t-1), on devrait limiter le résultat à 2t :

$$S\ (x)\sigma\ (x) = \omega\ (x) \bmod (x2t\ )$$

Cette expression est l'équation clé pour les codes de Reed – Solomon. Si le nombre d'erreurs v dans le mot-code transmis c (x) est plus petit ou égal à t , l'équation clé a une seule paire de solutions σ (x) et ω (x) . Les deux degrés des polynômes doivent respecter la contrainte qui suit :

$$\deg(\omega(x)) < \deg(\sigma(x)) \leq t$$

L'équation clé peut être résolue selon l'algorithme d'Euclide en appliquant r0(x) = x2t et r1(x) = S(x). Le calcul du théorème d'Euclide nous donnera comme solution le polynôme de localisation des erreurs et le polynôme d'amplitude. L'algorithme d'Euclide, pour le calcul du polynôme de localisation des erreurs et le polynôme d'amplitude, est montré dans la figure suivante.[29]

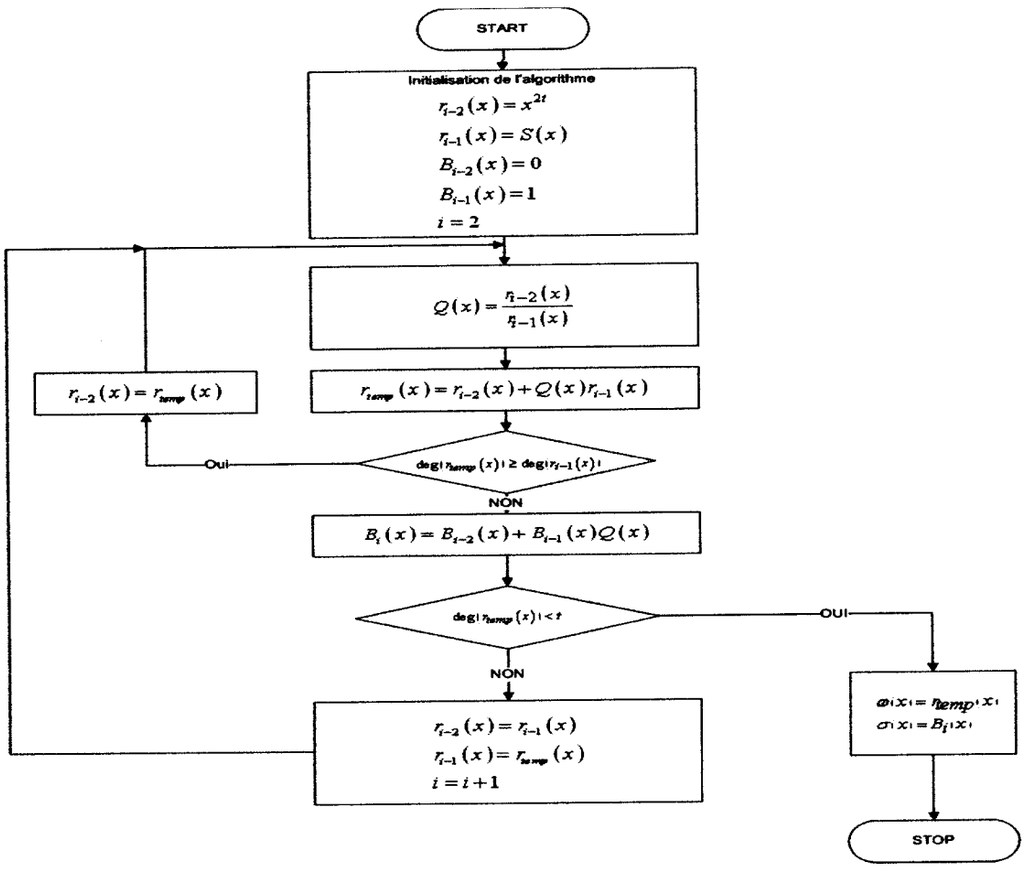


Figure 3.7algorithme d'Euclide pour le calculant du polynôme de localisation et pour le polynôme d'amplitude.

Le dernier reste de la division nous donnera le polynôme d'amplitude. Le polynôme de localisation des erreurs est donné selon la relation :

$$\sigma i\ (x) = \sigma i\text{-}2\ (x) + \sigma i\text{-}1\ (x)\ Qi(x)$$

Avec : $\sigma i\ (x) = Bi\ (x)$

La théorie montre que l'on est obligé d'avoir deux blocs dans l'implémentation.

Un bloc qui effectue la division et qui donnera le polynôme d'amplitude des erreurs, et également un bloc de multiplication qui donnera le polynôme de localisation des erreurs.

4.7.2 Chien Search :

Une fois le polynôme de localisation des erreurs calculé, on doit évaluer ses racines et sa dérivée.

L'évaluation des racines est effectuée avec l'algorithme appelé « Chien Search » qui est du type « brute force », c'est-à-dire, qu'il évalue toutes les possibilités. Par exemple pour un RS(7,3), on évalue le polynôme de localisation des erreurs et sa dérivée pour tous leséléments du « champ de Galois » GF (2^3), sauf pour l'élément nul.

A la sortie de ce bloc, on obtiendra une séquence de symboles. Lorsque les symboles sont nuls, ceux-ci nous indiqueront qu'une racine a été détectée.[29]

4.7.3 Algorithme de Forney :

Cet algorithme permet de construire le polynôme d'erreurs e (x) à additionner avec le polynôme reçu r (x) pour reconstituer le polynôme c (x). Pour le calcul du polynôme e (x), les polynômes $\sigma\ (\alpha^i)$, $\sigma'\ (\alpha^i)$, $\omega\ (\alpha^i)$ sont nécessaires. Le polynôme de localisation des erreurs et sa dérivée sont déjà évalués pour les différentes valeurs de α, il nous reste à évaluer $\omega\ (\alpha\ i)$.

Une fois les différentes valeurs de $\omega(\alpha^i)$ calculées, on applique l'algorithme de Forney. Cet algorithme est défini comme : [29]

$$e_i = w(\alpha^i) / \sigma'(\alpha^i)$$

Avec :

$\omega(\alpha^i)$: polynôme d'amplitude évalué pour les valeurs de GF (2^4)

$\sigma'(\alpha^i)$: dérivée du polynôme de localisation des erreurs pour les valeur GF (2^4)

5. Avantages des codes de Reed-Solomon

- ✓ Pour des corps de Galois GF(q), lorsque l'on a besoin de coder des messages de longueur inférieur à q, l'encodage de RS est facilement utilisable.
- ✓ Ils peuvent être combiné ou ajouté à autres codes afin de réaliser des codes plus efficaces.
- ✓ L'encodage est assez facile.
- ✓ Ils sont très efficaces pour la correction d'erreurs consécutives, qu'ils soient utilisés seuls ou en conjonction avec d'autres codes. Bien entendu, cela est valide pour les cas où le nombre d'erreur demeure en deçà de la capacité de correction du code employé.
- ✓ Leurs algorithmes de décodages sont très développés.
- ✓ Pour des corps de Galois GF (q = 2r), on peut les représenter par des codes binaires puisque chacun des éléments de ce corps de Galois peuvent être représenté par une séquence binaire de longueur r. [26]

6. Conclusion

Dans ce chapitre et en premier lieu, les codes auto correcteurs d'erreurs sont présentés. Ces derniersinterviennent dans divers domaines d'applications et notamment dans le domaine de la cryptographie.

En deuxième lieu, nous avons présenté les codes auto correcteurs de Reed Solomon. Ces codes sont très efficaces et très utilisés dans divers domaines d'application.

Au chapitre suivant, nous allons décrire notre méthode de génération de clés cryptographiques à partir du signal ECG en se basant sur les codes auto correcteur de Reed Solomon.

Chapitre4

1. Introduction

Jusqu'à présent, des systèmes de sécurité qui s'appuis sur l'empreinte digitale, l'iris…etc ; ne dépendent pas de temps, donc la clé généré sera unique pour l'individu, par contre les systèmes qui utilisent le signal ECG dépendent des facteurs spatio-temporels, les clés générés pour un seul individu seront renouvelables.

Dans le cadre de ce projet, nous allons générer des clés cryptographiques de taille de 128 bits à partir des séquences RR du signal ECG.

Selon [30], la distance de Hamming intra personne est de 22 bits et celle inter personne est de 90 bits (fig.4.1).

Dans notre projet, nous avons exploité les signaux ECG de la base de données MIT-BIH pour la génération des clés cryptographiques. Le mécanisme de génération de clés est donné par la figure Fig4.2.

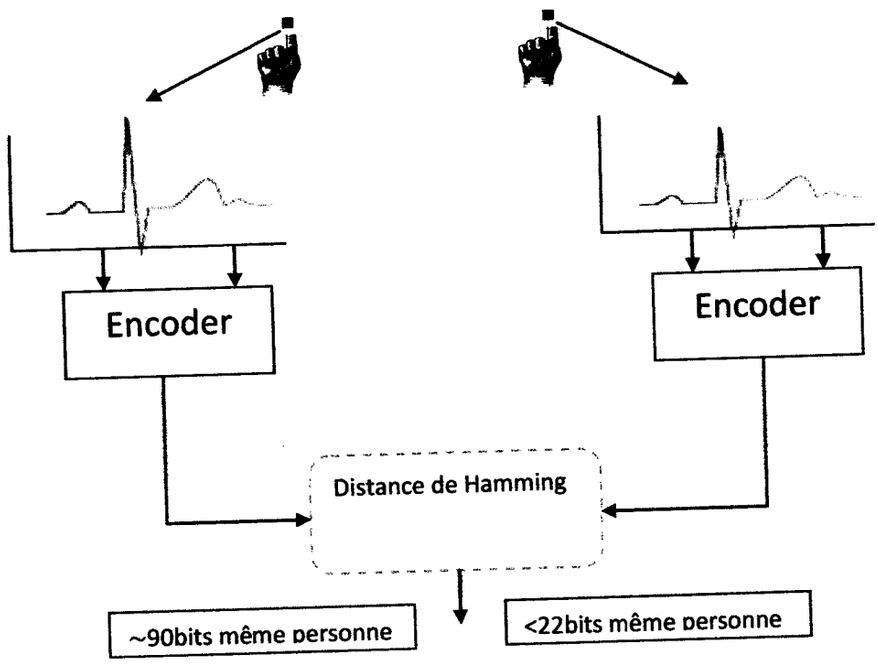


Figure 4.1 Distance de hamming intra et inter personne[24]

2. Schéma de génération de clés

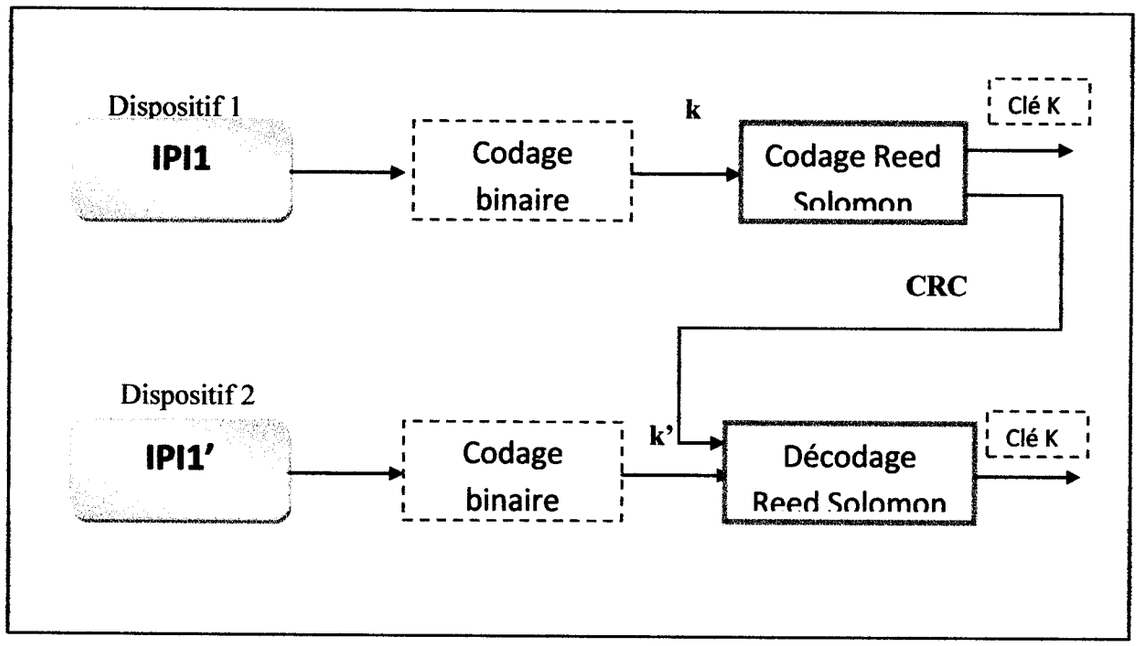


Figure4.2 Génération des clés cryptographiques à partir des IPI

3. Explication du processus de la génération des clés

3.1 IPI (Inter Pulse Interval) : les valeurs de temps entre les intervalles RR.

Figure 4.3 Représentation simplifié d'un IPI[24]

3.2 Codage Binaire

Cette étape consiste à coder les valeurs des IPI en une séquence de 128 bits. Il existe également une méthode basée sur une observation rythmique des battements de cœur. Pour cela, on code la variation de durée des intervalles RR par des nombres: « 0 » quand la durée est réduite, ou elle ne change pas, « 1 » quand la durée s'allonge. [Web11]

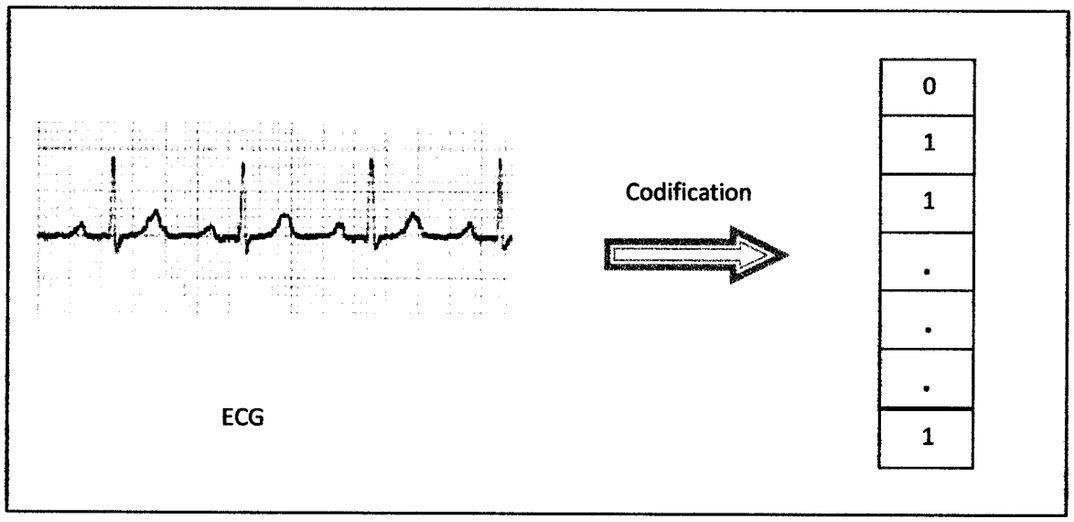


Figure 4.4 Codification des IPI du signal ECG en un vecteur 128 bits

3.3 Codage Reed Solomon

Cette étape consiste à coder la clé k (la séquence de 128 bits) générée dans l'étape précédente en appliquant le codage matricielle de Reed Solomon.

☑ Choix des paramètres

Le choix des paramètres de tel code dépend du nombre d'erreurs qu'on veut corriger.

Dans notre cas, le nombre d'erreurs égale à 22 bits. Donc le choix des paramètres de notre code sera comme suit:

- ✓ n= 63
- ✓ k= 55

Justification de notre choix:

RS (n, k)=RS(63,55) : n indique la longueur totale d'un bloc de Reed – Solomon, c.à.d. 63 symboles dans ce cas et k indique la longueur du bloc d'information, c.à.d. 55 symboles.

La capacité de correction des erreurs du système est:

$$2t = n - k = 63 - 55 = 8$$

$$t = \frac{n-k}{2} = \frac{63-55}{2} = 4$$

Ce code permettra de corriger 4 symboles. Le nombre de bits m par symbole est :

$$n = 2^m - 1$$

$$m = \frac{\ln(n+1)}{\ln(2)} = \frac{\ln(64)}{\ln(2)} = 6$$

Le nombre de bits utilisés pour coder les symboles est donc de 6. Ce qui nous amène à utiliser un « champ de Galois » de $GF(2^6)$.

Le polynôme primitif utilisé pour construire le champ de Galois dans le RS(63,55) égale :

$$p(x) = x^6 + x + 1$$

$$p(\alpha) = \alpha^6 + \alpha + 1$$

$$p(\alpha) = 0 \Rightarrow \alpha^6 + \alpha + 1 = 0$$

$$\alpha^6 = \alpha + 1$$

Le polynôme générateur dans ce code sera :

$$p(x) = 1x^8 + 55\,x^7 + 61\,x^6 + 37\,x^5 + 48\,x^4 + 47\,x^3 + 20\,x^2 + 6\,x + 22$$

3.3.1 Processus de codage RS

La première chose à faire dans le codage Reed Solomon matriciel est de trouver la matrice génératrice G. Cette matrice est construite à partir du polynôme générateur du code RS (63,55). La méthode de génération de cette matrice est décrite dans le chapitre précédent.

La matrice G sera représentée comme suit :

$$G = \begin{matrix} 1 & 0 & 0 & 0 & . & . & 0 & 14 & 6 & . & . & 36 \\ 0 & 1 & 0 & 0 & . & . & . & 49 & 19 & . & . & 61 \\ 0 & 0 & 1 & 0 & . & . & . & . & . & . & . & . \\ . & . & . & 1 & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & 45 & 35 & . & . & 52 \\ . & . & . & . & . & . & 0 & 20 & 19 & . & . & 19 \\ 0 & 0 & 0 & 0 & 0 & . & 1 & 55 & 61 & . & . & 22 \end{matrix}$$

Maintenant et après la détermination de la matrice G, nous passons au codage de l'information (message initial) « m » par la multiplication de m par la matrice G:

$$c = m.G$$

Considérant l'exemple suivant:

m= {44, 46, 6, 45, 31,..., 0, 0,..., 0}

Le mot code c sera égale à : le message m plus la redondance c-a-dire :

c = {44, 46, 6, 45, 31,..., 0, 0,..., 0, **23, 43, 13, 23, 61, 1, 30, 42**}

Algorithme de codage matriciel :

Entré	k : message, G : matrice génératrice
Sortie	C : message reçu
	C = k . G
	C = k + CRC
Fin.	

3.4 Décodage Reed Solomon:

L'idée de base du décodeur de Reed Solomon est de corriger la séquence K' générée au niveau du deuxième dispositif en se servant du CRC généré après codage de Reed Solomon au niveau du premier dispositif (figure 4.2).

Avant d' aborder le décodage, il faut d'abord déterminer la matrice de contrôle, qui permet de calculer les syndromes, cette matrice est calculée comme suit :

H = $(tA \mid I)$ avec ^{t}A est la transposée de la matrice A.

La multiplication de la deuxième séquence (K'+CRC) par la transposée de la matrice de contrôle H donne le vecteur de syndromes $S_{(1*k)}$.

$$\begin{matrix} 24 & 30 & 11 & 8 & . & . & . & 1 & 0 & . & . & 0 \\ 61 & 19 & 54 & 22 & . & . & . & 0 & 1 & . & . & 0 \\ . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & 0 & 0 & . & 1 & 0 \\ . & . & . & . & . & . & . & 0 & 0 & . & . & 0 \\ 2 & 35 & 26 & 44 & . & . & . & 0 & 0 & . & . & 1 \end{matrix} * {}^{t}(62\ 21\ \ldots\ldots 22) = (38\ 57\ \ldots\ 17)$$

Après le calcul des syndromes on peut voir s'il y a des erreurs ou pas selon l'algorithme suivant :

Entré	S : vecteur des syndromes
Sortie	e : booleen
	Si S[i] = 0 pour tout i =1→n-k+1
	Afficher (pas d'erreur)
	Sinon Afficher (existe erreur)
Fin.	

Si tous les coefficients du syndrome sont nuls, alors les étapes suivantes du décodage n'ont pas lieu d'être car la séquence générée au niveau du deuxième dispositif ne contient pas d'erreurs. Par contre, si le syndrome est non nul, on devra calculer le polynôme de localisation des erreurs et le polynôme d'amplitude des erreurs. Il y a plusieurs méthodes de calcul de ces deux polynômes, parmi ces méthodes on a choisit l'algorithme de *Berlekamp – Massey*. Cet algorithme itératif vise à accélérer le décodage Reed Solomon.

Cependant le polynôme localisateur est définit comme suit:

$$\sigma(x) = \pi\ (1 + \alpha ji\ x)$$

Le but de l'algorithme de Berlekamp-Massey est de trouver le polynôme σ(x).

Une fois le polynôme de localisation des erreurs est calculé, il nous reste de calculer le polynôme d'amplitude de degré t-1 :

$$\omega(x) = [S(x)\ \sigma(x)] \bmod (x^t)$$

On doit évaluer les racines de ce polynôme et la dérivée du polynôme localisateur d'erreurs par l'algorithme de chien searche.

Nous passerons maintenant à la construction du polynôme d'erreur e(x), en additionnant le polynôme e(x) avec la séquence r(x)=k'(x)+CRC, on trouve la séquence initiale, c.à.d. k(x) la séquence corrigée.

$$e_i = w(\alpha^i) * \sigma(\alpha^i)$$

4. Implémentation

4.1 Langage et environnement de programmation

Notre choix du langage de programmation s'est porté sur le langage JAVA et cela pour diverses raisons :

- ☑ C'est un langage orienté objet simple, ce qui réduit les risques d'incohérence.
- ☑ Il est portable et multi – plateforme.
- ☑ Il possède une riche bibliothèque de classes.

En plus nous sommes familiarisés avec ce langage.

Nous avons réalisé notre application java en utilisant l'IDE NetBeans 6.8.

4.2 Architecture générale de l'application

Le schéma suivant (figure 4.5) présente les différents modules utilisés pour la réalisation de notre projet.

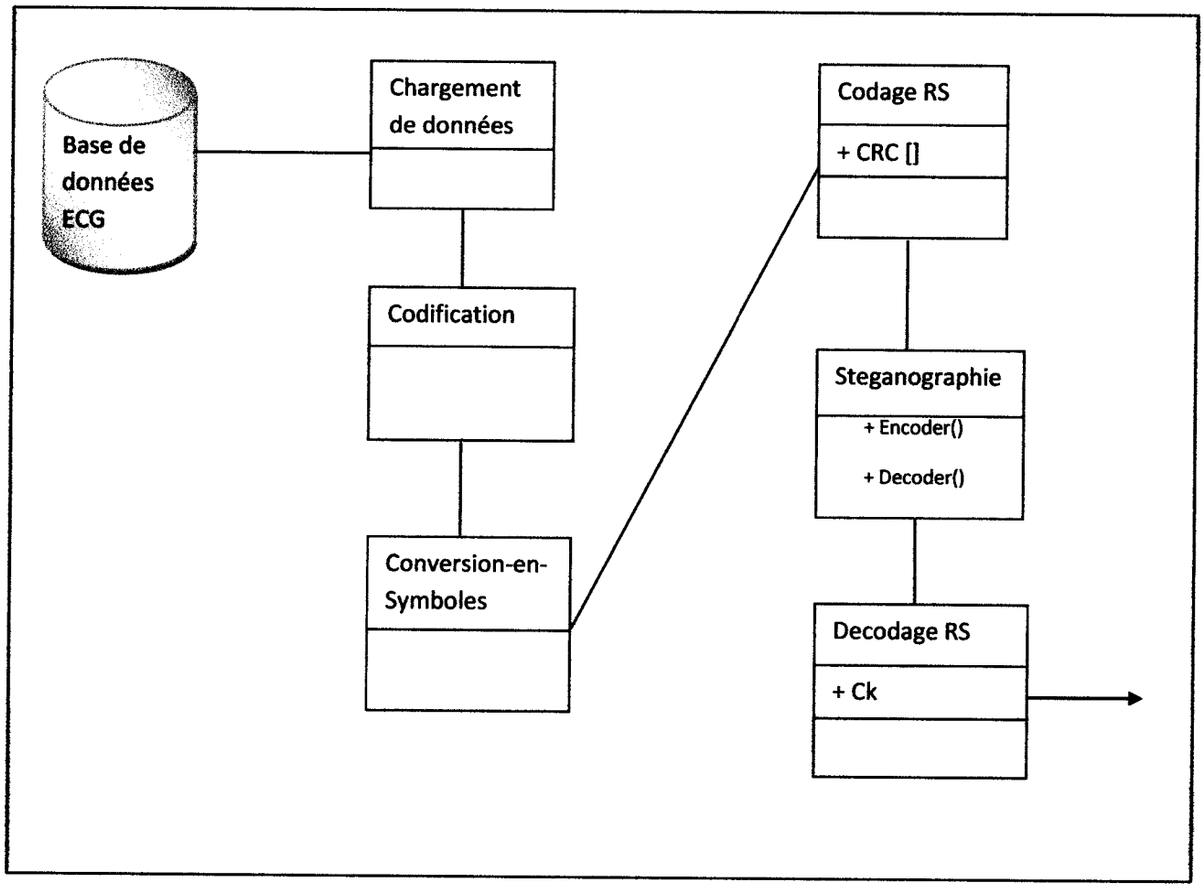


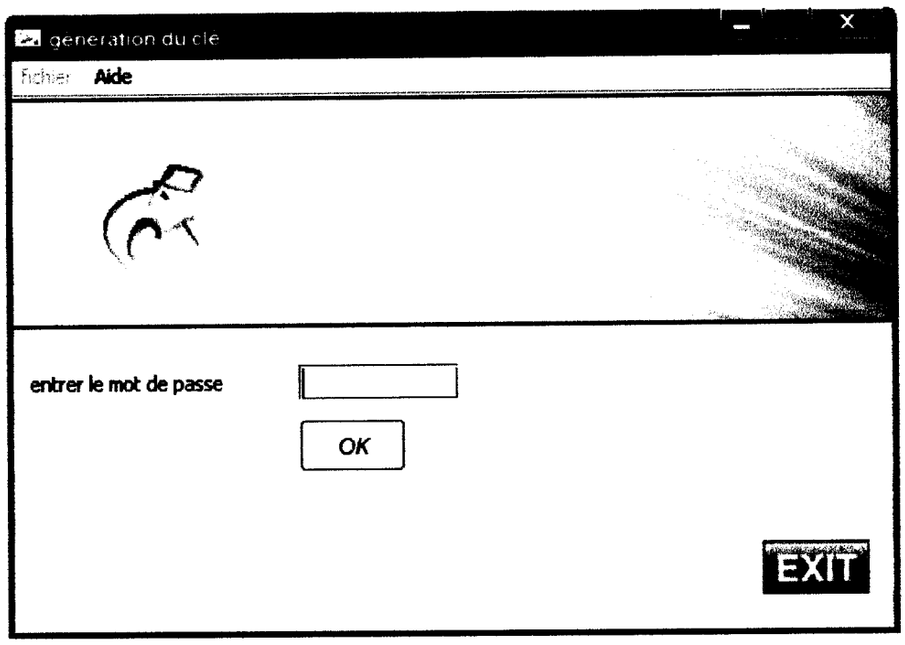
Figure 4.5 Représentation d'Architecture générale des classes.

Description des classes utilisées :

- ☑ Chargement des données : cette classe permet la liaison entre l'application et la base de données c-a-dire, elle fait le chargement des signaux ECG à partir de la base.
- ☑ Codification : cette classe permet d'obtenir une séquence binaire de 320 bites, (128+192 bits à 0) pour l'adapter aux paramètres de code Reed Solomon.
- ☑ Conversion en symboles : cette classe consiste à convertir la séquence binaire de 320bits et la convertir en 55 symboles, chaque symbole est composé de 6bits.

- ☑ Codage RS : cette classe à pour but de construire la redondance CRC qui sera envoyé vers le deuxième dispositif pour faire le décodage.
- ☑ Stéganographie : cette classe permet la sécurité de la redondance CRC dans l'étape de leur transmission.
- ☑ Decodage RS : cette classe consiste à corriger la séquence générer par le deuxième dispositif, afin de regénérer la clé k.

4.3 Interface de l'application :



Figur4.6 : interface principale

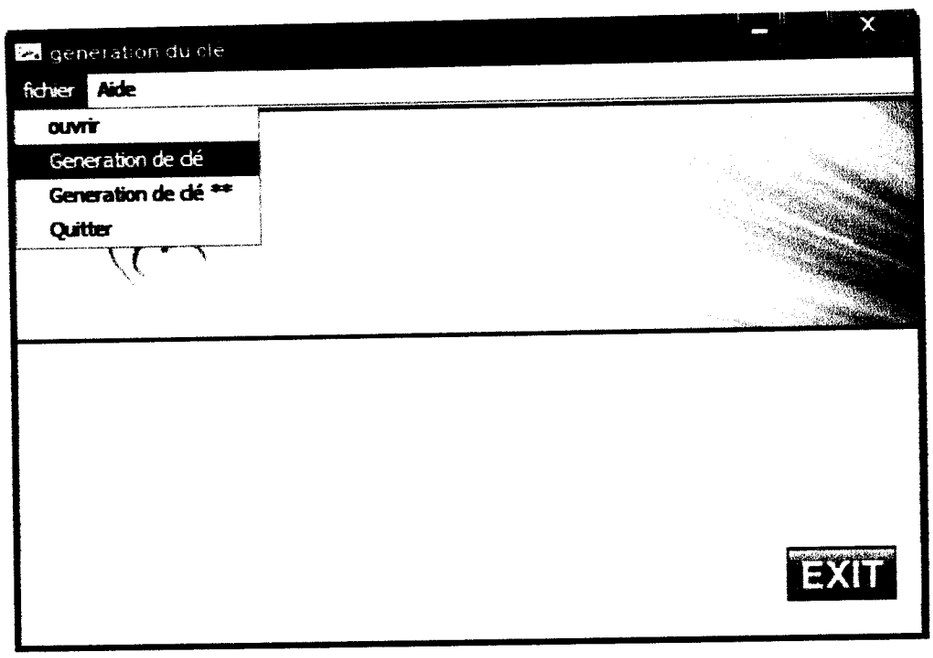


Figure4.7 : interface principal après la saisie du mot de passe

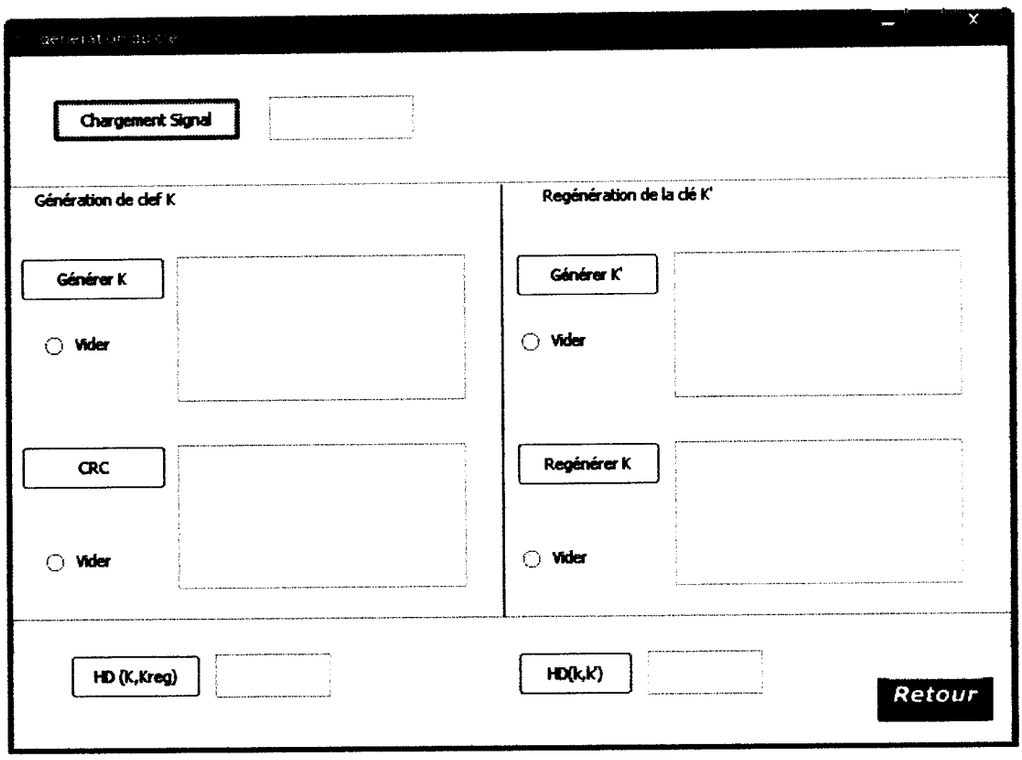


Figure4.8 : interface de génération de clé

5. Teste et résultat :

On utilise la base de donnée MIT-BIH pour montre l'exécution de notre application qui consiste a générer la clé cryptographie, les résultats sont montrés au dessous dans les figures suivantes :

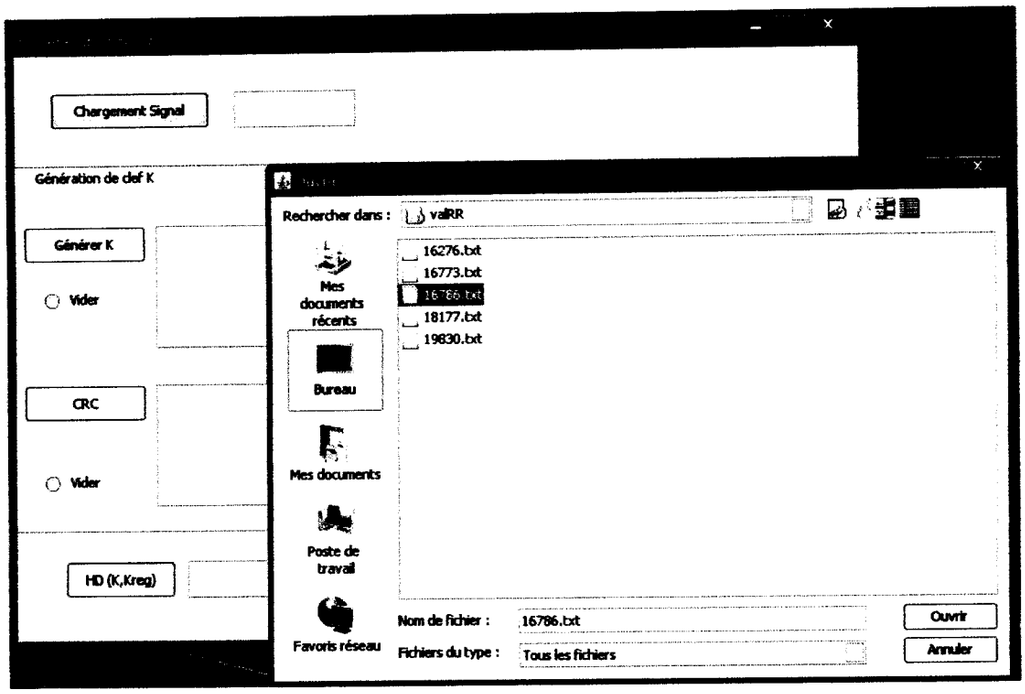


Figure4.9 : chargement du signal

☑ Chargement du signal ECG

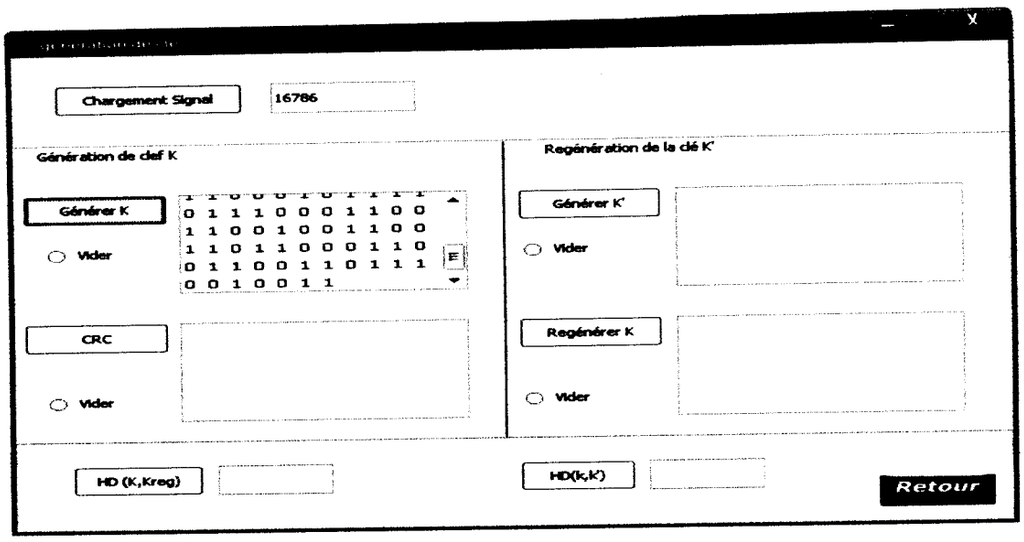


Figure4.10 : génération de k

☑ Extraction d'une clé K (128 bits)

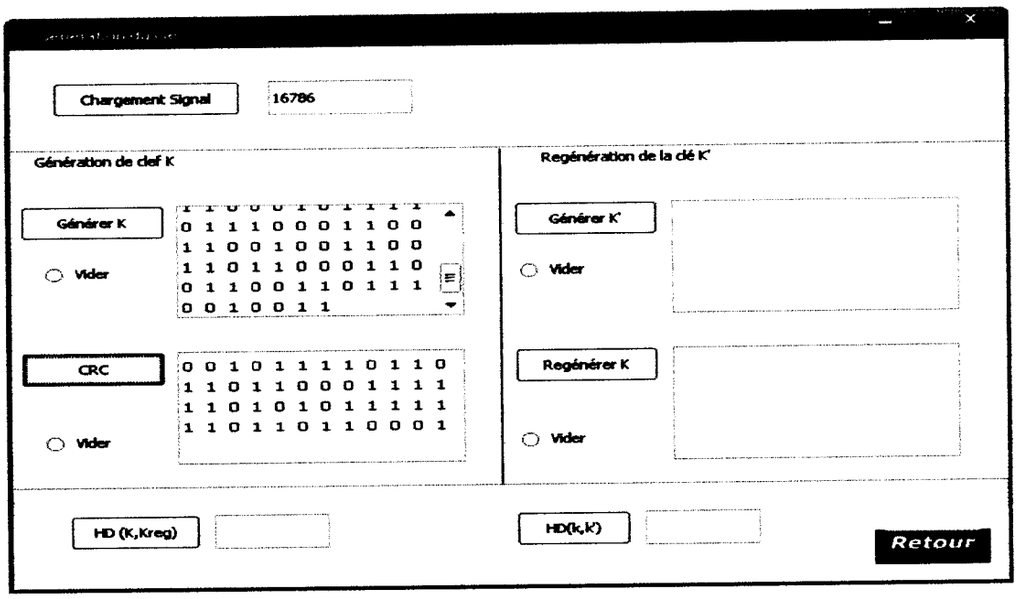


Figure4.11 : calcule de la redondance

☑ Evaluation du codage Reed Solomon

☑ Obtention de la redondance CRC

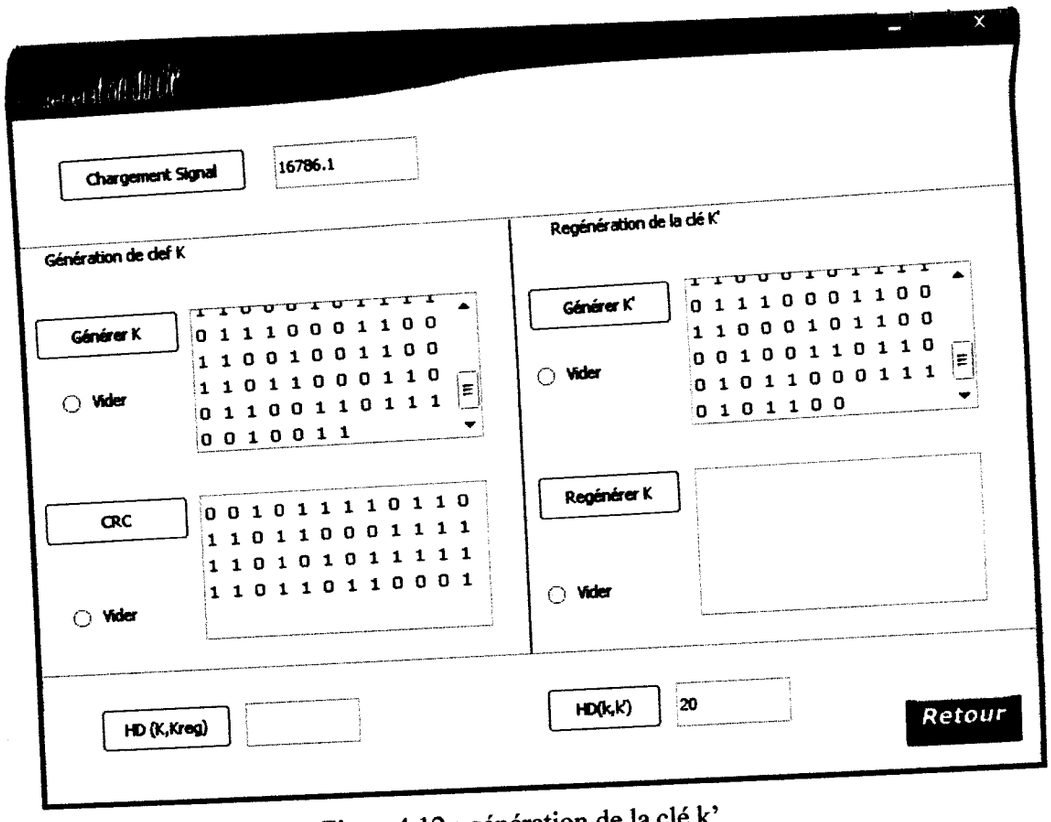


Figure4.12 : génération de la clé k'

- ☑ Chargement du deuxième signal
- ☑ Extraction de clé k' (128bits)
- ☑ Distance de Hamming <22

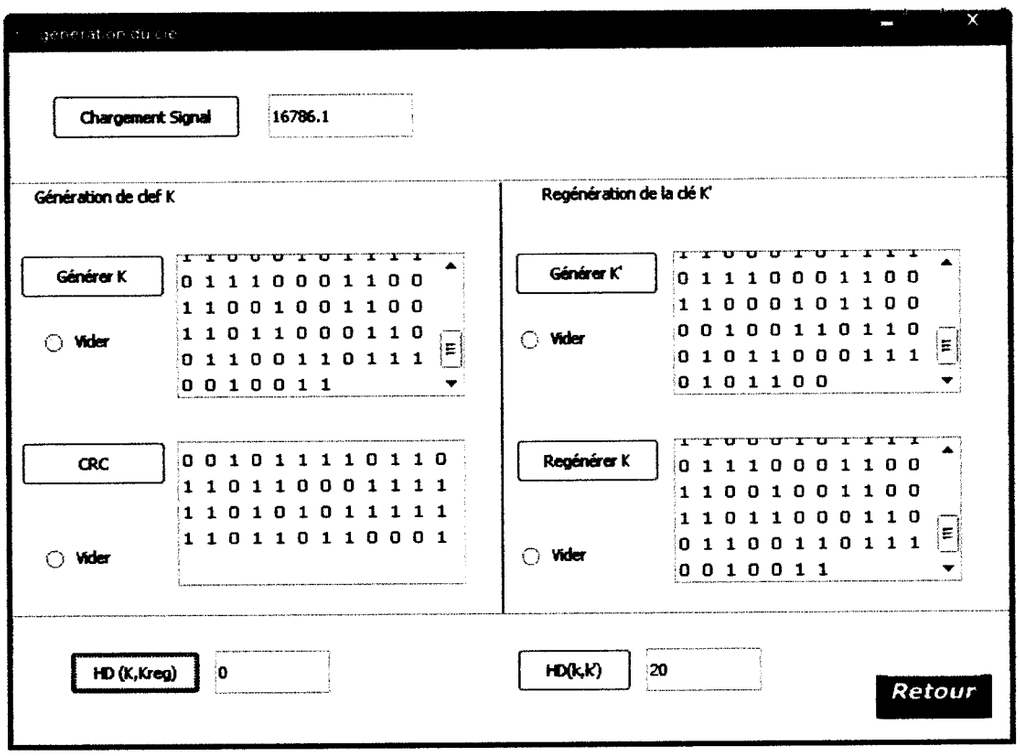


Figure4.13 : Regénération de la clé k

- ☑ Reconstruction de la clé K ($HD_{(k, k')}$<22)
- ☑ Clé générer à partir de la même personne ($HD_{(k, kreg)}$=0)

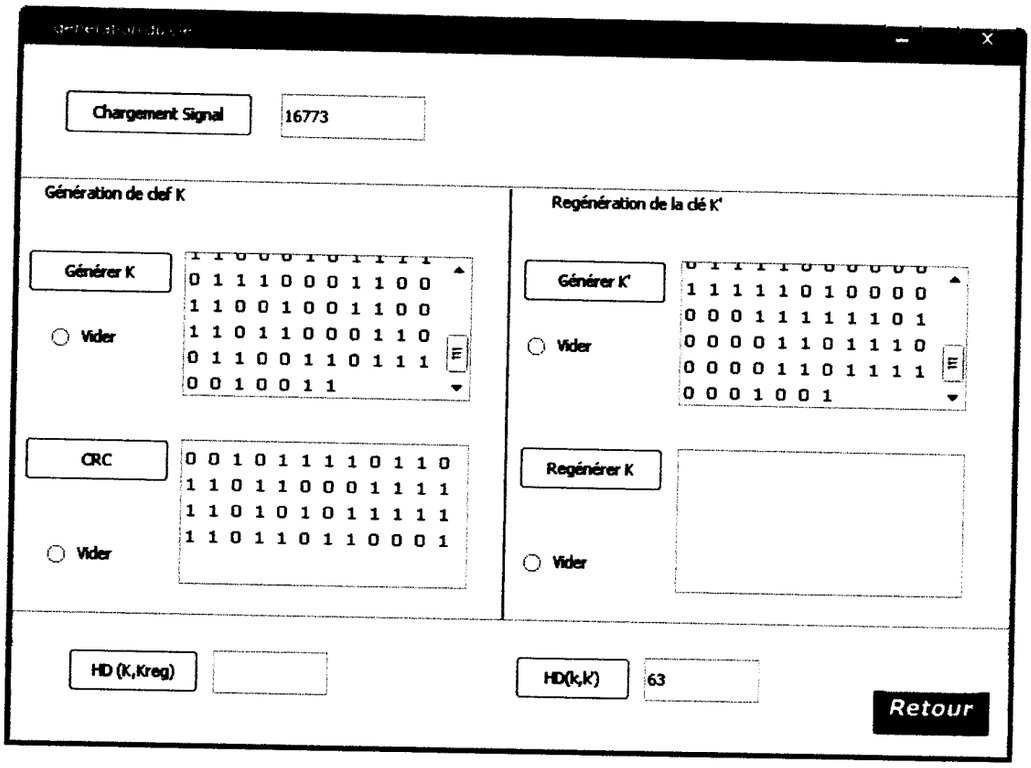


Figure4.14 : génération de k' à partir d'un autre signal

- ☑ Extraction d'une clé k' d'un deuxième signal
- ☑ La distance de Hamming obtenue entre k et k' > 22

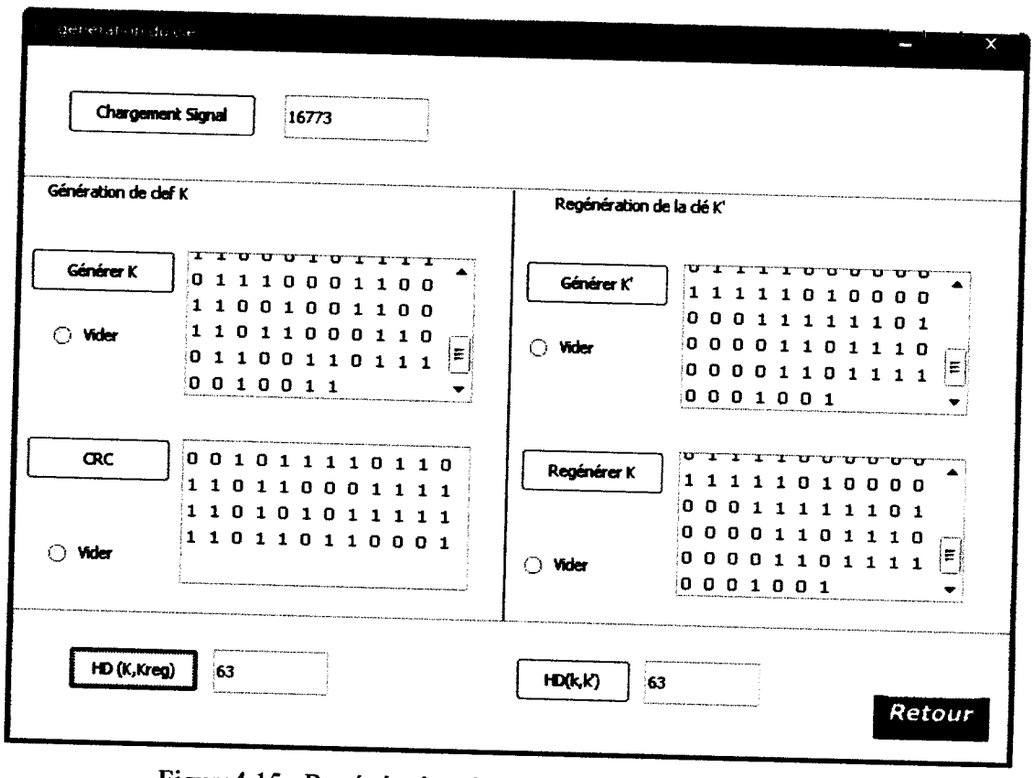


Figure4.15 : Regénération de k à partir d'un autre signal.

- ☑ La distance de Hamming entre k et k regénérer est égale a 63 (>22) alors les deux clé k et k' sont générés à partir des personnes différents.
- ☑ Reconstruction de la clé k échoué.

6. Conclusion :

Ce chapitre a été consacré à la réalisation de notre projet qui consiste à générer des clés cryptographiques à partir des signaux ECG. Un signal ECG se caractérise par un aspect aléatoire ce qui est une propriété importante en cryptographie. Deux signaux ECG acquis d'une même personne à deux instants différents, seront totalement différents, et considérés comme s'ils sont issus de deux personnes différentes.

Nous avons exploité les séquences RR du signal ECG pour générer des clés cryptographiques de taille de 128 bits. La distance de Hamming inter personne est de 22 bits. Nous avons utilisé les codes de Reed Solomon pour corriger ce nombre d'erreurs et générer des clés identiques au niveau de chaque point d'acquisition du signal ECG.

Conclusion générale

Conclusion générale

Le présent travail consiste à générer des clés cryptographique à partir des signaux ECG. Les clés générés sont ensuite dissimulés en utilisant les méthodes stéganographiques, nous avons faire intervenir la stéganographie pour fournir un niveau de sécurité élevé à notre système de génération et distribution de clés.

Un signal ECG représente l'activité électrique cardiaque. Il est reconnu comme un moyen biométrique variant dans le temps; car l'acquisition de deux signaux ECG d'une même personne à deux instants différents ne présente pas la même information. Un signal ECG est caractérisé aussi par son aspect aléatoire ce qui est une propriété importante de la cryptographie.

Dans ce travail, nous avons exploité les séquences de temps entre les intervalles RR pour générer des clés de taille 128 bits. Le codage binaire des séquence IPI (Inter Pulse Interval), séquence de temps entre les intervalles RR s'était basé sur l'observation rythmique du cœur.

La distance de Hamming inter personne entre les séquences binaires générées en même instant vaut 22 bits et celles intra personne vaut 80 bits. La correction de cette erreur de 22 bits est nécessaire pour générer des clés identiques. Nous avons utilisé les codes auto correcteurs de Reed Solomon pour corriger ce nombre d'erreurs.

Dans les futurs travaux, on vise à exploiter d'autres caractéristiques du signal ECG pour la génération des clés cryptographiques avec un minimum de temps.

LISTE DES FIGURES

Résumé

Dans les *cryptosystèmes* traditionnels, l'authentification d'utilisateur est basée sur la possession d'une clé secrète (code PIN ou mot de passe par exemple) ; mais l'inconvénient majeur de cette solution est que la clé peut être oubliée, perdue ou volée. Ainsi, on ne peut pas assurer le non répudiation car la clé peut être utilisée par une autre personne non légitime.L'utilisation des caractéristiques physiologiques de l'être humain tels que l'iris, empreinte digitale, rétine ... ; fournissent une solution aux problèmes de la *cryptographie* et remplacent les *cryptosystèmes* traditionnels. Dans ce cadre, *la génération des clés cryptographiques* est primordiale, cependant nous avons tenté de générer des *clés cryptographiques* à partir des *signaux ECG*, en se basant dans la génération sur les codes auto correcteurs d'erreurs, notamment les *codes Reed Solomon*. Des expériences sont exécutées sur une base des *signaux ECG* (base de données MIT) et les résultats sont satisfaisants.

Mots Clés : cryptographie, génération de clés, codes Reed Solomon, signaux ECG.

فيما يتعلق بأنظمة التشفير التقليدية؛ التعريف بالمستخدم كان يعتمد على امتلاك مفتاح سري سواء كان الرمز السري" بين" أو كلمة المرور؛ إلا أن هدا كان من بين أكبر السلبيات لهده الأنظمة؛ خاصة في حال أن المستخدم قد ينسى المفتاح؛ يضيعه أو تتم سرقته من طرف أشخاص غير شرعيين؛ في مثل هده الظروف لا نستطيع ضمان الأمن و الحماية الأساسيين للمستخدم ؛ على هدا الأساس فإن استخدام الخصائص الفيزيلوجية للإنسان بات ضروريا ؛ هده الخصائص نذكر من بينها بصمة الأصبع؛ حدقية العين ... ؛ تمنح حلول متعددة لمشاكل التشفير؛ فهي تعوض أيضا أنظمة التشفير التقليدية. و في هدا الإطار فإننا ارتأينا إلىتوليد مفاتيح التشفير من خلال الرسم التخطيطي للقلب (أ س ج) و دلك عن طريق استخدام رموز التصحيح و على وجه الخصوص رموز "الريد سولومون" ؛ قد أجرينا تجاربنا على مجموعة من الرسومات التخطيطية للقلب (أ س ج) الموجودة في قاعدة البيانات "أم أي تي بيه" و النتائج كانت إيجابية .

كلمات مفتاحية: أنظمة التشفير؛ مفاتيح التشفير؛ رموز الريد سولومون؛اشارة أ س ج.

summary

In conventional cryptosystems, user authentication is based on the possession of a secret key (PIN or password, for example); but the major drawback of this solution is that the key can be forgotten, lost or stolen. Thus, we can not ensure the non-repudiation because the key can be used by another person not légitime.L'utilisation physiological characteristics of human beings such as iris, fingerprint, retina ...; provide a solution to the problems of cryptography and replace traditional cryptosystems. In this context, the generation of cryptographic keys is essential, however, we tried to generate cryptographic keys from the ECG signals, based on the generation correctors auto error codes, including Reed Solomon codes. Experiments are performed on a database of ECG signals (MIT database) and the results are satisfactory.

Keywords: cryptography, key generation, Reed Solomon codes, ECG signals.