République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITÉ ABOU BEKR BELKAID DE TLEMCEN

FACULTÉ DE TECHNOLOGIE

DÉPARTEMENT DE GENIE BIOMEDICALE

MÉMOIRE DE MASTER EN GENIE BIOMEDICALE

OPTION : Télémédecine

Sécurisation des données médicales sous Android

Présenté par :

CHETTI Imene Hachania & LATRACHE Imene

Soutenu le 17 septembre 2017 devant le jury:

Président:	Mme ZIANI CHERIF SOUHILA	Maitre conférence	UABB Tlemcen
Examinateur:	Mme MEZIANI FADIA	Maitre assistant	UABB Tlemcen
Encadreur :	Mr MERZOUGUI RACHID	Maitre conférence	UABB Tlemcen

Année universitaire: 2016-2017

« L'extraordinaire nous attire un instant : la simplicité retient plus longtemps par ce que c'est en elle seule que réside l'essentielle. »

Garry Winogrand

Remerciements

Nos *remerciements, avant tous, à* ***DIEU*** *tout puissant pour la volonté, la santé et la patience qu'il ma donnée durant toutes ces longues années d'études afin que je puisse arriver à ce stade.*

A *monsieur* **MERZOUGUI.Rachid,** Maitre de Conférence à la faculté de technologie de l'université de Tlemcen, *qu'il me soit permis de le remercie, et de lui exprimer nous profondes reconnaissances pour son aide au cours de ce travail, pour ses conseils et pour la confiance dont il fait preuve à notre égard.*

Notre *reconnaissance va également à madame* ***ZIANI CHERIF.S*** *maitre conférence à l'université de Tlemcen; qui a bien voulu présider le jury de ce mémoire, je lui adresse mes plus vifs remerciements.*

Nous tenons à remercier infiniment madame ***MEZIANI.F*** *maître assistance à l'université de Tlemcen, a bien voulu examiner ce travail, aussi pour leurs conseils, et son intérêt durant notre étude.*

Nous exprimons également notre gratitude à tous les enseignants qui ont collaboré à notre
formation depuis notre premier cycle d'étude jusqu'à la fin de notre cursus universitaire.

Enfin nous remercions tous ceux qui ont contribué de près ou de loin à la concrétisation de
ce travail.

Dédicace

Du profond de mon cœur, je dédie ce travail à tous ceux qui me sont chers.

A mon cher père (BACHIR) que rien au monde ne vaut tes efforts fourni, jour et nuit, pour mon éducation et mon bien être.

A ma très chère aimée mère(SAKINA) tu es l'exemple de dévouement qui n'a pas cessé de m'encourager et de prier pour moi, Que Dieu, le tout- puissant, te préserve et t'accorde santé, longue vie et bonheur.

J'espère qu'ils trouveront dans ce travail toute ma reconnaissance et tout mon amour.

À ma chère grand-mère, dont ces conseils précieux m'ont guidé et leurs soutiens moraux. Que dieu la protège.

A mes frères, AYMEN et mon petit AKRAM.

A ma très chère sœur, KHAOULA.

A mes tantes mes oncles surtout MAHMOUD et NORA (fLEURISTA).

A toute mes ami(e) : KHADIDJA , FAYDA , SOUMIA , DJAMILLA, AMEL, DINA, AMIRA, RAYAN et tous les amis approches qui a vécu avec eux pendant la durée de l'étude, et NACHWA, MAHDI, AMINE ,NADJIM,SALAHDINNE qui n'ont cessé de m'encourager et de me soutenir.

A mon binôme CHETTI IMENE

A toute la promo TELEMEDECINE 2017.

A tous les enseignants qui ont contribué à ma formation.

Latrache Imene

Dédicace

Avec un énorme plaisir, un cœur ouvert et une immense joie que je dédie ce mémoire :

A mes chers, respectueux et magnifiques parents ma mère et mon père pour leur patience, leur amour, leur soutien et leur encouragement au long de ma vie.

A mon frère « «Abdelmoumen » et ma sœur « Wissal sawsawti »

A mes grands parents, tous mes oncles et mes chères tantes

A mes petits cousins : *« Alaa elddine, Amir, Taha yacine, Nizar, A.elmoeze, Moslime, Boalam, Wadie, Mohamed et A.elbari »* et mes petites cousines : *« Rayan, Djihan, Rymasse, Ryhame, Ibtihal, Aridje »*

A mes amis et mes camarades*: Mustafa.Bachir.Tidjani. Bachir.A/elbasset.Manel.Amina.Nachwa.Zahra.Salsabil .Fatma.Amina.Abir.Khadidja.Halima. Warda.Zakia.*

Ibtissem.Hanan.Safa.Sabrina.Fatima.

Boutaina.Hadjer.Sara.

A ma binôme et mon amour ***Imene***

A toute la promo TELEMEDECINE 2017.

A tous ce que j'aime

A toutes personnes qui m'ont encouragé et aidé au long de mes études

Chetti Imene Hachania

Résumé

Le développement d'applications et services dans le domaine de M-health sont devenus un enjeu majeur dans le monde des communications sans fil. L'ensemble de ces services touchera positivement à court terme le vieillissement de la population et les personnes exposées à des risques d'accident dans leur vie quotidienne ou de dégradation de leur état de santé.

Le but de notre travail est de sécuriser les échanges Patient/Médecin. Pour cela le codage base64 a été implémenté sous Android pour deux raisons :

- Transformation de l'image médicale aux formats caractères (format crypté).
- Optimisation de la taille de l'image et par conséquent accélération de débit de transmission.

Cette solution non couteuse et facilement réalisable peut contribuer efficacement aux services de santé en particulier la télé-imagerie tout en exploitant des Smartphones comme outils de base.

Mots clés = *M-health – échanges - crypté - télé-imagerie - base64 - Android.*

Abstract

The development of applications and services in the field of M-health become of majeure issues in the word of wireless communication .All this services will affect positively in the aging of the population and those exposed risks of accidents in daily life of degradation of their state of health.

The purpose of our world is to secure the patient/doctor changes; the coding base 64 has been in demented under android for two reasons:

- Transform the medical image to format characters (encrypted format).
- Image size optimization and consequently acceleration transmission rate.

This solution is not counted and easily realizable may contribute effectively health services in particular tele imaging smartphones like basic tool

Keywords = M-HEALTH – patient/doctor changes – base 64 – Android – encrypted - tele imaging

الملخص

إن تطوير التطبيقات والخدمات في مجال الصحة المتنقلة ، قد أصبح قضية رئيسية في عالم الاتصالات اللاسلكية ، وستؤثر إيجابا جميع هذه الخدمات في الأجل القصير على شيخوخة السكان والمعرضين لخطر الحوادث أو الذين تتدهور صحتهم في حياتهم اليومية.

والهدف من عملنا هو تأمين التبادلات المريض / الطبيب. لهذا السبب تم تنفيذ الترميز base64 عن طريق الاندرويد لسببين:

- تحويل الصورة الطبية إلى صيغة حرفية مشفرة (شكل مشفر).

- تحسين حجم الصورة وبالتالي تسارع معدل تدفق الانتقال.

هذا الحل غير مكلف وسهل التحقيق بحيث يساهم بشكل فعال في تحسين خدمات الرعاية الصحية ، وخاصة التصوير عن بعد ، في حين تستخدم الهواتف الذكية كأدوات أساسية.

الكلمات المفتاحية : الصحة المتنقلة — التبادلات- تشفير- التصوير عن بعد- ترميز قاعدة64 - الاندرويد.

Table de Matière

II. Chapitre II : Techniques de chiffrement et de cryptographie

III. Chapitre III : Application Androïde cryptage/transmission

Liste des Figures

Chapitre I :

Chapitre II:

Chapitre III:

Liste des Tableaux

Glossaire

TIC : Technologie de l'information de la communication.

DTE: Data terminal equipment.

DCE: Data Communication Equipment.

RTC: Réseaux de transport de la capitale.

ADSL: Asymmetric Digital Subscriber Line.

NTIC : Nouvelles technologies de l'information et de la communication.

OMS : Organisation mondial de santé

DMP : Dossier médicale personnelle

SSP : Personnalisation de la santé est des soins

XOR: Exclusive OR.

ASC: Aquaculture stewardship council **.**

RC5 : Protocole de communication**.**

DES : Data Encryption Standard.

RSA: Rivest shamir-adleman algotiyhm.

JDK : Java Développement Kit.

JVM : La machine virtuelle Java

API : Application programme interface

JRE : Java runtime environment.

SDK : Software Development Kit Android.

IDE : Environnement de développement intégré.

ADT : Androïde développent Tools.

AVD : Androïde Virtuel Device.

JPEG: Joint photographic experts group.

SMS: Short message service.

« L'imagination est plus importante que le savoir »

Albert Einstein

Introduction Générale

Au cours des dernières années, l'usage croissant des technologies de l'information et de la communication (TIC) dans le champ de la médecine et de la santé fut accompagné par une éclosion de concepts. Au début des années 1990, la télémédecine a utilisé les TIC pour soigner les patients des régions éloignées. Avec l'apparition du concept du M-health (mobile health), la télémédecine devient un outil de communication et de diagnostic pour aider les médecins dans leur travail de soin et les patients dans leur environnement mobile.

L'intégration de la technologie mobile a réformé la qualité de vie des individus et des organisations dans le secteur de la santé en définissant la voie à une discipline de recherche émergente et innovante. Les systèmes m-health connaissent une variété de défis, y compris la prévalence des maladies liées au style de vie, la nécessité de donner aux patients des informations pour une meilleure prise de décision, les demandes de meilleurs outils pour auto-prise en charge et la gestion de détérioration des conditions sanitaires, ainsi que la nécessité d'un accès continu aux services de soins via les appareils mobiles.

Dans ce projet, nous exploitons les Smartphones pour des services mobiles dédiés à la médecine. Pour cela, nous proposons une application Android permettant de sécuriser les données échangées entre patient/médecin. Il s'agit d'implémenter un algorithme de chiffrement basé sur le codage base64. Pour cela nous transformons les formats des images médicales aux formats caractères (chaine de symboles) avant leurs transmissions tout en assurant la confidentialité, l'efficacité et la fiabilité.

Le présent mémoire est structuré en 3 chapitres organisés comme suit :

I. Le premier chapitre : comprend une étude générale sur les aspects de la télémédecine, M-health et l'importance de la sécurisation dans le secteur médical.

II. Le second chapitre : nous présentons une généralité sur cryptographies, les attaques de systèmes actuels, les techniques de cryptage en précisant le codage base64 implémenté dans notre algorithme.

III. Le troisième et le dernier chapitre : Dans cette partie du projet, nous présentons notre application réalisée sous l'outil Android en interprétant les résultats obtenus.

- Enfin, une conclusion générale et des perspectives de travail viennent clôturer ce mémoire.

Chapitre I :

Aspects généraux sur la télémédecine

I.1. Introduction

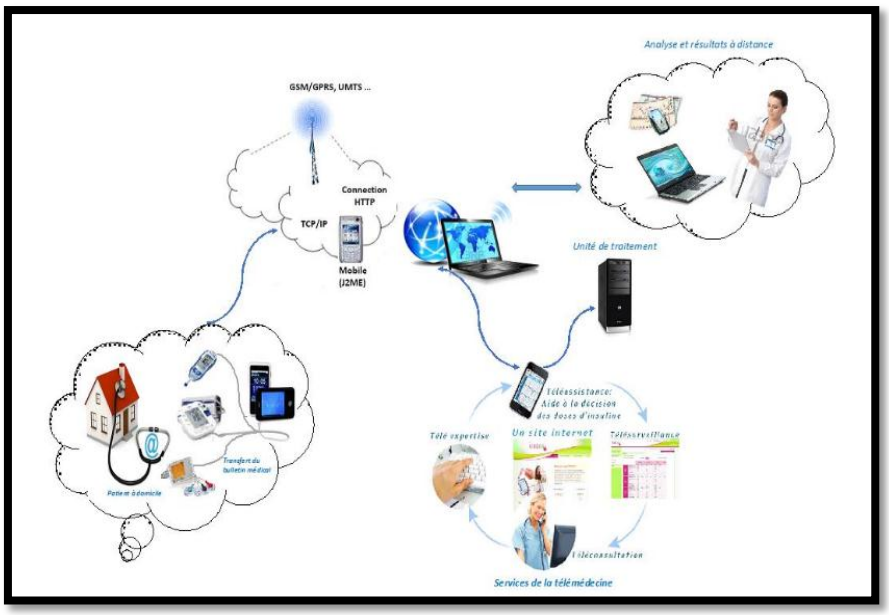
Les Technologies de l'Information et de la Communication (TIC) sont en voie de révolutionner les relations entre les individus et les collectivités. De façon plus spécifique, cette technologie est plus présente dans les systèmes de santé qui permet d'envisager de nouvelles façons d'exercer la médecine. [**1**]

En effet, ces réseaux permettent le transfert électronique des données médicales. Dans ce chapitre, nous nous intéressons à l'étude des services de télécommunication dans la santé relevant de la télémédecine et enfin nous citons quelques travaux déjà réalisés en Télémédecine.

I.2. La télémédecine

La télémédecine est une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication.

Elle met en rapport, un ou plusieurs professionnels de santé entre eux ou avec un patient, parmi lesquels figurent nécessairement un professionnel médical et, le cas échéant, d'autres professionnels apportant leurs soins au patient.



http://www.dsih.fr/article/421/telemedinov-valorise-la-telemedecine-en-vendee.html

Figure I .1 : La télémédecine.

La télémédecine est un levier fondamental de la mise en place de nouvelles organisations susceptibles de relever les défis actuels dans le secteur médical, tels que le vieillissement de la population, l'augmentation des maladies chroniques, l'inégale répartition des professionnels de santé sur le territoire et les contraintes budgétaires. [**2**]

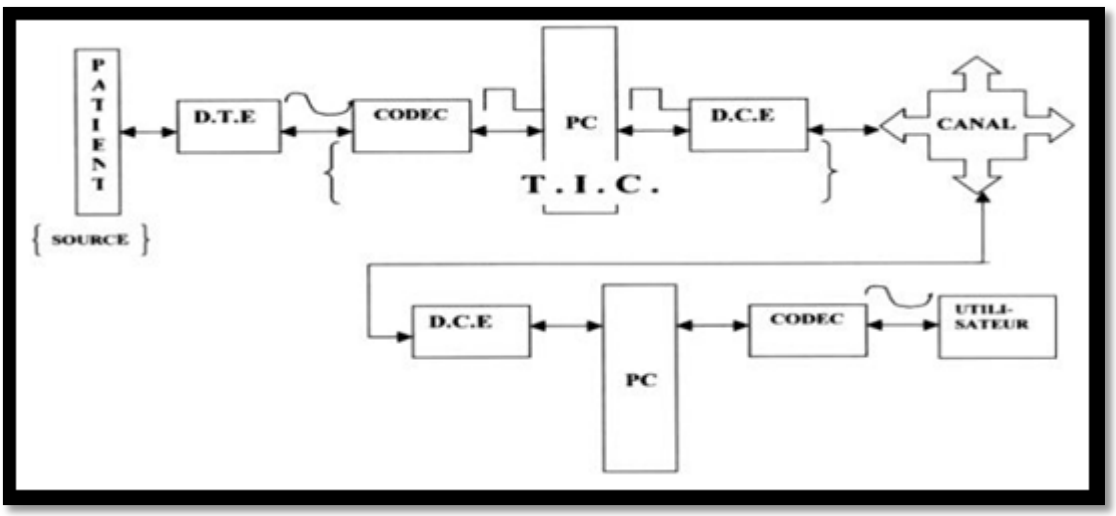
I.2.1. Objectif de télémédecine

L'objectif de la télémédecine est de :

- Offrir un cadre interactif d'échange en information médicale, télédiagnostic, télé thérapeutique et en recherche médicale.
- Permettre l'accès aux réseaux internet et de messagerie électronique.
- Encadrer à distance les professionnels de la santé tout en assurant leur formation Continue. [**3**]

I.2.2. Chaine télé médicale

Le système de la transmission numérique des donnés en médecine comprend tout une chaine qui -dessous :



http://dspace.univ-tlemcen.dz/handle/112/4516?mode=full

Figure I .2 : Représentation de la chaine télémédecine.

A- Le patient : Le patient est la source de destination d'information médicale **D.T.E** Chargé de prélever sur le corps humain l'information médicale et selon la nature de cette dernière dans le sens homme machine les D.T.E peut être :

- **Unidimensionnelle**: Mettant en jeux des capteurs qui transformant les grandeurs physiologique en une grandeur électrique représentative d'une activité physiologique (ECG, activité hémodynamique cardiaque ….)
- **Bidimensionnelle** : Mettant en jeux les différents rayonnements du spectre électromagnétique (radio fréquence, ultrasonore, infrarouge, rayon X..) et l'interaction avec le liquide et les tissus biologiques pour la reconstruction des images médicales.
- **Tridimensionnelle** : Mettant en jeu une cameras a l'intérieur ou à l'extérieur du corps humain. Donnant l'exemple de la fibroscopie ou ont introduit un tube souple équipé d'une fibre optique et une caméra à l'intérieur du corps par voie oral .en revanche pour la fluoroscopie utilisé dans le cathétérisme cardiaque, Cette appareil est équipé d'une cameras externe et au fur et à mesure le spécialiste introduit le cathéter dans le corps du patient en regardant l'image vidéo capté par la cameras qui est fichée sur le moniteur.

B- Codeur/Décodeur: A pour charger la transition de l'information médicale vers le pc locale.

C- Pc Locale: Permet de présenter l'information médicale au praticien de la médecine et de stoker ces informations dans un système d'archivage et d'enverger une plate de forme de traitement numérique et le transfert de l'information via un protocole de communication.

D- D.C.E :(Data Communication Equipment) : Chargé d'adapter le signal informationnel au canal de transmission et de transférer les données médicales vers les terminaux distants (Pc Distant) via le canal de transmission au moyen des techniques hauts débits à titre d'exemple réseau RTC dopé ADSL.

L'objectif de telles plateformes de services de télémédecine est de permettre aux patients de vivre dans des conditions plus performantes, dans un environnement de confort et de sécurité.

Ainsi, cette plateforme envisagée permet, à tout moment et en tout lieu, à un patient d'être en contact permanent avec son praticien traitant. En effet, ils pourraient bénéficier de la sécurité d'un suivi médical 24h/24h, sans l'inconvénient de la prise en charge hospitalière et sans dépenses excessives.

Il s'agit de détecter et de prévenir l'occurrence de situations critiques ou la dégradation de l'état de santé d'une personne. Le patient n'est alors plus contraint de renoncer à distance (domicile...) et à la vie en société. Il conserve une large autonomie dans son environnement social et privatif, tout en bénéficiant de services préventifs de santé **[4]**.

I.2.3.Différents actes de télémédecine

L'application de La télémédecine joue dans une vaste zone avec ses nombreux domaines (radiologie, cardiologie…) ou les professionnelles de santé les pratiqués avec 4 actes.

A la suite, nous présentons les quatre catégories d'applications en télémédecine :

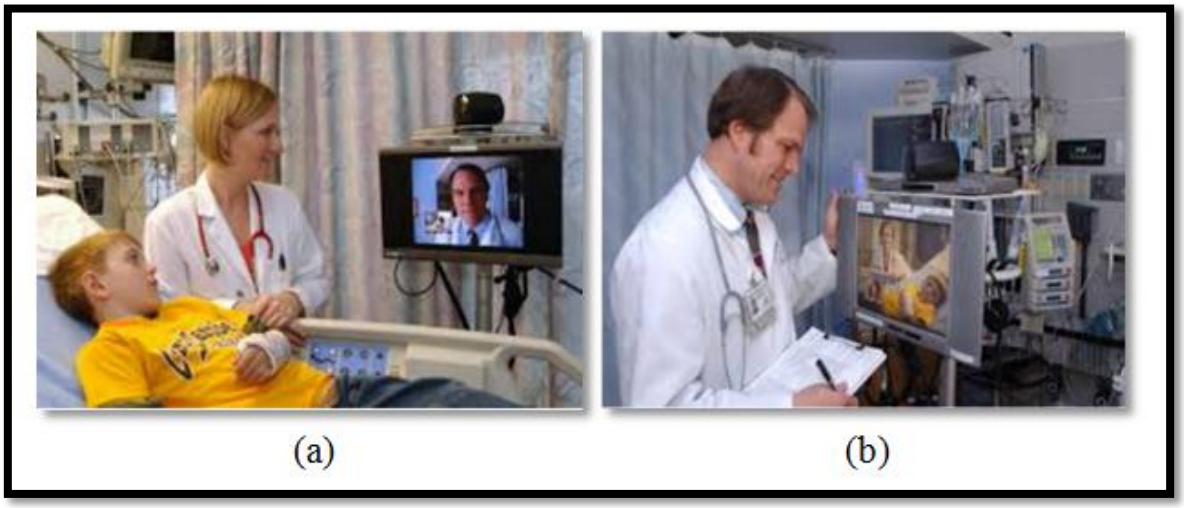
http://www.esante-picardie.com/newsletter/la-lettre-du-gcs-e-sante-picardie-n%C2%B05/

Figure I .3 : Types d'applications de la télémédecine.

La télémédecine est très vaste et diverses et de nombreuses utilisations peuvent être définies. Ces différentes applications visent des objectifs précis mais elles se mélangent à des degrés divers si bien que la classification proposée se révèle quelque peu schématique.

I.2.3.1. Téléconsultation

Examen d'un patient et analyse des données le concernant sans interaction physique directe. On distingue deux types de téléconsultations :



http://www.francetvinfo.fr/sante/professions-medicales/sante-telemedecine-teleconsultation-telesurveillance-des-patients-servons-nous-de-l-innovation-pour-reduire-les-distances_2319177.html

Figure I .4 : Téléconsultation ;(a) : médecin requit ; (b) : médecin requérant.

- Soit le patient consulte, de sa propre initiative un médecin par un réseau de communication interposé.

- Soit le médecin consulté sollicite un avis diagnostic (télé diagnostique) ou thérapeutique (Télé expertise) auprès d'un confrère situé à distance. **[5]**

On peut également citer dans ce cadre, l'envoi et la consultation d'images médicales à distance (télé imagerie, télé radiologie).

I.1.3.2. Téléassistance

La téléassistance médicale a pour objet de permettre à un professionnel médical d'assister à distance un autre professionnel de santé au cours de la réalisation d'un acte médical.

https://www.tele-assistance-senior.fr/teleassistance-des-personnes-agees.html

Figure I .5: Téléassistance.

Elle a aussi pour objet de prescrire à distance une conduite à tenir à un patient (thérapeutique, hygiène de vie ...). **[6]**

I.1.3.3. Télé-expertise

La télé-expertise a pour objet de permettre à un professionnel médical de solliciter à distance l'avis d'un ou de plusieurs professionnels médicaux.

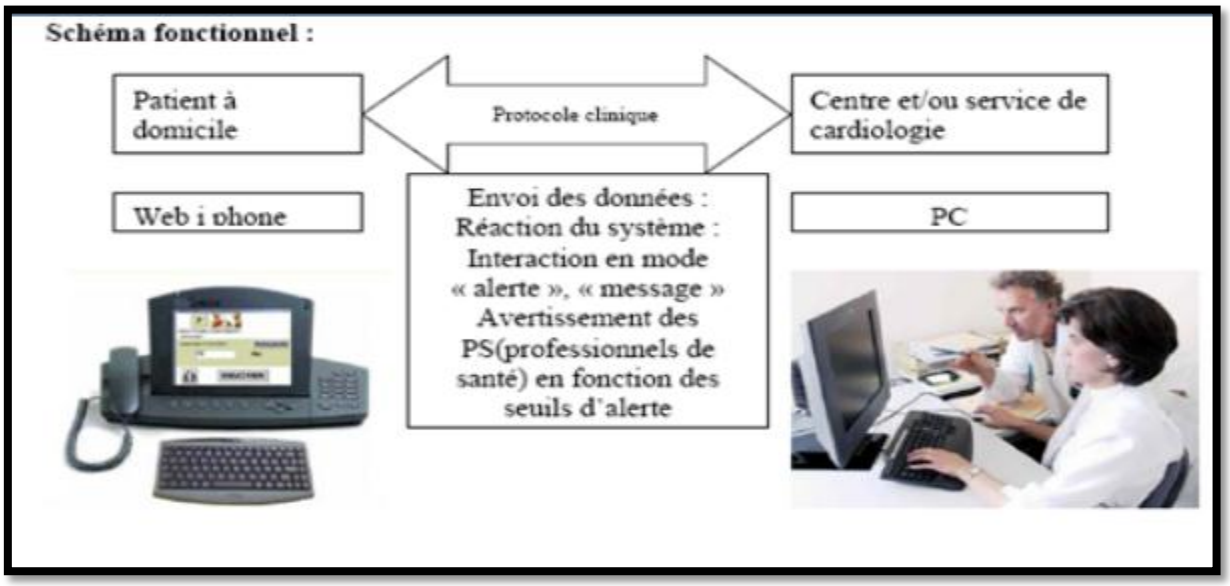
http://www.medicalexpo.fr/prod/polycom/product-83803-528209.html

Figure I.6 : la Télé expertise.

Elle permet d'améliorer de leurs formations ou de leurs compétences particulières, sur la base des informations médicales liées à la prise en charge d'un patient. **[2]**

I.1.3.4. Télésurveillance

La télésurveillance a vocation de permettre à un médecin d'interpréter à distance les données nécessaires au suivi médical d'un patient.



http://slideplayer.fr/slide/3144849/

Figure I.7 : Enregistrement télémétrique.

Elle permet au médecin de prendre des décisions à distance concernant la prise en charge du patient et éventuellement de déléguer des actions à un autre professionnel de la santé. **[7]**

I.2.5. Rapport et enjeux de télémédecine

La télémédecine s'impose déjà à travers l'usage d'outils comme le téléphone et la télécopie. Les progrès actuels des NTIC appliquées au domaine médical (imagerie médicale, débits de transmission, convivialité des systèmes, etc.) et la miniaturisation des dispositifs, ouvrent des perspectives d'une part, pour le développement de la télémédecine en termes d'accroissement et d'autre part pour l'efficacité, la qualité des soins, le partage des connaissances et de réduction des coûts de santé publique. Pour chaque acteur de la télémédecine, les avantages de ce type d'organisation sont nombreux.

Pour les praticiens, il s'agit de développer une plus grande coopération entre les différents réseaux du milieu médical : ville-hôpital, généraliste-spécialiste, secteur public-secteur privé. L'idée est de créer des passerelles de communication, d'information et de transmission du savoir.

Un des enjeux du développement de la télémédecine concerne ainsi les aspects de partage de données et de connaissances : nécessité de l'interopérabilité des systèmes, définition de protocoles de communication, d'ontologies, création d'un dossier médical électronique partagé, etc. Pour les patients, la télémédecine permet d'améliorer la qualité des soins grâce à l'expertise possible à distance et, par conséquent, à la réduction des délais de prise en charge diagnostique et thérapeutique.

Elle permet également de répondre au problème d'isolement géographique en assurant l'égalité d'accès aux soins. Si on considère le cas particulier de la surveillance à distance, la télémédecine répond aux besoins d'autonomie, de sécurité et d'intégration sociale de patients souhaitant rester à leur domicile, et s'inscrit alors dans la dynamique des alternatives à l'hospitalisation. **[8]**

I.2.6. Frein de développement :

Le frein majeur au développement de la télémédecine aujourd'hui consiste en l'absence de modèles de financement clairement établis. Malgré les perspectives de croissance très encourageantes pour le secteur de télémédecine, l'assurance Maladie et l'Etat ne souhaite pas encore participer au débat sur les modes de financement, laissant tout ce secteur dans l'incertitude.

Si l'on regarde les expériences menées à l'étranger, en Europe et aux Etats-Unis. Notamment, on constate que les actes de télémédecine sont de plus en plus intégrés dans le système de santé et bénéficient des mêmes modalités de prise en charge que n'importe quel acte médical. Ainsi, Les médecins et les patients craignent notamment qu'elle porte atteinte à la liberté d'exercice, au secret médical, et conduise finalement à une déshumanisation de la relation entre le médecin et son patient.

L'exploitation de l'outil informatique pour la détection, la consultation, le transfert et la sauvegarde des informations concernant les patients, ne doit pas nuire à leur confidentialité leur efficacité et à leur fiabilité. D'autres points importants résident dans la responsabilité et la rémunération des praticiens [**9**].

La télé-pratique médicale n'est pas encore reconnue comme un acte médical à part entière. Le choix de la méthodologie et la politique tarifaire de la télémédecine et également un problème à résoudre. Une autre crainte est celle de la fuite des compétences médicales des centres de soins les plus isolés [**10**].

La délocalisation d'opérations médicales est en effet, accompagnée du risque de regroupement des meilleurs spécialistes dans quelques grandes unités. Au niveau méthodologique, hétérogénéité des besoins de chaque praticien et patient impose de développer des applications et services à un degré de compatibilité et d'interopérabilité important. Leur efficacité dépend d'une bonne gestion de la grande quantité d'informations générées, la précision dans les calculs numériques et de l'adaptation de services développés au contexte de l'environnement mobile [**11**].

Et un autre frein au développement de la télémédecine c'est l'absence de cotations spécifiques permettant de facturer les actes. Ces services de télémédecine nécessitent en

particulier un traitement personnalisé des informations, dans le contexte d'un patient, et prend ainsi on compte bien peu des règles d'interprétation générales issues des connaissances médicales [**12**].

I.2.7. Avantage de télémédecine :

1- Bénéfices directs :

**Bénéfices directs tangibles :*

Les bénéfices de la télémédecine sont nombreux, mais relèvent tous d'une meilleure qualité de prise en charge :

- économies dues à la réduction des frais de déplacement de spécialistes pour des consultations ou des formations.
- économies dues à la réduction des frais de déplacement des patients.
- économies réalisées sur les coûts d'hospitalisation des patients pouvant être traités à distance
- économies réalisées sur les coûts hospitaliers de prise en charge des patients pouvant être traités à distance.
- économies dues à l'utilisation de centres médicaux décentralisés ou d'unités de soins mobiles, par opposition à l'extension d'hôpitaux urbains ou régionaux (différence de coûts de construction et de fonctionnement des installations)

**Bénéfices directs intangibles :*

- Plus grandes facilités pour obtenir un deuxième avis ou une consultation, d'où une réduction des retards et des erreurs coûteuses.
- Réduction du temps d'attente et des délais de transfert susceptibles d'entraîner de graves complications ou le décès du patient.
- Réduction de la perte de revenus des patients n'ayant pas besoin de se déplacer.
- Meilleure utilisation des spécialistes audience plus large.
- Meilleure gestion du système de santé en général, sur le plan à la fois interne et externe.

- Plus grande disponibilité et coûts de formation réduits des professionnels de santé locaux soutien collégial renforcé pour les personnels médicaux travaillant dans les régions isolées, d'où une plus grande satisfaction dans le travail.
- Possibilités accrues de formation et d'enseignement.

2- <u>Bénéfices indirects :</u>

L'amélioration des connaissances et des qualifications parmi les personnels spécialisés et techniques, aussi la décentralisation des soins et répartition des compétences et l'utilisation maximisée de ressource ces centrales limitées (spécialistes, ordinateurs et appareils de diagnostic, etc.) [**13**].

I.3. La M-santé et la santé connectée

Les applications et l'objet connecté de santé peuvent constituer des outils complémentaires utiles à la prise en charge des patients. Ils peuvent soutenir et renforcer la relation patient-médecin. Des dispositifs de M-santé, sous réserve de leur fiabilité, peuvent contribuer à améliorer l'adhésion des patients aux conseils de prévention, d'hygiène de vie et aux protocoles de soins, à faciliter les contacts entre les médecins et les patients. Les patients se montrent d'ailleurs en attente de conseils en la matière de la part de leurs médecins.

I.3.1.Définition de l'E-santé

Le terme E-Health serait né fin 1999 à l'occasion de la présentation d'une étude australienne, lors du 7ème congrès international de télémédecine. Son auteur, John Mitchell, l'a alors défini comme : « l'usage combiné de l'internet et des technologies de l'information à des fins cliniques, éducationnelles et administratives, à la fois localement et à distance ».

Selon l'OMS, « E-santé » est :

« Consiste à utiliser les TIC à l'appui de l'action de santé et dans des domaines connexes, dont les services de soins de santé, la surveillance sanitaire, la littérature sanitaire et l'éducation, le savoir et la recherche en matière de santé.

On peut citer comme des exemples :

- Télémédecine.
- surveillance électronique des patients.
- dossier médical électronique (notamment le DMP – Dossier Médical. Personnel – qui commence à percer en France).
- systèmes informatiques hospitaliers.
- remboursement électronique des soins.
- e-learning.

Le champ est très vaste, il inclut la télémédecine, passe par les infrastructures jusqu'à l'apprentissage. [**s1**]

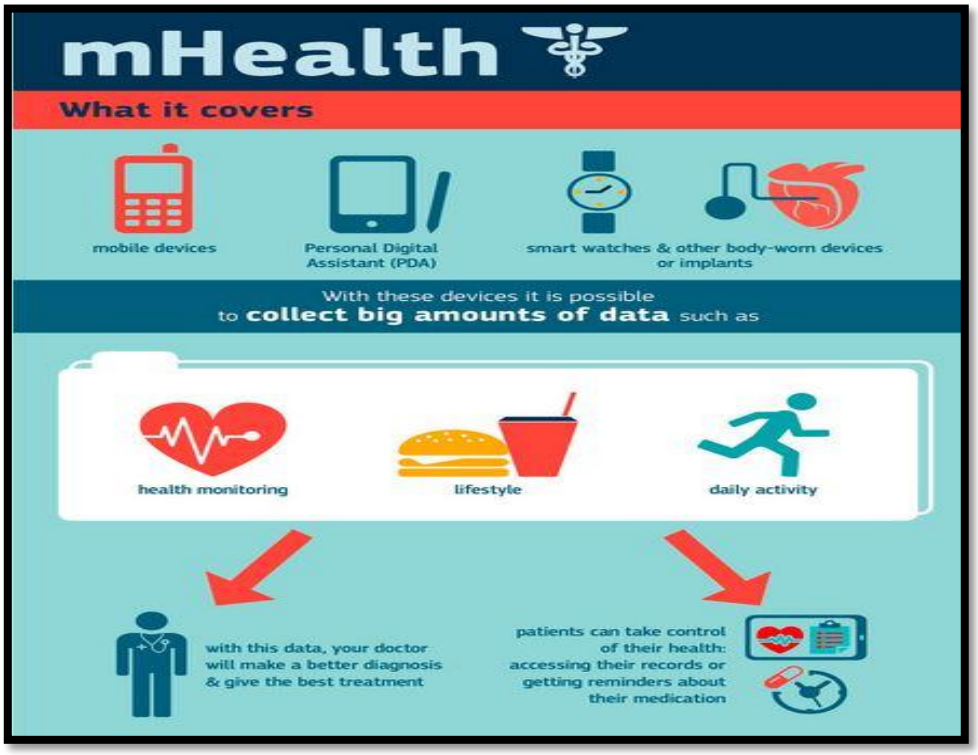
I.3.2.Définition de M-santé

Six ans après la consécration du terme e-Health, celui de Mobile Health (M-Health) est apparu, en 2005, sous la signature du Pr Robert Istepanian, universitaire londonien, pour désigner : *« L'utilisation des communications mobiles émergentes en santé publique ».*

Phénomène mondial, la santé mobile n'a ensuite pas tardé à être définie par l'OMS (2009) comme recouvrant :

« Les pratiques médicales et de santé publique reposant sur des dispositifs mobiles tels que téléphones portables, systèmes de surveillance des patients, assistants numériques personnels et autres appareils sans fil » [**14**].

*M-santé (M-helth en anglais) « M est Mobile » : est un sous-segment de l'e-santé. Il s'agit de tous les services touchant de près ou de loin à la santé disponibles en permanence via un appareil mobile connecté à un réseau.



https://upstatebusinessjournal.com/mhealth-links-docs-patients-wirelessly-247-lowers-costs/

Figure I .8 : M-santé.

Actuellement les Smartphones et les tablettes sont les plus répandus auprès du grand public.

Via des applications digitales (matériel et logiciel), Mobile Health permet au patient, à son entourage et à différents dispensateurs de soins de collecter, visualiser, partager et utiliser intelligemment de manière permanente, des informations relatives à la santé et au bien-être.

I.3.2.1. Qu'est-ce qu'une application. Mobile de santé ?

**Pour le grand public et les patients :*

Éducation à la santé, prévention primaire et secondaire, mieux se suivre, meilleur observation, être acteur de sa santé et renforcer la relation médecin-patient.

**pour les professionnels de santé :*

Mieux se former, être mobile (hors cabinet, au domicile des patients, dans l'hôpital, en staff…), avoir des outils pratiques (calculateurs, base de données…), mieux suivre ses patients notamment chroniques, et renforcer la relation médecin-patient.

I.3.2.2. Applications de M-santé

La **Fondation des Nations Unies** a même organisé la définition de la m-Health avec les six catégories d'applications dans le domaine de la santé mobile :

1. Éducation et sensibilisation.
2. Téléassistance.
3. Diagnostic et traitement de soutien.
4. Communication et formation pour les professionnels de santé.
5. La maladie et le suivi d'une épidémie.
6. La surveillance et la collecte de données à distance

Au sein de ces applications, on retrouve diverses typologies de services et outils proposés tels que :

- Guides thérapeutiques.
- Calculatrices et scores médicaux.
- Analyses de courbes. Cotations des actes médicaux.
- Aides aux premiers secours, gestes d'urgence.
- Fiches pratiques.
- Géolocalisation.
- Applications de bien-être (ma grossesse, iSommeil…).
- Applications de prévention (Kisovki, Zerotracas, Besoin d'aide…).
- Mise en relation avec un panel d'experts.
- Mise en relation avec une communauté de patient (ex : PatientsLikeMe).
- Scanner un produit ou un médicament (permettant notamment le suivi de son traitement mais également s'assurer de la traçabilité. Sproxil permet par exemple de savoir si un médicament est faux par l'envoi d'un simple SMS). [**s2**]

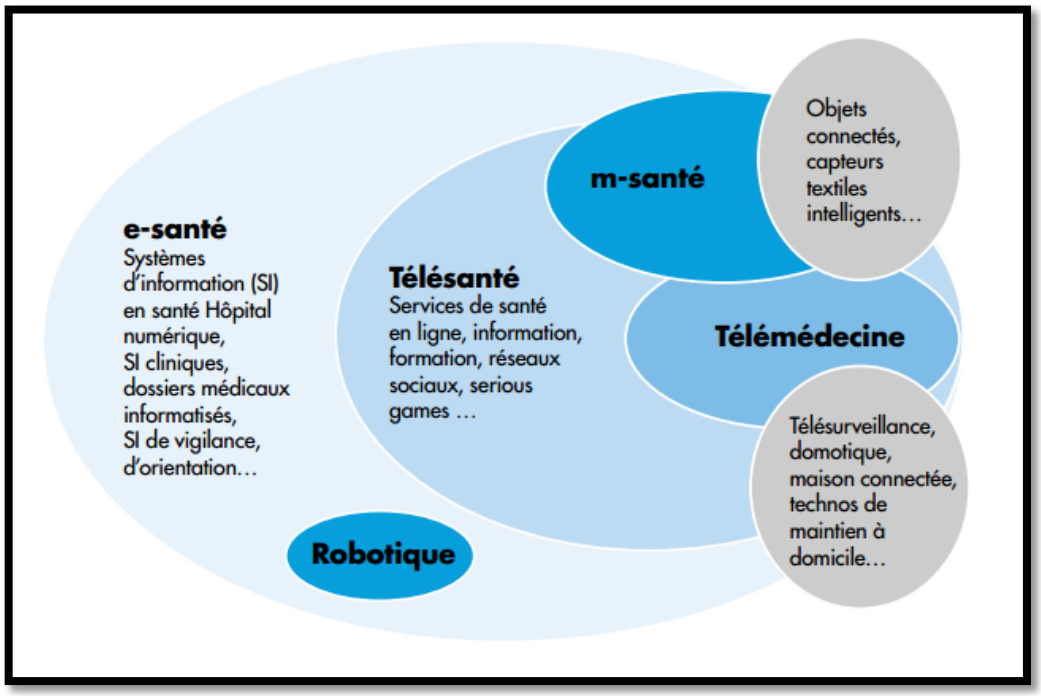
I.3.2.3. Recherche et innovation en m Health

Les programmes de financement de la recherche et de l'innovation de l'UE visent à créer des incitations qui encouragent le développement de solutions m Health innovantes. La commission a financé plusieurs projets de recherche et d'innovation liée à m Health, soit en développant des applications ou d'autres outils de santé mobiles.

Horizon 2020, le programme actuel de recherche et d'innovation, met l'accent sur la personnalisation de la santé et des soins (SSP), qui soutient l'autonomisation des citoyens par l'autogestion de la santé et des maladies, la promotion de la santé et la prévention des maladies.

I.3.2.4. Imbrication de ces disciplines

L'idée est de cartographier toutes ces activités, avec les hypothèses suivantes:



www.conseil-national.medecin.fr

Figure I.9 : Représentation générale de la santé connectée.

- La m-santé est inclue dans la e-santé car elle concerne la santé de manière globale, avec un recours aux TIC en situation de mobilité.

- La télé-santé est inclue dans la e-santé, ceci est vrai si l'on considère uniquement les moyens de communication électroniques (ce qui, avec le déclin des signaux de fumée, n'est pas loin d'être le cas).
- La tendance de la télé-santé est à la m-santé car elle exploite tout le potentiel des communications mobiles.

- e-santé et m-santé ne sont pas forcément des activités de télémédecine qui nécessite un professionnel de santé au bout de la connexion.
- Le quantified self peut intervenir dans la télé/e/m-santé, mais il sort également largement de ce cadre avec une finalité très souvent ludique et/ou sportive. [**s2**]

I.4. Les techniques de transmission utilisées en télémédecine :

La télétransmission est l'échange des données informatisées entre les divers secteurs de santé, afin de pouvoir être consultées et interprétées par des différentes professionnelles de santé. Elle peut être considérer comme « une pratique médicale coopérative aide à la décision clinique ».

Les techniques suivantes ne s'excluent pas mutuellement une application ou un service de télémédecine peut en employer une seule ou toute combinaison des trois :

I.4.1. La transmission audio

La transmission audio est une application courante et bien connue, utilisée par exemple pour une consultation médicale entre un patient et son médecin, ou pour un échange d'avis entre deux médecins. Un service de télémédecine à faible contenu technologique a été mis en place avec succès au Royaume-Uni. Une assistance téléphonique assurée par des infirmières permet aux patients de consulter un professionnel par téléphone pour être conseillés sur des problèmes simples.

I.4.2. La transmission de données

La transmission de données permet d'acheminer des données médicales de type statique (dossier médical, matériel de formation...) comme l'accès d'un médecin au dossier d'un

patient enregistré sur l'ordinateur d'un établissement spécialisé éloigné. Un transfert de documents par télécopie, ou la consultation par un généraliste d'une base de données ou d'une bibliothèque médicale informatisée afin d'actualiser ses connaissances, ou dynamique. Quant au transfert de données dynamiques, on peut donner comme exemple le monitorage depuis un hôpital des fonctions vitales d'un patient transporté en ambulance. Depuis peu, on trouve sur le marché des systèmes de télémesures médicales de ce type destinés à être installés sur des avions de transport de passagers.

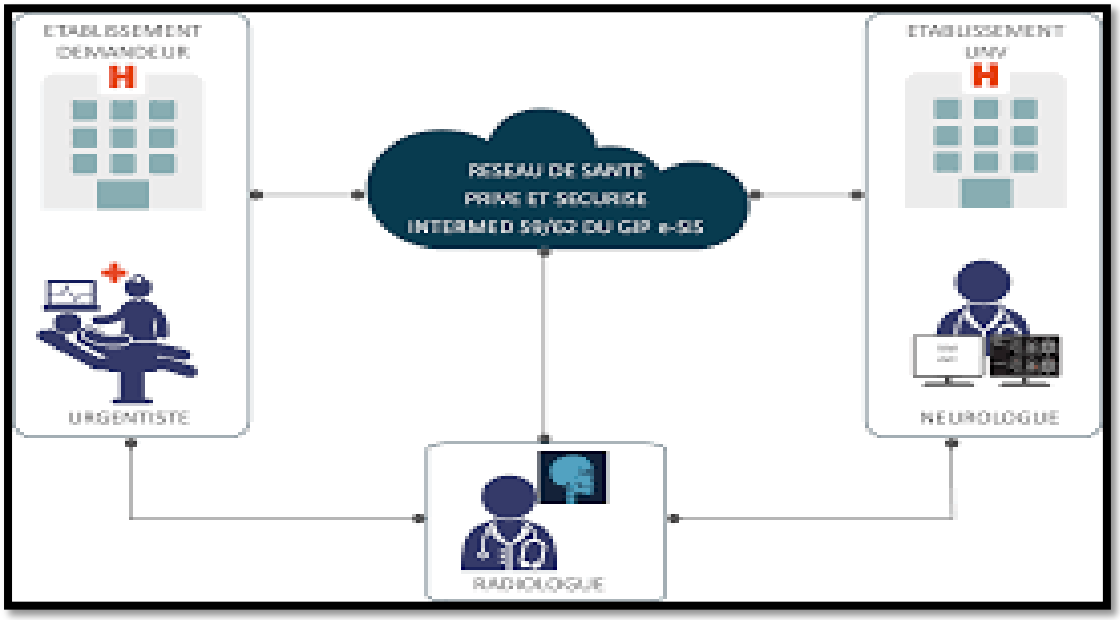
I.4.3. La transmission d'images

La transmission d'images peut concerner des images fixes (radiographies, etc.) ou animées (vidéo, etc.), à des fins de consultation, d'interprétation diagnostique ou de visioconférence. Les plus couramment échangées dans la pratique actuelle de la télémédecine sont les images radiologiques, qui comprennent les différents types suivants radiographie conventionnelle, scanographie, résonance magnétique, échographie, nucléaire (rayons gamma), thermographie, radioscopie, angiographie et angiographie par soustraction numérique. Dans certaines de ces techniques, l'image produite est analogique mais doit être numérisée pour une transmission efficace. [**15**]

I.4.3.1. la Télé-Imagerie :

La télé-imagerie est l'échange et le partage entre professionnels de santé, d'examens d'imagerie médicale et de données cliniques ou biologiques permettant le diagnostique de la maladie.

Elle répond au besoin croissant des professionnels de santé prenant en charge le même patient d'accéder à ses données médicale, dans un contexte de complexification du parcours de soins de ce dernier.



https://ronia.info/pages/b/bilan-t%C3%A9l%C3%A9-avc-littoral-pas-de-calais/

Figure I.10 : Le réseau Télé-imagerie.

*Sur le plan strictement réglementaire, la télé-imagerie relève de la télé-expertise.

La télé-imagerie repose sur des technologies largement diffusées s'articulant essentiellement auteur de deux outils:

- ♠ Le premier permettant le partage des images statiques (ex: scanner, IRM…) ou dynamiques (vidéo) entre deux ou plusieurs sites.
- ♠ Le second permettant l'organisation des professionnels de santé autour d'un workflow donnée. Des architectures techniques pour répondre aux contraintes de sécurité, d'archivage et de sauvegarde des données.

I.4.3.2. Avantages de la télé-imagerie

D'un point de vue clinique:

- ♣ Améliorations du diagnostic par l'accès à l'expertise et/ou par l'accès aux examens antérieurs.
- ♣ Diminution des examens redondants.

D'un point de vue économique:

- Diminution des transferts patients dans les cas d'urgences.
- Optimisations des gardes et astreintes au sein d'une communauté hospitalières territoriale.

D'un point de vue organisationnel:

- Répondre aux problèmes posés par la non-disponibilité d'expert d'imagerie médicale, plus particulièrement dans les cas permanences de soins.
- D'accéder à une expertise distante dans le cas des diagnostics complexes. [**16**]

I.5. Sécurisation des données médicales

L'échange d'informations médicales entre professionnels de la Santé est critique pour établir un diagnostic et pratiquer les soins adaptés au patient. Cependant, elle soit devenue incontournables, les gains de productivité engendrés par l'adoption de ces méthodes ne doivent pas masquer les menaces qu'elles peuvent impliquer.

Les informations médicales sont pour la plupart nominatives ou identifiables et doivent faire l'objet d'une sécurisation importante. Le respect du secret médical implique que, lors d'échanges électroniques, ces données soient protégées et sécurisées afin d'éviter qu'elles ne soient interceptées et consultées par des personnes non autorisées, voire modifiées ou altérées.

En résumé, pour ce type d'informations sensibles, la mise en œuvre d'échanges des données médicales doit s'accompagner d'un processus de réflexion sur les méthodes utilisées visant à d'une part respecter le secret professionnel et d'autre part à recueillir le consentement éclairé des patients. **[s3]**

La sécurité nous le permet d'assurer la confidentialité et l'intégrité des données reçus.

I.6. Conclusion:

La télémédecine est une nouvelle forme d'amélioration de la qualité des soins grâce aux nouvelles technologies d'informations et communications, et l'échangé de ses informations doit être sécurisé pour assurer une meilleur transmission qui est le but de notre projet de fin d'étude. L'innovation des différents actes de télémédecine facilitent la vie quotidienne des patients.

Le chapitre suivant est consacré à la présentation générale des méthodes et les algorithmes de chiffrement utilisés.

Chapitre II :

Techniques de Chiffrements et de Cryptographie

II.1. Introduction

Les systèmes de sécurité de transmissions des informations donnent une grande importance au domaine de cryptologie qui a le bénéfice de garantir la confidentialité et l'intégrité des messages envoyés. La cryptographie est utilisée depuis l'antiquité, mais depuis l'apparition des ordinateurs. Cette discipline a pris une ampleur sans précédente. Ses domaines d'utilisation sont très vastes et vont du domaine militaire au domaine commercial, en passant par l'utilisation privée, et en remarquant que le secteur médical est aussi besoin de ce système dans le transfert des données des patients.

Dans ce chapitre, on doit définir c'est quoi un cryptage ? Et quels sont les techniques utilisées pour le chiffrement des données ?

II.2. Cryptologie et cryptographie

Cryptologie : Est une science mathématique comportant deux branches : la cryptographie et la cryptanalyse.

Cryptographie : Est l'étude des principes, méthodes et techniques mathématiques reliées aux aspects de sécurité de l'information donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.

La cryptographie vous permet de stocker des informations sensibles ou de les transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne peuvent être lues par personne à l'exception du destinataire convenu.

Elle est l'art de chiffrer et coder les messages pour éviter une guerre ou une menace, protéger un peuple et parfois pour cacher des choses. En résumant les buts de cryptographie en quatre points essentiels :

- **Confidentialité :** mécanisme pour transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.
- **Intégrité :** mécanisme pour assurer que les données reçues n'ont pas été modifiées durant la transmission.

- **Authentification :** mécanisme pour permettre d'identifier des personnes ou des entités et de certifier cette identité.
- **Non-répudiation :** mécanisme pour enregistrer un acte ou une sorte que celle-ci ne puisse pas nier avoir accompli cet acte ou pris cet engagement. **[17]**

Cryptanalyse : opposée à la cryptographie, elle a pour but de trouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.

Étudie la sécurité des procédés de chiffrement utilisés en cryptographie. Elle consiste alors à casser des fonctions cryptographiques existantes, c'est-à-dire à démontrer leur sécurité.

La cryptanalyse mêle une intéressante combinaison de raisonnement analytique, d'application d'outils mathématiques, de découverte de redondances, de patience, de détermination et de chance. **[18]**

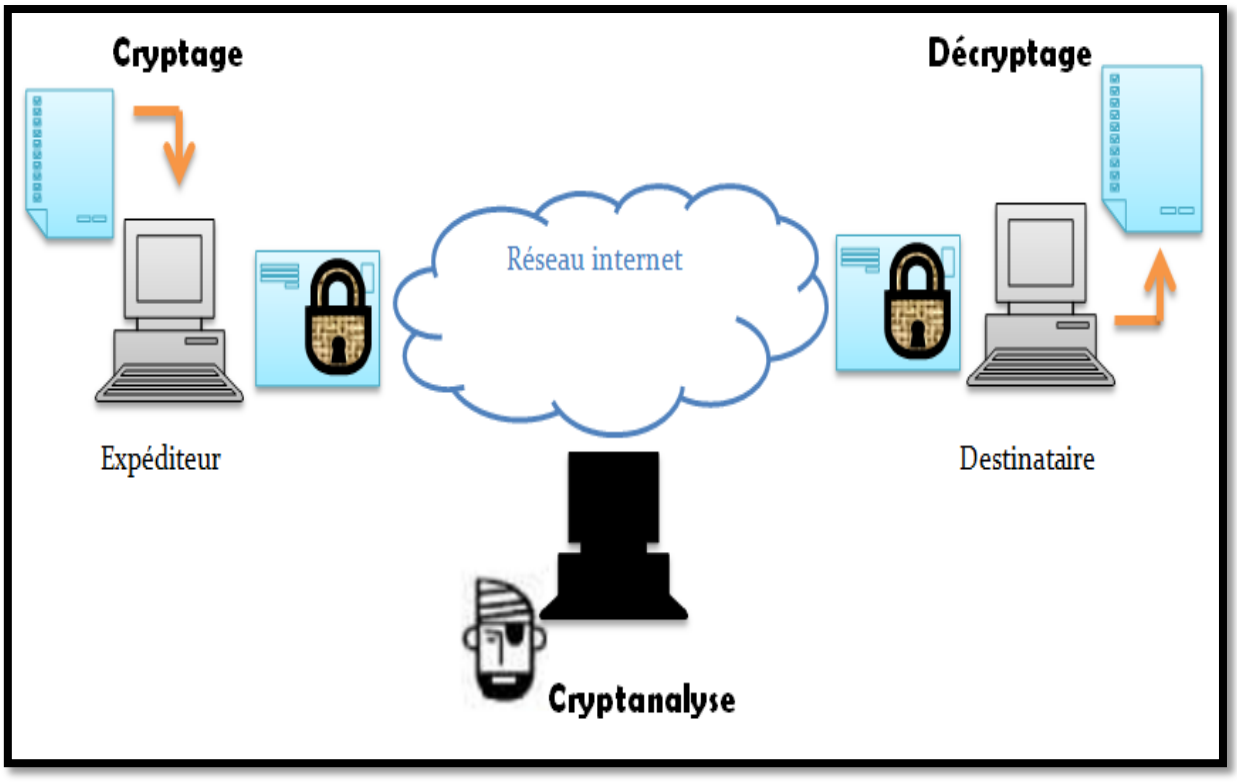


Figure II.1 : Principe de cryptographie.

Notions et définitions :

- ✓ **Cryptage :** aussi dite chiffrement ; consiste de transformer un message clair à un message crypté à l'aide d'une clef.
- ✓ **Décryptage :** dite aussi déchiffrement ; est la transformation inverse du cryptage qui permet de trouver à partir d'un message crypté, le message clair correspond.
- ✓ **Texte clair :** est le message réel avant aucune transformation.
- ✓ **Texte crypté :** appelé également cryptogramme, le message chiffré est le résultat de l'application d'un chiffrement à un texte clair.
- ✓ **Clef :** il s'agit du paramètre impliqué et autorisant des opérations de chiffrement et /ou déchiffrement.
- ✓ **Stéganographie :** quand notre information est non-chiffrée veut dire la connaissance de l'information. C'est un faible niveau de sécurité (message : ouvert, illisible ou invisible).

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 (l'antique méthode algorithmique en cryptographie). Avant d'entamer les différents algorithmes de la cryptographie, nous allons parcourir quelques attaques générés dans les réseaux.

II.3. Sécurité et attaques de systèmes actuels :

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, fonction de hachage, etc.) **[19]**

Les types d'attaques sur les algorithmes sont :

- **L'attaque en force (ou Brute force attack, Exhaustive keysearchattack) :** 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.

- **L'attaque à l'aide de l'analyse statistique (ou Statisticalanalysisattack) :** 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.

- **L'attaque à l'aide de textes chiffrés seulement (ou Ciphertext-onlyattack) :** 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.

- **L'attaque à l'aide de textes clairs (ou Known-plaintextattack) :** 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.

- **L'attaque à l'aide de textes clairs choisis (ou Chosen-plaintextattack) :** 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.

- **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.

- **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.

II.4. Techniques de Cryptage

Le cryptage est donc un moyen de transmettre les informations confidentielles de telle sorte qu'elles puissent être lues uniquement par des personnes autorisées.

La cryptographie n'est pas un technique moderne, ni un produit de l'ère informatique. En effet de tout temps, l'homme a besoin de cacher des informations confidentielles. Au cours des siècles, de nombreux systèmes de chiffrage ont été inventés, tous de plus en plus perfectionnés.

La majeure partie des méthodes d'antan reposait sur deux principes fondamentaux :

- **La substitution :** consiste à remplacer chaque lettre par une autre.
  - La substitution simple ou mono-alphabétique : Pour chaque lettre de l'alphabet de base on se donne une autre lettre utilisée dans le texte chiffré.
  - La substitution poly-alphabétique : qui utilise plusieurs alphabets décalés pour crypter le message.
  - La substitution homophonique.
  - La substitution poly-gramme.
- **La transposition :** consiste à permuter les lettres de message afin de les brouiller.

Cryptosystème: est un système de cryptographie qui constitué d'un algorithme de cryptographie, ainsi que de toutes les clés et tous les protocoles nécessaires à son fonctionnement.

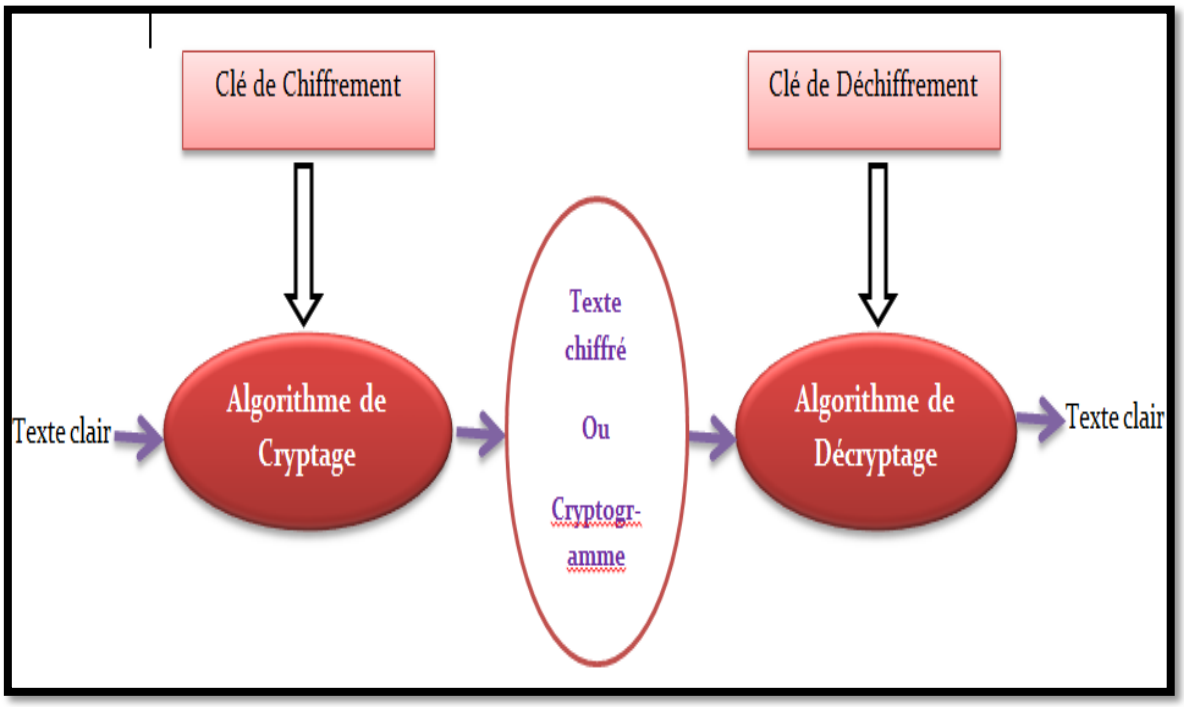


Figure II.2 : protocole de cryptographie.

On distingue deux principaux types de cryptage :

II.4.1. Cryptage symétrique

Ce type de cryptage consiste à l'utilisation d'une clé pour crypter l'information. Cette clé sera le même pour le décryptage après l'envoie. Ce type de sécurité repose sur le fait que la clé est connue uniquement par l'émetteur et le récepteur du message.

Cryptographie à clefs privées :

La cryptographie symétrique nommée cryptographie à clef privée est l'approche la plus authentique du chiffrement de données et mathématiquement la moins problématique. Cette clef sert à chiffrer les données, elle peut être facilement déterminé si l'on connait la clef utilisée pour le déchiffrement et vice-versa.

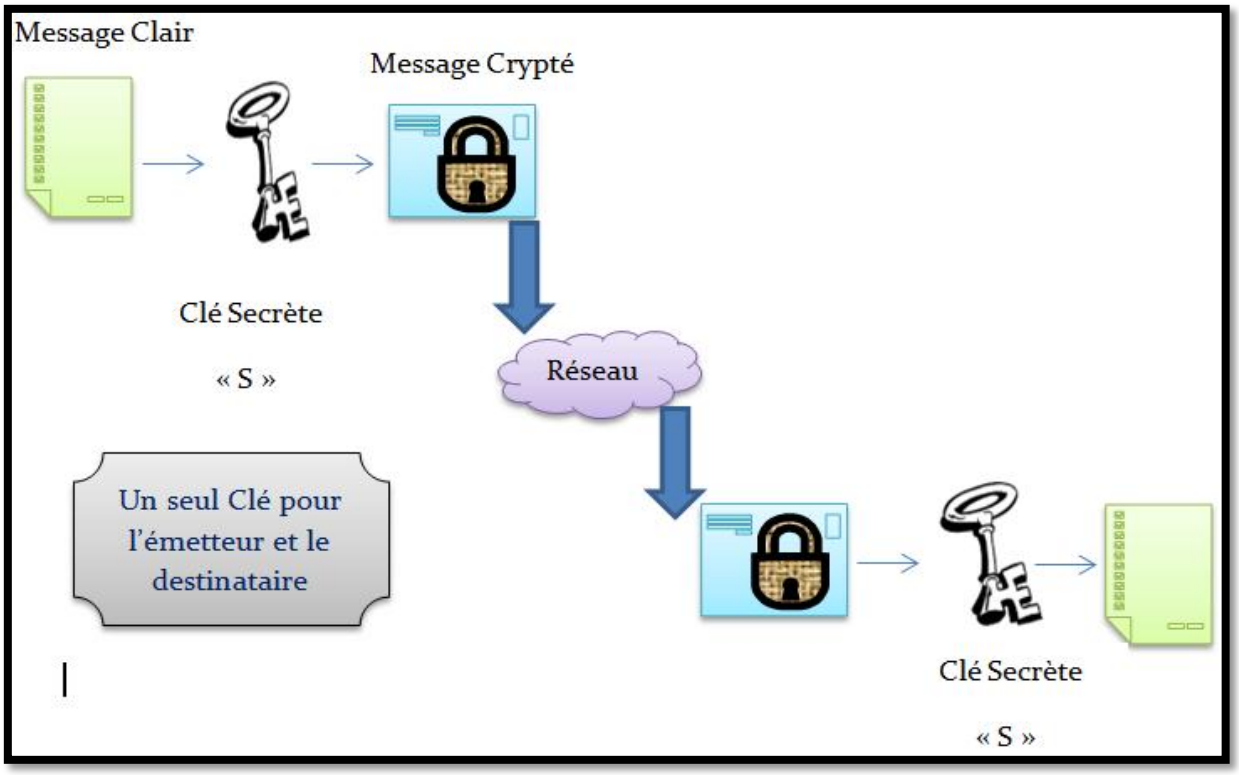


Figure II.3 : Cryptage de type symétrique.

Les principaux types de cryptosystème à clef privée sont : *Cryptosystème par flots* et *Cryptosystème par bloc.*

Cryptosystème par flots : Chiffrement en continu. Dans le Cryptosystème par flots, le cryptage ce fait caractère par caractère ou bit par bit. Leur principe est d'effectuer un chiffrement de Vernam, appelé aussi « One Time Pad » c'est-à-dire que la clef n'est utilisée qu'une seule fois. Cette clé (qu'on appellera par la suite pseudo-aléatoire) est générée par différents procédés à partir d'une clé secrète d'une longueur juste suffisante pour résister.

Cryptosystème par bloc : Dans un schéma de chiffrement par blocs, le message est divisé en blocs de bits, de longueur fixe. Les blocs sont chiffrés l'un après l'autre. Le chiffrement peut être effectué par substitutions et par transpositions. La substitution permet d'ajouter de la confusion, c'est-à-dire de rendre la relation entre le message et le texte chiffré aussi complexe que possible. La transposition permet d'ajouter de la diffusion, c'est-à-dire de réarranger les bits du message afin d'éviter que toute redondance dans le message ne se retrouve dans le texte chiffré.

On distingue le chiffrement par blocs itératifs. Une fonction constituée de combinaisons complexes de substitutions et/ou de transpositions, appelée fonction de tour ou fonction de ronde, est appliquée itérativement. Une itération est appelée un tour ou une ronde. Chaque ronde prend en entrée la sortie de la ronde précédente et chiffre cette entrée à l'aide de la fonction de ronde et d'une sous-clé de ronde générée à partir de la clé secrète K. La fonction de chiffrement n'est pas la fonction de ronde, mais elle est constituée par l'ensemble de toutes les rondes. **[20]**

II.4.1.2. Exemples

*Le cryptage XOR :

Le cryptage XOR est un système de cryptage basique mais pas trop limité. Ainsi, il a beaucoup été utilisé dans les débuts de l'informatique et continue à l'être encore aujourd'hui car il est facile à implémenter, dans toutes sortes de programmes. **[s5]**

Mécanisme :

Le XOR est un opérateur logique qui correspond à un "OU exclusif": c'est le (A OU B) qu'on utilise en logique mais qui exclue le cas où A et B sont simultanément vrais.
Voici sa table de vérité :

Table de vérité du XOR		
A	**B**	**(A XOR B)**
FAUX	FAUX	FAUX
FAUX	VRAI	VRAI
VRAI	FAUX	VRAI
VRAI	VRAI	FAUX

Tableau.1 : mécanisme de XOR

En informatique, chaque caractère du message à coder est représenté par un entier, le code ASCII.
Ce nombre est lui-même représenté en mémoire comme un nombre binaire à 8 chiffres (les bits).

On choisit une clé que l'on place en dessous du message à coder, en la répétant autant de fois que nécessaire, comme dans le cryptage de Vigenère. Le message et la clé étant converti en binaire, on effectue un XOR, bit par bit, le 1 représentant VRAI et le 0 FAUX. Le résultat en binaire peut être reconverti en caractères ASCII et donne alors le message codé. L'algorithme est complètement symétrique : la même opération est réappliquée au message final pour retrouver le message initial.

Remarque : Parfois, on applique une permutation circulaire aux bits du message final pour donner le message codé.

*RC5:

Le RC5 a été conçu en 1995. Il a l'avantage d'avoir une longueur de bloc de données variable, un nombre de rounds variable et une clé de longueur variable. Ainsi, l'utilisateur a le contrôle sur le rapport entre la vitesse d'exécution et la sécurité de son chiffrement. En général, une longue clé et un nombre élevé de rounds assurent une plus grande sécurité.

La taille des blocs de données pour sa part accommode différentes architectures de systèmes. La simplicité de l'algorithme du RC5 rend son implémentation facile et, le plus important, rend son analyse plus aisée. De plus, la forte utilisation des décalages de bits (appelés rotations) dans le chiffrement prévient l'usage de la cryptanalyse linéaire et différentielle. **[17]**

Chiffrement:

Il y a deux parties dans l'algorithme, soit une procédure d'expansion de la clé et une procédure de chiffrement. Les opérations utilisées sont l'addition modulo 2 (nombre de bits des blocs) (+), l'OÙ-Exclusif (XOR) et le décalage de bits vers la gauche.

.

En équations : Soient ;

K[0], K[1], ..., K[n] les sous-clés dérivées de la procédure d'expansion de la clé et A et B les deux parties d'un bloc de texte clair à chiffrer.

A = A + K[0] B = B + K[1].

Pour i allant de 1 jusqu'au nombre de rounds

A = ((A XOR B) <<< B) + K[2i]

B = ((B XOR A) <<< A) + K[2i + 1]

Fin Pour.

Déchiffrement:

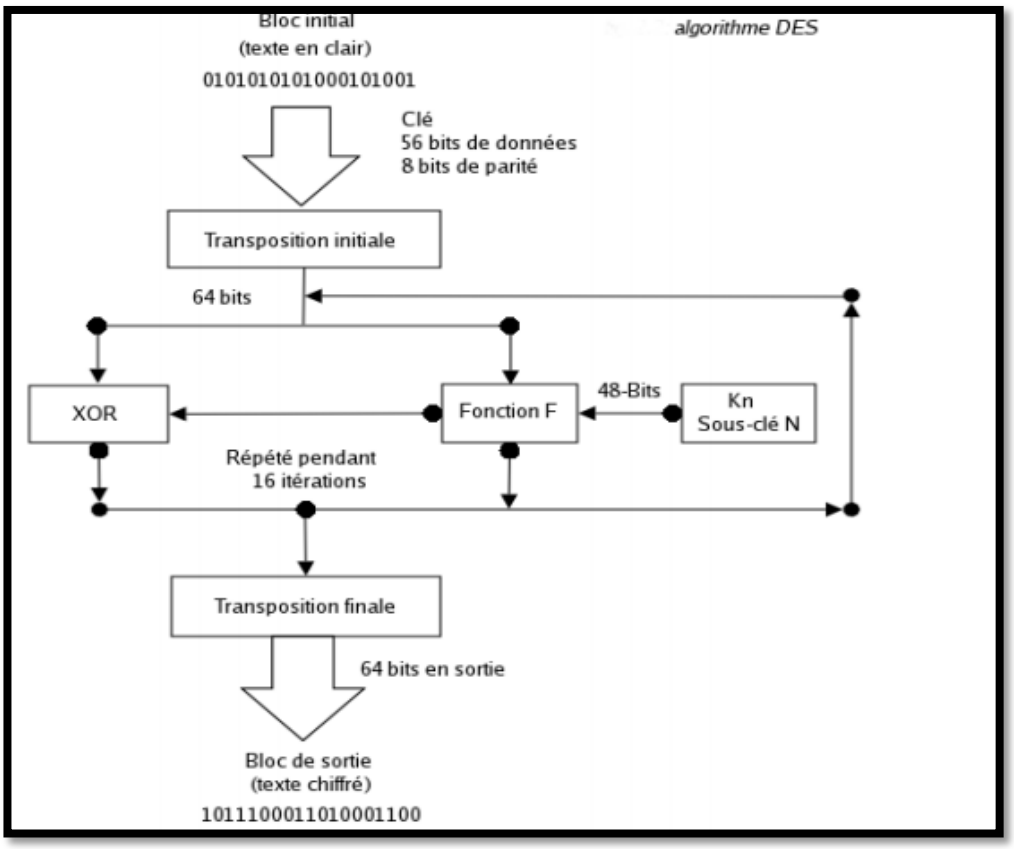
Le déchiffrement est exactement l'inverse du chiffrement.

*Algorithme DES: Data Encryption Standard

Le D.E.S. (Data Encryption Standard, c'est-à-dire Standard de Chiffrement de Données), publié en 1977, est un algorithme de chiffrement de donnée commandé par les organisations à caractère fédéral, commercial ou privé. Il est un algorithme symétrique par bloc qui permet de chiffrer des mots de 64 bits à partir d'une clef de 56 bits (56 bits servant à chiffrer plus de 8 bits de parités servant à vérifier l'intégrité de la clef en réalité). **[**21**]**

L'algorithme repose principalement sur 3 étapes, en plus de la gestion spécifique de la clé :

1. Permutation initiale.
2. Calcul médian (16 fois) : application d'un algorithme complexe appliqué en fonction de la clé.
3. Permutation finale.



https://fr.scribd.com/document/329124433/crypto-pdf

Figure II.4 : Principe de DES.

Déchiffrement : Il suffit d'appliquer le même algorithme mais inversé en tenant bien compte du fait que chaque itération du déchiffrement traite les mêmes paires de blocs utilisés dans le chiffrement. Il viendra :

$Rn-1 = Ln$ (1)

Et $Ln-1 = Rn \oplus f(Ln,Kn)$. (2)

II.4.1.3. Avantages et inconvénients d'un cryptage symétrique

- ***Avantages de cryptage symétrique :***

- La rapidité d'exécution (une seule clé utilisée).
- La simplicité d'implémentation (gestion d'une seule clé).

- Permet de concevoir différents mécanismes cryptographiques (fonctions de hachage, etc.)

- Clés relativement courtes.

- ***Inconvénients de cryptage symétrique :***

- La complexité de fonctionnement : une obligation d'avoir le nombre de clés privées égal au nombre de destinataires.
- La sécurisation de la chaîne de transmission de la clé.
- Impossibilité de garantir la propriété de non-répudiation dans les schémas de signature électronique **[s6].**

II.4.2. Cryptage asymétrique

Contrairement de cryptage symétrique, se base sur l'utilisation de deux clés : une clé « publique » pour crypté, et une autre clé « privée » (secrète) pour décrypté. Pour bien comprendre le principe, on peut l'illustrer avec l'échange d'une lettre entre un émetteur et un destinataire :

- L'émetteur possède deux clés : privé et publique. Il envoie sa lettre contenant la clé publique au destinataire.
- Le destinataire utilise la clé publique pour crypter son message; Il envoie tout à l'émetteur initial.
- L'émetteur utilise sa clé privée pour décrypter le message.

Cryptographie à clefs public :

L'idée de base des cryptosystèmes à clefs publiques est d'utiliser des clefs de chiffrement et déchiffrement différentes, non reconstructibles l'une à partir de l'autre :

- Une clef publique pour le chiffrement.
- Une clef secrète pour le déchiffrement.

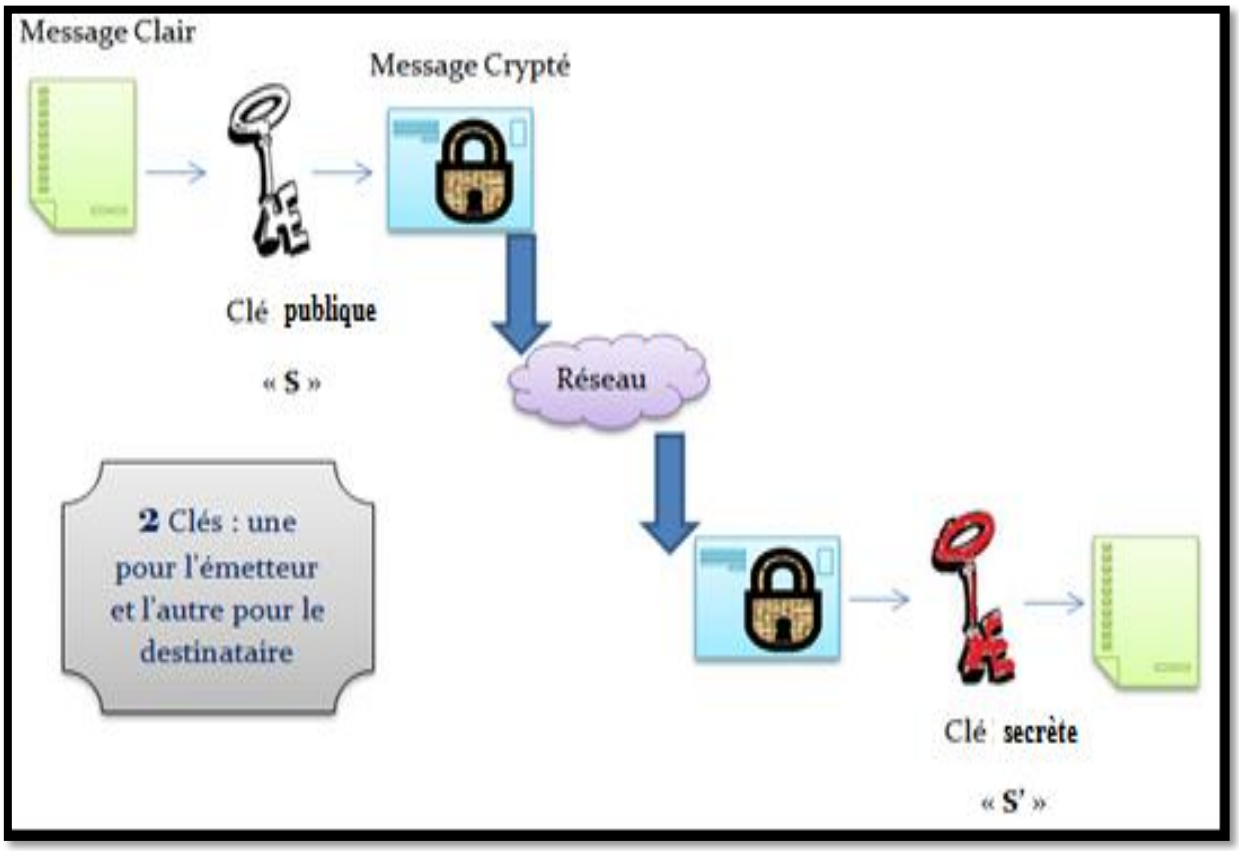


Figure -II.5. : schéma de cryptage de type Asymétrique

Ce système est basé sur une fonction à sens unique, soit une fonction facile à calculer dans un sens mais très difficile à inverser sans la clef privée.

Pour faire une explication imagée, la clef publique joue le rôle d'un cadenas. Imaginons que Bob possède la clef (clef secrète), Alice enferme son message dans une boite à l'aide du cadenas et l'envoie à Bob. Personne n'a pas pouvoir de lire le message puisque seul Bob possède la clef.

II.4.2.1. Exemple

*L'algorithme RSA :

L'algorithme fonctionne de la manière suivante : Imaginons que Bob souhaite recevoir d'Alice des messages en utilisant RSA.

1. ***génération des clefs:*** Le procédé de chiffrement RSA est un algorithme de chiffrement à clef publique. Celle-ci est constituée de la paire **(*n, e*)** où ***n*** est un entier de la forme : $n=p*q$ **(3)**
   où ***p*** et ***q*** sont deux entiers premiers (par exemple, $n=15$ car $15=3\times5$)
   et $e< (p-1)(q-1)$ est un entier premier avec1 $(p-1)(q-1)$ (par exemple, si $n=15$, alors $(p-1)(q-1)=2\times4=8$ et on peut prendre e=3 qui est premier avec 8).
   La clef privée est ***(p, q, d)*** où ***d*** est l'inverse de ***e*** modulo $(p-1)(q-1)$**:** cela signifie que : $e*d=k\,(p-1)(q-1)+1$ **(4)**
   pour un certain entier ***k.***.

2. ***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 quand à lui sa clef privée.

3. ***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 $C= M^e \bmod n$ grâce à la clef publique *(n, e)* de Bob et envoie *C* à Bob.

4. ***déchiffrement du message :*** Bob reçoit *C* et calcule grâce à sa clef privée $C^d \bmod n$. Il obtient ainsi le message initial M. **[22]**

II.4.2.2. Avantages et inconvénients

- ***Avantages de cryptage Asymétrique :***

- L'élimination de la problématique de la transmission de clé
- La possibilité d'utiliser la signature électronique
- L'impossibilité de décrypter le message dans le cas de son interception par une personne non autorisé.

-Une paire de clés (publique/secrète) peut être utilisée plus longtemps qu'une clé Symétrie.

- ***Inconvénients de cryptage Asymétrique :***

- Le temps d'exécution : plus lent que le cryptage symétrique.

- Le danger des attaques par substitution des clés (d'où la nécessité de valider les émetteurs des clés).

-Taille des clés, plus grand que celle des systèmes symétriques.

Une autre technique de chiffrement consiste à encoder les données de manière différente. Il est principalement utilisé pour la transmission de messages (courrier électronique et forums Usenet) sur l'Internet.

Dans ce contexte, nous implémentons le code64 sur Smartphone Android pour transformer des images médicales en chaine de caractère pour pouvoir les transmettre d'un dispositif à un autre. L'encodage des images en base64 permet non seulement l'optimisation d'espace de stockage et par conséquent accélération de débit binaire mais aussi la protection des données Médecin-Patient. La section suivante sera consacrée au principe de ce codage.

II.5.Code Base64

Le codage base64 est un codage permettant de transformer toute donnée binaire en une donnée n'utilisant que 64 caractères ASCII disponibles sur la plupart des systèmes informatiques, et acceptés dans les protocoles de transmission de messages (courrier électronique par exemple). **[s7]**

II.5.1.Principe du codage

Le principe de ce codage consiste à découper la donnée binaire en tranches de six bits, que nous nommerons *sextets*, et d'associer à chaque sextet un caractère choisi parmi les 26 lettres majuscules (A, …, Z), les 26 lettres minuscules (a, …, z), les 10 chiffres décimaux (0, …, 9), et les deux caractères + et /.

L'alphabet cible de ce codage comprend donc 64 caractères. La table ci-dessous montre les codes associés à chaque sextet.

Sextet	Code	Sextet(déc.)	Code	Sextet(déc.)	Code	Sextet(déc.)	Code
000000 (0)	A	000001 (1)	B	B000010 (2)	C	000011 (3)	D
000100 (4)	E	000101 (5)	F	000110 (6)	G	000111 (7)	H
001000 (8)	I	001001 (9)	J	001010 (10)	K	001011 (11)	L
001100 (12)	M	001101 (13)	N	001110 (14)	O	001111 (15)	P
010000 (16)	Q	010001 (17)	R	010010 (18)	S	010011 (19)	T
010100 (20)	U	010101 (21)	V	010110 (22)	W	010111 (23)	X
011000 (24)	Y	011001 (25)	Z	011010 (26)	a	011011 (27)	b
011100 (28)	c	011101 (29)	d	011110 (30)	e	011111 (31)	f
100000 (32)	g	100001 (33)	h	100010 (34)	i	100011 (35)	j
100100 (36)	k	100101 (37)	l	100110 (38)	m	100111 (39)	n
101000 (40)	o	101001 (41)	p	101010 (42)	q	101011 (43)	r
101100 (44)	s	101101 (45)	t	101110 (46)	u	101111 (47)	v
110000 (48)	w	110001 (49)	x	110010 (50)	y	110011 (51)	z
110100 (52)	0	110101 (53)	1	110110 (54)	2	110111 (55)	3
111000 (56)	4	111001 (57)	5	111010 (58)	6	111011 (59)	7
111100 (60)	8	111101 (61)	9	111110 (62)	+	111111 (63)	/

Tableau 2: Table du codage base64.

Exemple :

- Le mot Codage, codé en ASCII, a une longueur de 6× 8 = 48 bits :

  01000011 01101111 01100100 01100001 01100111 01100101,

- Ce qui donne un découpage de 8 sextets :

  010000 110110 111101 100100 011000 010110 011101 100101,

- Qui conformément au codage base 64 donné :

  Q29kYWdl.

Un traitement spécial est effectué si moins de 24 bits sont disponibles à la fin de la séquence de données à coder (elle n'a pas forcément une taille multiple de 24 bits). Dans un tel cas, des zéros sont ajoutés à la droite des données initiales pour aller vers le multiple de 6 bits le plus proche. Chaque paquet de 6 bits est converti dans l'alphabet. Puis on ajoute des caractères « = » complémentaires pour former quand même 4 caractères.

Puisque les données d'entrée doivent être constituées d'un nombre entier d'octets, seuls trois cas sont possibles en fin de séquence :

- Il reste exactement 3 octets à coder (24 bits), alors on obtient directement 4 caractères sans traitement complémentaire.
- Il reste seulement 2 octets (16 bits) à coder, alors on ajoute à droite 2 bits à zéros pour former 3 caractères de l'alphabet (3×6 = 16+2 = 18 bits) suivis d'un quatrième caractère « = » en complément.
- Il reste un seul octet (8 bits) à coder, alors on ajoute à droite 4 bits à zéros pour former 2 caractères de l'alphabet (2×6 = 8+4 = 12 bits) suivis de deux caractères « = » en complément.

II.5.2.Intérêt

L'intérêt de l'encodage base64 ne se trouve donc pas dans la représentation de données textuelles, mais surtout dans la représentation de données binaires.

Lorsque l'on veut représenter des données binaires (une image, un exécutable) dans un document textuel, tel qu'un courriel, la transcription hexadécimale en ASCII des octets multiplierait la taille par deux, l'encodage en base64 permet de limiter cette augmentation.

Par ailleurs, le reproche fait sur la lisibilité des données tombe de lui-même dans ces conditions : les données binaires n'ont pas vocation à être compréhensibles sans interprétation par un logiciel dédié (cas d'une image, par exemple). **[s8]**

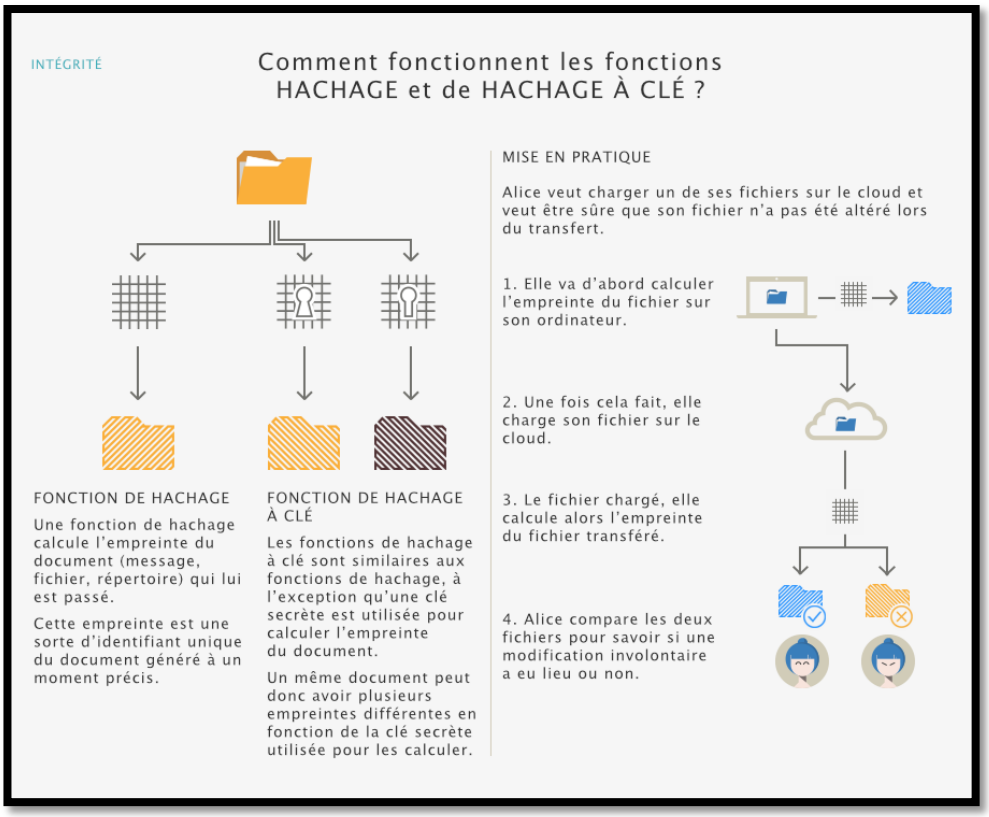
II.6.Fonction d'Hachage

La cryptologie permet justement de détecter si le message, ou l'information, a été involontairement modifié. Ainsi, une « **fonction de hachage** » permettra d'associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous. Cette empreinte est souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l'algorithme utilisé.

Il ne faut pas confondre le chiffrement, qui permet d'assurer la confidentialité, c'est-à-dire que seules les personnes visées peuvent y avoir accès, et le hachage qui permet de garantir que le message est intègre, c'est-à-dire qu'il n'a pas été modifié.

Le hachage est pour faire :

- *sauvegarder les photos sur votre espace d'hébergement et vérifier que le téléchargement s'est bien déroulé.*
- *synchroniser les dossiers et détecter ceux qu'il faut sauvegarder à nouveau et ceux qui n'ont pas été modifiés.*



https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

Figure -II.6. : la fonction d'hachage.

Fonctions de hachage à clé :

Il existe aussi des « **fonctions de hachage à clé** » qui permettent de rendre le calcul de l'empreinte différent en fonction de la clé utilisée. Avec celles-ci, pour calculer une empreinte, on utilise une clé secrète. Pour deux clés différentes l'empreinte obtenue sur un même message sera différente. Donc pour qu'Alice et Bob calculent la même empreinte, ils doivent tous les deux utilisé la même clé.

C'est parmi ces fonctions de hachage à clé que l'on trouve celles utilisées pour stocker les mots de passe de façon sécurisée. **[s9]**

II.7.Conclusion

Dans ce chapitre nous avons décrit la cryptographie et ses différentes attaques en parcourant les solutions et les méthodes de chiffrement. En outre, une comparaison entre cryptage symétrique et asymétrique a été présentée en termes de robustesse et efficacité.

Le chapitre suivant aborde la partie de simulation de notre projet de fin d'étude. Il s'agit de développement d'une Application Android sur mobile permettant le transfert des images sécurisées entre deux Smartphones.

Chapitre III :

Application mobile de transfert des images sécurisées

III.1. Introduction

Dans ce chapitre, nous nous sommes intéressés de réaliser une application Android permettant de communiquer des données sécurisées entre patient/médecin ou entre les professionnelles de santé dans le contexte du M-health.

Le but de ce travail est d'assurer la confidentialité et la fiabilité de la transmission pour une meilleure exploitation des services de télémédecine.

III.2. Description de l'application

III.2.1. L'idée de base

En partant de ce constat, l'idée de détourner ces appareils de leur fonction de base et d'en faire des outils exploités dans la télémédecine est apparue, et par conséquent à n'importe quel moment, à n'importe où, nous pouvons recevoir et envoyer des fichiers médicaux en temps réel.

L'idée de base est d'implémenter une application pour Smartphones Android, ayant la fonction de transformer des images médicales aux d'autres formats (base64) pendant la transmission.

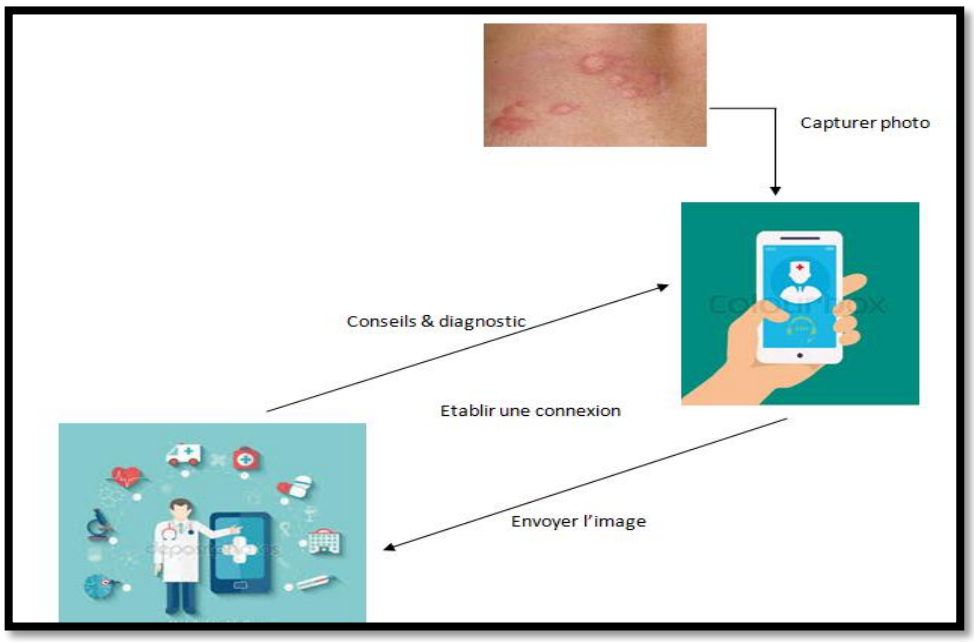


Figure III.1 : L'idée initiale de l'application.

III.2.2. Cahier de charge

Le cahier de charge de ce projet consiste à:

- Créer deux applications:
    - Une à installer sur le Smartphone pour capturer les photos, les cryptées, puis les envoyées.
    - La deuxième aussi installer sur un autre Smartphone/tablette pour recevoir le code et le décrypté.

- L'application doit être simple à utiliser et à installer.
- Programmer une interface utilisateur simple à exploiter.

III.2.3. Fonction

- Etablissement d'une connexion entre les deux terminaux mobiles.
- Capture de la photo.
- Codage/Décodage et transmission.
- Récupération de la photo.
- Lecture des images à l'écran.

III.2.4. Description générale

Cette partie comprendra une description générale sur le travail réalisé :

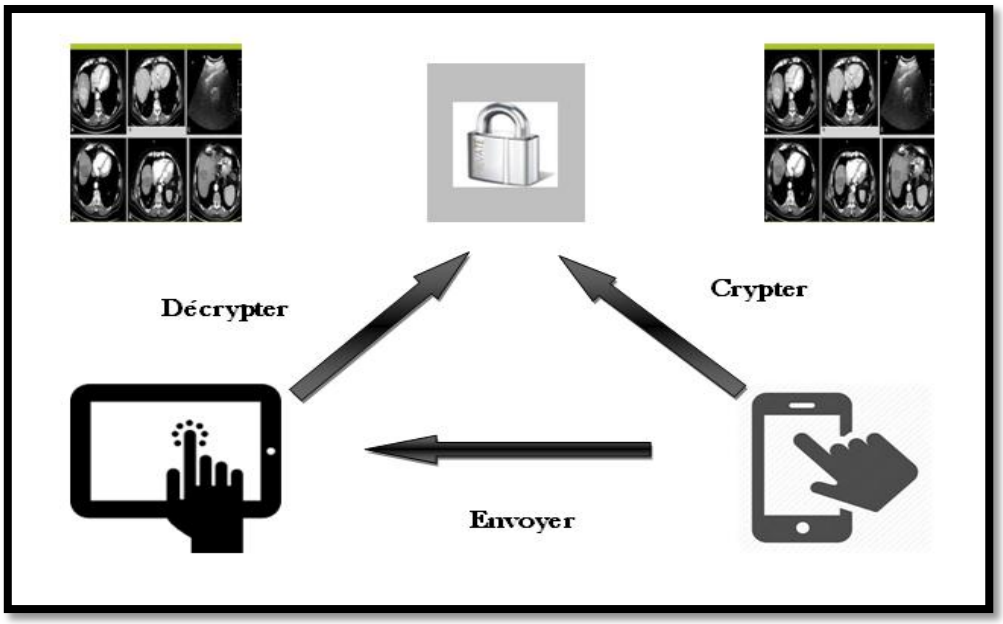


Figure III.2 : L'application réalisée.

- **Capture et l'enregistrement de l'image :** Cette partie ne nécessite pas d'étude particulière, si ce n'est la recherche des librairies qui permettent une telle manipulation d'un capteur.
- **Codage et décodage de l'image :** En implémentant le chiffrement ***Base64*** (cité en Chapitre II. **Page 39**), pour crypter et décrypter l'image capturée précédemment.
- **Etablissement de la connexion :** Cette partie qui devra être réalisée concerne l'interconnexion à distance des deux Smartphones. Il faudra se mettre d'accord connecter au réseau GSM ou 3G entre les deux appareils pour qu'ils puissent échanger leurs données.
- **Transmission de l'image :** La quatrième partie du projet consiste à trouver le meilleur moyen pour envoyer l'image à celui qui l'a demandée. Il existe plusieurs possibilités. On peut transférer une image par *SMS*, par *MMS* etc. Ces différentes possibilités font appel à un grand nombre de technologies, qu'il va falloir étudier et tester de manière à évaluer quelle sera la plus adaptée à ce projet.

III. 3. Réalisation

III. 3.1. Outils de développement

- **JDK (Java Développement Kit):**

L'écriture des applets et des applications Java nécessite l'utilisation d'outils de développement tels que le kit JDK. Ce dernier comprend l'environnement JRE, le compilateur Java et les API Java. Ainsi que les outils avec lesquels le code Java peut être compilé, transformé en byte-code destiné à JVM (la machine virtuelle Java).

- **SDK (Software Development Kit) Android:**

Le kit de développement (SDK) d'Android est un ensemble complet d'outils de développement pour un environnement précis.

Le SDK Android donc permet de développer des applications uniquement pour Android.

Au premier lancement de SDK, un écran semblable s'affichera (figure suivante):

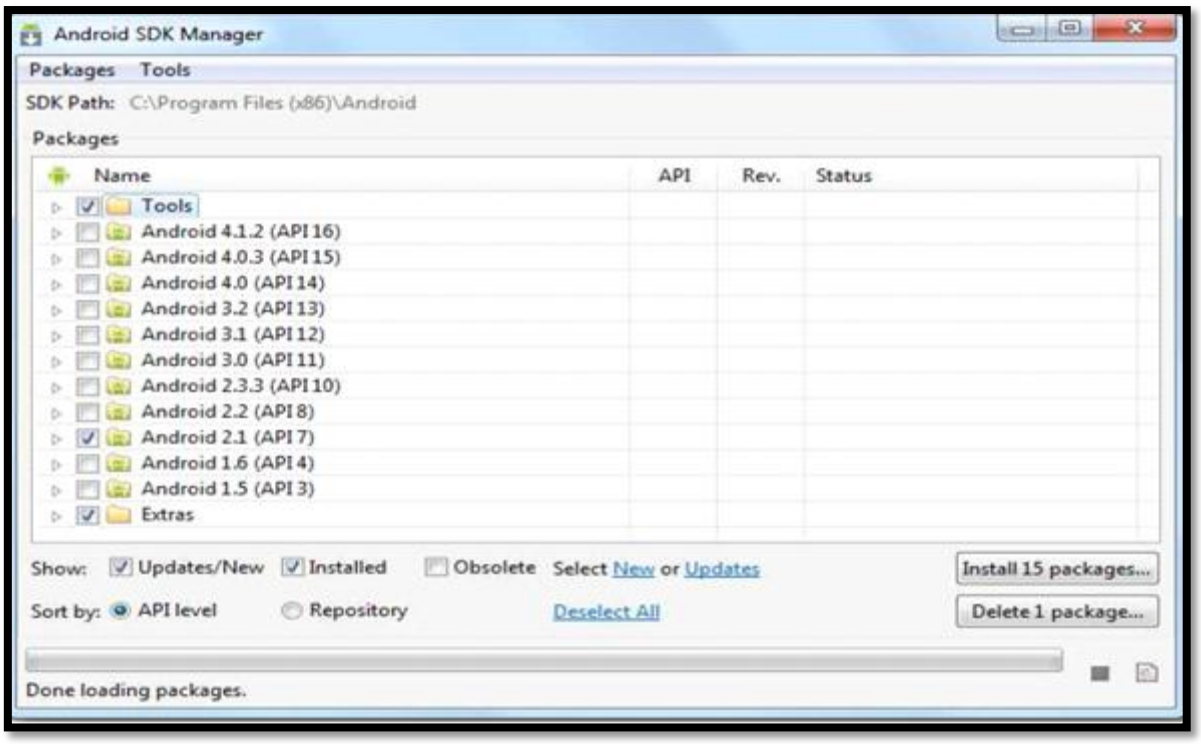


Figure III.3: SDK Android.

Pour développer une application Android, il faut prendre en compte la version d'Android (premier nombre) et la version d'API d'Android associée, puis qu'une application développée pour une version précise d'Android ne fonctionnera pas pour les versions antérieures.

- **IDE Eclipse:**

Eclipse est un IDE (environnement de développement intégré) écrit en Java, extensible par des greffons, multi-langages et multi-plates-formes, qui s'intègre particulièrement bien à GNOME (Acronyme de GNU Network Object Model Environnent).

Il est d'abord conçu pour le langage Java mais ses nombreux greffons en font un environnement de développement pour de nombreux autres langages de programmation (C/C++, Python, PHP, Ruby, …).

Toutes les fonctions qu'on peut attendre de ce genre de logiciel sont présentes ou existent sous forme de greffons (coloration syntaxique, complétion, debuggé, gestion de projets, intégration aux gestionnaires de versions, …).

- **Plugin ADT (Android developpement Tools):**

Un ADT est un plugin pour Eclipse fournit par Google, la fonction principale de ce plugin est de créer un pont entre éclipse et SDK Android.

- **L'émulateur de téléphone (Android Virtuel Device):**

Emulateur de terminal sous Android, c'est un logiciel qui fait croise a votre ordinateur qu'il est un appareil sous Android utilisé pour tester la plupart de vos applications.

Figure III.4: Emulateur

III. 3.2. Conception :

La conception est une étape préliminaire et primordiale qui doit précéder l'étape de développement de toute application informatique.

Pour décrire la conception de l'application, on montre le diagramme de cas d'utilisation.

❖ Diagramme de cas d'utilisation :

Le diagramme de cas d'utilisation ci-dessous nous montre l'interaction entre l'utilisateur et l'application. Les fonctionnalités principales sont : **le cryptage, l'envoie, la réception et décryptage.**

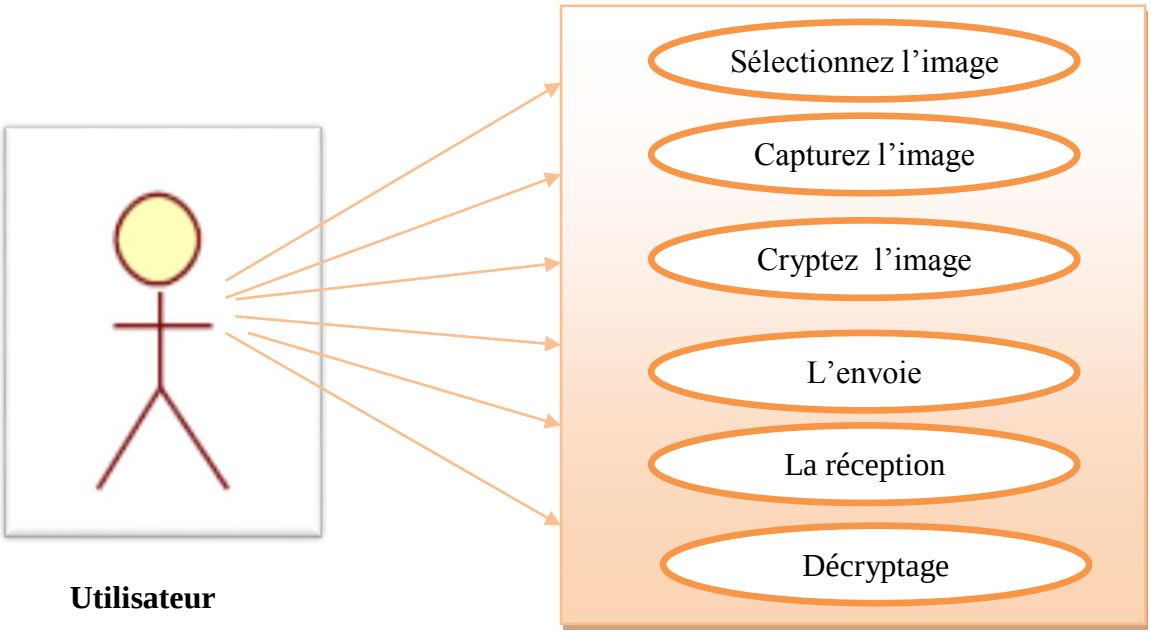


Figure III.5 : Diagramme cas d'utilisation

III. 3.3. Application :

Notre application a une structure Client/Serveur via SMS réalisée dans un projet Android.

L'émetteur va charger une image sur l'écran pour l'envoyer. Mais avant faire la transmission, il peut la cryptée puis l'envoyée en toute sécurité.

Ce qui nous s'intéresse c'est la partie émission (la 1ère App) puisque la même application soit installée chez le récepteur.

Ce qui concerne la réception, nous avons testé deux méthodes à l'envoi du SMS (longues distances). Alors, nous avons deux types (cas) de réception des données.

Pour aller au détail du notre travail, on suit les étapes suivantes :

Figure III.6 : Page d'accueil

❖ Partie Emission

Le menu principal de notre application

Cette interface contient cinq bottons **(voir la figure III.9)** :

- **Capturer :** Permet à prendre une photo et l'enregistrée à la Galerie.

 ***Botton cliqué pour capturer.**

- **Sélectionner :** Permet à l'utilisateur de sélectionner une photo enregistrée dans la Galerie.

 ***Botton cliqué pour sélectionner.**

- **Crypter :** Ce bouton lance l'algorithme de cryptage des images en format JPEG.

 ***Botton cliqué pour crypter.**

- **Envoyer :** Pour l'envoie des images cryptées via SMS.

***Botton cliqué pour envoyer.**

- **Décrypter :** Permet de décoder l'image et l'affichée autre fois.

***Botton cliqué pour décrypter.**

Figure III.7: La page Initiale (Menu).

1ère Etape : Chargement d'image :

- Dans cette étape, l'utilisateur peut prendre une photo et l'enregistrée (Figure **III.8**), ou sélectionner une image depuis la galerie de son mobile (Figure **III.9**).
- L'image s'affichera sur l'écran.

- **Fonctions :**
  1) L'utilisation d'une activité de méthode **StartActivityForResult** qui a deux paramètres pour la caméra :
  - **Intent (**appeler le système pour ouvrir la caméra avec l'instruction :

```
new Intent(android.provider.MediaStore.ACTION_IMAGE_CAPTURE);
```

  - **CAMERA_REQUEST :** cette variable est permet d'identifier la réponse de la caméra, on la déclarer par cette instruction :

```
private static final int CAMERA_REQUEST = 1888;
```

Deux autres paramètres pour la sélection :

  - **Intent :**

```
Intent(Intent.ACTION_PICK,android.provider.MediaStore.Images.Media.EXTERNAL_CONTENT_URI);
```

  - **ACTIVITY_SELECT_IMAGE :** `final int ACTIVITY_SELECT_IMAGE = 2;`

  2) Déclarer la méthode **onActivityResult :** cette méthode recevait le code requis (**request code**), code de résultat (**result code**) et **intent**;
  pour inclure les données de l'intention que nous avons commencées**.**

  3) Ajout des permissions dans le fichier manifest.xml :

```
<uses-permission android:name="android.permission.CAMERA"/>
<uses-permission
android:name="android.permission.READ_EXTERNAL_STORAGE"/>
<uses-permission
android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
```

  4) Les résultats doivent s'afficher dans une « ImageView ».

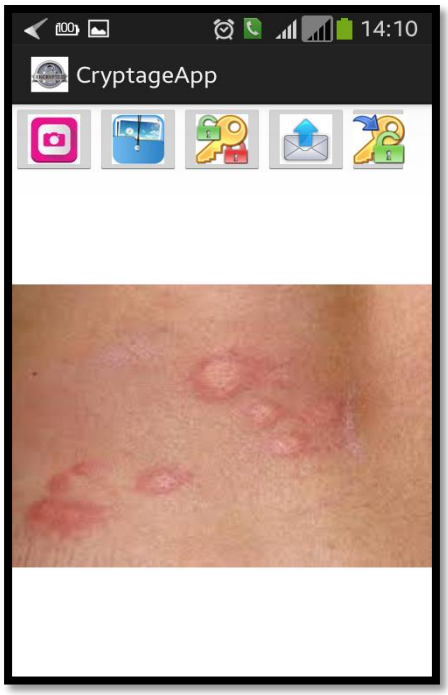


Figure III.8 : Photo capturée.

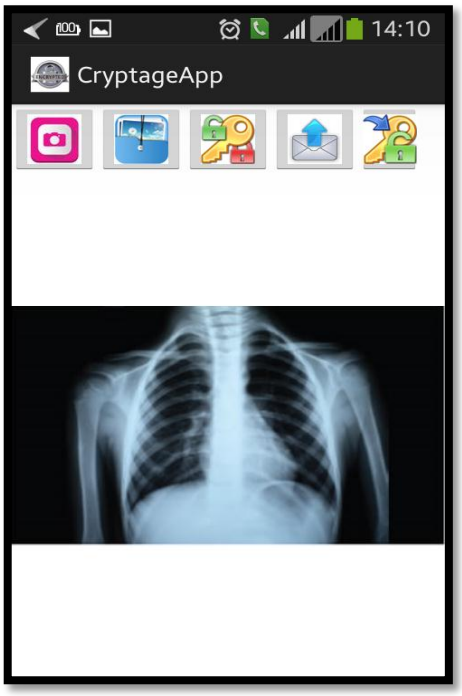


Figure III.9 : Une image sélectionnée.

2ème Etape : Cryptage de l'image :

- L'image sélectionnée doit être cryptée si l'utilisateur appuie sur le bouton de cryptage.
- Notre image doit convertir à une chaine de caractères.

- Nous avons appliqué l'algorithme de code *Base64*. Il sert à convertir l'image à des caractères de *Base64*.
- Notre algorithme est marche comme suit :
    1. Premièrement, convertir l'image au **bitmap ;**
       Bitmap : est un type de variable en Android qui va stocker des images en format bitmap.

    2. Compresser **bitmap** to **ByteArrayOutputStream;**
       ByteArrayOutputStream **:** permet de diriger le flux de sortie vers un tableau d'octets.

    3. Convertir **ByteArrayOutputStream** au **byteArray**:
       ByteArray : il consiste à stocker les données en octets dans une zone mémoire.

    4. Finallement, convertir **byte array** to **base64 string**.
- La chaine de caractère est affichée en un « TextView ».

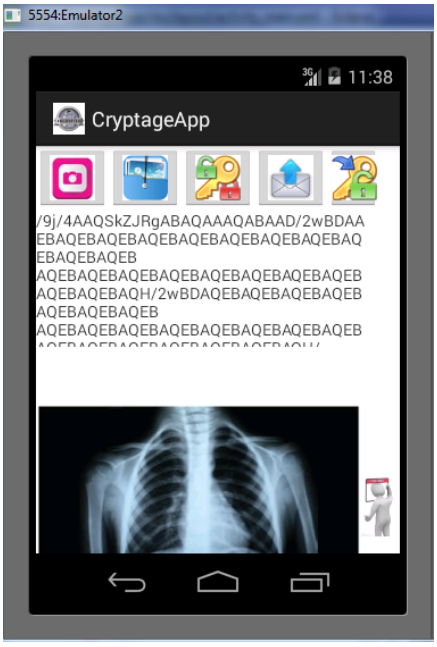


Figure III.10 : L'image cryptée.

3ème Etape : **Décryptage de l'image :**

- Cette étape revient après la transmission au deuxième Application installée au Tablette (autre mobile).
- Maintenant, on peut voir l'image reçoit par l'appuie au bouton décrypter.
- Dans le décryptage, on a utilisé l'inverse de code Base64.
- Employer le décodage de *Base64* en suit ces étapes :
    1) Convertir les caractères de Base64 en ByteArray.
    2) Ensuite, convertir ByteArray en Bitmap.
    3) Aperçu de l'image.

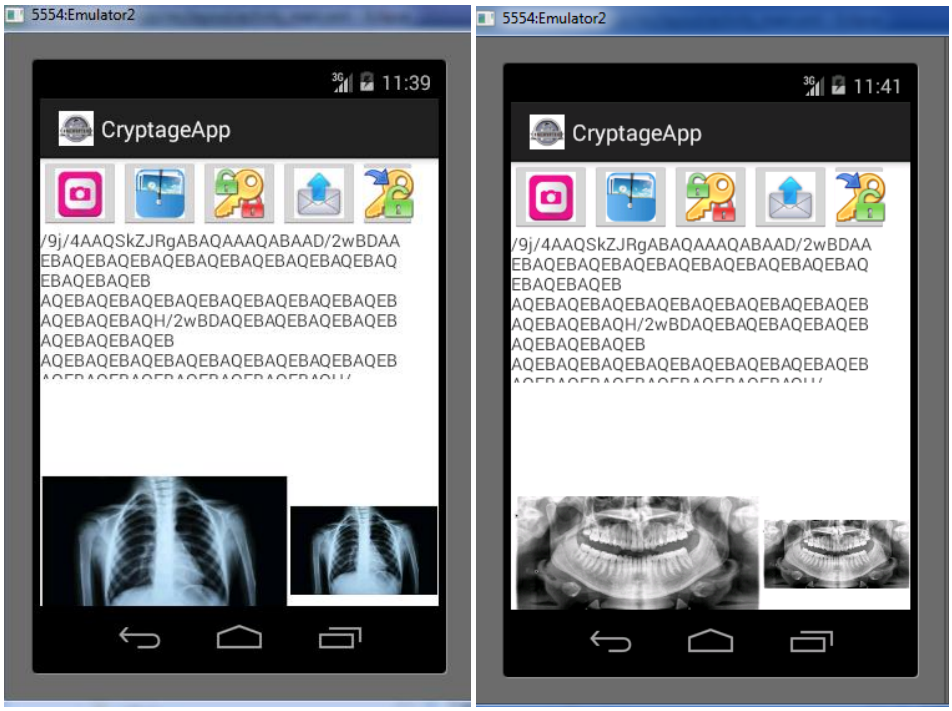


Figure III.11 : L'image cryptée et l'image décryptée.

4ème Etape : **L'envoie :**

- Dans cette étape, nous avons utilisé un algorithme de l'envoie par SMS.
- Nous avons effectué la méthode **sendMultipart :**

  Cette méthode permet de diviser le message en partie (des sous messages) et envoyer chaque partie seule. L'utilisation de cette technique est pour raison que notre message est très long, et la capacité d'un SMS est environ 164 caractères.

- Les figures suivantes montrent le lancement des deux émulateurs (5554 et 5558) en même temps pour faire l'envoie entre eux.

Figure III.12 : Interface de l'émulateur 5554.

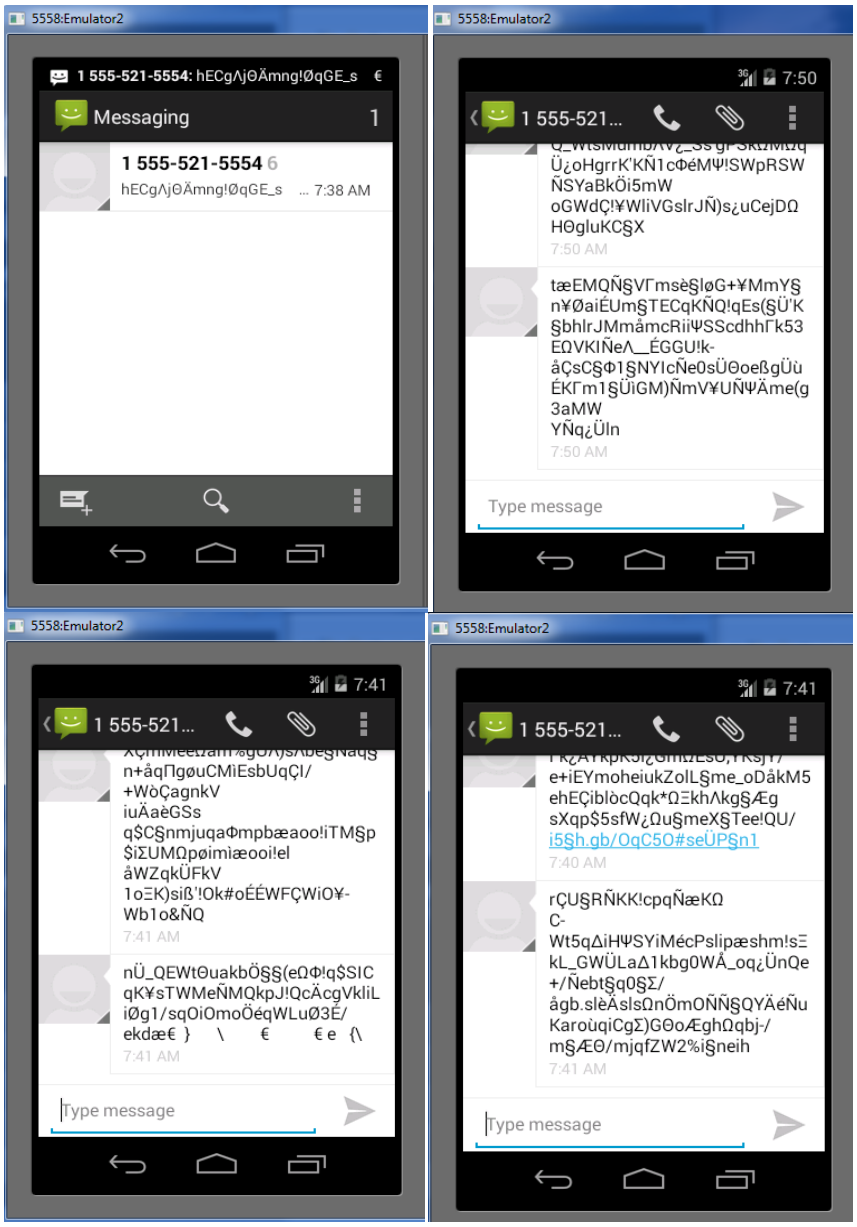


Figure III.13 : Interfaces de l'émulateur 5558 (reçois des SMS).

❖ Partie Réception

La réception dans la deuxième Smartphone doit être :

- Des sous messages que les doits recueillir pour former la chaine de caractère complète (**Figure III.13**). Et celui-ci se transforme par un décryptage Base64 à l'image initial.
- Une chaine de caractère affichée sur un TextView, elle est prête pour le décryptage.

Figure III.14: L'envoi à une application SMSReceive.

Interprétation de ces résultats :

- On remarque que l'image finale décryptée a les mêmes caractéristiques de l'image initiale cryptée.
- Notre algorithme de codage implémenté permet la transformation totale de l'image en cours. Comme montre les résultats on ne trouve pas une grande différence entre les images originales et les images après leurs décryptages. Donc, c'est une solution optimale qui assure la sécurité de notre image. Dont le but de faciliter leurs transferts à distance et par conséquent offre un outil d'échange sécurisé et de diagnostic efficace et fiable au médecin traitant.

Obstacles :

Durant notre travail, nous avons rencontré quelques problèmes :

Notre premier pratique de langage java et l'environnement éclipse.

La difficulté d'envoyer notre codage dans l'application réelle à cause des paramètres spécifique du réseau.

III.4.Conclusion

On peut conclure que notre travail nous a permis d'améliorer notre niveau en Informatique Industriel, mais surtout à la réalisation d'une application Android sous Eclipse.

Ce chapitre est consacré pour montrer les différentes fonctionnalités et étapes de notre application dédiée à la télé-imagerie. Nous avons converti l'image à une chaine de caractère de Base64 et nous avons pu la récupérée autrefois après sa transmission et l'affichée dans l'écran.

Les résultats obtenus par l'algorithme implémenté sur le Smartphone ne présentent pas une grande distorsion. Ce qui les rend fiable au niveau de prises de décision médicale par les médecins et les professionnels de santé.

Conclusion Générale

Le besoin de la transmission des données médicales et la communication entre les acteurs médicaux nécessitent une sécurité des échanges afin de garder le secret professionnelle Médecin/Patient.

Dans ce contexte, nous avons développé un algorithme sous l'outil Android basé sur le codage base64 afin d'assurer la sécurité des échanges entre deux Smartphones. Cet algorithme permet de capturer ou charger une photo puis les transformer en formats adéquats aux ressources et caractéristiques offertes par les terminaux mobiles. Il nous offre la possibilité d'optimiser la taille et d'accélérer le débit de la transmission afin de répondre aux besoins des services de la télémédecine et santé.

Les résultats de ce projet de fin d'étude ont été satisfaisants. Le travail effectué facilite le transfert des ressources gourmandes entre les acteurs médicaux et offre un service fiable et efficace aux professionnelles de santé. C'est le cas que l'on peut trouver dans de nombreux domaines tel que la télé-imagerie.

C'est une expérience très enrichissante sur tous les domaines. Enfin, ce travail nous a permis d'ouvrir d'autres horizons surtout avec l'intégration des Smartphones en domaine de santé. L'une des préoccupations majeures qui reste à développer comme une suite logique à notre travail consiste à réaliser l'application décrite précédemment mais avec d'autres type de chiffrement tel que RSA, DES, etc.

Bibliographie

[1] : E. CAUCHY, «Pôle d'excellence en médecine de montagne au pays du Mont Blanc», Projet en médecine.

[2] : Groupe de travail technique en télémédecine LA TELEMEDECINE EN ACTION: 25 PROJETS PASSES A LA LOUPE UN ECLAIRAGE POUR LE DEPLOIEMENT NATIONAL .Tome 1 : les grands enseignements mai 2012

[3] : B. BENLADGHAM et S. BAHRI «la télésurveillance cardiaque», D'ingénieur d'état en électronique biomédical, Université Abou Bekr Belkaid, Tlemcen, Algérie, Juin2003.

[4] : Rerbal Souhila,thèse de doctorat «traitement numérique du signal physiologique en télémédecine». Université Aboubekrbelkaid, Tlemcen, Algerie.2014

[5] : PierreSimon et Dominique Acker (Conseillers généraux des établissements de santé) Rapport:«La place de la télémédecine dans l'organisation des soins». NOVEMBRE 2008.

[6] : OLGA FEVER «HANDBOOKOFTELEMEDICINE» .indicissa 1998.

[7] : F.DUCHENE.«FUSION DE DONNEES MULTI CAPTEURS PAR UN SYSTEME DE TELESURVEILLANCE MEDICALE A DOMICILE» .thèse de doctorat en traitement du signal et imagerie. Université Joseph-Fourier -Grenoble I, 2004. French.

[8] : Faiçal hamza chrif, «TRANSFERT DU SIGNAL ECG D'UN POSTE LOCAL A UN POSTE DISTANT POUR LA TELESURVEILLANCE MEDICALE», master au télémédecine, université Abou BEKER BELKID, Tlemcen, Algérie ,2015.

[9] : «Développement et intégration de la télémédecine dans l'organisation des soins : les exemples à l'étranger», Mars 2013.

[10] : I. OUIS, «téléformation mobile entre les professionnels de santé», Master aux signaux et images en médecine, Université Abou Bekr Belkaid, Tlemcen, Algerie, Juin 2013.

[11] : F. DUCHENE, «Fusion de données multi capteurs pour un système de télésurveillance médicale de personnes `a domicile», thèse de Doctorat en traitement de signal et image, Université Joseph Fourier, Grenoble, France, Octobre 2004.

[12] : P. BURNEL, «Télémédecine: les premiers «tarifs préfigurateurs» versés avant la fin de l'année», délégué à la stratégie des systèmes d'information de santé au ministère de la Santé, Mars 2014.

http://www.lequotidiendumedecin.fr/actualite/exercice/telemedecine-les-premiers-tarifs-prefigurateurs-verses-avant-la-fin-de-l-annee.

[13]: Sommer .T, «Economic aspects of telemedicine», Health Telematics, DG XIII/C4, Commission européenne, Avril 1994.

[14] : « SANTÉ CONNECTÉE » : DE LA E-SANTÉ À LA SANTÉ CONNECTÉE, Le Livre Blanc du Conseil national de l'Ordre des médecins, 180 boulevard Haussmann 75008 Paris, conseil-national@cn.medecin.fr, JANVIER 2015.

[15]: Androuchko L. et Wright D., «Telemedicine and developing countries», Journal of Telemedicine and Tele care, vol. 2, nº 2, 1996, RSM Press Ltd.

[16] : C. Ducro, La Télé-imagerie , European Research in Telemedicine / La Recherche Européenne en Télémédecine, Volume 3, Issue 3, Septembre 2014, Pages 133-135.

[17] : Master Pro {Ingénierie Mathématique Cryptographie}- Chapitre1 : Introduction à la cryptographie, http://math.univ-lyon1.fr/~roblot/masterpro.html

[18] : Kebir Bahia , Rahmouni Samia, Développement d'une application pour

l'échange des messages sécurisés, Département d'Informatique ,Faculté des Sciences, Université Abou Bakr Belkaid– Tlemcen, 2014-2015.

[19] : Sandrine JULIA, « TECHNIQUES DE CRYPTOGRAPHIE », Jonathan BLANC Adrien DE GEORGES, 2003/2004.

[20] : NKAPKOP Jean De Dieu, Mémoire de Master en EEA. Cryptage chaotique des images basé sur le modèle du perceptron Université de Ngaoundéré.

[21] : Renaud Dumont, Cryptographie et Sécurité informatique, université de Liège, 2009-2010.

[22] : L. Poinsot, Projet Cryptographie, Université Paris 13, 30 novembre 2011.

Webographie

[**s1]**: http://www.qualitiso.com/esante-quantified-self-msante-telemedecine-definition/.

[s2]: https://lemondedelaesante.wordpress.com/2011/11/04/definition-de-la-m-sante/.

[s3]: http://www.safenet-inc.fr/data-protection/healthcare-information-security-solutions/.

[s4]: http://www.primenumbers.net/Renaud/fr/crypto/XOR.htm.

[s5]:http://www.bart-konieczny.com/fr/blog/securite-des-applications-web/cryptage-symetrique-et-asymetrique.

[s6]: http://www.fil.univ-lille1.fr/~wegrzyno/portail/Codage/Doc/TP/TP-Base64

[s7]: http://www.fr.wikipedia.org/wiki/Base64.

[s8]:https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement.

Références des figures

- http://www.dsih.fr/article/421/telemedinov-valorise-la-telemedecine-en-vendee.html
- http://dspace.univ-tlemcen.dz/handle/112/4516?mode=full
- http://www.esante-picardie.com/newsletter/la-lettre-du-gcs-e-sante-picardie-n%C2%B05/
- http://www.francetvinfo.fr/sante/professions-medicales/sante-telemedecine-teleconsultation-telesurveillance-des
- WWW.patients-servons-nous-de-l-innovation-pour-reduire-les-distances_2319177.html
- https://www.tele-assistance-senior.fr/teleassistance-des-personnes-agees.html
- http://www.medicalexpo.fr/prod/polycom/product-83803-528209.html
- http://slideplayer.fr/slide/3144849/
- https://upstatebusinessjournal.com/mhealth-links-docs-patients-wirelessly-247-lowers-costs/
- www.conseil-national.medecin.fr
- https://ronia.info/pages/b/bilan-t%C3%A9l%C3%A9-avc-littoral-pas-de-calais/
- https://fr.scribd.com/document/329124433/crypto-pdf