الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement Supérieur et de la Recherche scientifique

Université Mohamed Khider Biskra
Faculté des Sciences et de la Technologie
Département de Génie Electrique
Filière : Electronique
Option : Télécommunication

Réf:.....

Mémoire de Fin d'Etudes
En vue de l'obtention du diplôme:

MASTER

Thème

Système de cryptage de données sur dispositifs disponibles

Présenté par :
ATIA Naoual
Soutenu le : Juin 2013

Devant le jury composé de :

Mr. GUESBAYA Taha	MCA	Président
Mme. ELKOURD Kaouther	MCA	Encadreur
Melle. DJAALAL Nedjwa	MAA	Examinateur

Année universitaire : 2012 / 2013

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement Supérieur et de la recherche scientifique

Université Mohamed Khider Biskra
Faculté des Sciences et de la Technologie
Département de Génie Electrique
Filière : Electronique
Option : Télécommunication

Mémoire de Fin d'Etudes
En vue de l'obtention du diplôme:

MASTER

Thème

Système de cryptage de données sur dispositifs disponibles

Présenté par :

ATIA Naoual

Avis favorable de l'encadreur :

ELKOURD Kaouther *Signature*

Avis favorable du Président du Jury

GUESBAYA Tahar *Signature*

Cachet et signature

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement Supérieur et de la Recherche scientifique

Université Mohamed Khider Biskra
Faculté des Sciences et de la Technologie
Département de Génie Electrique
Filière : Electronique
Option : Télécommunication

Thème :

Système de cryptage de données sur dispositifs disponibles

Proposé par : ATIA Naoual
Dirigé par : Mr. GUESBAYA Tahar

RESUMES (Français et Arabe)

Résumé :

Dans ce travail, nous avons présenté la cryptographie et le chiffrement, explicité ces concepts de base pour arriver à prouver son efficacité dans le monde des transmissions sécurisées. Pour cela ,on à réaliser quelques algorithmes de chiffrement asymétrique(RSA, Signature RSA, ELGAMAL et signature ALGAMAL) dans un réseau local. Les résultats obtenus sont utilisés pour sécuriser les fichiers textes de toutes modifications, destructions ou consultations non autorisés. Cette application est exécutée dans un environnement sécurisé par plusieurs utilisateurs qui sont gérés à l'aide d'une base de données répartie. Le logiciel utilisé est le Builder C++.

ملخص :

في هذا العمل،درسنا الترميز التشفير، وعليه أوضحنا مفاهيم الأساسية للوصول إلى إثبات فعاليتها في عالم سرية البيانات .وعليه قمنا بتطبيق تقنيات التشفير الغير متناضرة وهي(RSA, Signature RSA, ELGAMAL et signature ALGAMAL) , حيث يتم تشغيل هذا التطبيق في تأمين متعدد المستخدمين, تدار البيئة باستخدام قواعد البيانات الموزعة.

Dédicace

Remerciement et louanges à mon Dieu, de m'avoir donné la foi et la force pour accomplir ce modeste travail.

Je dédie ce modeste travail

A mes très chers parents et ma grande famille.

A mes très chers frères et mes sœurs, surtout notre

Encadreur : Dr.Elkurd Kaouther.

A tous les enseignants de département

D'électronique a université de Biskra.

A toutes personnes qui m'ont encouragée et aidée de près

ou de loin merci de tout mon cœur.

Atia Naoual

REMERCIEMENT

Je tiens à remercier en premier lieu mon grand dieu qui j'ai donné la force et le courage pour continuer et j'avoir aidé et éclairé le chemin pour réaliser de ce modeste travail.

Je exprime mos remerciements à mon encadreur :" ***Dr.Elkourd kaouther****", pour ses merveilleux conseils et aides pendant mon travail de fin d'étude.*

Je remercie également tous les membres du jury, qui acceptent d'évaluer mon projet de fin d'étude.

Je remercie aussi mon famille, mes amis et tous les enseignants du département d'électronique pour ses grands efforts afin d'assurés une formation complète durant mon cycle d'étude.

Introduction générale :

Le besoin d'assurer la « sécurité » des communications entre les personnes se faisait toujours sentir. Ainsi, être sûr que les messages échangés n'ont pas été modifiés en cours de route ou encore interceptés par une tierce personne était un souci permanent qui ne s'est dissipé que par l'apparition des procédés de sécurisation avancés.

En effet de tout temps, les hommes ont ressenti le besoin de cacher des informations confidentielles. Bien évidemment depuis ses débuts la cryptographie a grandement évolué. Au cours des siècles, de nombreux systèmes de chiffrage ont été inventés, tous de plus en plus perfectionnés, et il est vrai que l'informatique y a beaucoup contribué. Mais au commencement les algorithmes étaient loin d'être aussi complexes et astucieux qu'à notre époque. Les messages secrets ont été depuis longtemps un sujet d'étude passionnant. Cette passion remonte au moins à l'Égypte antique (1900 avant J.-C.), ou à la Chine antique. En Europe, bien que les Grecs et les Romains aient déjà utilisé des messages chiffrés, la cryptographie et la cryptanalyse n'ont réellement démarré que dans la seconde moitié du treizième siècle et se sont développées plus sérieusement à partir du quinzième siècle.

En effet, la cryptographie est traditionnellement utilisée pour dissimuler les messages aux yeux de certains utilisateurs et garantir que seul les destinataires légitimes auront la possibilité de les consulter. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications circulent dans des infrastructures dont nous ne pouvons garantir la fiabilité et la confidentialité. La cryptographie sert, non seulement, à préserver la confidentialité des données, mais aussi à garantir leur intégrité et leur authenticité.

De ce fait, la cryptographie a pris une grande ampleur et elle est devenue une discipline scientifique à part entière, qui utilise des concepts mathématique et informatiques pour prouver la sécurité. Cependant, des attaques viennent périodiquement pour nuire la confiance des utilisateurs.

Dans ce travail, on a parler de chiffrement asymétrique dans un crypto-système qui repose sur un codage à deux clés utilisées par chaque utilisateur. Une clé privée et n'est connue que de l'utilisateur, l'autre est publique et donc accessible publiquement, et permet de faire la communication entre deux personnes à travers un canal peu sûr de telle sorte qu'un opposant (cryptanalyse) ne puisse pas comprendre ce qui est changé.

Les algorithmes proposé dans notre étude d'un système de chiffrement asymétrique a pour sécuriser un document quelconque qui sont : L'algorithme RSA, signature de RSA, El Gamal et signature d'El Gamal.

D'après ces algorithmes ci-dessus on pause quelque question comme problématique de ce projet :

Comment garante la sécurité de notre information ?quelle est le meilleur algorithme de chiffrement ?

Le travail est organisé comme le suivant :

Le premier chapitre présente un aperçu général sur la sécurité d'un système d'information, en parlant de ses critères, ses objectifs, ses menaces et ses attaques, ainsi que ses différentes techniques.

Le deuxième chapitre passe en revue la notion de chiffrement symétrique, chiffrement asymétrique, et on va concentrer surtout sur les algorithmes du chiffrement asymétrique qui est l'objectif de notre travail.

Dans le troisième chapitre on va présenter la conception et la mise en œuvre de notre crypto système en commençant par environnement du développement, conception globale, conception détaillé, les structures de données utilisées, et les algorithmes

La référence la plus importante utilisée dans ce projet est : Douglas Stinson. « CRYPYOGRAPHIE Théorie et pratique » 2^{eme} édition. Traduction de serge Vaudenay, Gildas Avoine et Pascal Junod.

Pour la préparation de ce projet ,on a trouvé des difficulté a cause de manque documentaires sur le système de sécurité, plus obligatoire d'utiliser et maitrisé nouveau logiciel qui est le Builder C++ ; ce dernier a un manque bibliographie.

I.1.Introduction :

L'information se présente sous trois formes : les données, les connaissances et les messages.

Un système d'information désigne l'ensemble des moyens techniques et humains qui permet de stocker, de traiter ou de transmettre l'information **[1]**.

Aujourd'hui les systèmes d'information sont fortement sollicités dans les affaires et ceci augmente considérablement les risques liés aux utilisateurs finaux, à la circulation des données au travers de périphériques mobiles et aux défauts de conformité et de sécurité des biens informatiques (matériels, logiciels, les applications de gestion, les données sensibles). Donc les entreprises prennent conscience qu'elles doivent gérer et maintenir un niveau de sécurité et de conformité en regard des attentes du business.

I.2.Sécurité d'un système d'information (SSI) :

Le concept de **(SSI)** recouvre un ensemble de méthodes, techniques et outils chargés de protéger les ressources d'un système d'information afin d'assurer les critères de sécurité **[1]**.

I.3.Critères de la sécurité d'un système d'information :

La sécurité des systèmes d'information repose sur cinq critères **[2]** :

I.3.1. Disponibilité :

Garantir la continuité du service et assurer les objectifs de performances (temps de réponse) en respectant les dates et les heures limitées de traitement. **[3]**

I.3.2. Intégrité :

Garantir l'exhaustivité, l'exactitude, la validité et le non redondance de l'information et éviter sa modification, par erreur ou par malveillance. **[3]**

I.3.3. Confidentialité :

Réserver les accès aux données en fonction de leur niveau de classification et du niveau d'habilitation des «utilisateurs», afin de garantir le secret des données échangées entre deux correspondants sous forme de messages ou de fichiers. **[3]**

I.3.4. Traçabilité :

Vérifier le bon déroulement d'une fonction, pour garantir la possibilité de reconstituer un traitement à des fins de contrôle de preuve (non-répudiation : impossibilité pour une entité de nier avoir reçu ou émis un message). **[3]**

I.3.5. Authentification :

L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées. **[3]**

I.4.Objectif de la sécurité des systèmes d'information :

La sécurité des systèmes d'information est une stratégie préventive à plusieurs objectifs, bien sûr liés aux types de menaces ainsi qu'aux types de ressources, etc.... **[4]**

L'objectif de la sécurité des systèmes d'information est de garantir qu'aucun préjudice ne puisse mettre en péril la pérennité de l'entreprise. Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits, et autoriser le retour à un fonctionnement normal à des coûts et des délais acceptables en cas de sinistre. **[5]**

I.5.Menaces d'un système d'information :

Ce sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité **[4].**

I.5.1.Catégories de menaces :

Il existe cinq grandes catégories de menaces : divulgation, interruption, modification, destruction et enlèvement ou perte.**[6]**

I.5.1.1.Divulgation :

Les biens exigeant une grande confidentialité sont vulnérables à la divulgation. Cette catégorie de menaces met les biens sensibles en danger par la divulgation non autorisée de renseignements de nature délicate. **[6]**

I.5.1.2.Interruption :

L'interruption touche principalement les services en s'attaquant à leur disponibilité. Une panne de courant est un exemple parfait de menace entrant dans cette catégorie. **[6]**

I.5.1.3.Modification :

Ce genre de menace compromet essentiellement l'intégrité des biens, laquelle, selon la PGS, englobe l'exactitude et l'intégralité des renseignements. Une tentative de piratage informatique ferait partie de cette catégorie s'il y avait des changements d'apportés. **[6]**

I.5.1.4.Destruction :

Tout ce qui détruit ou contribue à détruire les biens entre dans cette catégorie. Les biens qui nécessitent une grande disponibilité sont particulièrement vulnérables à la destruction . Les tremblements de terre, les inondations, les incendies et le vandalisme sont tous des éléments destructeurs. **[6]**

I.5.1.5.Enlèvement ou perte :

Lorsqu'un bien a été volé, perdu ou égaré, ce sont surtout les facteurs confidentialité et disponibilité qui sont en cause. Les ordinateurs portatifs ou portables sont particulièrement vulnérables à un enlèvement ou une perte.**[6]**

- Exemples de catégorie de menaces :

CATÉGORIE DE MENACES	EXEMPLES DE MENACES
DIVULGATION	Signaux compromettants Interception Procédures d'entretien inadéquates Piratage informatique
INTERRUPTION	Tremblement de terre Incendie Inondation Code pernicieux Panne de courant
MODIFICATION	Erreur d'entrée de données Piratage informatique Code pernicieux

DESTRUCTION	Tremblement de terre Incendie Inondation Pointes de courant
ENLÈVEMENT	Vol de données Vol de systèmes

Tab. I.1. Exemples de catégorie de menaces. [6]

I.5.2. Description de la menace :

Les menaces pouvant guetter les biens à l'étude doivent être décrites par le praticien. Elles peuvent être de nature accidentelle ou intentionnelle. **[6]**

I.6. Attaques d'un système d'information :

Elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables **[4].**

Le risque en terme de sécurité est généralement caractérisé par l'équation suivante **[7]** :

$$\textbf{Risque} = \frac{\textbf{Menace} * \textbf{vulnérabilité}}{\textbf{Les contres mesures}} \quad (\textbf{Equ. I. 1})$$

- **Les vulnérabilités :**

Ce sont les failles de sécurité dans un ou plusieurs systèmes.Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non **[4]**.

- **Les contre-mesures :**

Ce sont les procédures ou les techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité) **[4].**

I.6.1. Classification des attaques :

On peut classifier les attaques selon leurs adversaires dans les critères de sécurité comme suit

I.6.1.1. Attaques visant l'authentification :

- Spoofing IP :(en français mystification)

Est une technique permettant à un pirate d'envoyer à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate **[8][9][10].**

I.6.1.2. Attaques visant l'intégrité** :

-Bombe logique :

Ce sont les dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système. Les bombes logiques doivent être repérées au niveau applicatif, par un antivirus performant **[11].**

-Cheval de Troie :

Est un programme qui se cache lui-même dans un autre programme apparemment au-dessus de tout soupçon. Quand la victime (l'utilisateur normal) lance ce programme, elle lance par là même le cheval de Troie caché **[11].**

-Ver :

Est un programme capable de se propager et de s'auto-reproduire sans l'utilisation d'un programme quelconque ni d'une action par une personne. Sur chaque ordinateur où il agit, le ver crée une nouvelle liste de machines distantes cibles **[11].**

-Virus :

Est un programme susceptible d'entraîner des perturbations dans le fonctionnement d'un ordinateur en dénaturant ses programmes exécutables ou ses fichiers système **[11].**

I.6.1.3. Attaques visant la confidentialité :

- Le logiciel espion (spyware) :

Fait de la collecte d'informations personnelles sur l'ordinateur d'un utilisateur sans autorisation. Ces informations sont ensuite transmises à un ordinateur tiers **[12].**

- Scanner :

Est un programme qui permet de savoir quels ports sont ouverts sur une machine donnée. Les scanners servent pour les hackers à savoir comment ils vont procéder pour attaquer une machine **[13].**

- Sniffer :

Est un dispositif, logiciel ou matériel, qui permet de capturer les informations qui transite sur la machine où il se trouve **[13].**

I.6.1.4. Attaques visant la disponibilité :

-Le Mail Bombing :

Consiste à envoyer plusieurs milliers de messages identiques à une boîte aux lettres électronique afin de la saturer. En effet les mails sont stockés sur un serveur de messagerie, jusqu'à ce qu'ils soient relevés par le propriétaire du compte de messagerie. Ainsi lorsque celui-ci relèvera le courrier, ce dernier mettra beaucoup trop de temps et la boîte aux lettres deviendra alors inutilisable **[14].**

I.7. Techniques de la sécurité informatique :

Les techniques de la sécurité informatique se divisent comme suit **[15][16][17]** :

-Analyse de risques

-Politique de sécurité

-Politique de sécurité

I.7.1. Analyse de risques :

Plus aucune entreprise ne peut se passer de l'outil informatique, d'où la nécessité d'en assurer la sécurité, et de la protéger contre les risques liés à l'informatique. Or, comme on ne se protège efficacement que contre les risques qu'on connaît, il importe de mesurer ces risques, en fonction de la probabilité ou de la fréquence de leur apparition et de leurs effets possibles. Les risques et les techniques de sécurisation seront évalués en fonction de leurs coûts respectifs. **[15][16][17]**

I.7.2. Politique de sécurité :

A la lumière des résultats de l'analyse de risques, la politique de sécurité :

- Définit le cadre d'utilisation des ressources du système d'information;
- Identifie les techniques de sécurisation à mettre en oeuvre dans les différents services de l'organisation;
- Sensibilise les utilisateurs à la sécurité informatique. **[15][16][17]**

I.7.3. Techniques de sécurisation :

Les techniques de sécurisation d'un système incluent **[15] [16] [17]** :

- Contrôle des accès au système d'information ;
- Surveillance du réseau : sniffer, système de détection d'intrusion ;
- Sécurité applicative : séparation des privilèges, audit de code, rétro-ingénierie ;
- Emploi de technologies ad-hoc : pare-feu, UTM, anti-logiciels malveillants (antivirus, anti pourriel (SPAM), anti-espiogiciel (spyware) ;
- Cryptographie: authentification forte, infrastructure à clés publiques, chiffrement **[12].**

I.8. Conclusion :

Comme on vient de le voir, la question de la sécurité de l'information n'a pas de réponse standard. Sachant qu'il n'existe ni sécurité absolue, ni solution passe-partout.

Ce sont les entreprises elles-mêmes, qui peuvent apporter une réponse après avoir analyser ce qu'elles doivent protéger et déterminer les risques et l'origine des menaces qui lui sont spécifiées. Elles pourront alors identifier une politique de sécurité désignant un ensemble de règles qui fixent les actions autorisées et interdites dans le domaine de la sécurité, et incluant des mécanismes de sécurité permettant de réaliser les critères de la sécurité d'un système d'information précédemment citée. Parmi ces mécanismes, on va étudier dans le chapitre suivant le chiffrement.

II.1. Introduction :

Depuis toujours, l´être humain a cherché à conserver certaines informations ou données secrètes, à défaut, à en restreindre l´accès à certaines personnes. Un des plus anciens exemples de cryptographie est celui de Jules César **[18][19].**

Jules César utilisait une méthode spécifique pour ses échanges avec son état-major. En effet, les messages étant transportés par des messagers, il tenait à protéger la confidentialité des données. La méthode consistait à remplacer une lettre par un décalage de trois. De cette manière, seules les personnes au courant de ce subterfuge étaient capables de déchiffrer le message. Jusqu´au début du XXème siècle, la cryptographie a gardé une importance mineure, et les méthodes utilisées étaient bien souvent rudimentaires.

Lors de la seconde guerre mondiale, l´apparition de technologies de communication évoluées, telles que la radio, a rendu nécessaire la mise au point de mécanismes de cryptage empêchant l´interception des signaux par l´ennemi. Il était devenu indispensable de chiffrer les données transmises par les ondes (Enigma). On peut dire que, pour la première fois, la cryptographie a eu une réelle incidence sur le conflit **[18][19].**

II.2. Définitions :

II.2.1. Cryptologie :

La cryptologie est une science mathématique qui comporte deux branches sont la cryptographie et la cryptanalyse **[20][21]**.

II.2.2. Cryptographie :

La cryptographie est l'étude des méthodes permettant de transmettre des données de manière confidentielle .Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c'est ce qu'on appelle le chiffrement, qui, à partir d'un texte en clair, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré **[20][21]**.

II.2.3. Cryptanalyse :

La cryptanalyse, à l'inverse, est l'étude des procédés cryptographiques dans le but de trouver des faiblesses et, en particulier, de pouvoir décrypter des textes chiffrés **[20][21]**.

II.2.4. Chiffrement :

Définition du mot chiffrement, cryptage de données numériques par l'intermédiaire de fonctions mathématiques, et utilisant une clé de transformation. L'opération inverse nécessite cette même clé sinon les informations restent incompréhensibles **[22]**.

II.2.5. Déchiffrement :

Définition du mot déchiffrement, Opération faisant écho au chiffrement, ayant pour but l'obtention de version originale d'un message précédant chiffré **[23]**.

II.2.6. Décryptage :

Action de « casser » le chiffrement, et donc de retrouver le texte clair d'un chiffré, sans connaître la clé secrète **[24]**.

II.2.7. Clé :

Valeur qui paramètre un crypto système. Si elle est confidentielle, on parle alors de clé secrète ou privée, sinon on parle de clé publique **[24]**.

II.2.8. Crypto-système :

Un crypto-système est un terme utilisé en cryptographie pour désigner un ensemble composé d'algorithmes cryptographiques et de tous les textes en clairs, textes chiffrés et clés possibles (définition de Bruce Schneier **[25][26]**). Cette dénomination est toutefois confuse car très souvent associée à la cryptographie asymétrique avec l'utilisation d'une clé privée et d'une clé publique pour les opérations de chiffrement et de déchiffrement **[25][26]**.

II.2.9. Signature numérique :

Les digests de message sont très pratique pour indiquer qu'un message ou un autre objet a été, accidentellement ou délibérément, altéré, mais ils ne peuvent pas dire s'ils ont effectivement été créés par un individu ou une organisation donnée. C'est la qu'interviennent les signatures numériques.

Une signature numérique est une valeur calculée à partir d'une séquence d'octets en utilisant une clé secrète. Elle indique que la personne possédant cette clé secrète à vérifier que le contenu du message est correct et authentique. Les signatures numériques utilisent souvent les algorithmes de cryptage à clé publique avec une légère modification : une clé privée est utilisée

pour le cryptage et une clé publique pour le décryptage. Cette approche est souvent mise en oeuvre de la manière suivante :

La génération de la signature s'effectue par les étapes suivantes :

1. Un digest de message est calculé.

2. Le digest de message est crypté en utilisant la clé privée d'une paire de clés publiques/privée, pour générer la signature numérique du message.

La vérification de la signature s'effectue par les étapes suivantes :

1. La signature est décryptée en utilisant la clé publique de la paire de clés publique/privée, pour générer la valeur de digest de message.

2. La valeur de digest de message est comparée avec le digest de message calculé à partir du message d'origine.

3. Si les deux digests correspondent, la signature est authentique. Dans le cas contraire la signature ou le message ont été falsifies **[27]**.

II.3. Types de chiffrement :

Comme nous venons de le voir dans la partie précédente de nombreuses méthodes de chiffrement différentes ont été imaginées pour se protéger de la curiosité et de la malveillance de ses ennemis depuis de nombreux siècles. On peut classer ces méthodes en trois grandes classes, comme nous le montre le schéma qui suit **[28]**:

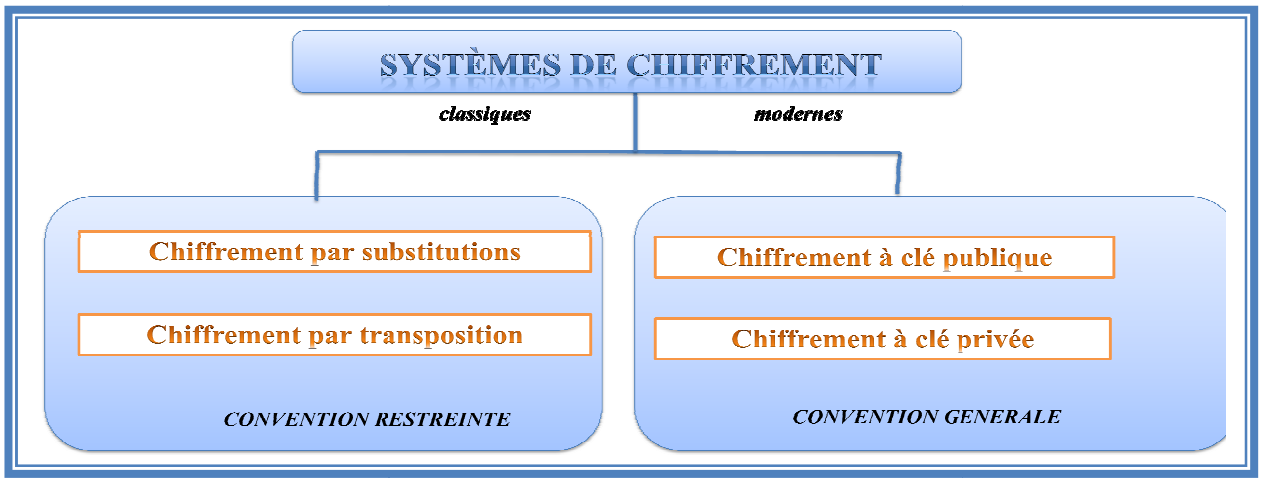


Fig. II.1. Types de chiffrement [28].

II.4. Chiffrement classique :

Il existe des centaines de façon de chiffrer des données représentées par l'alphabet classique, tout en gardant les opérations réalisées secrètes. Ici on ne va pas présenter toutes ces méthodes, mais plutôt les concepts mathématiques (connus depuis très longtemps) qui sont à la source de celles-ci. On va ainsi voir que finalement il n'y en a pas tant que l'on pouvait le penser, et surtout qu'elles sont extrêmement simples **[28]**.

II.4.1. Substitution:

La substitution consiste effectuer des dérivations pour que chaque caractère du message chiffré soit différent des caractères du message en clair. Le destinataire légitime du message applique la dérivée inverse au texte chiffré pour recouvrer le message initial. La complexité des systèmes à substitutions dépend de trois facteurs : **[28]**

- la composition spécifique de l'alphabet utilisé pour chiffrer ou pour communiquer,

- le nombre d'alphabets utilisés dans le cryptogramme,

- la manière spécifique dont ils sont utilisés.

On distingue couramment quatre types de substitutions différentes :

- **Substitution simple ou substitution monoalphabétique :**

Chaque caractère du texte en clair est remplacé par un caractère correspondant dans le texte chiffré. En effet avec ce principe, les lettres les plus fréquentes dans le texte en clair restent les plus fréquentes dans le texte chiffré.

-Faiblesse : il ne cache pas les fréquences d'apparition des caractères. Donc les algorithmes à base de substitutions monoalphabétiques sont facilement cassés par les spécialistes des techniques statistiques. Parmi les algorithmes de ce type de chiffrement en citant : **[28]**

-Algorithme de **Jules Cézar :** il est basé sur le décalage de 3.

-Algorithme de **ROT13 :** Il désigne simplement le code de Cézar, ou on choisit une ROTation de 13 lettres.

- **Substitution homophonique :**

Comme pour le principe précédent, sauf qu'à un caractère du texte en clair, on fait correspondre plusieurs caractères dans le texte chiffré. Par exemple, " A " peut correspondre à 5, 13, 25 ou 56 ; " B " à

7, 19, 31, ou 42 ; etc. Ce procédé est plus sûr, mais aussi craqué par les cryptanalyses ou des espions expérimenté**.** Parmi les algorithmes de ce type on a l'Algorithme de **Polybe. [28]**

- **Substitution polyalphabétique :**

Le principe consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prise dans un ou plusieurs alphabets aléatoires associés. Parmi les algorithmes de ce type on a l'Algorithme de **Vigenère. [28]**

- **Substitution par polygrammes :**

Les caractères du texte en clair sont chiffrés par blocs. Par exemple, " ABA " peut être chiffré par " RTQ " tandis que " ABB " est chiffré par " SLL ". Parmi les algorithmes de ce type on a l'Algorithme de **Hill. [28]**

II.4.2. Transposition :

Avec le principe de la transposition toutes les lettres du message sont présentes, mais dans un ordre différent. Il utilise le principe mathématique des **permutations**.

Il est important de faire remarquer que les transpositions sont plus contraignantes que les substitutions, car elles ont besoin de plus de mémoire et ne fonctionnent que sur des messages à chiffrer d'une longueur limitée ; c'est pourquoi elles sont moins utilisées dans les algorithmes bien que pourtant un peu plus sûres que les substitutions. **[28]**

II.5. Chiffrement moderne :

II.5.1. Chiffrement symétrique :

Pour cette technique, l'émetteur et le récepteur du message disposent de la même clé secrète. L'émetteur va utiliser cette clé secrète pour chiffrer le message. Le récepteur utilisera cette pour déchiffrer le message chiffré, et retrouver ainsi le message en clair d'origine **[29]**.

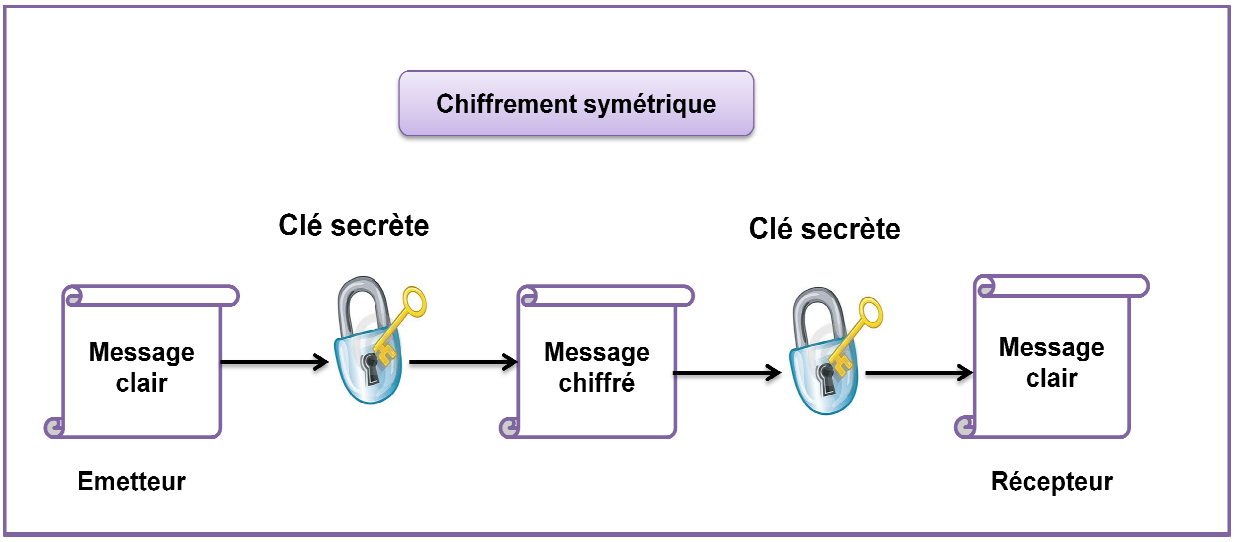


Fig. II.2. Chiffrement symétrique.

II.5.1.1. Avantages :

- Rapidité de chiffrement / déchiffrement,
- Confidentialité locale par un seul utilisateur (protection de fichiers dans une machine),
- Champs d'application très vaste (Banques, communications Téléphoniques),
- Longueur de la clé relativement petite codée entre 40 bits et 256 bits **[29]**.

II.5.1.2. Inconvénients :

- Si la clé est compromise (volée, piratée, …) le système n'est plus fiable et donc plus de confidentialité,
- Dans un réseau de N correspondants, il faut distribuer N (N-1)/2 clés par des canaux sûr et donc problème de distributions des clés par dévoies sécurisées14sécurisées. **[29]**

II.5.1.3. Outils :

- Substitution.
- Transposition.
- Ou Exclusif.
- Décalage logique.
- Combinaison des fonctions ci-dessus. **[29]**

II.5.2. Chiffrement asymétrique :

Cette technique repose sur le fait que la clé de chiffrement soit différente de la clé de déchiffrement. De plus, la clé de déchiffrement ne peut pas être calculée à partir de la clé de chiffrement et réciproquement. La clé de chiffrement appelée clé publique est destinée à être divulguée, tandis que la clé de déchiffrement appelée clé privée est gardée secrète.

Dans ce cas, la procédure à suivre est la suivante :

- l'émetteur E doit récupérer la clé publique du destinataire avec laquelle il va chiffrer le message en clair. Puis il va envoyer le message chiffré résultant au récepteur R ;
- ainsi le destinataire peut déchiffrer ce message chiffré avec sa clé privée et retrouver le message en clair d'origine. **[29]**

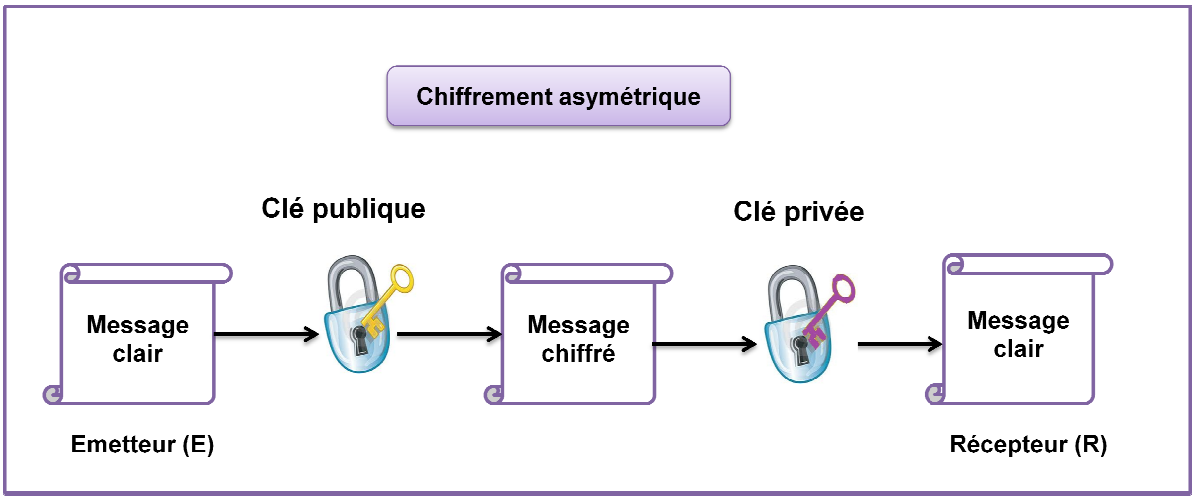


Fig. II.3. Chiffrement asymétrique.

II.5.2.1. Avantages :

- Échange de clé publique sur un canal non sécurisé (pas besoin d'un canal sécurisé),
- Possibilité de création de base de données des clés publiques,
- Authentification du message grâce à la signature numérique,

Nombre de clés croît linéairement avec le nombre d'utilisateurs →N utilisateurs →N pairs de clés. **[29]**

III.1. Introduction :

La conception est un processus créatif qui consiste à dégager les différents composants et outils nécessaires du projet, pour bien spécifier la méthodologie du travail et éclaircir les étapes ultérieures du développement de dernier.

L'implémentation (mise en œuvre du système) est une activité qui consiste à passer du résultat de la conception détaillée à un ensemble de programmes ou de composants de programmes.

Dans cette partie nous avant parlée la conception et mise en œuvre du notre système en décrivant son fonctionnement ainsi que son architecture détaillée, on va présenter dans ce chapitre l'implémentation de notre système qui se compose de trois éléments (émetteur, récepteur, connecteur).

D'abord, en va commencer de définir le logiciel utilisé et le type d'ordinateur appliqué.

II.2. Environnement du développement :

Le développement du notre système est basé sur l'environnement C++ Builder. Cet outil logiciel BORLAND, basé sur le concept de programmation orientée objet, permet à un développeur, même non expérimenté, de créer assez facilement une interface utilisateur/ordinateur d'aspect « WINDOWS ».

Builder C++ est un outil RAD, c'est à dire tourné vers le développement rapide d'applications (Rapid Application Development) sous Windows. En un mot, C++ Builder permet de réaliser de façon très simple l'interface des applications et de relier aisément le code utilisateur aux événements Windows, quelle que soit leur origine (souris, clavier, événement système, etc.).

Pour ce faire, C++ Builder repose sur un ensemble très complet de composants visuels prêts à l'emploi. La quasi totalité des contrôles de Windows (boutons, boîtes de saisies, listes déroulantes, menus et autres barres d'outils) y sont représentés, regroupés par famille. Leurs caractéristiques sont éditables directement dans une fenêtre spéciale intitulée éditeur d'objets. L'autre volet de cette même fenêtre permet d'associer du code au contrôle sélectionné.

Il est possible d'ajouter à l'environnement de base des composants fournis par des sociétés tierces et même d'en créer soit même.

Identification le système de mon micro-ordinateur :

Modèle : DELL.

Evaluation : 1.0 L'indice de performance Windows doit être actualisé.

Processeur : Intel® Core™ i3-2328M CPU @ 2.20 GHz.

Mémoire installée (RAM) : 4.00 Go utilisable).

Type de système : Système d'exploitation 32 bit.

Stylet et fonction tactile : La fonctionnalité de saisie tactile ou avec un stylet n'est pas disponible sur cet écran.

III.3. Conception :

III.3.1. Objectif du projet :

L'objectif du notre application est de réaliser quelques méthodes de «chiffrement» pour la sécurité d'un système d'information. Cette application visant à protéger les fichiers textes contre l'accès, l'utilisation, la diffusion, la destruction, ou la modification non autorisée.

III.3.2. Fonctionnement générale de l'application :

Le fonctionnement de l'application consiste à suivre les étapes suivantes (Voir fig. III.1):

- Ouvrir un fichier texte;
- Déterminer l'opération à effectuer (chiffrement / déchiffrement);
- Choisir la méthode concernant l'opération (RSA, signature RSA , EL Gamal ou signature EL Gamal);
- Enregistrer les modifications (fichier chiffré / fichier clair);
- Envoyer le fichier chiffré vers un autre poste dans le réseau (si on veut).

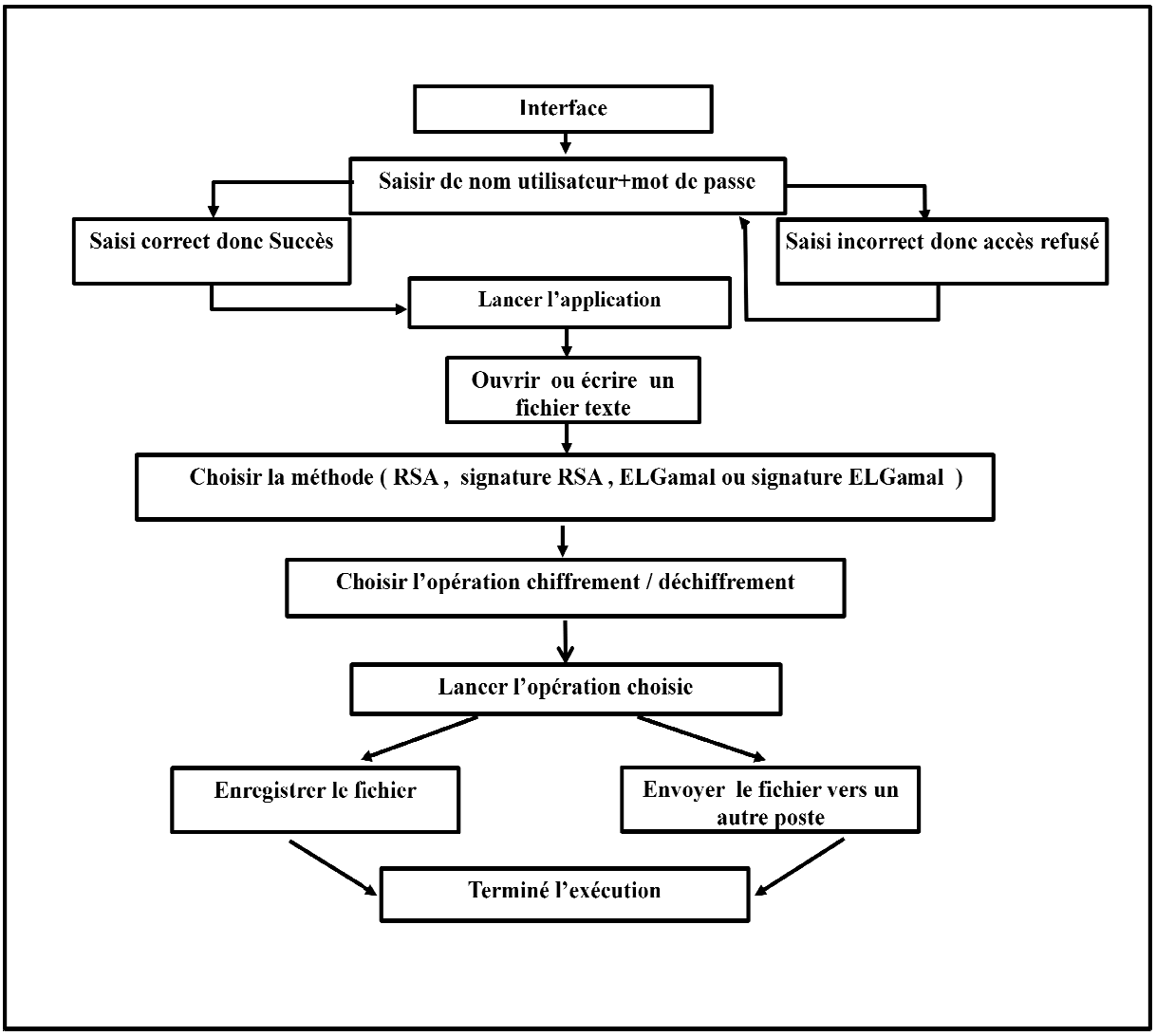


Fig. III.1. Fonctionnement générale de l'application.

III.3.3. Conception globale :

Dans cette étape, on parle de l'architecture globale de l'application et de l'architecture globale de ses composants.

Le schéma ci dessus présente l'architecture globale de notre application, qui est composée de deux composants principaux : Interface, Application. (Voir fig. III.2)

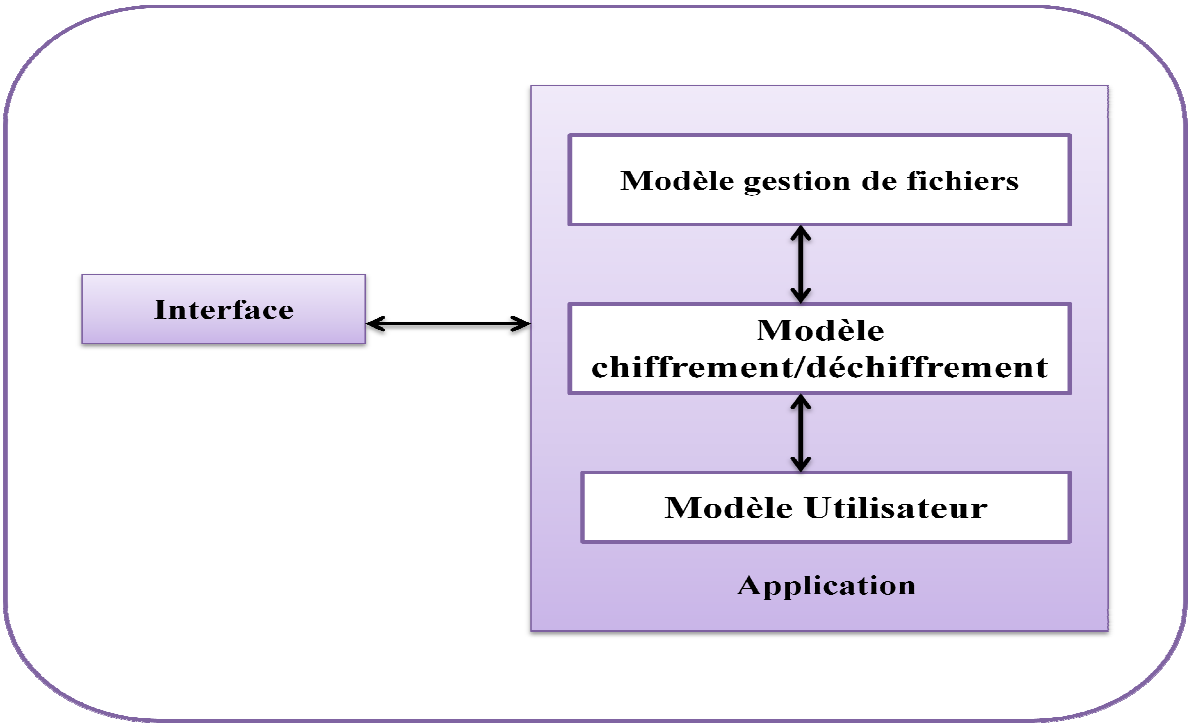


Fig. III.2. Architecture globale de système.

III.3.3.1. Interface :

C'est une frontière de communication entre l'utilisateur et notre application, elle contient une phase d'identification pour sécuriser l'ensemble de notre application.

III.3.3.2. Application :

Contient tous les modèles nécessaires dans la sécurité de fichiers textes :

III.3.3.2.1. Modèle gestion de fichiers :

Contient les méthodes de gestion de fichiers conçus afin de s'assurer que les fichiers peuvent être immédiatement identifiés, organisés, extraits, transféré, et conservés. Parmi les méthodes exploitées pour la gestion des fichiers sont les suivants (Voir Fig. III.3) :

a. Ouverture (ligne(1)) :

C'est l'opération qui consiste à ouvrir un fichier existant après l'identification de son nom et son type (depuis son extension) pour le consulter ou le modifier (chiffrer/déchiffrer), si le fichier n'existe pas on aura une erreur.

b. Sauvegarde (ligne(2)) :

C'est l'opération qui consiste à enregistrer les nouvelles modifications du fichier après son ouverture.

c. Transfert (ligne(3)) :

Cette opération sert à envoyer un fichier existant vers un autre ordinateur (destinataire) dans le réseau.

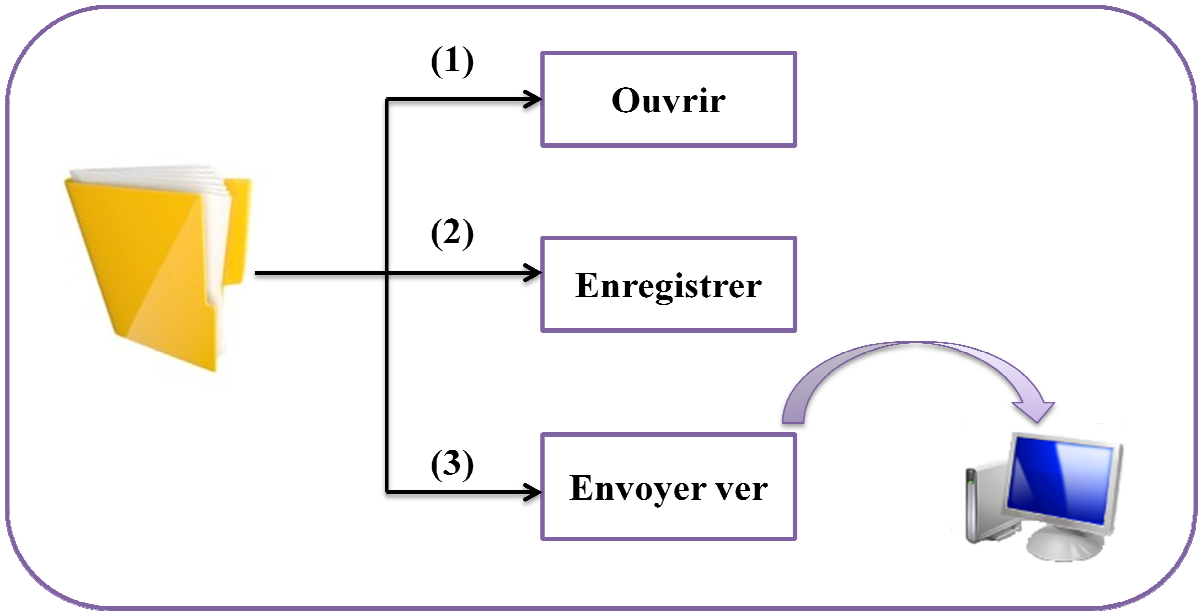


Fig. III.3. Architecture globale de Modèle gestion de fichiers.

III.3.3.2.2. Modèle chiffrement/déchiffrement :

Le chiffrement est un processus qui consiste à transformer une information claire, compréhensible de tout le monde, en une information chiffrée, incompréhensible à toute personne autre que le destinataire. Le chiffrement est toujours associé au déchiffrement (l'action inverse). Alors, ce modèle contient 4 algorithmes:

- RSA algorithme de chiffrement et déchiffrement.
- Signature RSA.
- El Gamal algorithme de chiffrement et déchiffrement.
- Signature El Gamal.

III.3.3.2.3. Modèle utilisateur :

Il y a deux types d'utilisateurs, chacun a ses droits spécifiques pour manipuler la base de données (Voir fig. III.4):

a. Administrateur : Il a les droits suivants:

a.1. Ajout (ligne(1)) :

Pour ajouter un nouvel utilisateur (son nom, mot de passe), qui va y avoir le droit (utilisateur) d'accéder à l'ensemble de l'application.

a.2. Suppression (ligne(2)) :

Consiste à éliminer un utilisateur, qui ne sera pas capable alors d'accéder à l'ensemble de l'application.

a.3. Liste (utilisateur) (ligne(3)) :

Pour afficher tout les informations d'utilisateur sans leur mot de passe.

a.4. Recherche (ligne(4)) :

Pour tester la présence de l'utilisateur et afficher le droit d'accès.

b. Utilisateur :

il a le droit de faire la :

b.1. Modification (ligne(5)) :

Pour le changement du mot de passe d'un utilisateur après sa demande, dans le cas où il y aurait par exemple divulgation de l'ancien mot de passe d'accès.

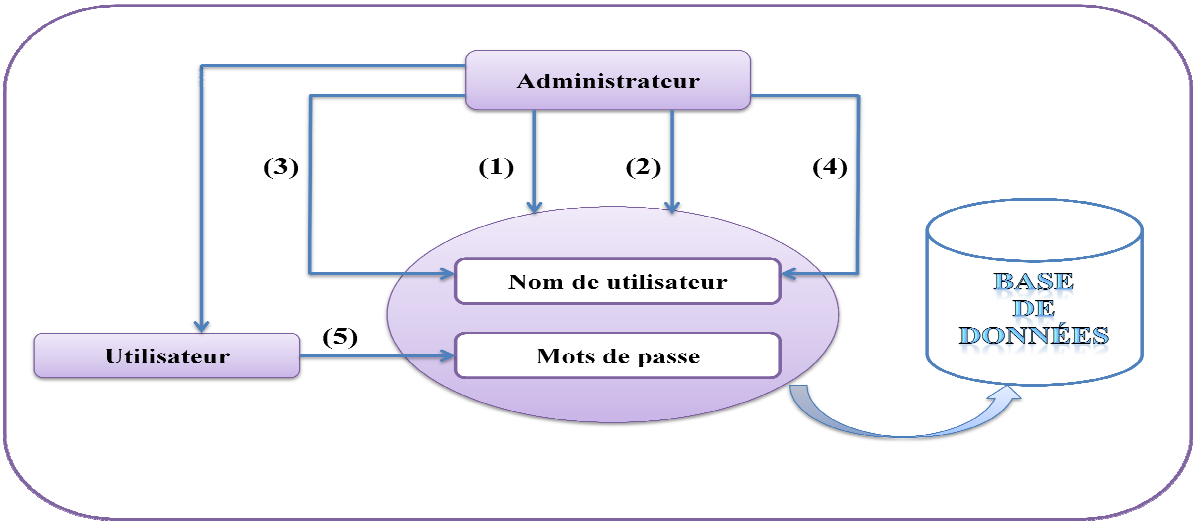


Fig. III.4. Mises à jour sur la base de données globale.

III.3.4. Conception détaillée :

Dans cette étape, on va expliquer en détailles fonctionnalités de chaque composant citée dans l'architecture globale.

III.3.4.1. Fonctionnement de composants principaux :

III.3.4.1.1. Activation d'identification :

a. Entrées des données (Nom d'utilisateur + le mot de passe)

Fig. III.5. L'identification de l'utilisateur en saisissant son nom+ son mot de passe.

b. Valider les données entrées.

Pour le mot de passe incorrecte

Le résultat obtenu :

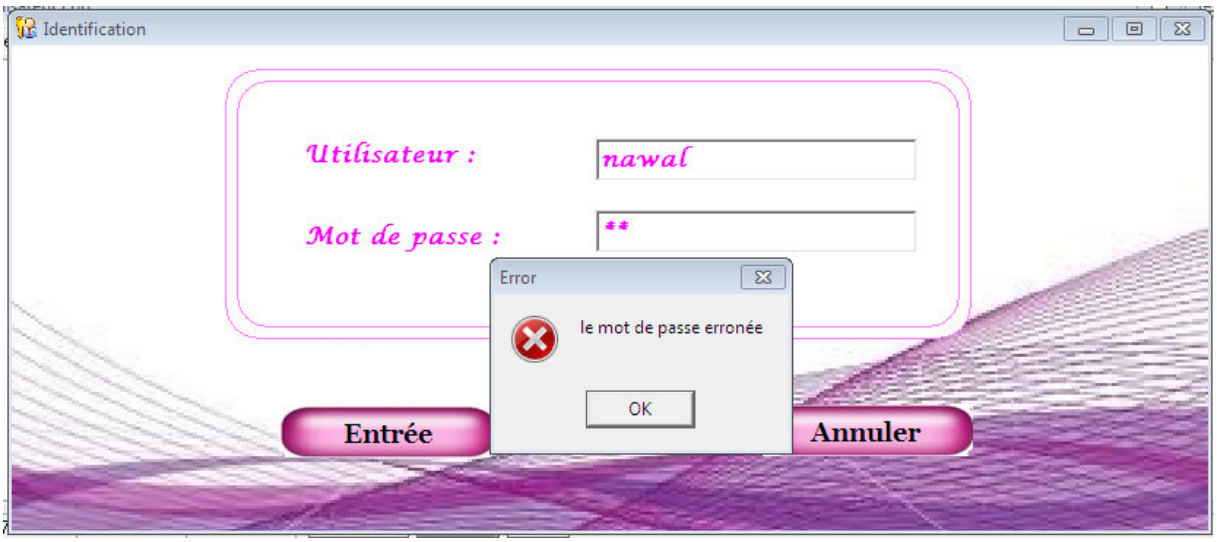


Fig. III.6. Erreur d'identification de mot de passe.

Pour l'utilisateur incorrect

Le résultat obtenu :

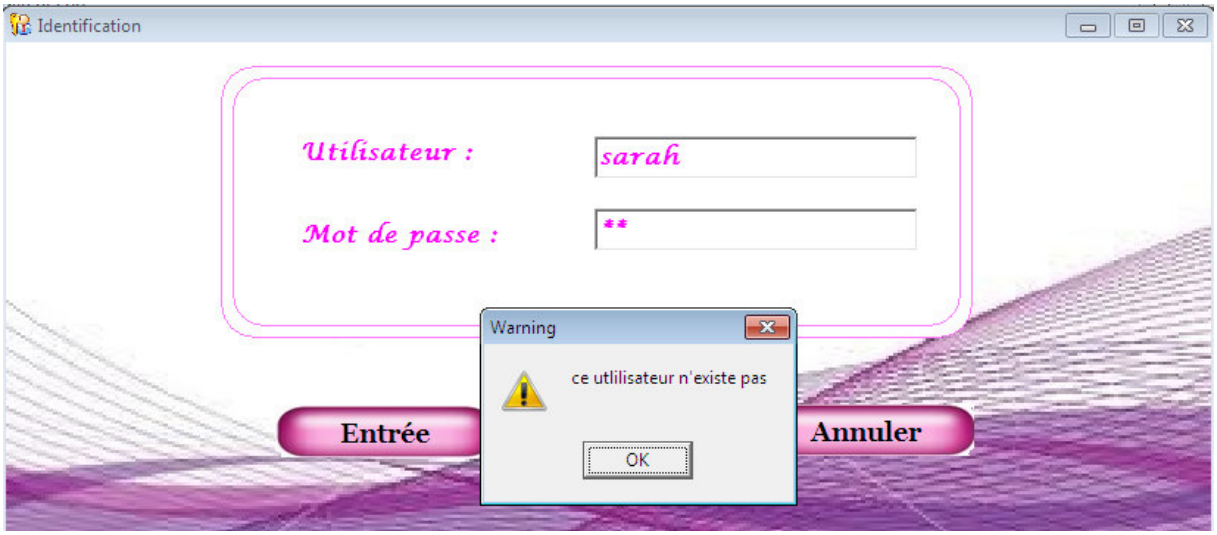


Fig. III.7. Erreur d'identification d'utilisateur.

Pour l'utilisateur et le mot de passe correcte le compte est ouvert

Le résultat obtenu (de la fig. III.8) :

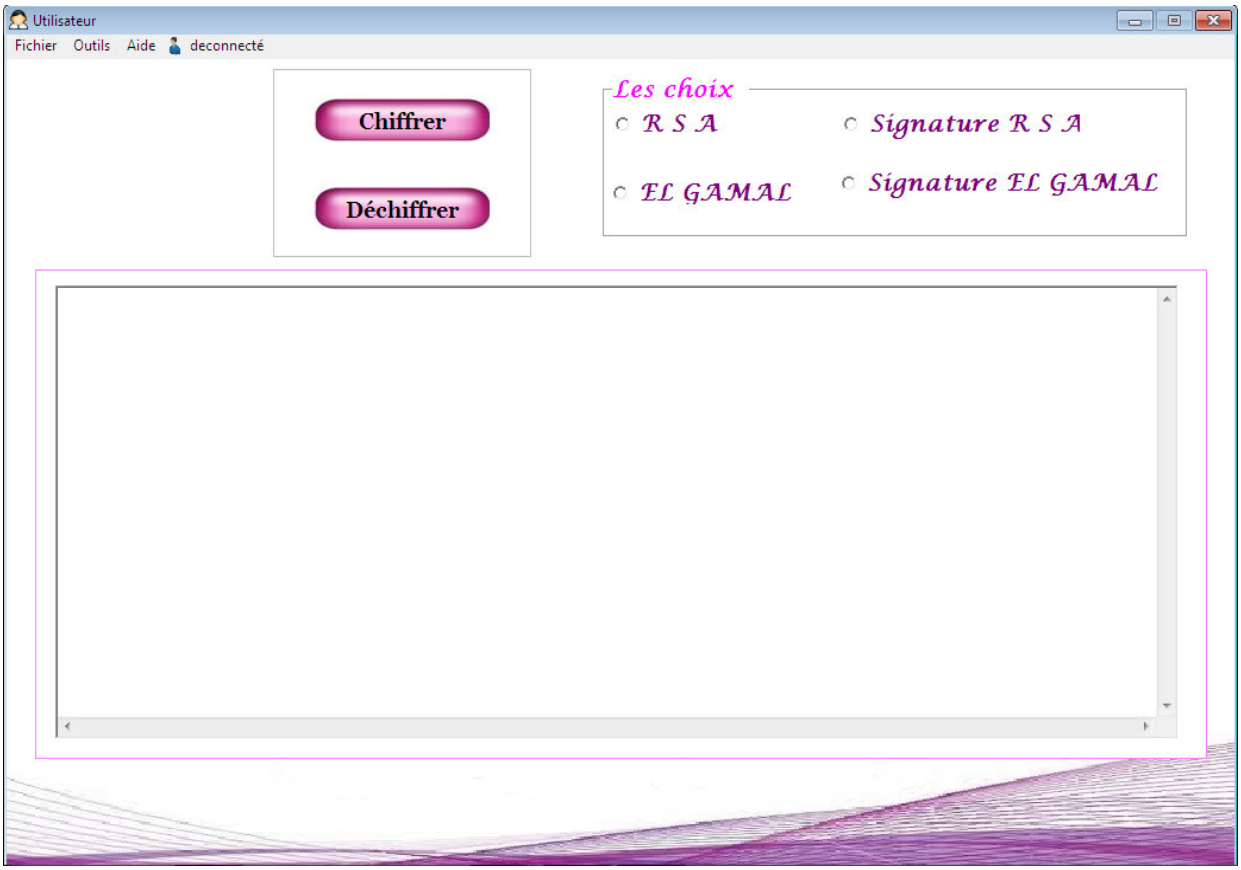


Fig. III.8. Le compte d'utilisateur.

III.3.4.1.2. Activation de gestion de fichiers :

a. Déterminer des méthodes à effectuer sur le fichier (de la fig. III.9)

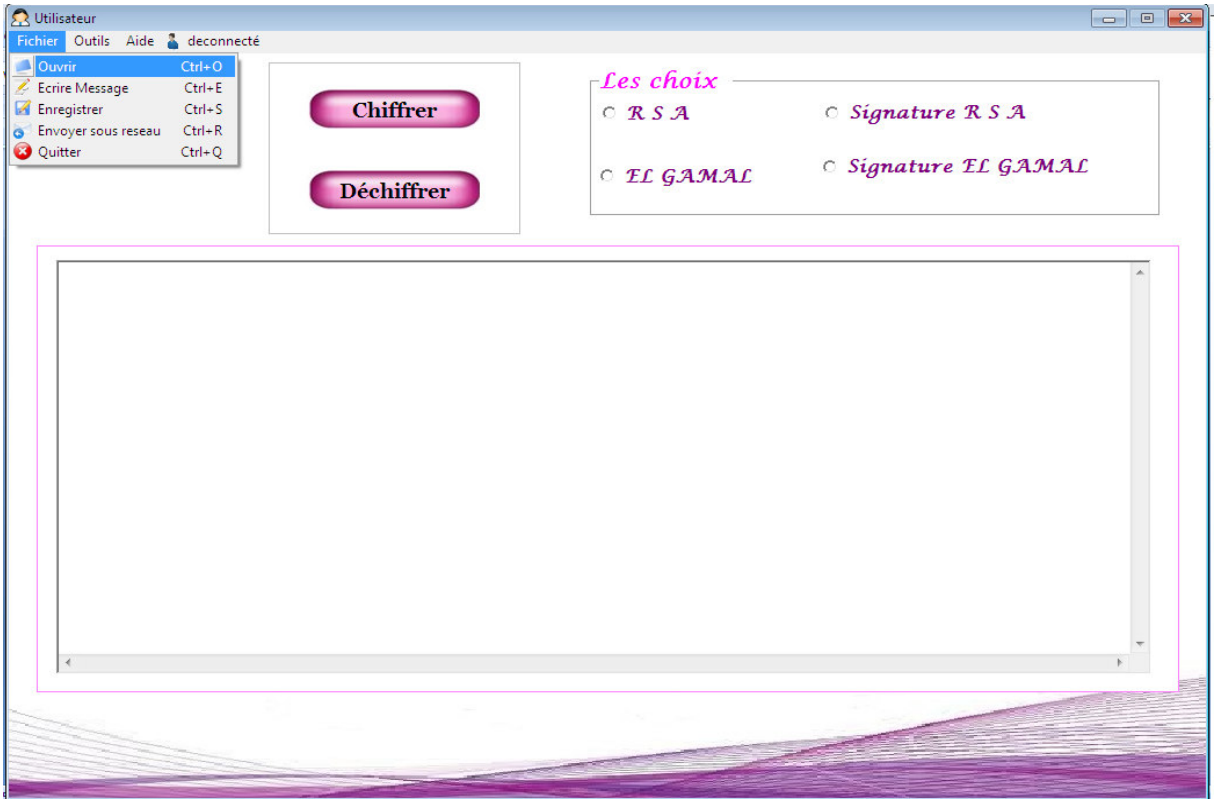


Fig. III.9. Le choix d'ouverture de fichier.

b. Choisir une méthode et l'appliquer. (Voir fig. III.10)

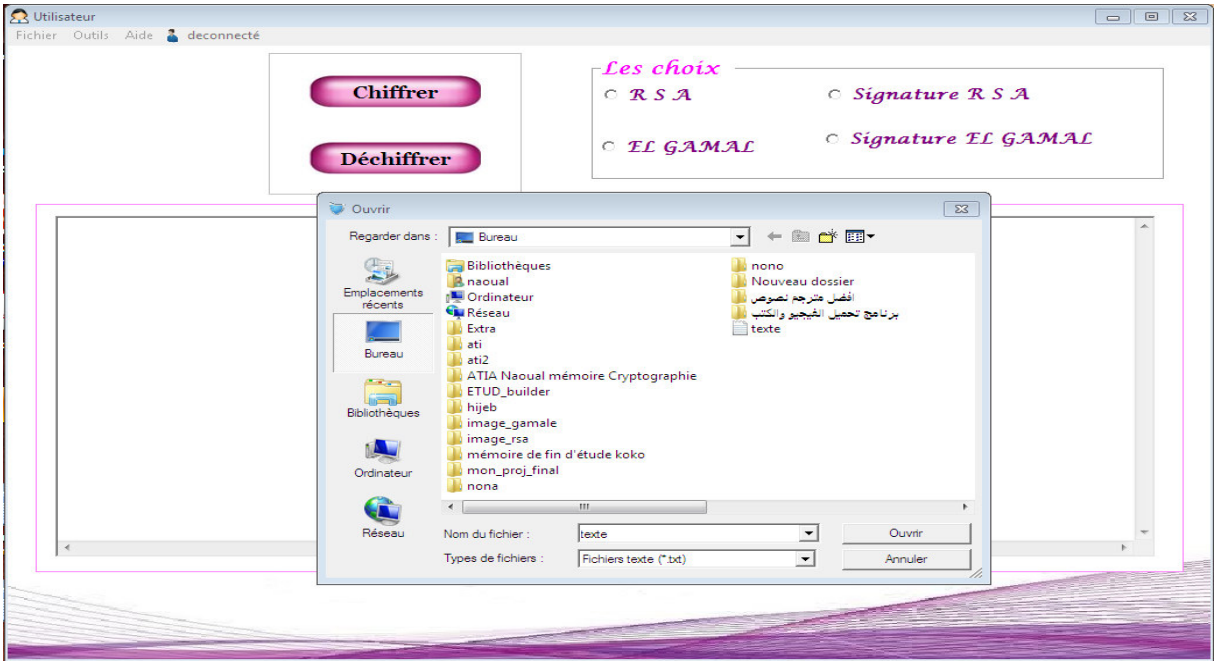


Fig. III.10. L'exécution de leur choix.

III.3.4.1.3. Activation de chiffrement/déchiffrement :

a. Présenter la méthode de chiffrement/déchiffrement demandée par l'utilisateur après son Identification.

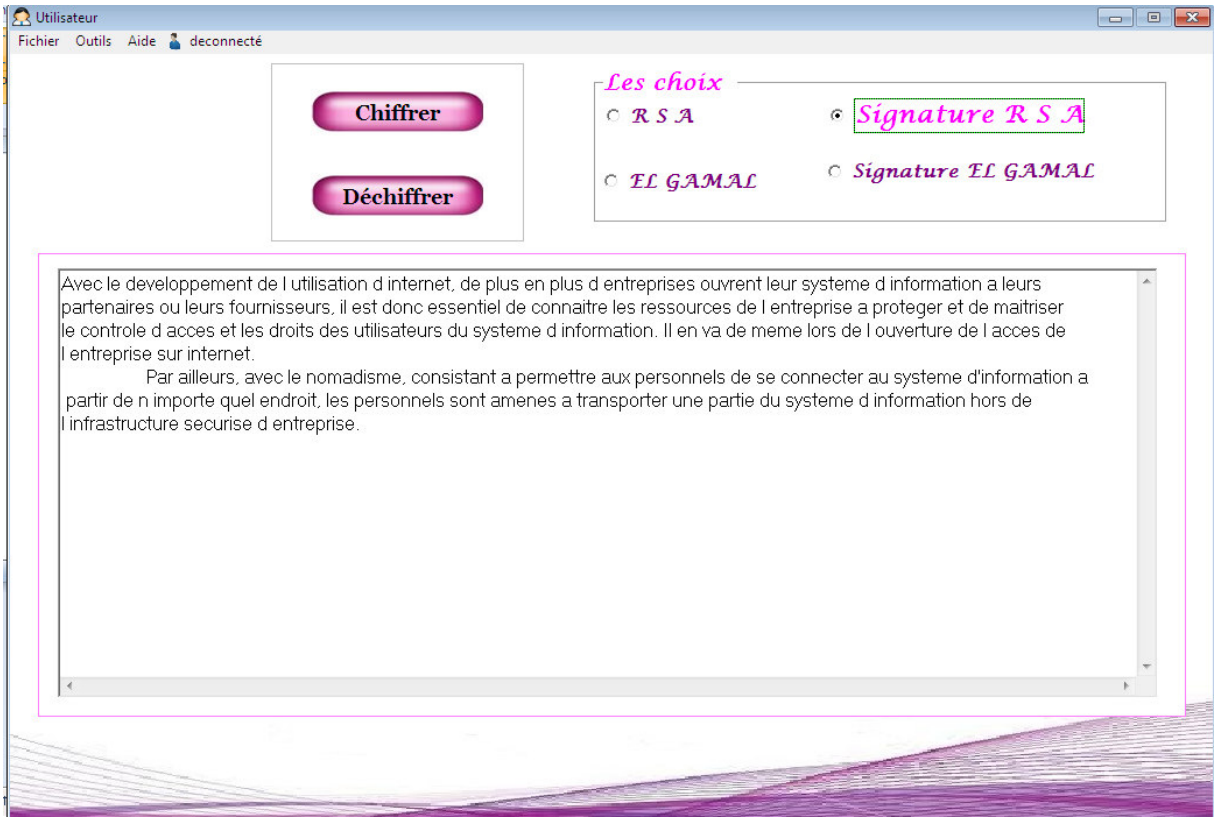


Fig. III.11. Choix d'algorithme de chiffrement (par exemple signature RSA).

b. Planification de méthode de chiffrement/déchiffrement à suivre: (Présenter la méthode) (Voir fig. III.12)

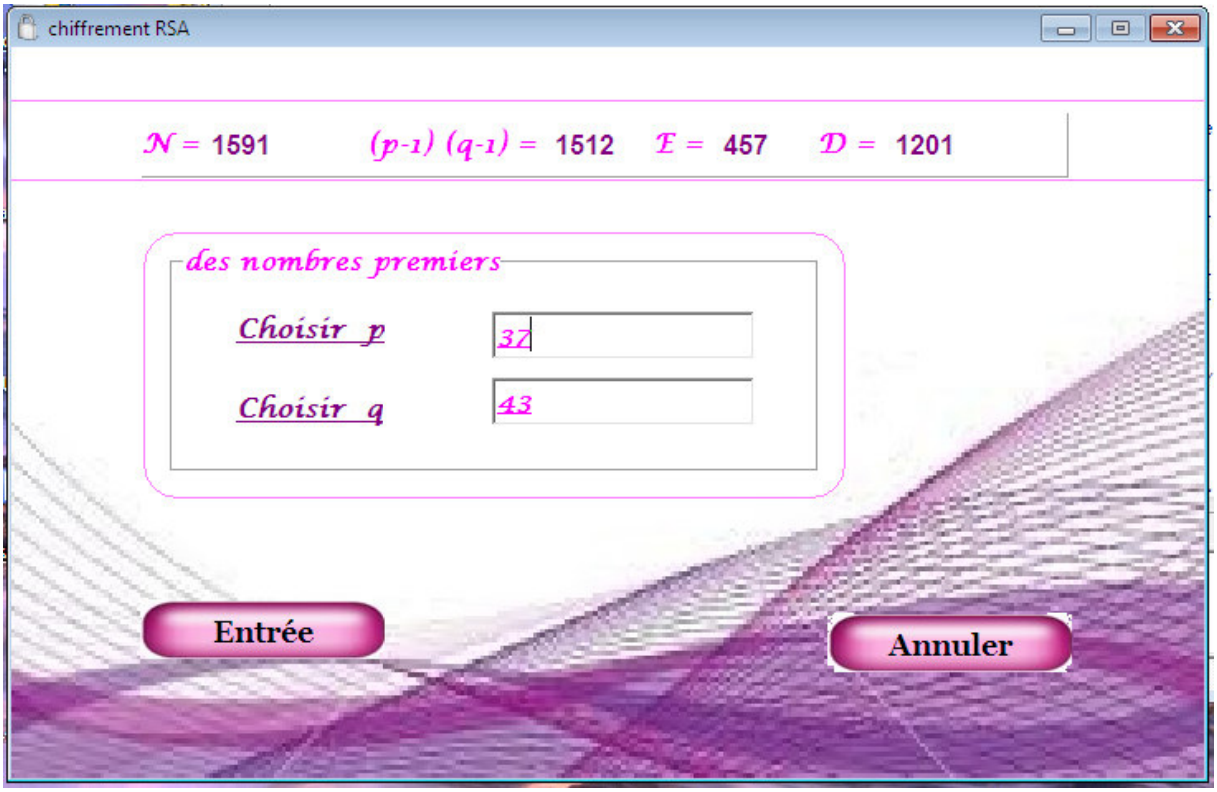


Fig. III.12. Génération des clés.

c. Exécution d'algorithme.

Exemple : (Voir fig. III.13)

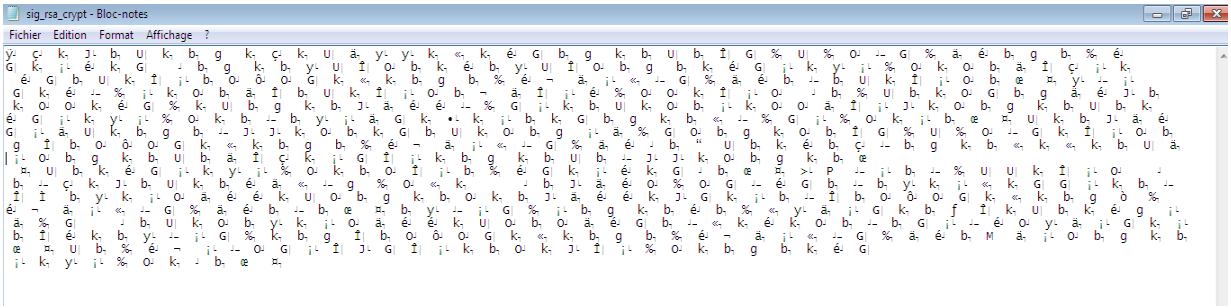


Fig. III.13. Le résultat d'exécution.

A. Méthode RSA (Chiffrement et Déchiffrement) :

Cette méthode très simple, l'algorithme RSA contient deux opérations déférentes, basée sur les nombres premiers.

Ce schéma on (Fig. III.14) considère les deux opérations différentes :

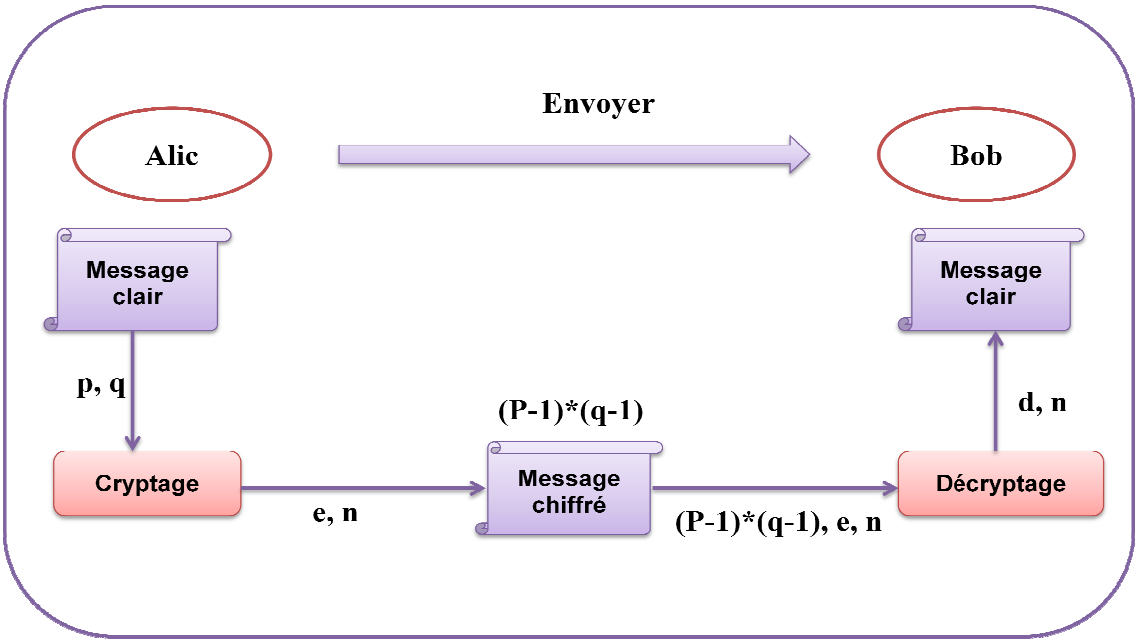


Fig. III.14. Schéma de Chiffrement et déchiffrement RSA.

Algorithme RSA :

- n est le produit deux nombres premiers p, q.
- (e, n) constitue la clé publique (enregistré sous BD).
- (d, n) constitue la clé privée.

B. Signature RSA :

Signature RSA basé sur l'algorithme RSA, pour signer un document sous une forme numérique. Ainsi, une signature peut être transmise par un réseau informatique.

Ce schéma on (Fig. III.15) considère les deux opérations signature et vérification :

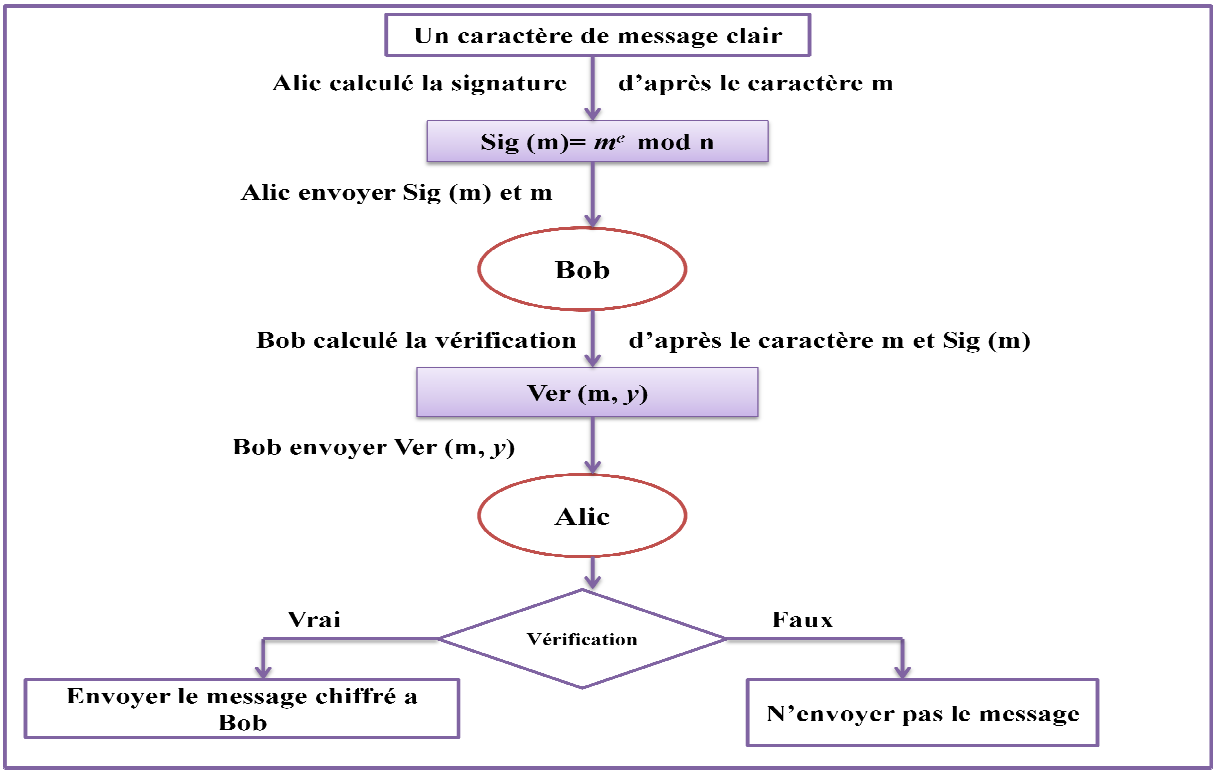


Fig. III.15. Signature RSA.

Algorithme signature RSA :

- m est un caractère de message.
- **sig (m) :** fonction de signature.
- Les valeurs **n**, **e** définit la clé publique.
- Les valeurs **n**, **d** définit la clé privée.
- Ver (m, y) : fonction vérification.
- **Ver (m, y) =vrai <=> m ≡ y^d(mod p)**, où **y=sig(m).**
- **Alic** est un Emetteur.
- **Bob** est un Récepteur.

C. Méthode El Gamal :

Cet algorithme se fonde sur la difficulté à calculer, il contient deux opérations déférentes, basée sur les nombres premiers, les éléments primitifs modulo et l'inverse modulaire.

Ce schéma on (Fig. III.16) considère les deux opérations différentes :

Conclusion générale :

Au cours de notre mémoire, nous avons étudié et implémenté les différents algorithmes de cryptographie asymétrique plus précisément la méthode RSA, Signature RSA, méthode EL GAMAL, et Signature EL GAMAL, avec l'idée de clé privé et clé publique donne une confiance d'être en sécurité.

Le crypto-système qu'on a implémenté, nous a permis d'avoir une nouvelle approche de la conception, où le temps, la réflexion et les études préalables sont bien plus importantes et difficiles que la programmation elle-même.

Nous avons également pu combiner les mathématiques et l'informatique dans un domaine concret et particulièrement d'actualité qui est la cryptographie.

Ce projet nous montré la nécessité d'optimiser nos algorithmes afin d'avoir des programmes plus performants.

Travers notre étude nous démontre que l'algorithme de chiffrement plus sécuritaire est l'algorithme EL GAMAL parce qu'il plus difficile.

Comme perspective nous proposons d'améliorer notre application par le chiffrement d'informations de différents types (image, son, animation).on conseil et on propose d'utilisé l'algorithme EL GAMAL pour chiffrement plus sécurisés.

Bibliographie :

[1] Robert Longeon, Jean-Luc Archimbaud, « Guide de la sécurité des

systèmes d'information à l'usage des directeurs » , Centre de la recherche scientifique n°82-993-JO, le 25 novembre 1982.P 10.

http://www.dgdr.cnrs.fr/FSD/securitesystemes/documentations_pdf/securite_systemes/guide.pdf 12/02/2013-17:15.

[2] Cadre commun de la sécurité Des systèmes d'information et de télécommunications, P 20.

http://www.cru.fr/ssi/_media/securite/sdssi-livret2 cadrecommun.pdf 12/02/2013-18:30.

[3] http://www.commentcamarche.net/contents/secu/secuintro.php312/02/2013-22:2O.

[4] http://www.securiteinfo.com/conseils/introsecu.shtml12/02/2013-22:20.

[5] http://dit-archives.epfl.ch/FI00/fi-sp-00/sp-00-page20.html12/02/2013-17:40.

[6] Brochure d'information sur la sécurité 5, « Guide d'évaluation de la menace et des risques pour les technologies de l'information », Sous-direction de la sécurité des technologies de l'information de la GRC, novembre 1994.

http://ar.kaced.free.fr/Securite/Securite/Docs/tra_guide_fr.pdf12/02/2013-17:15.

[7] http://www.commentcamarche.net/contents/secu/secuintro.php312/02/2013-22:15.

[8]http://www.lesoirdalgerie.com/articles/2005/07/07/article.php?sid=25346&cid=2025/02/2013-20:45.

[9] http://lesvansinfo.free.fr/attaques.php25/02/2013-20:45.

[10] http://www.hackermocking-cartel.com/infos-matique.php25/02/2013-20:45.

[11] http://linux.developpez.com/secubook/node42.php25/02/2013-22:40.

[12] http://ramesnkulu.unblog.fr/2010/12/22/cours-sur-la-securite-informatique/8/03/2013-19:10.

[13] http://goodsites.kazeo.com/les-dangers-du-web/piratages-hackers,a2528990.html8/03/2013-20:10.

[14] http://www.commentcamarche.net/contents/attaques/mailbombing.php323/03/2013-20:25.

[15] www.lamaisoninfo.com/userfiles/file/LMI-La sécurité informatique2.pdf23/03/2013-22:10.

[16] http://topnewsinformatique.blogspot.com/2012/07/radio.html23/03/2013-22:10.

[17] http://www.dicodunet.com/definitions/internet/securite-informatique.htm23/03/2013-22:10

[18]http://alexandremohr.free.fr/Documents/UTBM/IR00/Documents%20Internet/La%20cryptographie/1.htm10/04/2013-21:15.

[19]http://commerce.electronique.samadel.over-blog.com/pages/la-cryptographie-asymetrique-3396986.html10/04/2013-21:15.

[20] Ghislaine Labouret. « Introduction à la cryptographie ». Hervé Schauer 1999.

http://www.hsc.fr/ressources/cours/crypto/crypto.pdf12/04/2013-14:05.

[21] http://www.labouret.net/crypto/12/04/2013-19:00.

[22] http://dictionnaire.phpmyvisites.net/definition-chiffrement-4272.htm12/04/2013-19:45.

[23] http://dictionnaire.phpmyvisites.net/definition-Dechiffrement-11538.htm20/04/2013-16:35.

[24] Pierre-Alain FOUQUE. « **Cryptographie appliquée ».** Centre français d'exploitation http://n-pn.info/repo/Spirit_of_hack/cryptoappliquee.pdf22/04/2013-18:30.

[25] http://dspace.univ-tlemcen.dz/bitstream/112/1076/7/chapitre3.pdf22/04/2013-21:10.

[26] http://fr.wikipedia.org/wiki/Cryptosystème22/04/2013-21:45.

[27] ABOUNADA SAMI MAJERI SAMIR Mémoire Licence Informatique Introduction de la cryptographie 2002/2003.

[28] http://nopb.chez.com/crypto2.html02/05/2013-15:10.

[29] Khalil IBRAHIMI. « Sécurité des Systèmes d'Information et des Réseaux : Cryptographie **».** Université d'Avignon et des Pays de Vaucluse CERI, M1-M2 Alternance, Laboratoire d'Informatique d'Avignon (LIA) 2009-2010.

[30] DESTREE Lucile – MARCHAL Mickaël. « Mini-RSA programme d'initiation au chiffrement RSA ». Projet de Mathématiques pour l'Informatique N°1,P2 Groupe B. PP 04-06.

http://www.lesitedemika.org/ressources/cryptographie_rsa.pdf11/05/2013-15:30.

[31]http://www.commentcamarche.net/contents/208-algorithme-de-chiffrement-rsa#generation-des-cles11/05/2013-16:11.

[32] http://wakaziva.pagesperso-orange.fr/crypto/4.htm11/05/2013-19:25.

[33] http://sebsauvage.net/comprendre/encryptage/crypto_rsa.html11/05/2013-20:30.

[34] Vincent BROSSARD. **Cryptographie Asymétrique.** Formation Sécurité et Réseaux – CNAM. PP 05-07.

http://cnam.w3france.org/Securite/04%20-%20Cours%20Crypto%20Asy.pdf11/05/2013-22:10.

[35] http://dept25.cnam.fr/ITCE/Cours/Securite_12.pdf11/05/2013-22:30.

[36] Douglas Stinson. **CRYPYOGRAPHIE Théorie et pratique** 2^{eme} édition. Traduction de serge Vaudenay, Gildas Avoine et Pascal Junod. Imprimerie France Quercy – 46001 Cahors. N^0 d'impression : 32250 – Dépôt légal : octobre 2003.P 225 - 226 , P 273, P 278 – 279, P 286 - 287 .

[37] Jean-Louis POSS. Introduction à la cryptographie. Ecole Nationale Supérieure d'Arts et Métiers (ENSAM) Aix-en-Provence. Version 1.0, Juin 2003. P 16.

[38] BEKHOUCHE Saïda. **Fondements mathématiques et fonctionnement du standard de chiffrement avancé Rijndael (AES).** Résumé du Mémoire de Magister en Algèbre et Théorie des Nombres. Faculté de Mathématiques Université des Sciences et de la Technologie Houari Boumediène (USTHB) Alger. P 14.

http://www.usthb.dz/fmath/IMG/pdf/Bekhouche_Saida1.pdf16/03/2013-19:22.

[39]http://fr.wikipedia.org/wiki/%C3%89change_de_cl%C3%A9s_Diffie-Hellman16/03/2013-21:10.

[40]http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/elgamal18/03/2013-15:35.

Table des Matières :

Liste des Tableaux :

Liste des Figures :

Liste des abréviations :

SSI : Sécurité d'un Système d'Information.

RSA : Rivest Shamir et Adleman**.**

mod : Modulo.

Sig : Signature.

ASCII: American Standard Code for Information Interchange.

Ver : Vérification.

DSA : Digital Signature Algorithme**.**

RAD : Rapid Application Development.

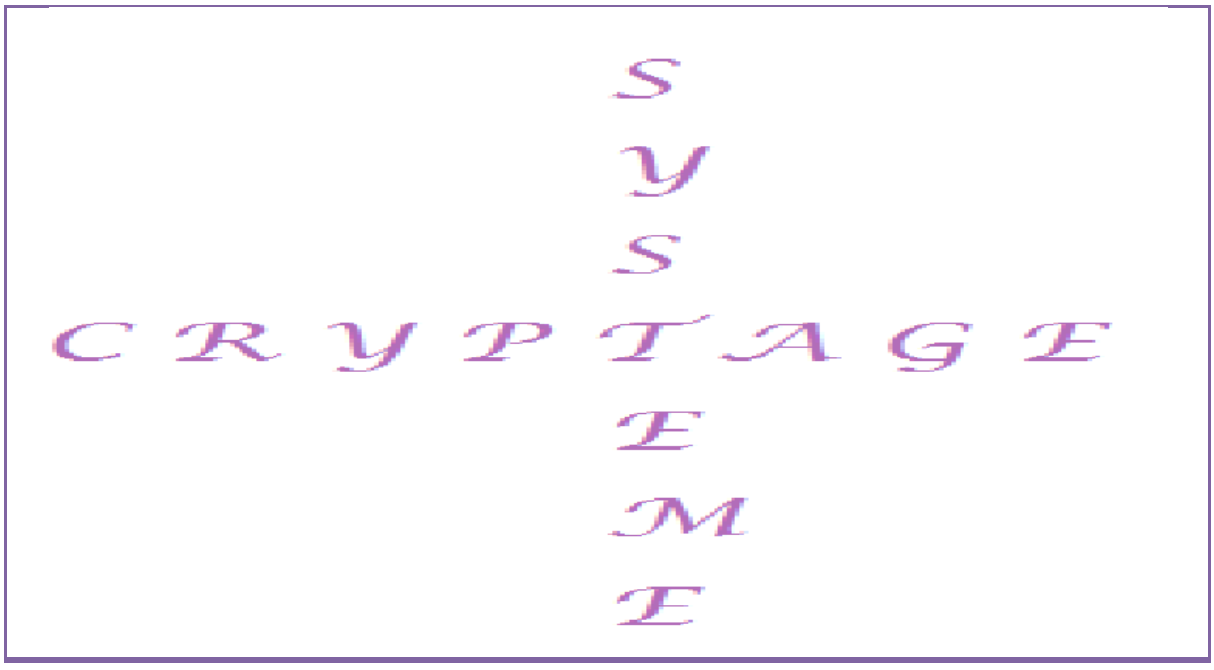
Annexe :

Introduction :

Dans cette section on va présenter l'aspect IHM (Interface Homme Machine) de l'application, et on va voir quelques cas de figure que l'utilisateur peut employer.

Présentation de l'application :

Cette figure représenter la page de garde l'application.



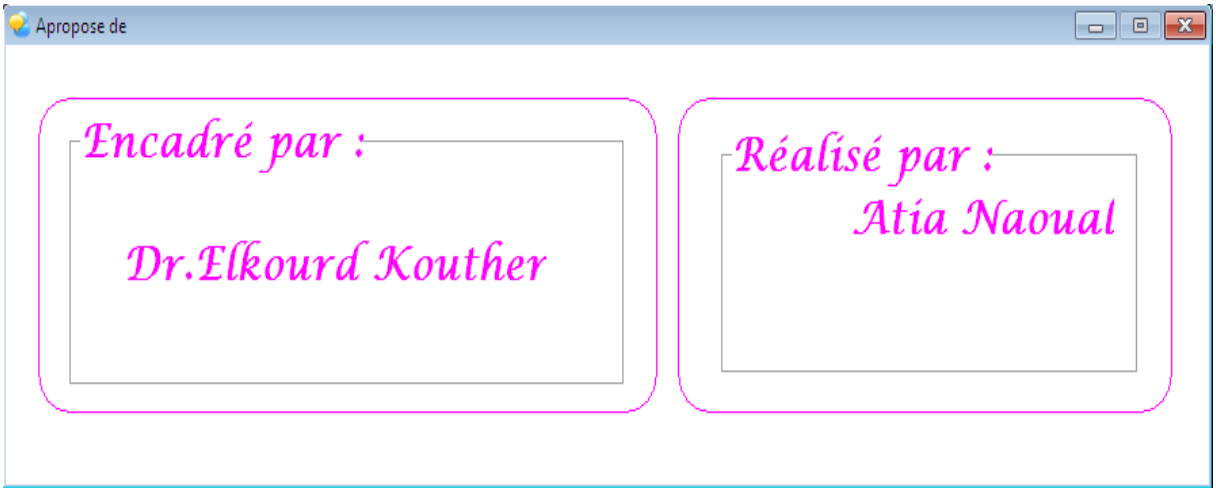
Cette figure représenter logo d'application

Cette figure reflète l'utilisateur et quels sont les points qui peuvent être utilisés.

L' administrateur	Nom	Clé publique RSA		Signature RSA	Clé publique ELGAMAL			Signature ELGAMAL	
	aichouche	E :	N:		P :	Alpha :	B :	Landa :	Gama :
	atia naoual	E :	N:		P :	Alpha :	B :	Landa :	Gama :
	elloard	E :	N:		P :	Alpha :	B :	Landa :	Gama :
L' utilisateur	Nom	Clé publique RSA		Signature RSA	Clé publique ELGAMAL			Signature ELGAMAL	
	kaouther	E :	N:		P :	Alpha :	B :	Landa :	Gama :
L' administrateur	Nom	Clé publique RSA		Signature RSA	Clé publique ELGAMAL			Signature ELGAMAL	
	marwa	E : 737	N: 2021	901	P : 3119	Alpha : 2	B : 16	Landa : 8	Gama : 11
	naoual	E :	N:		P :	Alpha :	B :	Landa :	Gama :
	nawal	E : 173	N: 1073	1279	P : 2347	Alpha : 2	B : 4	Landa : 8	Gama : 11
	sara	E :	N:		P :	Alpha :	B :	Landa :	Gama :

Cette figure contient la liste des utilisateurs.

Cette figure représente la modification de mot de passe.



Cette figure représente a propose de