TABLES DE MATIERES

NOTATION

C : Le texte chiffré

C_C : la clé publique de la Carte,

C_R : la clé publique de Référence

D : la fonction inverse de déchiffrement

D_C : la clé secrète de la Carte,

D_R : la clé secrète de Référence.

E : La fonction de chiffrement

e/s : entré et sortie

K : clé

k1 : clé de chiffrement

k2 : clé de déchiffrement

M : le texte clair

Oe : mesure de magnétique forte

Vcc : entrer de source d'alimentation

LISTE DES ABRÉVIATIONS

ANSI	: American National Standards Institute
ASCII	: American Standard Code for International Interchange
APDU	: Application Protocol Data Units
ATR	: Answer To Reset
BCD	: Binaire Decimal Code
CA	: Certificat Autority
CAD	: Card Acceptance Device
CB	: Carte Bancaire
CRL	: Certificate Revocation List
DAB	: Distributeur Automatique Bancaire
DES	: Data Encryption Standard
DN	: Distinguished Name
GAB	: Guichet Automatique Bancaire
EEPROM	: Electronically Erasable Programmable Read Only Memory
GND	: Ground
HiCo	: High Coercivity
IETF	: Internet Engineering Task Force
INS	: Instruction
ISO	: International Standard Organisation
JVM	: Java Virtual Machine
KBS	: KiloBits par Second
LoCo	: Low Coercivity
MAC	: Message Authentication Code
MHz	: MegaHerzt
Mb/s	: Megabit par second
PIN	: Personal Identification Number
PTS	: Protocol Type Selection

PKI : Public-Key Infrastructure

PVC : Polychlorure de vinyle

RAM : Read Access Memory

RFID : Radio frequency Indentificator

RFU : Reserved for Futur Use

ROM : Read Only Memory

RSA : R. Rivest, A. Shamir, L Adlema

RTC : Réseau Téléphonique Commuté

SCQL : Structured Card Query Language

SIM : Subscriber Identification Module

SWIFT : Society for Worldwide Interbank Financial Transaction

TPDU : Transport Protocol Data Unit

TPE : Terminal Payement Electronique

PTS : Protocol Type Selection

UIT : Union Internationale Telecommunication

UV : Ultra Violet

USB : Universal Serial Bus

Vcc : Virtual Channel Connection

V S : Valeur Signature

INTRODUCTION GENERALE

Grâce au développement des technologies informatiques, l'homme a pu mettre en place le réseau mondial d'ordinateurs permettant la communication et l'échange de données dans le monde entier, c'est l'internet ou INTERconnected NETworks. En fait, ce dernier devient une ressource indispensable au bon fonctionnement d'une organisation, d'une entreprise, d'une banque ...

Actuellement, le monde ne peut se séparer et aucun pays ne reste enclaver, puisque les réseaux télécommunications le recouvrent. Les différents operateurs, les fournisseurs de ce réseau est une grande société car ils allouent les fréquences aux utilisateurs donc il faut sécuriser les informations, les données.

La cryptographie existe depuis l'Antiquité et s'avère indispensable. Sans elle, l'information ne serait pas sécurisée car n'importe qui pourrait intercepter les échanges à travers le monde entier, aucune confidentialité ne serait plus assurée, outils indispensable dans les échanges bancaires, que ce soit par internet ou même aux terminaux bancaires, afin d'assurer une parfaite fiabilité. La confidentialité et la fiabilité que la cryptographie assure ne sont cependant pas absolues, car des technologies toujours plus puissants sont crées régulièrement afin de déjouer les codes mis en place. On doit donc chercher continuellement des chiffrements plus résistants aux attaques frauduleuses.

La sécurisation varie suivant le besoin du concepteur qu'il préfère et nous intéresse aussi à la sécurisation matière physique comme le carte bancaire durant la fabrication. On choisit d'analyser la carte bancaire car imaginons que nous vivrons un monde avec technologie de cartes, RFID, carte intelligente … ; ***toute est carte***, cela évite le vol, la violence, les falsifications et la criminalité. Seulement le piratage augmente le taux de fraude de la fabrication, de la fausse carte, pour cela nous portons des études pour améliorer cette sécurisation.

Ayant pris en compte de l'importance des sécurisations de données par les techniques cryptographies, nous avons décidé de travailler et en lui donnant le titre : « TRANSFERT DE DONNEES VIA LA BANQUE AVEC LA SECURISATION DE LA CARTE BANCAIRE ».

Ce mémoire a pour but de présenter les structures entourées par la carte, suivant des différentes techniques et la cryptographie avec les faiblesses et les performances des cryptographies qu'il est déjà inscrite et aussi des améliorations. Il est subdivisé en cinq chapitres :

- Le premier chapitre par l'environnement global de la carte bancaire

- Le second chapitre les principes de la sécurisation
- Le troisième chapitre la cryptographie
- Le quatrième chapitre les études de la carte bancaire et les améliorations
- Le cinquième et dernier chapitre on fera la simulation de ce mémoire suivant les différentes manipulations et interprétations.

CHAPITRE 1 : L'ENVIRONNEMENT DE LA TELECARTE BANCAIRE

1.1 Historique

La carte bancaire est un moyen de paiement apparu dans les années 50. À l'origine, elle sert à retirer des espèces aux distributeurs automatiques. Puis, dans les années 80, son utilisation s'étend au paiement électronique chez les commerçants. En 1990, la carte bancaire connaît une innovation majeure : elle est rééquipée d'une puce électronique, se combine avec la piste magnétique. Largement adoptée aujourd'hui par les consommateurs, la carte bancaire sert à effectuer des paiements auprès des commerces physiques possédant un terminal de paiement, des paiements virtuels sur l'internet ainsi que des retraits d'espèces aux distributeurs de billets. L'avenir de la carte bancaire, avec les innovations en face de l'enjeu sont performants, le garantit de niveau de la sécurité est plus élevé afin de résister aux fraudes et aux piratages, s'adapter à de nouvelles utilisations telles que le paiement en ligne et faire face à l'arrivée des paiements sans contact et sans carte.

Dans ce cas à cause de l'évolution de la nouvelle technologie actuelle, les chercheurs recherchent les stratégies pour améliorer la sécurisation de la carte bancaire.

1.2 Les télécartes

Le support est composé de plusieurs couches PVC assemblées, deux couches pour une carte classique, d'une épaisseur de 800 µm. Ces deux couches, recto et verso de la carte sont imprimées en offset, souvent ultra violet ou waterless, ou/et par sérigraphie. Elles sont ensuite assemblées avec un film plastique de protection transparent en PVC, appelé overlay, appliqué sur chaque face. L'overlay du recto est un simple film en PVC

1.2.1 Carte bancaire à piste magnétique

Une piste magnétique est préalablement déposée au verso avant l'application du film. Cette piste magnétique permet de stocker des informations

1.2.1.1 Aspect extérieur

On trouve des différents composants qui sont communs pour tous les types de carte bancaire.

Figure 1.01 : *carte bancaire vue recto*

Figure 1.02 : *carte bancaire vue verso*

On remarque que l'hologramme mesure quelques centimètres en argenté, il laisse apparaître les couleurs de l'arc-en-ciel en fonction de l'éclairage. L'hologramme est un élément de sécurité utilisé sur la carte bancaire.

1.2.1.2 L'aspect intérieur

La piste magnétique et son utilisation sont soumises à la norme ISO [18]. La piste magnétique en trois zones d'écriture, contenant un nombre limité de caractères. Cet ensemble de feuilles est ensuite découpé au format de la carte. Sur ce complexe, sont déposés :

- les éléments sécuritaires
- l'hologramme de surface
- le panneau pour la signature notamment.

1.2.1.3 La zone sécurisée

Les informations de la carte sont contenues exclusivement sur la bande magnétique. La bande est composée de micro particules ferromagnétiques dispersées dans un liant. Lorsqu'on applique un champ magnétique à ce mélange, les particules se comportent comme de petits cristaux aimantés qui prennent une certaine orientation selon la valeur du champ magnétique. En choisissant un champ définit on peut alors contrôler ces particules. Il existe plusieurs types de particules, mais ce qui est retenue pour la carte magnétique courante c'est l'oxyde de fer. Tous ces types de particules ont une certaine rémanence : cette propriété permet à un matériau magnétique d'acquérir et de conserver une aimantation permanente.

1.2.2 La puce électronique

Le module électronique constitue la majeure partie de la valeur ajoutée apporté par le fabricant de cartes bancaires. La première étape de sa fabrication est l'assemblage du circuit imprimé et du circuit intégré. Le circuit imprimé comporte le support permettant de relier les divers composants électroniques entre eux. Le circuit intégré, aussi appelé puce électronique, est quant à lui un composant permettant de reproduire des fonctions électroniques. Le câblage du circuit intégré sur le circuit imprimé se réalise à l'aide de fils d'or. L'ensemble est ensuite protégé à l'aide d'une résine.

1.2.3 L'assemblage de la puce électronique et la piste magnétique [8] [17]

Presque toutes les cartes bancaires, les informations personnelles sont imprimées sur la carte, souvent en monochromie noir. La technique d'impression majoritairement employée est le jet d'encre binaire ; elle consiste à expulser en intervalles de temps donnés par gouttes d'encre en direction du support. Elles passent dans un champ électrostatique : les gouttes chargées sont déviées vers une gouttière tandis que les gouttes non chargées se dirigent vers le support d'impression. La puce électronique contient des mémoires pour des calculs de cryptographie.

1.2.3.1 La zone sécurisée

Le cœur de la puce, le microprocesseur, est un bloc monolithique. Il contient à la fois les unités de calcul tels le processeur et éco-processeur cryptographique, les mémoires contenant le code de la carte dans la ROM, les mémoires de travail, persistantes comme l'EEPROM, ou temporaires telle la RAM, et les éléments de communication. La carte est enfin prête à être envoyée au client avec son code secret

1.2.3.2 Le codage de norme

Il existe une série de normes qui définissent différentes caractéristiques pour les cartes à bandes magnétiques. Notamment l'encodage et la répartition des informations sur la bande. Ces normes ont été définies par un organisme s'appelant ISO : International Organization for Standardization. Ces normes définissent 3 pistes sur la bande magnétique. Voici la disposition de ces pistes de manière standard :

- La piste ISO1, qui permet de stocker 210 bit par pouce, soit environ 82 bit par cm.
- La piste ISO2, qui permet de stocker 75 bit par pouce, soit environ 29 bit par cm.

- La piste ISO3, ayant les mêmes caractéristiques que la piste 1

Ces normes définissent aussi des codes alphanumériques faisant la correspondance entre une suite de bit et un caractère particulier. La piste ISO1 a pour codage un alphabet sur 7 bits et les piste 2 et 3 un alphabet à 5 bits. Ces codes contiennent aussi des caractères spéciaux de début et de fin de piste qui encadrent l'information et des séparateurs.

Il y a la carte puce à électronique qui se confond avec la piste magnétique, nous allons voir les aspects extérieurs dans cette figure suivante.

Figure 01.3 : *Composants d'une carte bancaire*

1.2.3.3 Les rôles des différents composants

Pendant de la fabrication de la carte, le fabricateur met les différents composants suivants les rôles et les significations différents.

Panneau de signature : panneau qui contient la signature de tutélaire

Adresse d d'établissement de l'émetteur : nom de la banque qui correspond à la carte

nom de tutélaire : nom et prénom de la tutélaire de la carte

Logo de CB : le signe ou le logo de la banque

date d'expiration : date la validité de la carte bancaire

Piste magnétique : c'est une bande noire pour stocker des informations

La puce : élément sécurisé de la CB

1.3 Principes de transactions bancaires : [2]

Issue de la rencontre entre les techniques de la communication, de l'informatique et de l'électronique, une véritable révolution dans les échanges économiques a permis l'apparition de la monétique. Cette dernière autorise la dématérialisation des espèces sonnantes et trébuchantes.

1.3.1 Monétique

1.3.1.1 Définition

La monétique est l'ensemble des techniques électroniques, informatiques, télématiques permettant d'effectuer des transactions, des transferts de fonds ou toute autre opération qui relie un utilisateur final équipé d'une carte avec un ensemble de services. Au sens strict du terme et à l'origine, la monétique est étroitement lié au système de paiement électronique qui intègre le triptyque :

- carte à puce ou à piste magnétique,
- terminal de paiement électronique ou distributeur automatique de billets
- établissement bancaire.

1.3.1.2 Terminal de paiement électronique

C'est un appareil électronique qui permet d'enregistrer une transaction de divers nature de banque en dialogue avec d'une part une CB ou une porte monnaie électronique téléphonie mobile d'autre part un serveur autorisé

1.3.2 Les différentes structures

Pour fonctionner, un terminal a donc besoin de connaître la liste de la carte existante. Chaque terminal devra envoyer les informations générées au serveur d'acquisition, devra attendre la réponse du serveur d'acquisition et affichera cette réponse à l'écran c'est-à-dire paiement autorisé ou non.

Les échanges entre le terminal et le serveur d'acquisition ont lieu suivant un protocole bien déterminé : les informations sont formatées d'une certaine façon. Ce sont les constructeurs de terminaux qui imposent leurs protocoles et ce sont les serveurs d'acquisition qui doivent s'adapter

pour parler les protocoles des différents terminaux qui sont connectés

1.3.3 Le Distribution Automatique Bancaire

1.3.3.1 Fonctionnement

Tous les guichets automatique bancaire sont activés permanents, il attend les actions des clients.

- Introduction de la carte
- La carte envoie son identifiant et signature de ce dernier aux terminaux
- Vérification de la signature
- Le terminal demande le code de 4 chiffres au client, le client rentre le code
- Vérification du code par la puce
- La puce demande alors au terminal le montant et la date et l'heure
- Le terminal reçoit la transaction chiffrée et la stockés en mémoire ; le client s'en va
- Le soir (généralement), le commerçant connecte son terminal à la banque pour envoyer les différentes opérations

1.4 Carte bancaire [4]

Depuis plusieurs années, l'utilisation des cartes bancaires occupe une place de plus en plus importante dans les opérations financières grâce notamment au développement des transactions effectuées à distance. Tout d'abord une carte bancaire est identifiée par les caractéristiques suivantes :

- la nature de la carte : VISA, EUROCARD, MASTERCARD,…
- le numéro et la date de validité de la carte,
- le cryptogramme visuel pour les cartes bleues

Typologie des cartes d'un paiement électronique trois types de cartes existent

1.4.1 Cartes de débit :

Le montant de paiements payés par la carte de débit sera directement prélevé sur le compte bancaire de l'utilisateur de la carte (Maestro, VISA Electron).

1.4.2 Cartes de crédit :

Permettent à son utilisateur de payer des marchandises à crédit en ayant l'autorisation de l'organisme émetteur de la carte. Le montant crédité pourra être débité plus tard sur le compte bancaire de l'utilisateur (Mastercard, VISA) mais ce montant est déterminé à l'avance.

1.4.3 Cartes accréditives :

Ce sont des cartes qui n'intègrent aucune limite de créance mais dont le montant doit être remboursé à chaque fin du mois.

1.5 Le commerce électronique

Grâce à la nouvelle technologie qui facilite notre travail et aussi le déplacement, le commerçant peut utiliser le commerce électronique s'il y en a mais le problème essentiel du commerce électronique consiste à garantir la sécurité des transactions (*authentification des interlocuteurs, confidentialité des échanges, sécurité bancaire*...). Deux approches du commerce électronique sont envisageables selon que l'organisme bancaire participe directement à la transaction (paiement on-line) ou que l'organisme bancaire est étranger à la transaction (paiement off-line).

1.5.1 Le payment off-line (e-cash)

Dans ce mode de paiement, le client approvisionne un compte local en monnaie électronique (monnaie virtuelle) et réalise la transaction commerciale avec elle. La figure ci- après illustre ce principe.

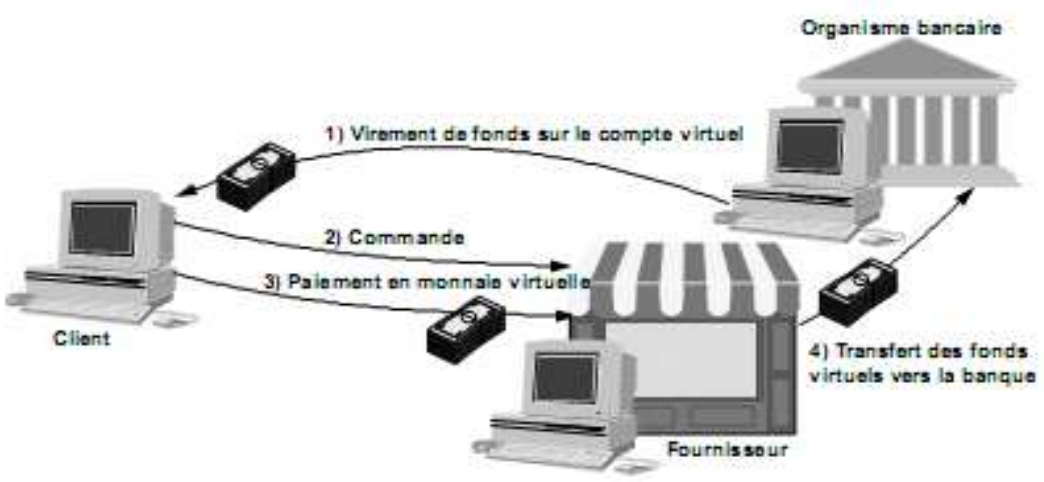


Figure 01. 4 : *Principe de paiement off-line*

1.5.2 Le paiement on-line

Dans ce type de relation, le paiement s'effectue à l'aide d'une carte bancaire. Le client joint à son bon de commande, son numéro de carte bancaire. Le vendeur transmet à la banque le numéro de carte et le montant de l'achat. La banque effectue le transfert de fonds.

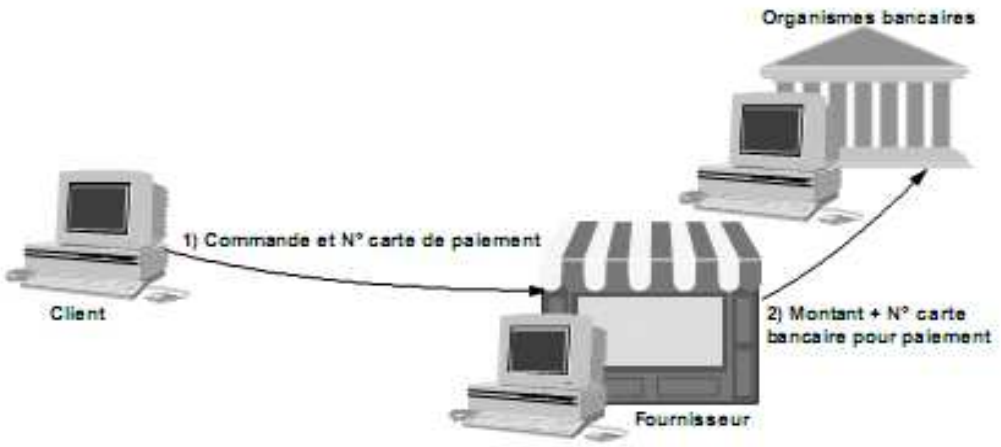


Figure 01.5 : *Principe de paiement on-line*

1.6 Dialogues [16]

1.6.1 Notion

Durant le passage d'un client sur la GAB, il y a pleins d'événements qui fonctionnent à l'intérieur de la GAB, alors notre objectif est de connaitre les échanges entre banques permettant à un particulier la consultation avec sa carte bancaire, même si celle-ci n'est pas émise par la même banque que celle du client. Nous examinons le fonctionnement de la carte bancaire. Le paiement par carte bancaire met en relation plusieurs acteurs :

Un client, souhaite de régler une consultation de son compte avec la carte bancaire qu'il possède et qui lui a été fournie par sa banque (on note banque X sa banque). Soit banque Y l'autre banque à laquelle il est connecte par le terminal de paiement ;

La banque Y va dire si la transaction est autorisée, à la banque X.

La banque Y est connectée à toutes les autres banques installées, et notamment à la banque X, grâce au réseau interbancaire

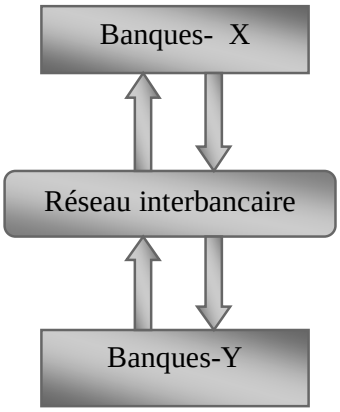


Figure 01.6 : *Réseau Interbancaire*

1.6.2 La structure

On sait que le terminal se connecte en passant par le réseau téléphonique au serveur de la banque Y et envoie le numéro de la carte bancaire ainsi que le montant de la transaction. Le serveur de la banque Y regarde le numéro de la carte et, se rendant compte qu'il ne s'agit pas l'une des cartes qu'il a mises, envoie le numéro de carte avec le montant de la transaction au serveur de la banque X, vers réseau interbancaire permettant de relier les différentes banques.

Le serveur de la banque X prend connaissance du numéro de la carte bancaire et vérifie que le compte correspondant à ce numéro dispose d'un solde suffisant pour honorer la transaction.

Si c'est le cas, il répond à la banque Y que le paiement est autorisé. Si ce n'est pas le cas, il répond le contraire.

Le serveur de la banque Y transmet la réponse au terminal du client.

La transaction est validée " *paiement autorisé* " ou refusé " *paiement non autorisé* ".

1.6.3 La demande d'autorisation

La suite des opérations décrites ci-dessus se nomme la "*demande d'autorisation*" a pour but de vérifier que le compte client est bien provisionné. Cette demande d'autorisation dépend à l'utilisation du terminal.

La demande d'autorisation transite via deux serveurs différents :

- Le serveur d'acquisition : Il s'agit du serveur de la banque du client auquel se connecte le terminal vers le réseau téléphonique. Une fois connecté, le terminal envoie au serveur d'acquisition toutes les informations concernant la transaction, notamment le montant, le numéro de carte et des données permettant d'assurer la sécurité de la transaction.
- Le serveur d'autorisation : Il s'agit du serveur de la banque du client auquel le serveur d'acquisition transmet l'autorisation de paiement émise par le terminal. La réponse à la demande suit le chemin inverse, à savoir serveur d'autorisation de la banque du client

1.6.4 Le routage

Pour effectuer le routage des demandes d'autorisation, c'est-à-dire pour déterminer à quelle banque chaque demande d'autorisation doit être transmise, le serveur d'acquisition utilise les premiers numéros de chaque carte bancaire concernée : ceux-ci indiquent la banque ayant émis cette carte. Nous partirons des principes suivants :

- un numéro de carte est constitué de seize chiffres décimaux ;
- les quatre premiers correspondent à un code spécifique à chaque banque ;

- les serveurs d'acquisition des banques sont directement reliés au réseau interbancaire.
- Chaque serveur d'acquisition analyse donc le numéro de la carte qui figure dans la demande d'autorisation qu'il reçoit, puis :

· si le client est dans la même banque et que le serveur d'acquisition, il envoie la demande directement au serveur d'acquisition de cette banque ;

· si le client est dans une autre banque, le serveur d'acquisition envoie la demande sur le réseau interbancaire, sans se préoccuper de la suite du transit.

Le réseau interbancaire n'est donc pas un simple réseau physique : il doit aussi effectuer le routage des demandes d'autorisation, c'est-à-dire analyser les demandes qui lui sont fournies, envoyer chaque demande vers le serveur d'autorisation de la banque correspondante et, enfin prendre en charge la transmission de la réponse lorsqu'elle lui revient.

1.7 Architecture fonctionnelle

Le réseau Interbancaire Banque du client, Serveur d'Autorisation, Serveur d'Acquisition Réseau Interbancaire sont en relations, on schématise par la figure ci- dessous

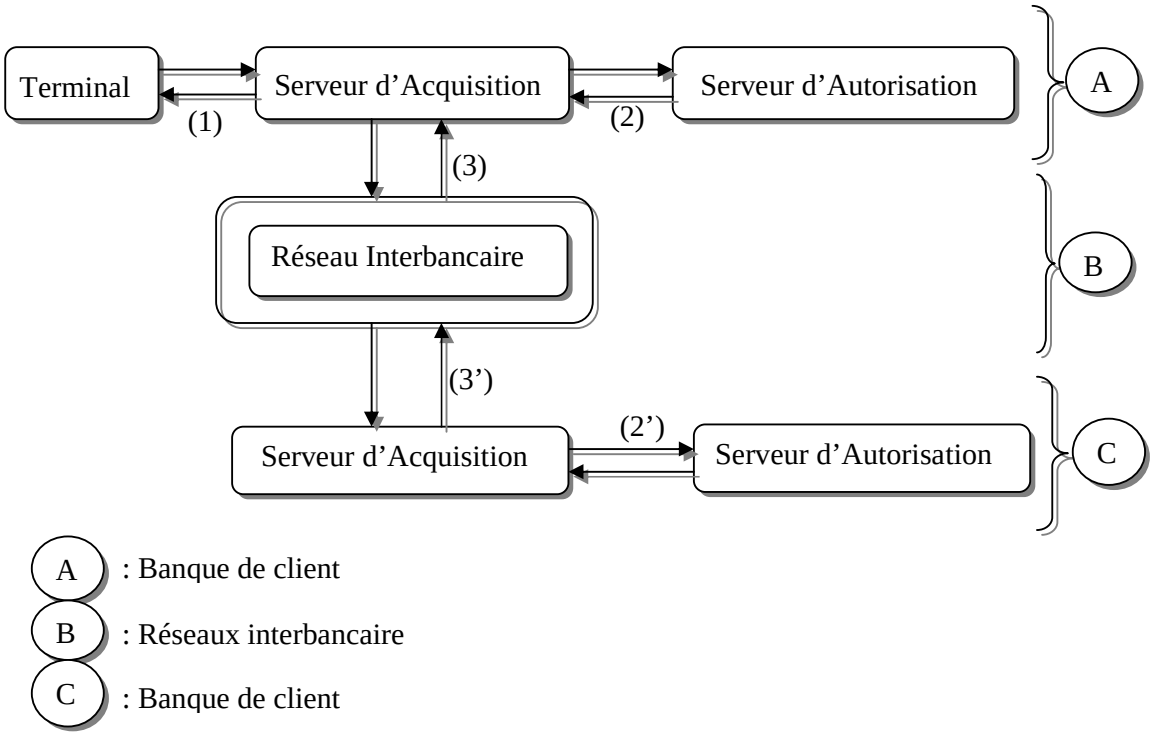


Figure 01.7 : Architecture *fonctionnelle*

Le terminal est relié via le réseau téléphonique (1) au serveur d'acquisition de la banque du client. Celui-ci est connecté au sein de la banque (2) au serveur d'autorisation de cette même banque. Le réseau interbancaire relie (3,3') les serveurs d'acquisition des différentes banques. Toutes les autres banques de la place sont également reliées au réseau interbancaire, mais ne sont pas représentées dans ce schéma.

Or le serveur d'acquisition n'a qu'une fonction de routage :

- il doit pouvoir accepter des demandes d'autorisation provenant de terminaux et du réseau interbancaire ;
- il doit pouvoir effectuer le routage des demandes d'autorisation vers le serveur d'autorisation de la banque ou bien vers le réseau interbancaire ;
- il doit pouvoir accepter les réponses provenant du réseau interbancaire ou du serveur d'autorisation de la banque ;
- il doit pouvoir envoyer les réponses vers le réseau interbancaire ou le terminal (en étant capable d'apparier chaque réponse à la demande initiale).
- Le serveur d'acquisition doit être capable d'utiliser le protocole de communication employé par les terminaux, ainsi que le protocole du réseau interbancaire et le protocole du serveur d'autorisation. Pour pouvoir effectuer correctement le routage des messages, le serveur d'acquisition doit connaitre les 4 premiers chiffres des numéros des cartes de sa banque.

1.7.1 Le serveur d'autorisation

Le serveur d'autorisation doit être capable de fournir une réponse à une demande d'autorisation. Pour fonctionner, le serveur d'autorisation doit donc avoir accès aux soldes des comptes des clients de la banque référencée par numéro de carte; lorsqu'une demande d'autorisation lui parvient, le serveur vérifie que le numéro de carte figure bien dans sa liste. Il contrôle alors que le solde de compte est suffisant pour effectuer la transaction, si c'est le cas il répond oui, sinon il répond non.

1.8 Le réseau interbancaire

Le réseau interbancaire n'a qu'une fonction de routage :

- il doit pouvoir accepter les messages provenant des serveurs d'acquisition ;
- il doit pouvoir analyser le contenu des messages pour déterminer vers quel serveur

d’acquisition il doit les envoyer.

Pour fonctionner, le réseau interbancaire doit posséder la liste des codes de 4 chiffres figurant en entête des cartes et les banques associées.

1.8.1 Gestion des échanges par tuyaux

Les terminaux connectés au même serveur d’acquisition les terminaux d’une même banque utiliseront chacun une paire de tuyaux pour dialoguer avec ce serveur. Le serveur d’acquisition aura donc comme rôle d’orchestrer simultanément les lectures et les écritures sur ces tuyaux. Les échanges entre un serveur d’acquisition et un serveur d’autorisation seront possibles au travers d’une paire de tuyaux fonctionnant d’une façon très classique.
En ce qui concerne le réseau interbancaire et les serveurs d’acquisition, il faudra utiliser une paire de tuyaux pour connecter chaque serveur d’acquisition au réseau interbancaire.

1.8.2 Raccordement

La mise en place des communications au sein d’une même banque, il faut maintenant créer d’une part une paire de tuyaux entre Acquisition et chaque terminal alors il y aura autant de paires de tuyaux que de terminaux, et d’autre part, une paire de tuyaux entre Acquisition et Autorisation, après avoir redirigé leurs entrées et sorties standards. Ecrire un programme banque acceptant sur sa ligne de commande le nombre de terminaux de la banque. Le programme devra également accepter sur sa ligne de commande les paramètres suivants :

- le nom de la banque à simuler ;
- les 4 chiffres associés à cette banque ;
- le nom d’un fichier contenant les soldes des comptes clients ;
- le nombre de terminaux à créer.

A la fin de recouvrir la banque par le programme d’acquisition sans oublier les redirections nécessaires des tuyaux avec les entrées et sorties standards.

1.8.3 Création du réseau interbancaire

1.8.3.1 Processus Interbancaire

Chaque serveur d’acquisition sera relié au processus Interbancaire par une paire de tuyaux. Celle-ci permettra à Interbancaire de recevoir les messages de demande d’autorisation et de transmettre les réponses en retour, après les avoir routés. L’architecture à mettre en place entre interbancaire et les différents processus d’acquisition sera similaire à celle mise en place entre chaque processus

d’acquisition et les processus terminal qui y sont reliés.

1.8.3.2 Délai d’annulation

Dans ce cas, les processus d’acquisition et interbancaire doivent pouvoir gérer une fonction d’annulation : une transaction est annulée lorsqu’il s’est écoulé plus de 2 secondes depuis le relai de la demande, sans qu’une réponse ne soit parvenue. Si une réponse parvient ultérieurement, elle sera ignorée. Ceci suppose que les processus Acquisition et Interbancaire conservent une trace datée de toutes les demandes qu’ils traitent et qu’ils vérifient régulièrement la date de péremption de chaque demande.

1.8.3.3 SWIFT

Le SWIFT Society for Worldwide Interbank Financial Transaction est une société privée basée à Bruxelles, dont l’objet est d’assurer un réseau international de communication électronique entre les acteurs financiers. La plupart des banques adhèrent au SWIFT.

C’est un réseau interbancaire à commutation de paquets. Il offre une palette de services extrêmement diversifiés tels les transferts de compte à compte, opérations sur devises ou sur titres, recouvrements, etc... La transmission des informations est chiffrée et les procédures d'authentification sont très strictes. L’architecture de réseau est centralisée sur trois centres de commutation aux Etats-Unis et en Europe (Amsterdam, Bruxelles). Ces commutateurs se rattachent à chaque pays concerné par des concentrateurs nationaux. Des réseaux de lignes ou des liaisons satellites relient les centres de commutation SWIFT entre eux et avec les commutateurs nationaux.

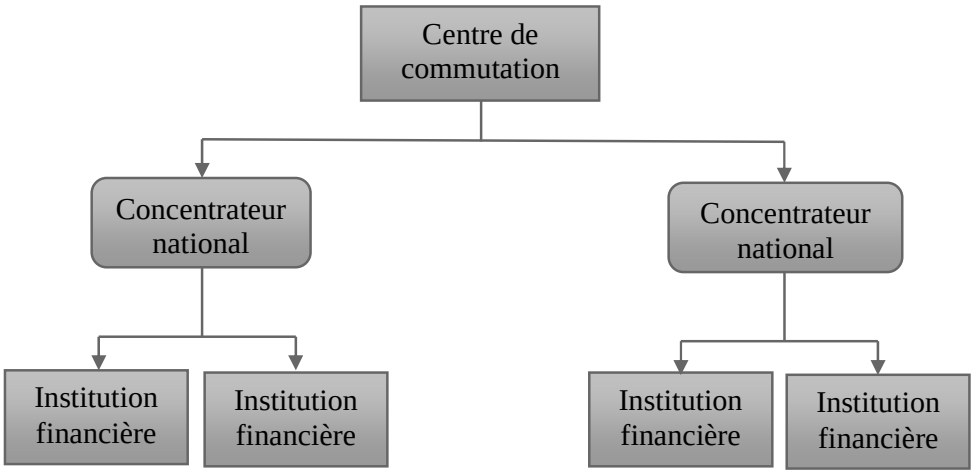


Figure **01.8 :** *Réseau SWIFT* SWIFT

1.9 Conclusion

L’environnement de la carte bancaire dépend toujours des aspects extérieurs et les autres éléments pour qu’elles fonctionnent correctement. Elle devenue portable on peut utiliser n’ importe où, n’importe quand, dés qu’une foi la carte est activée dans un terminal ; tous les données déjà enregistrer s’ouvre les différents passerelles à pour but de satisfaire des besoins et les différents consultations des clients, les réseaux interbancaires les bases de données de la banques se manifestent à partir de la donner crypter à l’intérieur de la carte bancaire

Même si la télécarte se différencie en deux types il y à des points qu’elles se ressemblent c’est la sécurisation

CHAPITRE 2 : LE PRINCIPE DE LA SECURISATION DE LA CARTE BANCAIRE

2.1 Piste magnétique [8][12][15]

Issue d'une technologie du début du 20ème siècle, l'enregistrement et la lecture magnétique sont encore très utilisés de nos jours. En effet, il existe de nombreuses utilisations des supports magnétiques. Mais nous intéresse à la piste magnétique de la carte bancaire.

2.2 Enregistrement et lecture magnétique

2.2.1 Principe général

Le principe de l'enregistrement magnétique repose sur la magnétisation de très petites zones de la bande magnétique constituée de pigments magnétiques tels que l'oxyde de fer, oxyde de chrome ou ferrite de baryum. Cette opération de magnétisation est effectuée par une tête magnétique d'écriture. En fait, il s'agit d'un genre d'électro-aimant. En passant sur la bande magnétique, pour une opération d'écriture, la tête va plonger les pigments dans un champ magnétique proportionnel au courant la traversant. Cette magnétisation va subsister et correspondra alors à un enregistrement

2.2.2 Les caractéristiques

Une caractéristique importante des supports magnétiques est leur champ coercitif ou *coercitivité*. C'est tout simplement leur résistance à la désaimantation. Une distinction est donc faite entre les supports HiCo et LoCo par conséquent, un support dit HiCo pourra être désaimanté plus désaimanté plus difficilement qu'un support LoCo. Pour l'opération de lecture, le passage de la tête sur la bande donnera naissance du flux magnétique dans son noyau, lequel induira une tension électrique proportionnelle aux variations du flux. Le signal électrique, les informations préalablement enregistré sur la bande magnétique est alors restitué.

2.2.3 Les données numériques

Le principe général est parfaitement adapté comme à l'enregistrement et la lecture de données analogiques. Concernant l'enregistrement de données numériques; un signal avec seulement deux états à savoir le 1 et le 0. Néanmoins, on se pose lors de la relecture puisque qu'il est alors impossible de séparer précisément une suite de 1 ou de 0. Effectivement, seule la transition entre l'état 1 et l'état 0 est marquée par une tension électrique contrairement à une succession de 1 ou de 0 où n'apparaît aucun changement d'état donc de tension. Pour palier à cela un codage spécial pour l'enregistrement a été adopté : le codage F/2F.

2.2.4 Principe du codage F/2F

Pour la lecture, la tête va parcourir la bande et suivant l'orientation des particules une intensité va être crée dans la tête. Cette intensité sera amplifiée puis modélisée par un signal rectangulaire de type niveau haut et niveau bas. Ce signal va ensuite être interprété par une suite de 0 et de 1 suivant le codage F/2F.

Ce codage est basé sur l'enregistrement par inversion de flux. Cette technique consiste à faire circuler le courant, dans la tête, dans un sens puis dans l'autre. Il y aura donc uniquement deux orientations diamétralement opposées des pigments constituant le support magnétique.

Le codage F/2F est en fait une évolution de cette technique. Dans ce codage le 0 sera alors représenté par une inversion de flux en début et en fin de bit tandis que le 1 aura une inversion supplémentaire en milieu de bit. Néanmoins, la "durée" la longueur du support magnétique occupé sera identique pour le 1 et le 0. Le bit 1 aura donc une fréquence double par rapport au 0.

2.3 Encodage de bande magnétique

Les cartes à bande magnétique déjà existées. Il s'agissait alors de cartes d'identification sur support en papier filmé et de cartes de crédit. La technologie des bandes magnétiques est largement répandue dans le monde et reste la technologie la plus utilisée pour le traitement des transactions et le contrôle d'accès

Figure 02.1 : *Bande magnétique*

2.3.1 Force coercitive

Ce terme technique indique quel niveau de force doit dégager un champ magnétique pour affecter les données encodées sur une bande magnétique. La force coercitive se mesure en Oersted (*Oe*). Elle mesure le niveau de difficulté d'encodage d'informations sur une bande magnétique.

2.3.2 HiCo, LoCo

Les bandes magnétiques *HiCo* résistent le mieux aux effets des champs magnétiques rayonnés.

Elles sont plus difficiles à encoder que les bandes magnétiques *LoCo* car l'encodage consomme plus d'électricité. Les cartes à bande magnétique *HiCo* sont légèrement plus chères pour cette raison. Le *LoCo* Ce type de bande est plus facile à encoder et légèrement moins précieux que les cartes à bande magnétique *HiCo.*

2.4 La durée de vie de la carte

2.4.1 L'usage

Le type de bande magnétique requis dépend de l'utilisation de la carte. La bande magnétique elle peut lire tous les jours, ou une fois par mois ou juste deux fois par an. Le tableau ci-dessous indique quelles bandes sont utilisées dans des applications, et à quelle fréquence elles sont lues.

Applications de carte à bande magnétique courantes, types et fréquence d'usage

APPLICATIONS	LOCO	HICO	USAGE
Contrôle d'accès		●	Quotidien
Cartes de fidélité (commerce de détail)	●		Hebdomadaire
Cartes d'adhérents	●		Hebdomadaire/Mensuel
Pointage et présence		●	Quotidien
Débit/Crédit	International	États-Unis	Hebdomadaire/Mensuel
Permis de conduire		●	Occasionnel*

Tableau 02.1 : *Application et usage de bande*

Le moyen le plus simple de déterminer si la bande d'une carte est de type HiCo ou LoCo est de vérifier sa couleur. Les bandes HiCo sont noires et les bandes LoCo sont d'un marron plus clair. Les lecteurs de carte magnétique ne savent pas discriminer une bande HiCo ou LoCo et ils sont conçus pour lire les deux.

2.4.2 Durabilité et sécurité des cartes

Même si le stockage des données en bande magnétique sont efficaces il y aussi des limites suivants leurs types. Alors il y a des différents types de matériaux permettent de protéger les cartes plastiques contre l'abrasion, l'usure, l'effacement, l'altération et la duplication. Les plus courants sont les vernis d'overlay et les films de laminage. Ils augmentent la durabilité de la carte et son niveau de sécurité. La durabilité d'une carte correspond à sa capacité à résister à différentes formes d'agressions extérieures. Il s'agit de la résistance à l'abrasion, lorsque la carte est insérée dans un lecteur de bande magnétique, sa résistance à l'effacement lorsque l'image est exposée aux rayons UV, sa résistance à l'endommagement lorsqu'elle est immergée dans l'eau ou exposée à

des agents chimiques.

2.4.2.1 Les matériaux

Il y à les valeurs de la carte mais elle ne peut être sûre car il est possible de vérifier son authenticité. Parmi les techniques utilisées, on applique un vernis d'overlay ou des matériaux de laminage avec des images holographiques. L'utilisation de ces matériaux dans la fabrication de cartes rend pratiquement impossible la réplication sans toucher aux matériaux qui comportent l'hologramme personnalisé. La durée de vie d'une carte dépend des matériaux qu'elles contiennent d'où on classe suivant le matériau

MATERIAU	DUREE DE VIE	DURABILITE	SECURITE
Vernis d'overlay	Jusqu' à 2 ans	Minimale	
Vernis d'overlay avec hologramme	Jusqu' à 2 ans	Minimale	Visuelle
Film du minage clair	De 5 à 7ans	Elevée	
Film du minage hologramme	De 5 à 7ans	Elevée	Visuelle

Tableau 02.2 : *Matériaux de protection de carte*

2.5 Les inconvénients

Les vernis d'overlay protègent les cartes, mais ont une durée de vie bien plus courte que les films de laminage, et leur niveau de sécurité est très faible à l'exception de certains vernis hologramme. Les vernis ne forment pas une couverture solide et leur surface est criblée de petits trous qui permettent d'évacuer les particules de cire de la carte. L'image risque donc de s'estomper sous l'effet des rayons UV, le couleur dépassé et l'impression de s'effacer.

2.6 La sécurité

2.6.1 La technique de sécurisation de bande magnétique

En ce qui concerne la sécurité, il n'y a aucun moyen plus sûr pour protéger physiquement les données enregistrées sur un support magnétique. En effet, la lecture et l'écriture sont entièrement libres. Il est donc indispensable de sécuriser l'application utilisant ce support. Concrètement, il faut crypter les données sensibles enregistrées sur le support et couplé l'utilisation de la carte avec un code secret.

2.6.2 L'opération XOR

L'opération xor est très différente car il y a la réponse 0 dans le résultat mais l'opération il y 1 où 0 et il y a la réponse 1 dans le résultat mais l'opération il y 0 où 1.

x	y	x ⊕ y
0	0	**0**
0	1	**1**
1	0	**1**
1	1	**0**

Tableau 02.3 : *Tableau de XOR*

Soit des données suivantes : 0000 1000 0100 1100 ⊕ CLES

0000 ⊕ 1000 = **1000**

1000 ⊕ **0100** = 1100

1100 ⊕ 1100 = **0000**

Les résultats des données protégées seront donc : **0000 1000 0100 1100 0000**

2.7 Avantage :

Grace à la résistance et la fiabilité de la monochrome noire, on peut stocker des plusieurs informations. Elles peuvent être modifiées par leur constructeur, et toutes les données qui étaient conservées dans la carte sont inscrites en binaire. On à plusieurs suites binaires or on connait l'opération *xor*, mais malgré cela la clé reste inconnue.

2.8 Faiblesses :

Presque la carte bancaire à bande magnétique simple est juste une carte qui ne contient que de la piste magnétique d' ou la façon de sécurisation est très vulnérable car on voit qu'il n'y a que l'opération *xor*. Si on fait plusieurs essais puis on trouve plusieurs résultats et on étudie, peut être qu'on trouve la clé de cette opération les données seront faciles à crypter.

On sait que la sécurisation d'une carte bancaire à bande magnétique est très fragile car il utilise que le ***xor*** avec son propre clé. Mais l'aspect physique grâce aux matériaux qu'elle contienne, les informations restent stocker puis on peut effacer et modifier par le constructeur de la carte bancaire. Pour cette raison que nous nous intéressons à étudier la puce électronique.

2.9 Carte puce

La carte à puce, dont le concept a été inventé par Roland Moreno puis repris quelques années plus tard par Michel Urgon, a fait une entrée remarquée dans le domaine des télécartes, si pratiques à utiliser. L'idée originale est de rassembler sur une seule puce toutes les fonctionnalités et de mettre en œuvre les mesures visant à protéger les données contenues ou calculées. Depuis, beaucoup de chemin a été parcouru : les cartes ont conquis de nouveaux marchés et se sont développées. Leur technologie s'est affinée permettant à la carte de réaliser de plus en plus de tâches, de contenir de plus en plus d'informations. La carte à puce apparaît le plus souvent sous son format « carte de crédit ou carte SIM » à cause de ce format il est facile à porter. La puce elle-même est définie par une norme ISO.

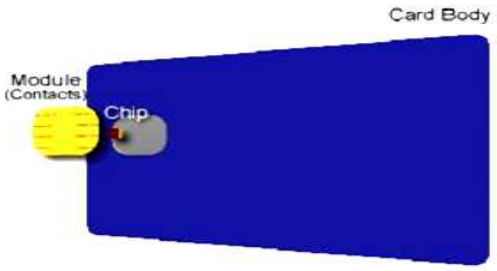


Figure 02.2 : *Carte puce*

2.9.1 Les différents types de la puce

Actuel il y à deux sortes de carte puce : la carte mémoire qui sert seulement au stockage d'information en utilisant la logique pour accéder les informations et la carte à puce intelligente qui est un mini-ordinateur comme la carte puce bancaire,

Pendant la fabrication de la carte puce il y à de norme ISO qu'il faut suivre.

Les normes ISO 7816 peuvent définir divers autres aspects d'une Smart Card comme les signaux électroniques, transmissions et protocoles. De plus, les points de contacts pour la communication entre une SC et le lecteur carte sont définis selon le schéma suivante :

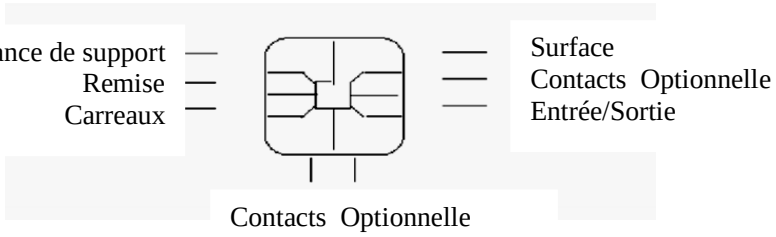


Figure 02.3 : *Puce électronique*

2.9.1.1 Carte mémoire à circuit intégrer

Ils peuvent supporter de 1 à 4 KBS mais n'ont aucun processeur pour manipuler les données. Ainsi elles dépendent du lecteur carte pour leurs traitements et conviennent pour des usages où les cartes effectuent une opération fixe

2.9.1.2 Carte de microprocesseur à circuit intégré

Les cartes de microprocesseur offrent un plus grand stockage de mémoire et une plus grande sécurité des données par rapport à la carte magnétique traditionnelle. Les cartes à mémoire peuvent également traiter des données. Le cœur de la puce, le microprocesseur est un bloc monolithique. Il contient à la fois les unités de calcul tels le processeur et le coprocesseur cryptographique, les mémoires contenant le code de la carte dans la ROM.

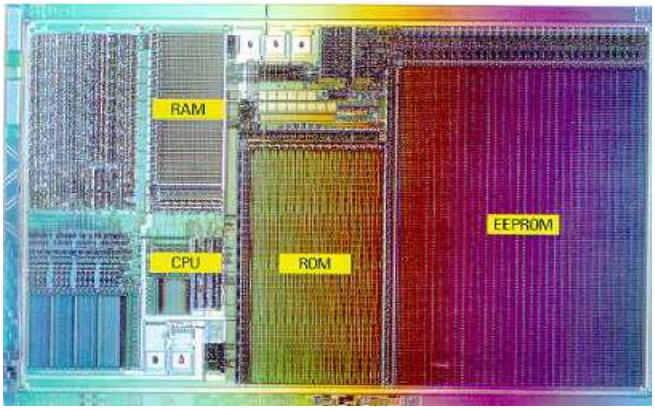


Figure 02.4 : *Microprocesseur*

Les cartes actuelles de haut de gamme proposent 64 ko de ROM, 64 ko d'EEPROM et 4 ko de RAM pour ce qui concerne la mémoire. Il faut donc tenir compte de ces restrictions qui touchent la mémoire mais aussi les performances des processeurs.

2.10 Evolution de carte puce [9] [14]

L'apparition des nouvelles technologies mémoires comme la RAM ainsi que la gravure de plus en plus fine des puces, permet d'espérer une constante croissance des capacités des cartes

Année	Taille du bus	Fréquence	RAM	Mémoire persistante
1981	8 bits	4,77 MHz	36 octets	1 ko d'EPROM
1985	8 bits	4,77 MHz	128 octets	2 ko d'EEPROM
1990	8 à 16 bits	4,77 MHz	256 octets	8 ko d'EEPROM
1996	8 à 32 bits	4,77 à 28,16 MHz	512 octets	32 ko de FLASH
2000	8 à 32 bits	4,77 à 28,16 MHz	1536 octets	32+32 ko de FLASH et d'EEPROM
2002	8 à 32 bits	4,77 à 28,16 MHz	3 à 4 ko	64+64 ko de FLASH et

Tableau 02.4 : *Evolution des caractéristiques des microprocesseurs aux cartes puce*

2.10.1 Norme

En général il y a plein de norme qui caractérise la puce électronique mais nous intéresses à celle de la puce de la carte bancaire. Alors nous voyons les aspects physiques de la carte, on trouve que les dimensions sont toutes les mêmes suites à des normes proposées par le fabricateur de carte.
La norme ISO 7816-2 définit les aspects électriques et la situation des contacts sur la carte. La carte comporte huit contacts dont voici l'utilisation :

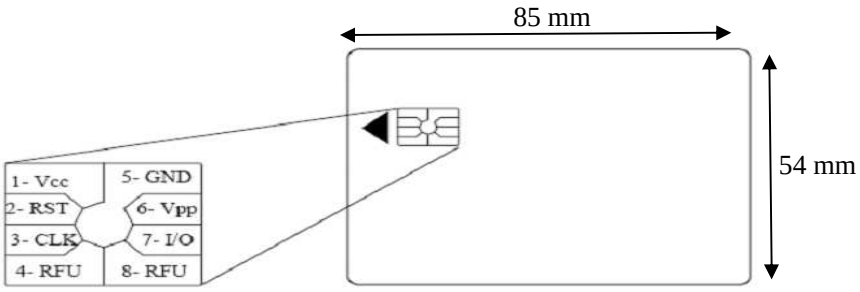


Figure 02.6 : *Les contacts à la carte puce*

Voici les différents types qui correspondent à des niveaux des contacts :

- Le contact 1 correspond à la tension d'alimentation en lecture (Vcc).
- Le contact 2 correspond au signal Reset (RST) : une tension appliquée sur ce contact déclenche l'initialisation physique et logique du composant.
- Le contact 3 correspond au signal d'horloge (CLK). Il fournit le signal d'horloge externe dont dérivera l'horloge interne.
- Le contact 4 est réservé à une utilisation future (RFU : Reserved for Futur Use).
- Le contact 5 correspond à la masse (GND).
- Le contact 6 correspond à la tension d'alimentation (Vpp) à appliquer, sur demande de la

carte, pour programmer la mémoire de données (tension en écriture). Il est seulement utilisé sur des cartes anciennes.

- Le contact 7 est le contact d'entrée/sortie (e/s) par lequel transitent en half-duplex toutes les données échangées entre la carte et le monde extérieur.
- Le contact 8 est réservé à une utilisation future (RFU). Une norme utilisant les contacts RFU serait en cours de préparation pour l'utilisation de l'USB avec la carte

2.10.2 Protocole de communication

Pour pouvoir se communiquer avec le terminal, il existe de protocole qui faire de liaison entre le carte et le terminal, c'est le protocole APDU.

Selon la norme ISO 7816-4 vise à assurer un inter - opérabilité. Il spécifie :

- Le contenu des messages entre la carte et le lecteur CAD : Card Acceptance Device qui utilise le protocole APDU Application Protocol Data Units pour les commandes et les réponses
- Les structures des fichiers et des données :
  - l'accès à ces données,
  - l'architecture de sécurité,
  - la sécurisation des communications.

Durant l'introduction de la carte à le terminal il y à le protocole APDU, c'est le niveau application comme son nom l'indique. Il existe deux types de messages APDUs qui se parlent:

- La commande APDU (C-APDU) qui est émise par le CAD en direction de la carte ;
- La réponse APDU (R-APDU) qui elle transite de la carte au CAD.

Le modèle de discussion entre le CAD et la carte est un modèle maître-esclave où le CAD est le maître et la carte est l'esclave. La carte est toujours en attente d'une commande APDU. Une réponse APDU aura toujours lieu en retour d'une commande APDU. Les deux types de structures de communication commande et réponse sont toujours couplés. La commande et réponse APDU est constituée par :

L'instruction APDU						
CLA	INS	P1	P2	Lc	Champ du données	Le

- CLA (1 octet): Classe d'instruction--- indique la structure et formate pour une catégorie d'instruction et réponse APDU
- INS (1 octet): code de l'Instruction: spécifie l'instruction P1 (1 octet) et P2 (1 octet): paramètres de l'Instruction--fournissez des qualifications à l'instruction plus loin
- Lc (1 octet): Nombre des octets qui présentent dans le champ du données de l'instruction
- Champ du données (les octets égalent à la valeur de Lc): Une séquence des octets dans le champ du données de l'instruction
- Le (1 octet): Maximum des octets a attendu dans le champ du données de la réponse à l'instruction

La response APDU		
Champ du données	SW1	SW2

- Champ du données (longueur variable): Une séquence des octetst a reçu dans le champ du données de la réponse
- SW1 (1 octet) et SW2 (1 octet): mots de la situation--dénotez l'état du traitement dans la carte

Tableau 02.5 : *Instructions des commandes et de réponses APDU*

Il y a quatre cas possibles d'échanges APDU :

- *cas 1* : Aucune donnée n'est échangée entre le CAD et la carte autre que l'entête de la commande APDU et l'en queue de la réponse APDU.
- *cas 2* : Aucune donnée (dans le champ de données de la commande APDU) n'est envoyée à la carte. Le corps de la commande contient le champ Le qui spécifie le nombre d'octets que la carte lui fournira dans le champ de données de sa réponse APDU.
- *cas 3* : Ici des données, de taille Lc octets, sont fournies à la carte (dans le champ de données de la commande APDU) et la carte ne renvoie dans la réponse APDU que son en queue.
- *cas 4* : On a des données échangées dans le champ de données de la commande et de la réponse APDU.

2.11 JavaCard [18]

2.11.1 Définition

C'est un langage à haut niveau, à objets permettant l'encapsulation des données et la réutilisation des codes, il est exécutable sur n'importe quelle carte à puce, car il exécute sur une machine virtuelle. Le code d'applications est compilé en *byte-code* qui est exécute sur la machine virtuelle java JVM. Donc cette portabilité permettra d'écriture de code qui fonctionnera sur n'importe quel micro-processeur de carte à puce "*Write Once RunAnywhere*"

2.11.2 Standardisation

La technologie de JavaCard soit indépendante du matériel du support, une collection de norme d'industrie appelées ISO 7816 a été faite pour la smart card. La norme définit la caractéristique physique, les dimensions et les endroits du contact d'une Smart Card, qui sont montrés par la figure ci-dessus

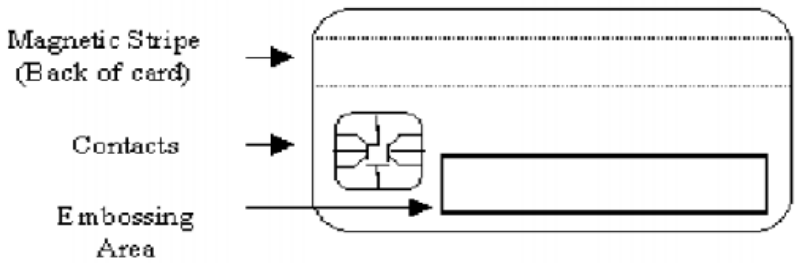


Figure 02.7 : *Caractéristiques physique d'une carte bancaire*

2.11.3 Avantages de Java pour la Programmation des cartes à puces

Presque toutes les carte à puce sont programmées par langage JavaCard mais la sécurisation est un autre domaine, le java aussi possède un modèle de sécurité qui permet à plusieurs applications de coexister en sécurité sur la même carte. A l'aide de JavaCard il est possible de charger dynamiquement, n'importe quand, une nouvelle applet sur la carte. Cela signifie que le code des applets pourra être mis à jour.

2.12 La sécurisation de la puce électronique [21]

La carte bancaire utilise en réalité trois types de sécurité : le code secret, la signature RSA et l'authentification DES. Elle possède actuellement une puce électronique munie d'un microprocesseur, ce qui lui ajoute une sécurité supplémentaire car auparavant, elle ne possédait qu'une piste magnétique sur laquelle étaient inscrites toutes les informations sensibles. Mais des pirates trouvèrent vite le moyen de recopier cette bande magnétique assez simplement.

2.12.1 La signature RSA

Elle sert à prouver l'authenticité de la carte, et non de l'utilisateur. Chaque carte bancaire munie d'une puce électronique possède une valeur de signature, appelée V S. C'est un grand nombre crypté qui lui est propre. La V S est calculée lors de la fabrication de la carte et insérée dans la mémoire de la puce dans des locaux ultra sécurisés. La puce ne calcule donc pas la V S, elle se contente de la garder en mémoire.

En pratique, lors de la transaction, le client introduit sa carte dans le terminal. Celle-ci fournit au terminal sa V S ainsi que des données propres codées (le numéro de carte, la date d'expiration, etc). La vérification s'effectue en deux étapes. Premièrement, le terminal calcule la valeur $X = VS\ (mod\ n)$, où n est la clef publique longue. Ensuite, le terminal calcule une autre fonction à partir des données propres à la carte. Si le résultat de cette fonction est X, alors la V S est validée et la transaction acceptée.

Pour pouvoir créer une V S valide, il faut connaître la factorisation de n. C'est pour cette raison que n est un nombre extrêmement grand, ceci est un bon compromis entre une sécurité suffisante et un rendement efficace.

2.13.1.1 Code confidentiel

Ensuite, le client doit encoder son code confidentiel de 4 chiffres. Mais ce moyen est limité car un voleur peut avoir vu le code, ou forcer son propriétaire à lui divulguer. La vérification du code s'effectue grâce à la puce électronique. Celle-ci contrôle que la valeur du code tapé corresponde bien à la valeur qu'elle a en mémoire.

2.13.1.2 L'authentification par DES

La vérification s'effectue en trois étapes. Première étape, le centre de contrôle envoie une valeur aléatoire. La puce code cette valeur à l'aide de la clef secrète qu'elle possède en mémoire. Rappelons que cette clef secrète n'a aucun rapport avec la V S et le code confidentiel. Une fois le nombre crypté, il est renvoyé vers le centre de contrôle qui possède toutes les clefs secrètes et peut donc vérifier si le résultat correspond à ce qu'il attendait.

2.13 Les avantages

Dans le domaine bancaire, la carte à puce peut être utilisée dans la reconnaissance d'identité. En effet, l'un de ses atouts majeurs est sa personnalisation et son inviolabilité. Nous pouvons donc donner un secret à la carte qui permet à son possesseur de s'identifier auprès de certains services.
Les avantages de la carte à puce sont la sécurité, la portabilité, la facilité d'utilisation et la personnalisation. La carte à puce est résistante aux attaques car elle n'a pas besoin d'être dépendante d'une ressource externe potentiellement vulnérable. La sécurité de la carte à puce se fait à plusieurs niveaux :
Grâce à des coprocesseurs cryptographiques qui permettent de calculer le DES en hardware. Les coprocesseurs mathématiques permettent d'implémenter des algorithmes tels que RSA.

2.13.1 Au niveau software :

Par des contrôles d'accès aux données grâce à un code secret ou par authentification cryptographique. Par un maintien de l'intégrité des données en utilisant la vérification des témoins, les calculs de signatures sur les données internes et l'atomicité des transactions. Grâce à des entrées/sorties sécurisées par chiffrement/signature et temps d'exécution des commandes constants. Par des commandes effectuant des opérations cryptographiques comme la signature des données et le chiffrement/déchiffrement de données.

2.13.2 Au niveau physiquement sécurisé :

La taille de la carte à puce qui rend celle-ci portable et mobile, est un gros avantage. En effet, elle permet de stocker des informations qui seront disponibles quelque soit l'endroit où se trouve le possesseur de la carte. Le dernier avantage de la carte est sa possibilité de personnalisation aussi bien pour le porteur de carte que pour le fournisseur de carte.

2.14 Conclusion

Par sa conception, la carte à puce apparaît comme un élément hautement sécurisé d'un système pouvant garder et protéger des secrets. Très intéressant en fonction du noyau qui se trouve dans le microprocesseur, en même temps la carte bancaire peut traiter des calculs, des données pendant son utilisation .puis qu'elle s'accorde avec les mémoires dans la puce. La carte est un outil de sécurité et prône en tant que telle une fermeture. La dualité et a contradiction de la carte à puce apparaissent dans l'ouverture vers l'extérieur et la connexion aux autres systèmes vers lesquels les acteurs de la carte se dirigent. Il faut, en plus de proposer de nouvelles fonctionnalités et de nouveaux services, continuer d'assurer la même sécurité qu'auparavant, c'est-à-dire assurer

l’intégrité, la confidentialité et la disponibilité des données et des applications de la carte. De nouveaux mécanismes de sécurité doivent être mis en place afin de garantir la sécurité de la carte et lui permettre ainsi de préserver ses qualités de sécurité et de fiabilité dans les futures applications.

CHAPITRE 3 : LA CRYPTOGRAPHIE ET SA LIAISON AVEC LA CARTE BANCAIRE

3.1 La cryptologie [3] [6]

3.1.1 Térmologie

Certaines personnes ont confondue des termes pour l'appellation sur l'entourage de cryptologie, en effet on va détailler quelques vocabulaires

La cryptologie est une science mathématique qui comporte deux branches : la cryptographie et la cryptanalyse et ses pratiquants sont appelés **cryptologues**.

La cryptanalyse, à l'inverse, est l'étude des procédés cryptographiques dans le but de retrouver des faiblesses et en particulier de pouvoir décrypter des textes chiffrés. Elle consiste surtout à retrouver le texte en clair sans connaître la clé de déchiffrement.

On appelle **cryptanalyse** la reconstruction d'un message chiffré en clair à l'aide de méthodes mathématiques. Ainsi, tout cryptosystème doit nécessairement être résistant aux méthodes de cryptanalyse. Lorsqu'une méthode de cryptanalyse permet de déchiffrer un message chiffré à l'aide d'un cryptosystème, on dit alors que l'algorithme de chiffrement a été « cassé ».

On distingue habituellement quatre méthodes de cryptanalyse :

- Une **attaque sur texte chiffré seulement** consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés ;
- Une **attaque sur texte clair connu** consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, connaissant le texte en clair correspondant ;
- Une **attaque sur texte clair choisi** consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de les générer à partir de textes en clair ;
- Une **attaque sur texte chiffré choisi** consiste à retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, l'attaquant ayant la possibilité de les générer à partir de textes en clair.

La cryptographie est science qui utilise les mathématiques pour le cryptage et le décryptage de données. Elle permet ainsi de stocker des informations confidentielles ou de les transmettre des données non sécurisés, afin qu'aucune personne autre que le destinataire ne puisse les lire. La **cryptologie traditionnelle** est l'étude des méthodes permettant de transmettre des données de manière confidentielle. A fin de protéger un message, on lui implique une transformation qui le rend incompréhensible, à partir d'un texte en clair donne un texte chiffré. Dans **la cryptographie moderne**, les transformations sont des fonctions mathématiques cryptographiques, qui dépendent

d'un paramètre appel clé.

La clé est une valeur utilisée dans un algorithme de cryptographie, afin de générer un texte chiffré et de le déchiffrer.

Un message est appelé **texte en clair**. Le processus de transformation d'un message de manière à le rendre incompréhensible est appelé **chiffrement** (ou encryption, cryptage). Le résultat de ce processus de chiffrement est appelé **texte chiffré** (ou encore cryptogramme).

Le processus de reconstitution du texte en clair à partir du texte chiffré est appelé **déchiffrement** (ou décryptage).

Un algorithme cryptographique est une fonction mathématique utilisée pour le chiffrement et le déchiffrement. Si la sécurité d'un algorithme est basée sur le fait que celui-ci est tenu secret, on parlera alors d'algorithme restreint. Un cryptosystème est composé d'un algorithme, tous les textes en clairs, textes chiffrés, et les clés possibles

3.1.2 La cryptographie répond à différents besoins :

En plus d'assurer la confidentialité des échanges, la cryptographie permet également d'en assurer l'authentification, la non-répudiation et l'intégrité, ceci bien sûr dans la mesure où le cryptage utilisé est efficace.

- ***Confidentialité***

L'échange privé à l'échange politique, militaire ou commercial, lorsque des informations sensibles doivent être transmises, les correspondants veulent être certains que leurs informations ne pourront être lues par d'autres personnes qui pourraient avoir de mauvaises intentions.

- ***Authentification***

La cryptographie peut également permettre de certifier qu'une information provient véritablement de l'expéditeur attendu. C'est-à-dire qu'elle permet à l'expéditeur d'apposer sa signature à la suite du données, et il est le seul à pouvoir le faire.

- ***Non-répudiation***

La contestation qu'une information a été émise peut aussi être évitée grâce à la signature numérique. L'envoyeur ne peut nier avoir envoyé un message à récepteur à partir du moment où il y a apposé sa signature numérique. Pour que les partenaires ne puissent ignorer le contenu des informations.

- ***Intégrité***

La quatrième fonction de la cryptographie est d'assurer que les données transmises ne seront pas altérées, que les informations ne seront pas interceptées puis modifiées par une autre personne.

3.2 Principaux systèmes de chiffrement

Nombreux systèmes de chiffrements différents ont été imaginés pour se protéger contre la curiosité et la malveillance des ennemis depuis des siècles jusqu' à nos jours mais on peut distinguer en trois grandes classes présentées par la figure suivante.

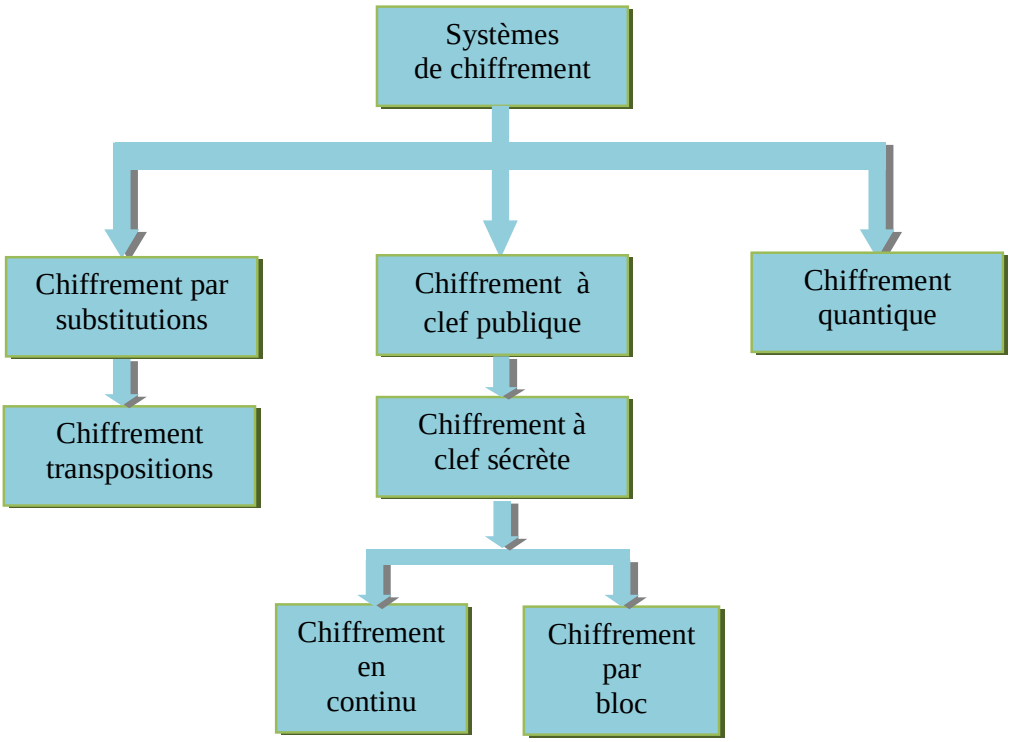


Figure 03.1 : *Systèmes de chiffrement*

3.2.1 Systèmes classiques

Avant l'avènement des ordinateurs, l'opération de chiffrement était basée sur des caractères. L'idée était de transposer ou de remplacer les caractères d'un texte par d'autres. Les meilleurs systèmes répètent ces deux opérations de base plusieurs fois.

3.2.1.1 Substitution

Historiquement, c'est le premier type de chiffrement utilisé. C'est un chiffrement dans lequel chaque caractère de texte en clair est remplacé par un autre caractère dans le texte chiffré.

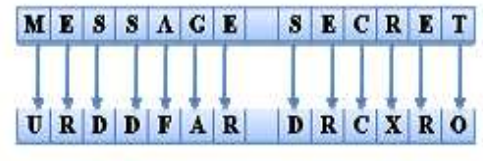


Figure 03.2 : *Principe de la substitution*

3.2.1.2 Transposition

Un chiffrement par transposition est un chiffrement dans lequel les caractères du texte en clair demeurent inchangés mais dont les positions respectives sont modifiées.

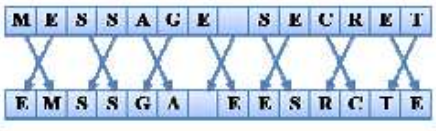


Figure 03. 3 : *Principe de la transposition*

La substitution et la transposition peuvent être facilement cassées car elles ne cachent pas les fréquences des différents caractères du texte en clair. D'ailleurs, les procédures de chiffrement et de déchiffrement doivent être gardées secrètes.

3.2.2 Systèmes de chiffrement quantique

Les systèmes de chiffrement quantique sont des systèmes fondés sur la mécanique quantique et les propriétés particulières de la matière dans ce domaine. Ils reposent sur le principe d'incertitude d'Heisenberg, selon lequel la mesure d'un système quantique perturbe ce système. Une oreille indiscrète sur un canal de transmission quantique engendre des perturbations inévitables qui alertent les utilisateurs légitimes. Ce système résout ainsi les problèmes de distribution de clé.

3.2.3 Systèmes modernes

Les systèmes modernes sont plus complexes, cependant la philosophie reste la même. La différence fondamentale est qu'ils exploitent la puissance des ordinateurs modernes en manipulant directement des bits, par opposition aux anciennes méthodes qui s'opèrent sur des caractères alphabétiques. Ce n'est donc qu'un changement de taille ou de représentation.

On distingue deux classes de chiffrement à base de clés : le chiffrement à clé publique et le chiffrement à clé secrète. Ce dernier type, qui est largement développé dans cet ouvrage, regroupe ceux opérant par bloc ou en continu.

3.3 Principe général du chiffrement [20]

Le texte en clair est noté M. Ce peut être une suite de bits, un fichier de texte, un enregistrement de voix numérisé, ou une image vidéo numérique, …Le texte en clair peut être transmis ou stocké. Le texte chiffré est noté C, qui a la même taille que M, parfois plus grand.

La fonction de chiffrement, notée E, transforme M en C. E(M) = C (3.1)

La fonction inverse, notée D, de déchiffrement transforme C en M : D(C) =M (3.2)

Figure 03. 4 : *Chiffrement et déchiffrement*

3.3.1 Chiffrement avec une clé

Dans ce type de chiffrement, les opérations de chiffrement et de déchiffrement utilisent toutes les deux la clé *k*, aussi, les fonctions s'écrivent de la même manière suivante :

$$E_k(M) = C \text{ et } D_k(C) = M \quad (3.3), (3.4)$$

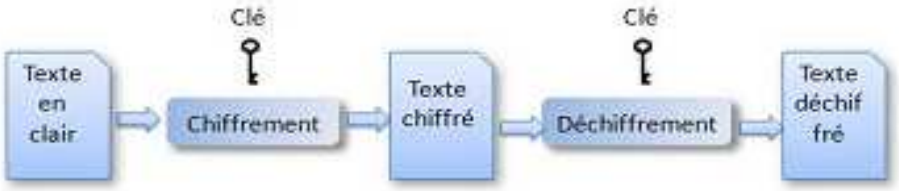


Figure 03. 5 : *Chiffrement et déchiffrement avec une clef*

3.3.2 Chiffrement avec deux clés

Certains algorithmes utilisent des clés différentes pour le chiffrement et le déchiffrement.

Dans ce cas, la clé de chiffrement, notée *k1*, est différente de la clé de déchiffrement, notée *k2* :

$$E_{k1}(M) = C \text{ et } D_{k2}(C) = M \quad (3.5), (3.6)$$

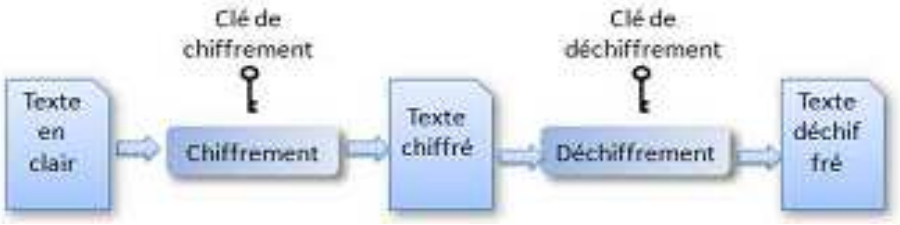


Figure 03. 6 : *Chiffrement et déchiffrement avec deux clés*

3.4 Algorithme cryptographique

Il y a deux types principaux d'algorithmes à base de clés : algorithme à clé secrète et algorithme à clé publique.

3.4.1 Algorithme à clé secrète

Les algorithmes à clé secrète sont des algorithmes où la clé de chiffrement peut être calculée à partir de la clé de déchiffrement ou vice versa. Dans la plupart des cas, la clé de chiffrement et la clé de déchiffrement sont identiques. Pour de tels algorithmes, l'émetteur et le destinataire doivent se mettre d'accord sur une clé à utiliser avant d'échanger des messages. Cette clé doit être gardée secrète. La sécurité d'un algorithme à clé secrète repose ainsi sur la clé : si celle-ci est dévoilée, alors n'importe qui peut chiffrer ou déchiffrer des messages dans ce cryptosystème.
Les algorithmes à clé secrète peuvent être classés en deux catégories. Certains opèrent sur le message en clair un bit ou un octet à la fois. Ceux-ci sont appelés algorithmes de chiffrement en Continu. D'autres opèrent sur le message en clair par groupes de bits de taille supérieure à un bit. Ces groupes de bits sont appelés blocs, et les algorithmes correspondants sont appelés algorithmes de chiffrement par blocs. La taille typique des blocs est de 64 bits.

3.4.2 Algorithme à clé publique

Les algorithmes à clé publique sont conçus de telle manière 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. De tels algorithmes sont appelés algorithmes « à clé publique » parce que la clé de chiffrement peut être rendue publique : n'importe qui peut l'utiliser pour chiffrer un message mais seul celui qui possède la clé de déchiffrement peut déchiffrer le message chiffré résultant. Dans de tels systèmes, la clé de chiffrement est appelée clé publique et la clé de déchiffrement est appelée clé privée. La clé privée est aussi appelée clé secrète.

Parfois, les messages seront chiffrés avec la clé privée et déchiffrés avec la clé publique ; une telle technique est utilisée pour les signatures numériques.

3.5 Cryptosystèmes à clef privée [7] [19]

La norme DES prend son origine dans l'algorithme LUCIFER d'IBM. Elle utilise des clés de 56 bits. Cette méthode de chiffrement est actuellement considérée comme peu sûre pour une attaque disposant de très gros moyens informatiques. Elle est tout de même encore souvent utilisée dans les milieux bancaires où le niveau de sécurité apporté par cette technique est jugé suffisant.
Le choix de cryptosystème dépend surtout des contraintes de l'application à sécuriser. Chacun d' entre eux présente des avantages et des inconvénients en termes de sécurité, et aussi en termes de synchronisation et de tolérance aux erreurs. Mais ici, nous avons décidé de développer les cryptosystèmes suivants DES et 3DES.

3.5.1 Le cryptosystèmes DES et son successeur

Le système cryptographie le plus utilisé dans le monde est le DES ou Data Encryption Standard, publié en 1975. Il a été réévalué régulièrement depuis et renouvelé comme standard, probablement pour la dernière fois, jusqu' à 1988 ;

3.5.1.1 Description de DES

Schéma général

Le DES utilise une clef K de 56 bits, pour chiffrer des blocs de 64 bits, les blocs chiffrés obtenus ayants 64 bits. Le bloc de texte clair subit d' abord une permutation initiale. Puis on itère 16 fois une procédure identique décrite ci- après, ou la moitié droite est copiée telle quelle à gauche, et la moitié gauche est transmisse à droite en subissant au passage une modification dépendante de la clef A la fin, on inverse les moitiés gauches et droites (ou bien comme sue le schéma, on supprime le croissement des dernières étapes), et on applique l'inversion de la permutation initiale pour obtenir de bloc chiffré. Sur la figure qui illustre le schéma général de DES (on a seulement représenté quelques-unes des 16 étapes)

La permutation initiale et son inverse sont décrits par la figure. Les tableaux se lisent de gauche à droite et de haut en bas, le *n-ième* nombre est la position avant permutation du bit qui se trouve en *n-ième* position après permutation.

Après la permutation initiale le message est séparé en deux moitiés de 32 bits, désignées par Lo et Ro, A chaque itération de la procédure, on détermine deux moitiés de 32 bits Li et en fonction de L_{i-1} et R_{i-1} obtenues précédemment. Pour cela, on utilise une clef intermédiaire K_i de 48 bits, calculés à partir de K et on applique les formules suivantes

$$L_i = R_{i-1} \quad \text{et} \quad R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \tag{3.7}$$

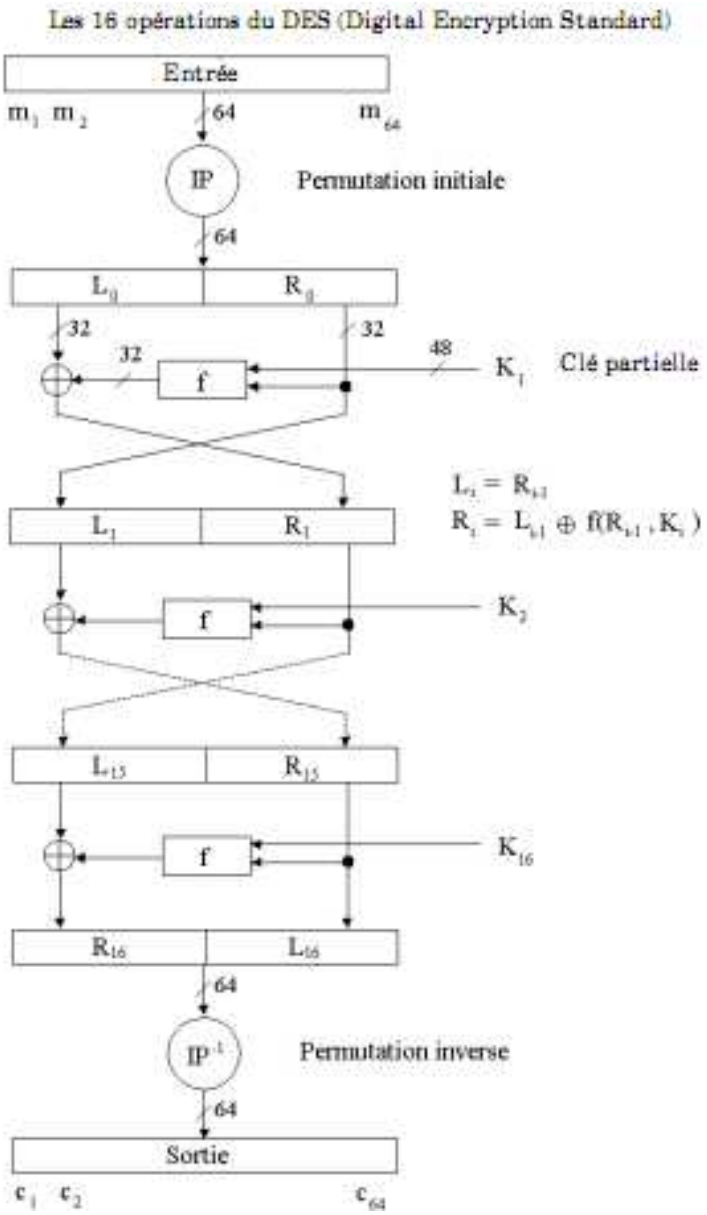


Figure 03. 7 : *Schéma général de DES*

2. Le D.E.S. et son successeur

Permutation initiale

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Permutation initiale inverse

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Figure 03. 8 : *La permutation initiale et son inverse*

La fonction f est schématisée par la figure ci- dessous. Tout d' abord, l'argument de gauche qui possède 32 bits est expansé en 48 bits en redoublant certains bits. Cette expansion est précisée par la figure. Ensuite, on calcule le ou exclusif de cet argument expansé avec le deuxième argument (qui n'est autre que la clef K_i). Le résultat possède 48= 8x6 bits est transformé en une chaine de 32= 8x4 bits en utilisant des dispositifs appelés boites - S qui calculent un bloc de 4 bits à partir d'un bloc de 6 bits. Enfin, on applique la permutation.

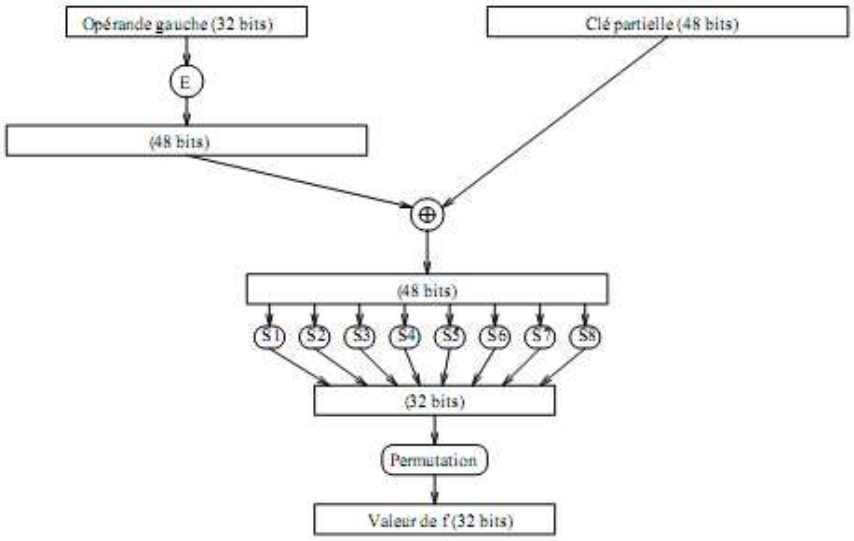


Figure 03. 10 : *Schéma de la fonction f*

Fonction E d'expansion

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Permutation P finale

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Figure 03. 11 : *L'expansion du premier argument et la permutation finale de f*

3.5.1.2 La diversification de la clef

Le principe de la diversification de la clef est schématisé par la figure ci- après. On applique une permutation PC1 à K. Puis, à chacune des 16 étapes, chaque moitié de la chaîne de 56 bits obtenus subit une rotation à gauche, d'un cran aux étapes 1, 2, 9,16 et deux crans aux étapes. A chacune de ces étapes on obtient une clef partielle de 48 bits en appliquant la règle d'extraction PC2. La permutation PC1 et la règle PC2 sont détaillées par la figure suivante les 56 bits de K sont numérotés de 1 à 64 en évitant les multiples de 8, puisque dans la pratique ces positions multiples

de 8 sont utilisées pour insérer des bits de parité (la convention utilisée est fréquemment est celle de la parité impaire).

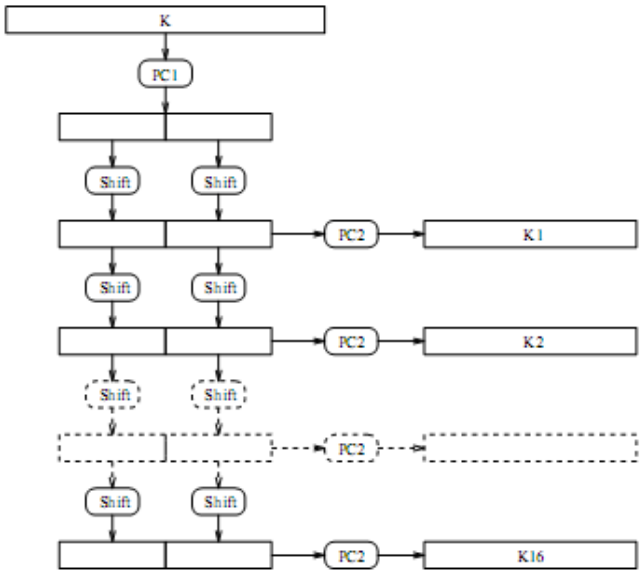


Figure 03. 12 : *La diversification de la clé*

Permutation PC_1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Règle d'extraction PC_2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Figure 03. 13 : *Les permutations pour la diversification*

3.5.1.3 Les boîtes- S

Il y a 8 boîtes – S différentes on les représente par des tableaux à deux lignes et seize colonnes. Les premiers et derniers bits de l'entrée déterminent une ligne du tableau, les autres bits déterminent une colonne. La valeur numérique trouvée à cet endroit indique la valeur des 4 bits sortie.

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Figure 03. 14 : *Les boites-S*

Notons que l'opération de décryptage, la permutation est l'inverse de la permutation finale. Il faudrait donc tenir compte que chaque itération du décryptage traite les mêmes paires de blocs utilisés lors de cryptage

3.5.2 Le cryptosystème 3DES

Puisque la faiblesse de DES est la minime longueur de sa clef, il est naturel de chercher à combiner plusieurs chiffrements DES pour obtenir un système de chiffrement global avec une clef plus longue.

La première qui vient à l'esprit est de composer deux chiffrements DES avec des clefs différentes. Mais on peut alors monter contre ces « double-DES » une attaque à message clairs dite « par le milieu » parce qu'elle s'appuie sur le message intermédiaire apparaissant entre les deux chiffrements DES successifs. Cette attaque consiste à construire la liste des messages intermédiaires possibles en chiffrant par DES un clair avec les 2^{56}clefs possibles. En déchiffrant par DES le chiffre correspondant avec des clés différentes, on obtient une autre liste de messages intermédiaires possibles et le véritable message intermédiaire est dans l'intersection des deux listes. Les coûts en mémoire de cette attaque sont très importants mais son coûts en temps n'est pas significativement plus élevé que l'attaque exhaustive sur DES

Triple-DES consiste à comparer deux chiffrements DES de même clef séparer par un

déchiffrement DES avec une autre clef. Plus précisément

$$3DES^{-1} = DES_{K1} \cdot DES_{K2}^{-1} \cdot DES_{K2} \tag{3.8}$$

Cette façon de faire est préfère à trois chiffrements parce qu'elle généralise DES qui se trouve être le cas particulier où K1=K2. Bien sur le déchiffrement est :

$$3DES_{K1,K2}^{-1} = DES_{K1}^{-1} \cdot DES_{K2} \cdot DES_{K1}^{-1} \tag{3.9}$$

Une clef 3DES est donc composé de deux clefs DES et fait 112 bits ce qui met 3DES largement hors de portée d'une attaque exhaustive. On peut aussi concevoir une variante à trois clefs DES différents mais elle reste vulnérable à une attaque de coût en 2112 s'appuyant sur l'un des deux messages intermédiaires.

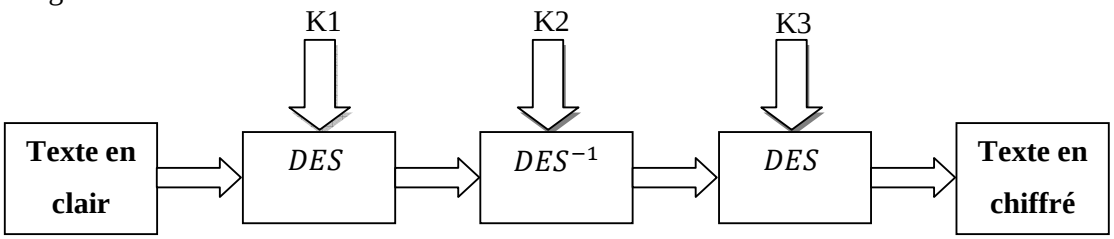


Figure 03.15 : *Chiffrement de texte grâce à 3DES*

3.6 Cryptosystèmes à clefs publiques

Nombreux RSA tire son nom de ses trois inventeurs : R. Rivest, A. Shamir, L Adleman. Le but ici est bien sûr de pouvoir transmettre un message chiffré, que seul le récepteur puis déchiffrer. On appellera Alice l'émetteur du message, et Bob le destinataire.

Bob choisit deux entiers N et E tel que N est le produit de deux grands nombres premiers distincts p et q tel que :

$$0 \leq E \leq \varphi(N) et\ pgcd\big(E, \varphi(N)\big) = 1 \tag{3.10}$$

Avec $\varphi(N) = (p-1)(q-1)$ (3.11)

D' autre part, il calcule l'entier d tel que :

$$0 \leq d \leq \varphi(N) \quad et \quad Ed \equiv 1(mod\varphi(N)) \tag{3.12}$$

Il diffuse les entiers N (le module) et E (l'exposant public) tout en gardant secrets p, q et d (l'exposant secret).

Alice convertit le message qu'elle veut transmettre en élément de ℤN. Pour chiffrer l'élément m ϵ ZN, elle calcule la formule donnée par l'équation ci-dessous qu'elle transmet

$$c = m^E \ mod\ N \tag{3.13}$$

Bob reçoit et déchiffrer en calculant $c^d \ mod\ N$. En effet, puisque $\varphi(N)$ est l'ordre du groupe

(Z/NZ) nous avons,

$c^d \equiv m^{Ed} \equiv m(modN)$ (3.14)

L'application E ⟶ d est un exemple typique de fonction trappe. Bob peut calculer l'inverse d de E modulo $\varphi(N)$ puisqu' il connaît la factorisation de N mais en attaquant éventuel, ne peut connaître que N et E, ne pourra pas calculer d comme le montrent les résultats suivants.

Lemme 1 : la connaissance de $\varphi(N)$ est équivalente à la connaissance de la factorisation de N. En effet, si la factorisation N= pq est comme, alors $\varphi(N) = (p-1)(q-1)$ est facile à calculer. Réciproquement, supposons que $\varphi(N)$ soit connu. Alors, en substituant N/p à q dans la relation $\varphi(N) = (p-1)(q-1)$, nous obtenons l'équation du second degré suivant :

$p^2 - (N + 1 - \varphi(N)p + N) = 0$ qu 'il est aisé de résoudre. (3.15)

Lemme 2 : si un attaquant réussit à calculer d connaissant N et E. alors il peut factoriser N. En effet, décomposons Ed − 1 sous la forme 2^K r impaire. Puisque$\varphi(N)|Ed-1)$ on a $m^{Ed-1} \equiv 1(modN)$ pour tout m tel que $pgcd(m,N) = 1$

Pour un tel m, on a donc trois possibilités :

- $m^r \equiv 1(modN)$ (possibilité 1)
- Il existe l tel que $0 \leq L \leq k\ et\ m^{2r} \equiv -1(modN)$ (possibilité 2) (3.16)
- Il existe l tel que $0 \leq L \leq k\ et\ m^{2r} \neq -1\ et\ m^{(2+l)r} \equiv 1$ (possibilité 3) (3.17)

Ainsi, on peut montrer que les deux premiers cas se produisent au plus pour la moitié des valeurs possibles de m. Lorsque le dernier cas se produit, x= m^{2r} est une racine carrée de I modulo N distinctes $\pm l$.

Pour factoriser N, l'attaquant peut donc procéder ainsi. Il choisit un m au hasard dans ZN. Si pgcd(m, n) $> l$ alors la factorisation est achevée. Sinon, il calcule $x_O =$ m^r $mod\ N$ puis la suite $x_{i+1} = x_i^2$ mod N tant que $x_i \neq \pm\ l$. S'il ne trouve pas d'entier l vérifiant les conditions de la possibilité (3) alors il recommence en choisissant une valeur de m. Mais d'après le paragraphe précédant, cet échec ne se produit qu'au plus une fois sur deux. Sinon, il dispose d'une racine carrée x de l modulo N, distincte de ± l. Les entiers (x-1) et (x+1) sont donc des diviseurs de zéro modulo N et il obtient un facteur non trivial de N en calculant par exemple *pgcd (x-1, N).*

Au niveau des performances, le DES est plus rapide que des systèmes de chiffrement de type RSA à clés publiques et privées. Les valeurs estimées sont : 100 fois plus rapide que RSA dans le

cadre d'un chiffrement logiciel et environ 1000 fois plus rapide que RSA dans le cadre d'une réalisation matérielle.

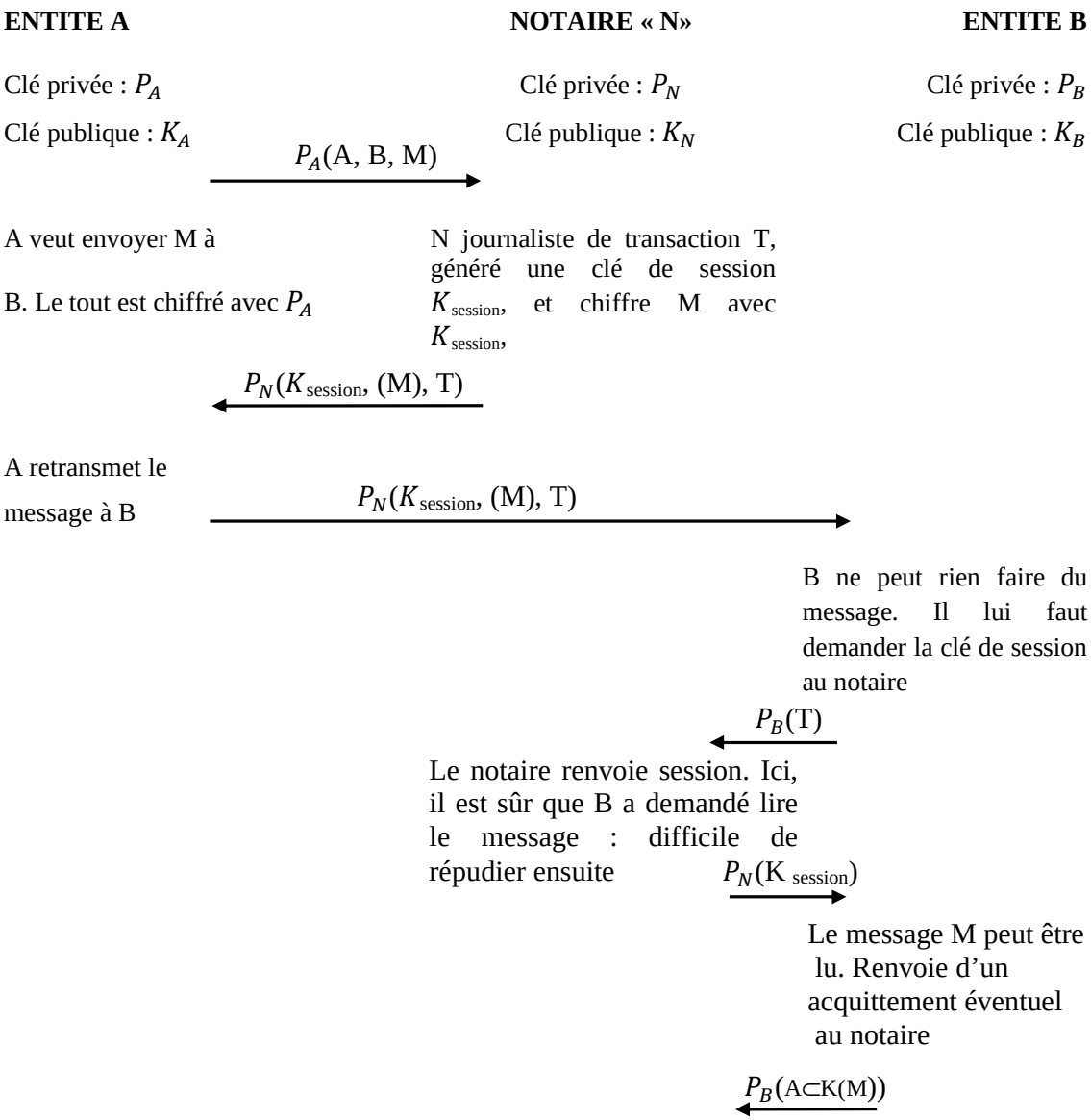
Le DES est probablement peu sûr pour un « *attaquant* » ayant de gros moyens. La version Triple DES assure malgré tout au niveau de la sécurité des performances acceptables.

3.6.1 Notarisation

Le rôle de la notarisation consiste à éviter un déni de responsabilité au cours d'un échange entre deux entités. Cet aspect peut être essentiel dans certains domaines tels que le milieu bancaire.

Pour éviter tout déni, il existe deux types de réponses :

La responsabilité du secret des clés : entièrement basé sur la bonne foi des intervenants. Dans ce cas, les conflits ne peuvent se régler en général que devant la justice, Le premier cas ne concerne pas réellement le cadre de notre propos. Le fonctionnement du deuxième cas, quant à lui, peut être illustré comme suit :



Le passage par un tiers, le notaire, permet de consigner les échanges. Cette notarisation est plutôt fiable, sous réserve d'avoir pleine confiance en le notaire qui traite tous les échanges.

3.7 Force de l'application

Malgré une apparente simplicité, le système RSA reste l'un des plus sûrs. Jusqu' à très récréments, la plupart des gens s'accordaient à l'idée que déchiffrer un message sans connaître les clefs était équivalente à factoriser l'entier n. D' autre part il est très difficile dans la pratique de factorisation n : même s'il existe beaucoup de méthodes plus efficaces que le procédé naturel de temps de calcul nécessaire reste incomparablement plus long. Enfin, nous signalons à transmettre

une clef servant à déchiffrer un message codé selon une autre méthode plus rapide, typiquement une méthode de chiffrement dit symétrique.

3.7.1 Sécurité et performances du RSA

Utiliser des longueurs de clés de plus en plus importantes valeurs envisagées 512 bits, 640 bits 1024 bits après quelques plusieurs années en 2048 bits Utiliser des circuits intégrés de cryptage de plus en plus

Performants Actuellement une dizaine de circuits disponibles. Vitesse de cryptage de base pour 512 bits: de 10 à 30 Kb/s Évolution en cours de l'ordre de 64 Kb/s A venir de l'ordre de 1 Mb/s Remarque: Compte tenu de la complexité des traitements le DES doit être environ toujours 100 fois plus rapide que le RSA.

3.7.2 Problèmes du RSA

L'un des problèmes des le RSA est de trouver de grands nombres. Choisir des clés secrètes et publiques assez longues. La réalisation des opérations modulo n est rapide.

3.7.3 Conclusion RSA

Problème principal Complexité algorithmique de la méthode. Solution assez générale. Utiliser le RSA brièvement au début d'un échange pour échanger des clés secrètes de session d'un algorithme efficace à clés privées.

Efficacité en sécurité La méthode est officiellement sûre si l'on respecte certaines contraintes de longueur de clés et d'usage. Personne depuis 2500 ans n'a trouvé de solution rapide au problème de la factorisation…

3.7.4 Les limites du RSA

Dans la pratique, le RSA est un code sûr, si l'on respecte les quelques règles suivantes :

Le RSA possède également quelques inconvénients d'ordre mathématique :

On ne peut pas choisir un *n* inférieur à la valeur maximale à coder. Ainsi, si on code caractère par caractère alors notre cryptage ne sera pas bijectif. Cela s'explique car nous effectuons le modulo n lors du cryptage et du décryptage. Si n est trop petit, plusieurs caractères pourront être cryptés par le même nombre, et ne pourront donc plus être différenciés lors du décryptage.

Les calculs sont souvent très lourds, du fait de la taille des entiers à manipuler. Le cryptage d'un

message long, avec des clés de grande taille, peut prendre plusieurs heures sur un ordinateur puissant.

3.8 La signature numérique d'un message

En combinant un système de cryptographie et une fonction de hachage, on peut à la fois garantir l'intégrité du message et son authentification. Selon que l'on utilise un système de cryptographie à clé secrète ou publique, on obtient une signature numérique dite symétrique ou asymétrique. Dans le système à signature symétrique, l'émetteur calcule le digest sur la concaténation de la clé secrète et du message Le destinataire procède de même, si le digest trouvé est identique à celui qui a été reçu, c'est d'une part que le message n'a pas été altéré et d'autre part qu'il a bien été émis par l'autre possesseur de la clé partagée.

Figure 03. 16 : *Le calcule d'une signature numérique symétrique*

3.8.1 Le possesseur de la clé publique

Dans le système à signature asymétrique, le digest est calculé sur le message puis chiffré à l'aide de la clé privée de l'émetteur, le résultat est joint au message envoyé. Le destinataire calcule le digest sur le message, déchiffre le digest reçu à l'aide de la clé publique de l'émetteur. Si les résultats sont identiques, le message n'a pas été altéré et l'émetteur est identité, c'est le possesseur de la clé publique.

Figure 03. 17 : *Le calcul d'une signature numérique asymétrique*

Les systèmes à signature numérique permettent d'assurer l'authentification (qui est l'émetteur du message) et l'intégrité de celui-ci (le message n'a pas été modifié par un tiers). N'ayant besoin

d'aucun secret partagé, l'authentification par signature numérique asymétrique est plus efficace. Cependant, elle nécessite une puissance de calcul supérieure et ralentit les échanges de messages.

3.8.2 La sécurisation des échanges

3.8.2.1 L'usurpation d'identité

L'un des problèmes de la cryptographie à clé publique est la possible intervention d'une tierce personne. Lorsqu'Alice veut entrer en relation avec Bob en utilisant un système de cryptographie à clé publique, elle doit demander à Bob sa clé publique. Cet échange peut être intercepté par Charlie, un intrus malveillant peut répondre en lieu et place de Bob avec sa propre clé publique. De cette manière, Charlie pourra se substituer à Bob lors des prochains échanges, Alice étant persuadée que les messages lui proviennent bien de Bob. La même opération est réalisée lorsqu'Alice envoie sa clé publique à Bob. Cette attaque est connue sous le nom de *« Man in the middle »*.

Figure 03. 18 : *La substitution d identité*

Afin d'éliminer la substitution d'identité, les clés publiques sont disponibles sur un serveur de clés publiques (annuaire) et donc accessibles à tous les utilisateurs, encore faut-il que soit confirmée la relation clé publique/possesseur.

C'est l'intervention d'un tiers de confiance CA, qui garantit la correspondance entre une clé publique et son propriétaire par la délivrance d'un certificat. Le certificat contient l'identifiant d'un utilisateur et sa clé publique, le certificat est signé avec la clé privée de l'autorité d'authentification.

3.8.2.2 Infrastructure de sécurité, la PKI

La PKI où l'infrastructure de clé publique est un ensemble de protocoles et de services associés qui assurent la gestion des clés publiques. Les différentes fonctions à assurer sont :

- La génération des clés : le système génère et gère deux types de clés, les clés de

chiffrement et les clés de signature numérique des messages. La paire de clés publique/privée peut être générée par le CA ou le client. Lorsqu'un client génère lui-même ses clés, il séquestre celle-ci chez le CA en vue d'obtenir la délivrance d'un certificat.

- L'archivage des clés et des certificats (séquestre) : l'agent de séquestre doit assurer le contrôle des accès aux clés privées.
- La délivrance des certificats et clés : celle-ci s'accompagne de la vérification de l'identité du demandeur.
- La gestion des listes de révocation CRL c'est-à-dire la liste des clés déclarées est invalidée avant leur date d'expiration.

La figure ci-après illustre dans un cas simple, celui où le client génère lui-même son couple de clés, le fonctionnement d'une infrastructure PKI. Bob formule une demande de certificat auprès d'une autorité de certification. Celui-ci, après vésication de l'identité de Bob, lui délivre un certificat et le signe avec sa clé privée. Bob envoie son certificat à Alice et le signe avec sa clé privée. Alice apprend ainsi la clé publique de Bob (validée par la signature numérique du CA et vérifie auprès du CA la validité du certificat (consultation de la liste des révocations).

Elle vérifie ensuite que Bob est bien l'émetteur du message par lecture de la signature de Bob (utilisation de la clé publique de Bob).

Figure 03. 19 : *Principe des échanges sous PKI*

La délivrance de certificats numériques est normalisée par l'UIT. Un certificat X.509 identifie la norme, v3 actuellement, il comporte entre autres les informations suivantes :

- un numéro de série unique,
- un identifiant de l'algorithme de signature utilisé,
- le nom de l'émetteur,
- la période de validité,
- la clé publique du sujet,
- l'identifiant de l'émetteur (CA),
- l'identifiant unique du sujet,

- un champ d'extension pouvant comporter du texte, une image...
- la signature de l'émetteur (CA),

Un second champ d'extension a été ajouté par la version 3, il permet notamment d'indiquer le nom et le prénom du titulaire, ses coordonnées...

3.9 RSA et la carte bancaire [11][12][13]

Jusqu'à présent le processus qui fait la sécurité d'une carte bancaire est la technique de la cryptographie RSA à cause de la performance et la fiabilité de la sécurisation.

3.9.1 Carte Bancaire

La procédure d'authentification d'une carte bancaire est différente suivant qu'on utilise un terminal relié au réseau bancaire ou pas. Si le terminal est relié au réseau carte bancaire il utilise un DES (et maintenant un triple-DES avec une clé secrète de 56 bits. Chaque transaction donne lieu à la délivrance d'un Certificat DES (rôle de juge de paix) inscrit sur le ticket, sur la carte bancaire et dans le journal du terminal. Ces trois traces permettent de résoudre les litiges. Si le terminal n'est pas relié, il effectue deux opérations successives :

1) L'identification du porteur, par le code confidentiel.

2) L'authentification de la carte, en utilisant deux niveaux de RSA 320 bits. De plus le dialogue entre le terminal et la CB utilise un masque réservé à des sources agréées fourni par un DES de 56 bits. Décrivons maintenant la procédure d'authentification. Le but est de distinguer si la carte est bien homologuée, ou bien s'il s'agit d'une contre façon. Pour cela, deux valeurs sont inscrites dans toute carte bancaire :

a) Une valeur d'authentification I, qui donne lieu au calcul d'une empreinte J (par exemple, J peut être obtenu par concaténation de I, c'est-à-dire que J=(I|I) représente le mot I répété deux fois).

b) Un mot K représentant le message J chiffré à l'aide d'une clé RSA privée.

Lors du paiement, le terminal lit l'empreinte J et le mot K, puis applique son propre algorithme RSA pour déchiffrer K. Si la valeur J et la valeur calculée à partir de K sont identiques, il estime que la carte est authentique.

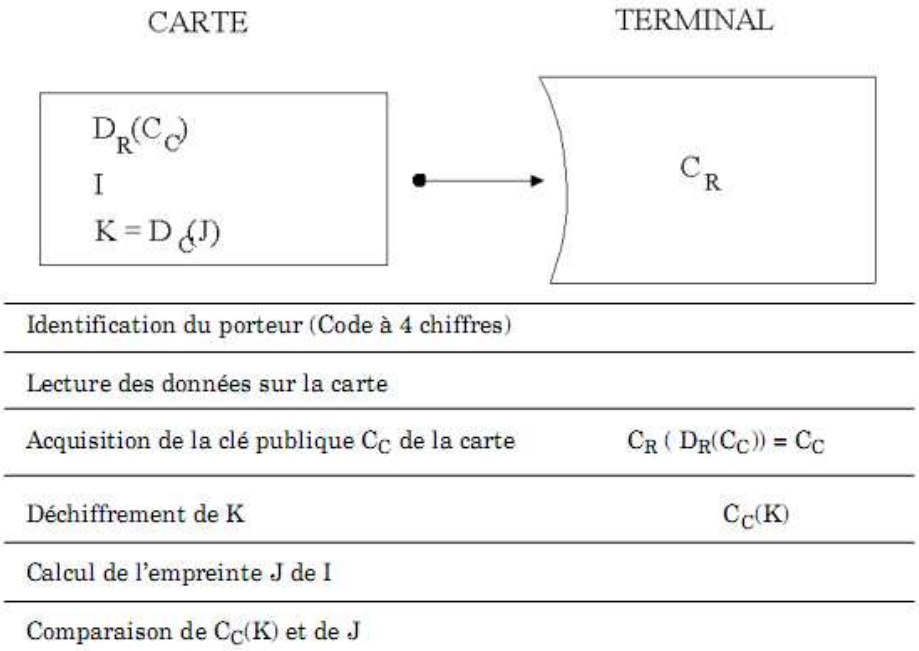


Figure 03. 20 : *Les échanges entre la carte bancaire et le terminal*

En fait, le terminal ne doit pas nécessairement détenir la clé publique correspondant à la clé secrète de la carte. Il peut seulement conserver une clé publique de référence, délivrée par une *« autorité de certification »*, et c'est la carte elle-même qui lui communiquera sa clé publique signée par la clé secrète de référence. Ce schéma à deux niveaux de RSA permet d'individualiser les clés par banque, par carte, etc., autorisant du même coup beaucoup plus de souplesse dans la gestion des cartes. Il limite aussi la quantité d'information détenue dans le terminal.

Pour bien comprendre ce processus, notons C_C la clé publique de la Carte, D_C la clé secrète de la Carte, C_R la clé publique de Référence, D_R la clé secrète de Référence. La CB contient les indications suivantes : sa clé publique de chiffrement $D_R(C_C)$ signée par l'autorité de certification, une valeur d'authentification I, et la valeur $K = D_C(J)$ correspondant au chiffrement de J par la clé secrète de la carte. Le terminal conserve seulement la clé C_R. La procédure d'authentification est alors celle qui est représentée sur la figure précédente.

- Identification du porteur : saisie du code à 4 chiffres.
- Lecture des données sur la carte.
- Acquisition de la clé publique C_C de la carte par le terminal : celui-ci calcule $C_R (D_R(C_C)) = C_C$.
- Déchiffrement de K : le terminal calcule $C_C(K)$.
- Calcul de l'empreinte J de I.
- Comparaison de $C_C(K)$ et de J.

3.10 Conclusion

La performance de l’outil mathématique s’oriente vers les différentes technologies comme l’informatique, pour faire les programmes de fonctionnement des matérielles ou sécurisent des informations. Mais ils sont incomplètes à cause de la limite du sa travail, le mathématique devenu incomplète s’il reste à lui-même. L’art de la cryptologie confondue avec la nouvelle technologie se termine vers la durabilité et des fiabilités des outils existent tel que la carte bancaire, grâce à forte calcul que le crypto logue s’invente et on inscrit les algorithmes très redoutables a fin de graver dans la télécarte bancaire.

CHAPITRE 4 : ETUDE DE LA CARTE BANCAIRE AVEC DES AMELIORATION SUR LES PARTIES SECURISEES

Puisque notre objectif est de capable d'analyser tous les fonctionnements d'une carte bancaire, sur sa structure, surtout la sécurisation, pour cette raison qu'on étudie brièvement la carte bancaire. On utilise de lecteur carte pour lire des informations contenues dans la carte alors elle subisse des différentes actions dans des différentes zones surtout dans la mémoire alors on distingue deux niveaux

1 ère niveau de sécurisation :

On peut définir un mot de passe pour la lecture et un mot de passe pour l'écriture

2ème niveau de sécurisation :

Authentification de la carte par rapport au lecteur et l'identification du lecteur par rapport à la carte ; c'est l'authentification mutuelle utilisée dans la carte à puce

4.1 Principe de l'authentification mutuelle

Lorsque la carte est insérée dans le lecteur, le lecteur envoie une commande d'authentification. La carte envoie au lecteur un numéro unique contenu dans un des registres. Le lecteur traite ce nombre avec un algorithme cryptographique et retourne le résultat obtenu à la carte. En même temps, la carte fait le même calcul

- La carte compare son résultat avec celui du lecteur, s'il y a égalité (le lecteur identifié la carte)
- La carte utilise ce résultat pour calculer une nouvelle valeur à l'aide d'un algo-cryptographique
- La carte envoie le nouveau résultat
- Le lecteur procède de la même manière, si égalité ;
  il a identifié la carte principe de l'authentification mutuelle

4.2 Les signatures

Une signature est un nombre publiquement vérifiable que seule une personne précise soit capable de produire. Un système de signature doit mettre en œuvre deux clés (par signataire) une clé secrète et une clé publique; la clé publique est connue de tout le monde, tandis que la clé secrète reste confidentielle au signataire. La condition pour choisir ces deux clés s'appelle justesse de la signature ;

L’information à signer est transformée en un message à l'aide de la clé secrète : c’est la phase de signature, elle est effectuée, une seule fois, par la personne autorisée. L’information et la signature sont dévoilées. La signature est transformée à l'aide de la clé publique; on compare le résultat à l'information qui accompagne la signature. C'est la phase de vérification, effectuable par n'importe qui puisqu'elle utilise la clé publique. La propriété de justesse veut que l'on retombe sur l'information. Les deux clés ne peuvent donc pas être choisies indépendamment.

4.3 La sécurisation de la CB à bande magnétique

4.3.1 La bande magnétique

Ce principe est la base de tout enregistrement magnétique et la lecture les magnétiques se produisent toujours par paire dans les matériaux aimantés, et les lignes de flux magnétique émergent dans le Nord et se terminer au Sud. Les parties élémentaires des pistes magnétiques sont particules ferromagnétiques environ 20 millions de pouce de long, chacune des actes qui comme un aimant petit bar. Les particules élémentaires magnétiques sont alignés avec leurs axes nord-sud parallèle à la bande magnétique au moyen d'un externe champs magnétiques tout en le liant durcir.

4.3.2 La force coercitive

Si une particule magnétique est placée dans un fort champ magnétique externe de la polarité opposé, il sera flip sa propre polarité (Nord devient Sud, Sud devient du Nord). La force champ magnétique externe nécessaire pour produire ce le clapet est appelé la force coercitive, ou coercivité de la particule.

Il y à une inversion de flux pendant, qu’une interface SS est crée quelque part sur la piste, les flux seront repoussés, et on obtient une concentration de lignes de flux autour de l'interface SS même avec la N-N de l'interface. Encodage consiste à créer des SS et des interfaces NN, et lecture se compose de la détection électromagnétique. Les interfaces S-S et N-N sont appelées inversions de flux.

4.3.3 Effacements

Pour effacer une piste magnétique, la tête d'encodage est maintenue à une polarité constante et la bande ne soit déplacée passer ; il n’y à pas inversions de flux, pas de données.

Inversion de flux unique est crée il s'engager à la mémoire. Une piste magnétique encodée est donc juste une série d'inversions de flux NN SS suivie par NN.

4.3.4 Lecture de pointe

Le plus fort des champs magnétiques sur une bande magnétique est au niveau des points d'inversions de flux. Ce sont détecté comme les pics de tension par le lecteur, avec + / - tensions correspondant aux NN / SS inversions de flux

La lecture de pointe carrée de forme d'onde est critique. Notez que le pic de tension reste le même jusqu' à une inversion du flux de nouvelles est rencontré.

4.4 Présentation des chiffres et lettres en binaire

Ils sont évidemment une infinité de nombres de normes possibles, mais heureusement les American National Standards Institute et les Normes internationales Organisation ont choisi deux normes pour différencier les différents caractères existants.

4.4.1 Normes

C'est un format de 5 bits décimal codé binaire. Il utilise un ensemble de 16 caractères, ce qui utilise 4 des 5 bits disponibles. Le bit de 5 est un bit de parité, cela signifie on doit avoir un nombre impair de 1 dans le caractère de 5 bits. Le bit de parité total doit être impair. En outre, les bits les moins significatifs sont lus en premier sur la bande.

La norme ANSI BCD montre les détails de la norme ANSI / ISO BCD.

ANSI / ISO BCD Format des données

- Rappelez-vous que b1 (bit n° 1) est le LSB (bit le moins significatif)
- Le LSB est lu en premier
- Conversions hexadécimales des bits de données sont indiqués entre parenthèses (XH).

- Bits de données - Parité

B1 B2 B3 B4 B5 - Fonction caractères

0 0 0 0 1 0 (0H) Données

1 0 0 0 0 1 (1H) "

0 1 0 0 0 2 (2H) "

1 1 0 0 1 3 (3H) "

0 0 1 0 0 4 (4H) "

1 0 1 0 1 5 (5H) "

0 1 1 0 1 6 (6H) "

1 1 1 0 0 7 (7H) "

0 0 0 1 0 8 (8H) "

1 0 0 1 1 9 (9H) "

0 1 0 1 1 : (AH) "

1 1 0 1 0 ; Sentinel Start (BH)

0 0 1 1 1 <(CH)

1 0 1 1 0 = (DH) Field Separator

0 1 1 1 0 > (EH)

1 1 1 1 1 ? (FH) Sentinel Fin

***** 16 caractères de 5 bits *****

10 caractères numériques et de données

3 Encadrement / Champ de caractères

3 caractères

4.4.2 Le principe

La piste magnétique commence par une chaine de zéro bit cellules pour permettre l'auto-horloge caractéristique de Biphase "*sync*" et commence le décodage. Un "*Sentinel Start*" caractère dit alors le processus de reformatage, pour commencer le regroupement des décodé bitstream en groupes de 5 bits chacun. A la fin des données, une fin " Sentinel " est rencontrée, qui est suivie par une redondance longitudinale Cochez (LRC) de caractère.

Le LRC est un contrat de la parité pour les sommes de toutes les B1, B2, B3 et B4 bits de données de tous les caractères précédents.

Le SENTINEL START, END SENTINEL, et LRC sont collectivement appelés encadrement personnages, et jetés à la fin du processus de reformatage.

** ANSI / ISO ALPHA Format des données **

Les données alphanumériques peuvent également être codées sur pistes magnétiques. La seconde norme ANSI / ISO de données format est ALPHA (alphanumérique) et implique un caractère 7- bit avec 64 caractères. Comme auparavant, un bit de parité impaire est ajouté à la 6 bits de données nécessaires pour chacun des 64 caractères.

ANSI / ISO ALPHA Format des données

- Rappelez-vous que b1 (bit n° 1) est le LSB (bit le moins significatif)!
- Le LSB est lu en premier.
- Conversions hexadécimales des bits de données sont indiqués entre parenthèses (XH).

Bits de données Parité

B1 B2 B3 B4 B5 B6 B7 Fonction caractères

0 0 0 0 0 0 1 espace (0H) spéciaux

1 0 0 0 0 0 0 !(1H) "

0 1 0 0 0 0 0 "(2H)"

1 1 0 0 0 0 1 # (3H) "

0 0 1 0 0 0 0 $ (4H) "

1 0 1 0 0 0 1% (5H) Démarrer Sentinel

0 1 1 0 0 0 1 & (6H) spéciaux

1 1 1 0 0 0 0 »(7H)"

0 0 0 1 0 0 0 ((8H) "

1 0 0 1 0 0 1) (9H) "

0 1 0 1 0 0 1 * (AH) "

1 1 0 1 0 0 0 + (BH) "

0 0 1 1 0 0 1, (CH) "

1 0 1 1 0 0 0 - (DH) "

0 1 1 1 0 0 0. (EH) "

1 1 1 1 0 0 1 / (FH) "

0 0 0 0 1 0 0 0 (10H) de données (numériques)

1 0 0 0 1 0 1 1 (11H) "

0 1 0 0 1 0 1 2 (12H) "

1 1 0 0 1 0 0 3 (13H) "

0 0 1 0 1 0 1 4 (14H) "

1 0 1 0 1 0 0 5 (15H) "

0 1 1 0 1 0 0 6 (16H) "

1 1 1 0 1 0 1 7 (17H) "

0 0 0 1 1 0 1 8 (18H) "

1 0 0 1 1 0 0 9 (19H) "

0 1 0 1 1 0 0: (1AH) spéciaux

1 1 0 1 1 0 1; (1BH) "

0 0 1 1 1 0 0 <(1CH) "

1 0 1 1 1 0 1 = (1DH) "

0 1 1 1 1 0 1> (1EH) "

1 1 1 1 1 0 0? (1FH) Sentinel Fin

0 0 0 0 0 1 0 @ (20H) spéciaux

1 0 0 0 0 1 1 A Données (21H)

0 1 0 0 0 1 1 B (22H) "

1 1 0 0 0 1 0 C (23H) "

0 0 1 0 0 1 1 D (24H) "

1 0 1 0 0 1 0 E (25H) "

0 1 1 0 0 1 0 F (26H) "

1 1 1 0 0 1 1 G (27H) "

0 0 0 1 0 1 1 H (28H) "

1 0 0 1 0 1 0 I (29H) "

0 1 0 1 0 1 0 J (2AH) "

1 1 0 1 0 1 1 K (2BH) "

0 0 1 1 0 1 0 L (2CH) "

1 0 1 1 0 1 1 M (2DH) "

0 1 1 1 0 1 1 N (2EH) "

1 1 1 1 0 1 0 O (2FH) "

0 0 0 0 1 1 1 P (30H) "

1 0 0 0 1 1 0 Q (31H) "

0 1 0 0 1 1 0 R (32H) "

1 1 0 0 1 1 1 S (33H) "

0 0 1 0 1 1 0 T (34H) "

1 0 1 0 1 1 1 U (35H) "

0 1 1 0 1 1 1 V (36H) "

1 1 1 0 1 1 0 W (37H) "

0 0 0 1 1 1 0 X (38H) "

1 0 0 1 1 1 1 Y (39H) "

0 1 0 1 1 1 1 Z (3AH) "

1 1 0 1 1 1 0 [(3BH) spéciaux

0 0 1 1 1 1 1 \ (3DH) spéciaux

1 0 1 1 1 1 0] (3EH) spéciaux

0 1 1 1 1 1 0 ^ (3FH)

1 1 1 1 1 1 1 _ (40H) spéciaux

***** 64 caractères 7-bit Set *****

* 43 caractères alphanumériques de données

* 3 Encadrement / Champ de caractères

* 18 Contre le / Caractères spéciaux

L'ANSI deux / ISO formats, ALPHA et BCD, permettent une grande variété de données stockées sur pistes magnétiques. La plupart des cartes avec pistes magnétiques utilise ces formats.

4.4.3 Stockage des données

Maintenant nous savons comment les données sont stockées. Normes ANSI / ISO le définisse, dont chacune est utilisée pour des fins différentes. Ces pistes ne sont définies que par leur emplacement sur la bande magnétique, puisque la bande magnétique comme un tout est magnétiquement homogène.

En ce qui concerne la sécurité, il n'y a aucun moyen sûr pour protéger physiquement les données enregistrées sur un support magnétique. En effet, la lecture et l'écriture sont entièrement libres contrairement aux cartes à puce qui possèdent des zones. Il est donc indispensable de sécuriser l'application en utilisant ce support. Concrètement, il faut crypter les données sensibles enregistrées sur le support et coupler l'utilisation de la carte avec un code secret. En outre, pour une sécurité accrue un contrôle de l'authenticité de la carte en temps réel.

4.5 Etude de la carte [5]

Durant cette étude de la piste magnétique on trouve que toutes les données sont transformées en binaire, chaque caractère correspond à un code qui le concerne et dans le carte à puce les données étant stockées dans les mémoires alors notre but c'est de faire connaitre l'événement qui circule dans l'intérieur de la carte bancaire.

4.5.1 Schéma de structure da fonctionnement

Figure 04.01 : *Les matérielles qui fonctionnent la lecture d'une carte*

Dans notre cas on interprète les différents résultats puis que il y à pas des matérielles pour faire des analyses, alors on voit les différents outils pour faire la préparation de la lecture de la carte bancaire, Après avoir fonctionné l'ordinateur, le cybermouse se connecte avec le port USB. Dans

le logiciel CardEasy il détecte automatiquement le port COM 1 ou COM2 ; puis on introduit la carte à puce dans le lecteur cybermouse

Figure 04.02 : *Cybermouse*

4.5.2 Card RESET OK

Le logiciel est capable de détecter automatiquement le contenu dans la carte ; on trouve cette partie ; si on a déjà insérer la carte dans la cybermouse on a les indications suivantes montrées par la figure ci- près

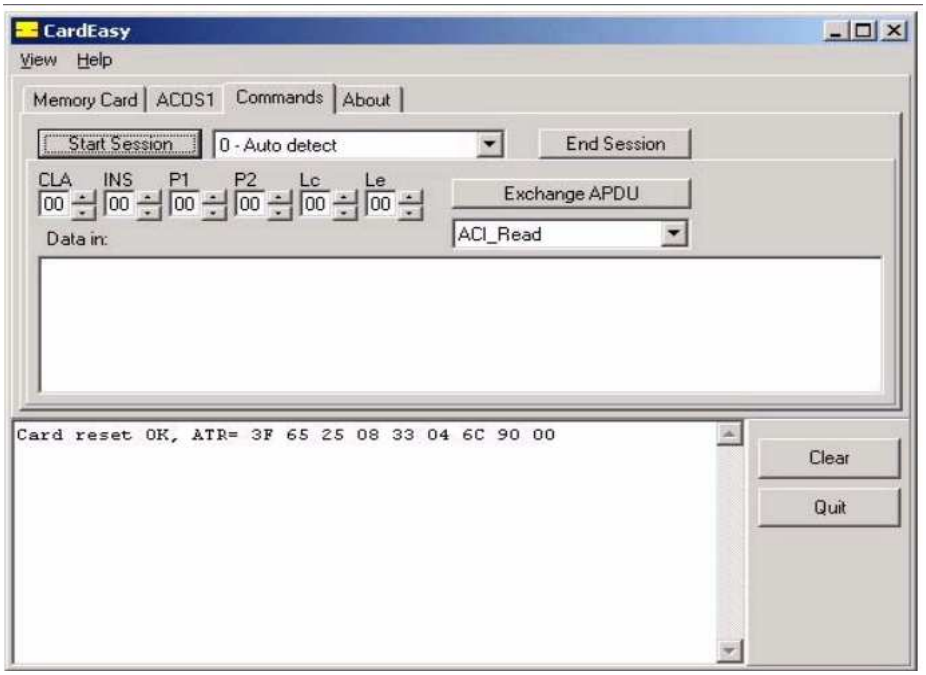


Figure 04.03 : *fenêtre d'affichage de l'ATR*

La réponse à un reset (ATR, ou Answer To Reset) qui correspond aux données envoyées par la carte immédiatement après la mise sous tension,

4.5.3 ATR (Answer To Reset):

Dès que la carte est mise sous tension, elle envoie un message de réponse d'initialisation appelé ATR, il peut atteindre une taille maximale de 33 octets. Il indique à l'application cliente les paramètres nécessaires pour établir une communication avec elle.

ATR : 3F 65 25 08 33 04 6C 90 00 = le commande de l'ISO de déroule correctement

4.5.3.1 Première lecture de zone libre de la puce

Maintenant on va lire une zone libre de la carte bancaire, prend 32 octets à partir de l'adresse 09 E0

• CLA (1 octet): Classe d'instructions qui indique la structure et le format pour une catégorie de commandes et de réponses APDU

• INS (1 octet): code d'instruction: spécifie l'instruction de la commande

• P1 (1 octet) et P2 (1 octet): paramètres de l'instruction

• Lc (1 octet): nombre d'octets présents dans Fle champ donné de la commande

• Avec Le=0, - Si cde d'écriture => pas de données utiles

- Si cde de lecture => la cde doit retourner 256 octets de données utiles

• Data field (octets dont le nombre est égal à la valeur de Lc): une séquence d'octets dans le champ de données de la commande

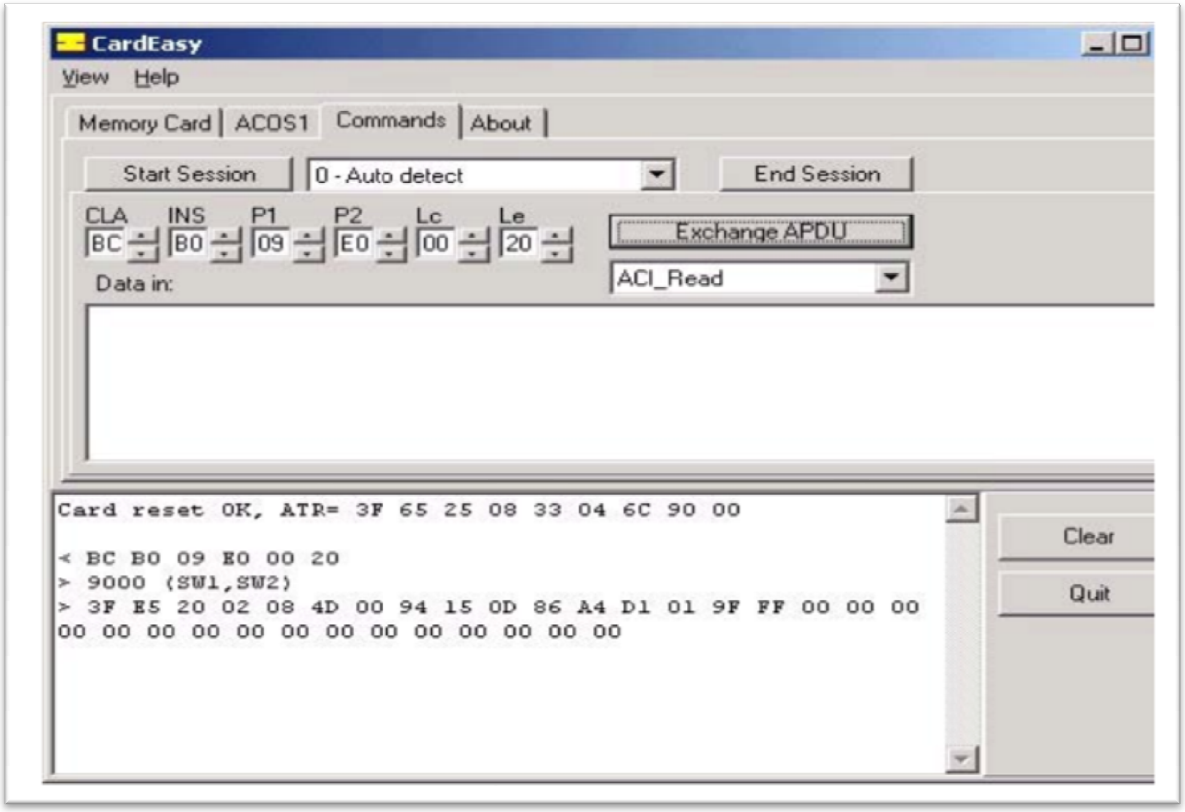


Figure 04.04 : *fenêtre d'affichage la réponse de la carte*

Lecture de la carte à 09E0 : la carte répond "3F E5 20 08 4D 00 94 15 0D 86 A4 D1 01 9F FF"

La fenêtre de la basse affiche :

< BC BO O9 EO OO 20 ce qui correspond à la commande envoyée à la carte (selon la convention de la cardEasy)

> 9000(SW1SW2) c'est le statut de la réponse de la carte

3F E5 correspond bien au type de la carte bancaire stocké en 09 E0 .on peut réussir à lire une carte

Il n'y a donc que 16 octets entre les adresses 09 E0 et 09 FF, or nous avons demande de lire 32 octets. Comme la zone d'adresse de la carte bancaire commence en 0200, il n'y donc qu'un kilo-octets de stockage sur la carte.

4.5.3.2 Lecture de la zone identifiant da la puce

Nous allons continuer l'exploration de carte en regardant la zone identifiant de prestataire 02 supposée stockée à partir de 09 48 sur notre carte et commençant par l'en tête 2E 02

Cela correspond aux valeurs suivantes à saisir dans la fenêtre de commande ISO envoyée à la

carte (voir l'image suivante)

Classe (CLA) : BC

Instruction (INS) : BO

Paramètre P1 : 09

Paramètre P2 : 48

Nombre d'octets lu (Le) : 40 (40h en hexadécimal est égal à 64 décimal)

On appui sur le bouton "Exchange APDU" on obtient le résultat suivant

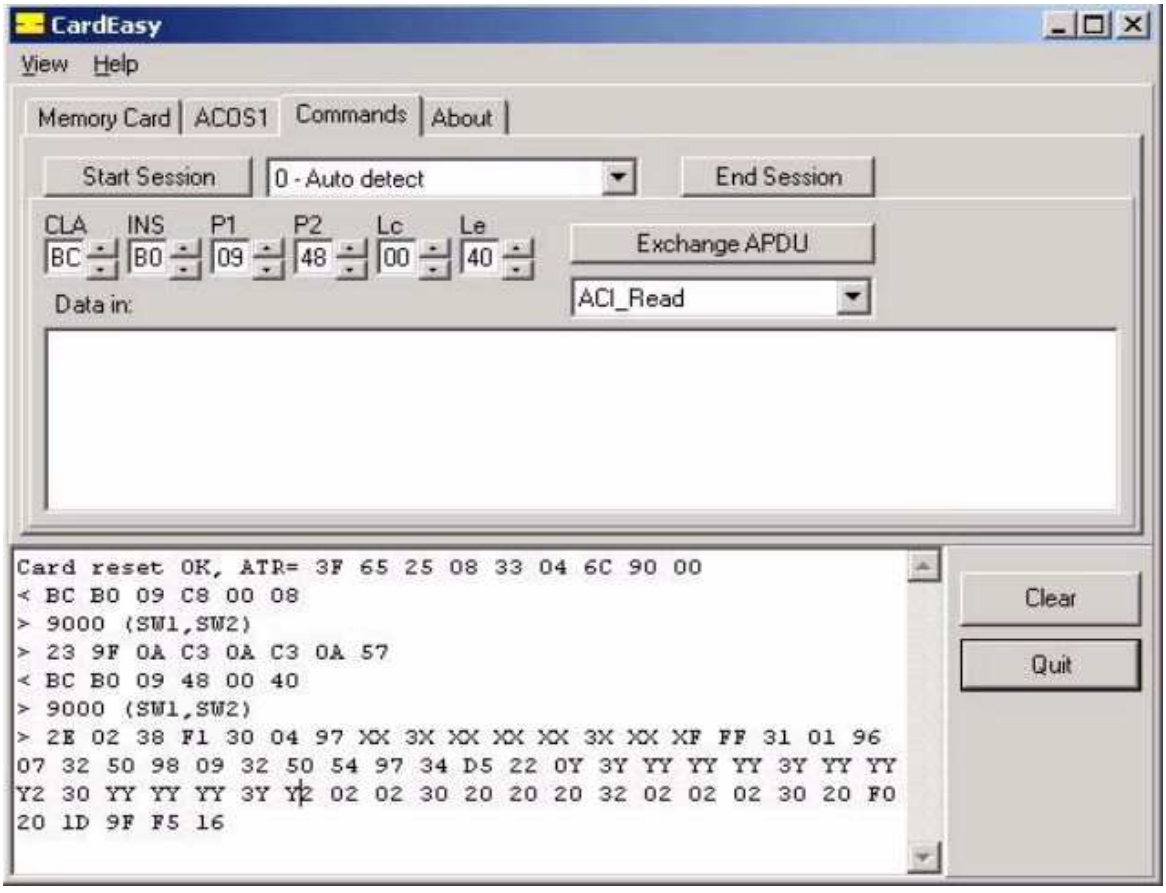


Figure 04.05 : *fenêtre d'affichage la structure interne d' une carte*

Lecture de la zone identifiant (le numéro de la carte bancaire a été masqué par des X, le nom du porteur a été masqué par un Y)

La fenêtre s'affiche donc les résultats suivants :

BC BO O9 48 00 40

9000 (SW1, SW2)

2E 02 38 F1 30 04 97 XX 3X XX XX XX 3X XX XF FF 31 01 96 07 32 50 98 09 32 50 54 97 34 D5 22 0Y 3Y YY YY YY 3Y YY YY YY Y230 YY YY YY 3Y Y2 02 02 30 20 20 20 32 02 02 30 20 F0 201D 9F F5 16

On voit bien l'entête 2E 02 pour le prestataire O2 puis suit la taille du prestataire : 38h soit 56 octets, en suite F1 puis un quartet avec un "3" de redondance il y a en fait des quartets de "3" de tels 3 de redondance tous les 8 quartets, c'est à dire tous les 4 octets, il convient d'ignorer ces quartets avec des "3" pour analyser la chaine convenablement.

La chaine initiale 30 04 97 XX 3X XX XX XX 3X XX XF FF 31 01 96 07 32 50 98 09 32 50 54 97 43 D5 22 0Y 3Y YY YY YY 3Y YY YY YY Y230 YY YY YY 3Y Y2 02 02 30 20 20 20 32 02 02 30 20 F0 201D 9F F5 16 devient donc, Apres suppression des 3 de redondances tous les 4octets :

04 97 XX 3X XX XX XX 3X XX XF FF 31 01 96 07 32 50 98 09 32 50 54 97 34 D5 22 0Y 3Y YY YY YY 3Y YY YY YY Y230 YY YY YY 3Y Y2 02 02 30 20 20 20 32 02 02 30 20 F0 201D 9F F5 16

Maintenant en regroupant par octets :

04 97 XX 3X XX XX XX 3X XX XF FF 31 01 96 07 32 50 98 09 32 50 54 97 34 D5 22 0Y 3Y YY YY YY 3Y YY YY YY Y230 YY YY YY 3Y Y2 02 02 30 20 20 20 32 02 02 30 20 F0 201D 9F F5 16

On reconnaît, au début après l'octet 00, le numéro à 16 chiffres 497X XXXX XXXX XXXX gravé sur la carte bancaire, il est tout simplement codé sur la puce en BCD (Binaire Decimal Code)

Ensuite suivant 3 "F", car le numéro de la carte pourrait passer sur 19 caractères. Puis il y a 3 quartets codés en BCD avec101 correspondant au code usage (code service)

Suit ensuite la date de début de validité sur 2 octets codes en BCD : 96 07 soit juillet 1996, c'est la date d'émission de la carte.

Suit ensuite 3 quartets codés en BCD 250 qui représente le code de langue ici 250, Suit ensuite 2 octets codes en BCD correspond à la date de la fin de validité de la carte : 98 09 La date d'expiration indiquée sur la carte est bien septembre 1998

Suit ensuite 3 quartets codés en décimal codés binaires avec le code divise en 250n cela dépend de la code numérique ISO de pays

Suit ensuite 1 quartets 5 correspond à l'exposant. 5 signifie unité, 3 signifie centième. Cela indique comment sont stockés les montants dans l'historique des transactions.

Comme sur cette carte il y a un 5, les décimales ne sont pas stockées dans l'historique des transactions, si un paiement de 133.33 est effectué, seul le 133 apparaîtra dans l'historique de transaction.

Ensuite suit 3 quartets 497

Ensuite suit une longue chaîne de 26 caractères ASCII stockés à partir de l'adresse 0980 qui vaut comme vu plus haut (après suppression des 3 de redondance tous les 8 quartets

4D 52 20 YY YY YY YY YY YY YY YY YY YY YY YY 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ; C'est l'identité du porteur stockée en ASCII)

Ainsi le code hexa 4D correspond à 77 en décimal et au code ascii de "M", 52h correspond à la lettre "R" et le code 20h à l'espace.

On arrive ainsi à lire le nom du porteur :"MR" suivi du prénom du porteur, d'un espace et du nom du porteur de la carte.

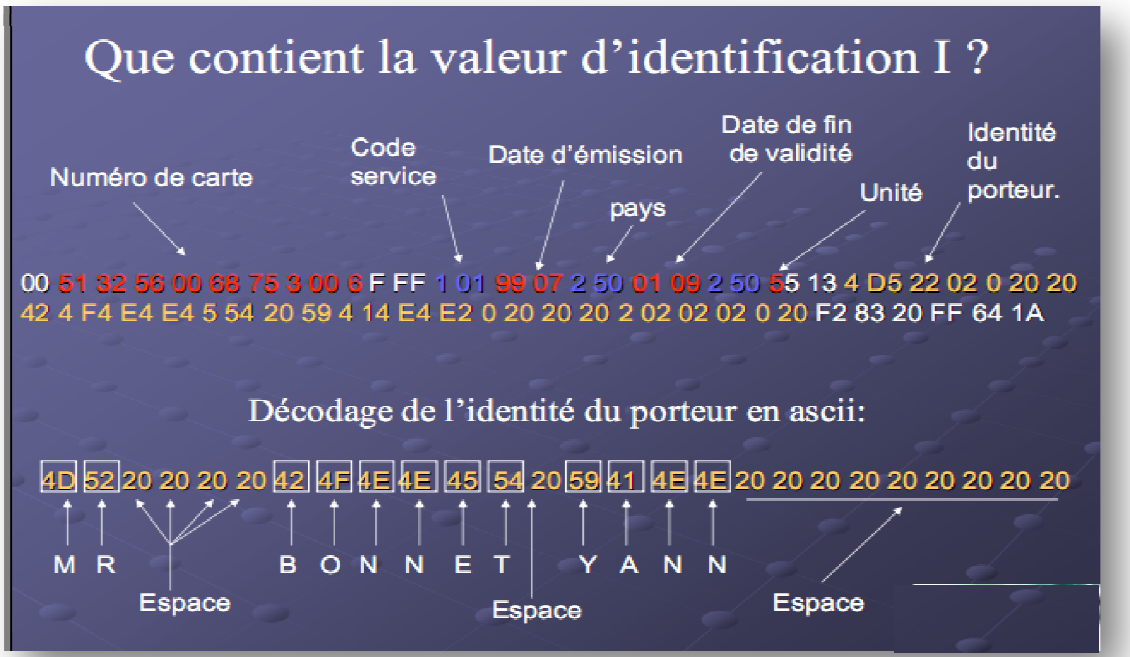


Figure 04.06 : *la valeur d'indentification*

4.6 La banque, le terminal et la carte bancaire

D'après l'étude du fonctionnement de la carte à puce on trouve que la plus part des informations s'écrivent en Code ASCII, et aussi les autres informations se stockent en binaire d'où le système de cette partie de sécurisation suit le principe comme la sécurisation de RSA.

Ils ont reliés par des protocoles APDU comme nous avons déjà vu et aussi relié aux réseaux RTC

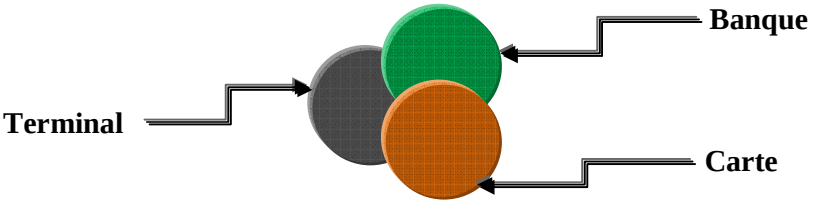


Figure 04.07 : *les assemblages des trois opérateurs*

Même si notre étude se base à la carte bancaire, on ne peut pas séparer la banque, le terminal, et la carte puisque ils sont dépendants. Les fonctionnements de la carte sont autorisés par le terminal si elle est activée par la banque. Alors on place séparément, on note comme ceci :

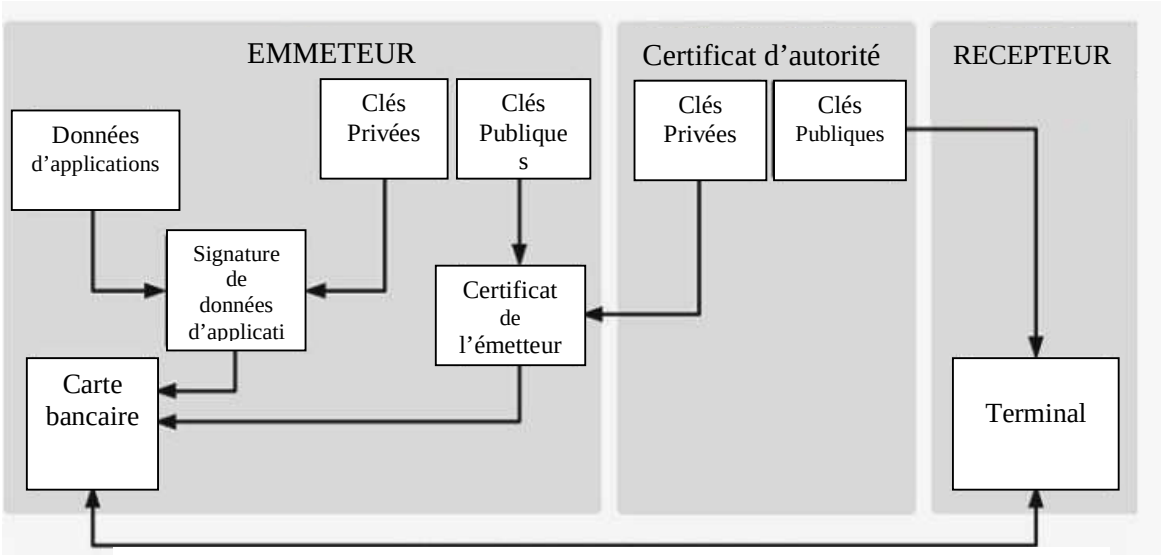


Figure 04.08 : *la structure de trois aspects*

On schématise comme dans cette figure précédente les équipes de la carte bancaire, dans la partie de l'émetteur on trouve plusieurs architectures,

Les données statiques d'application contiennent les renseignements du client et la banque

Puisque la carte est fabriquée par la banque, elle donne aussi de clé privée de l'émetteur de la clé

publique émettrice c'est-à-dire, les clés de la banque pour identifier la propre banque avec les autres. Durant l'utilisation de la carte bancaire, les opérateurs de banque aussi fabriquent les clés inscrites dans la carte et conservées par le terminal, cela se fait par le principe d'autorité de certificat.

Tout travail se déroule en fonction des données stockées dans la banque, et aussi la mis à jour des données du client. Pour cela on veut détailler brièvement les échanges entre les cartes bancaires et la banque.

Authentification des données statiques:

On va détailler

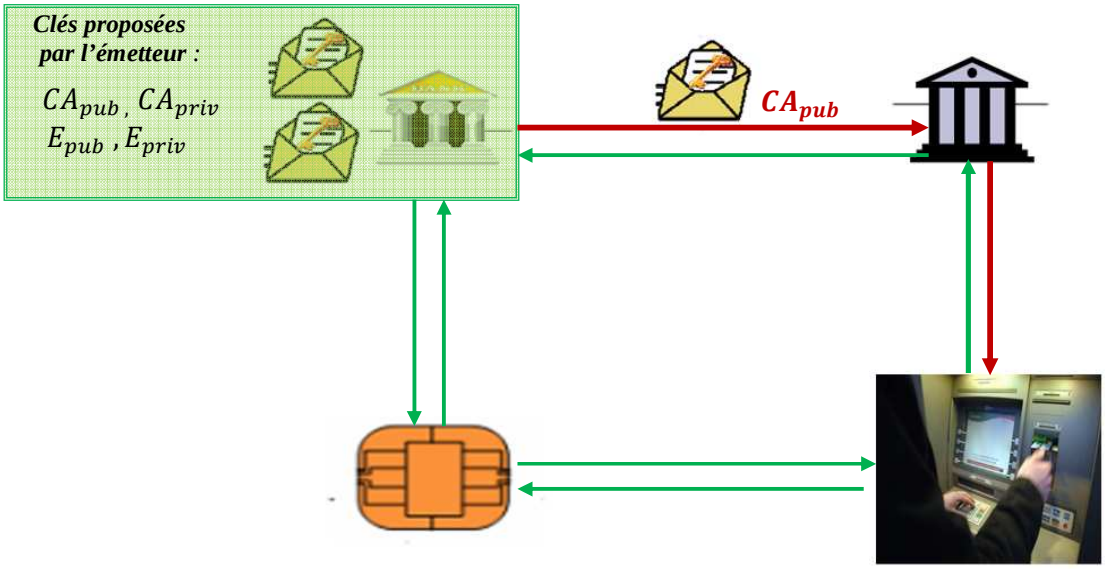


Figure 04.09 : *les différentes clés*

On a va citer les différents types des clés inscrites sur carte bancaire.

On note par :

E_{priv} et E_{pub} les clés proposées par l'émetteur.

CA_{priv} et CA_{pub} les clés désignées par les certifications.

Puisque les informations sont inscrites dans la carte et on trouve aussi la clé E_{pub} qui passe directement sur la carte bancaire, les informations signées par la clé E_{priv} donnent la valeur d'authentification. Dès qu'il y a aussi l'autorité de certification CA certifié par le terminal donc la clé CA_{pub} reste à la terminal elle attend l'introduction de différentes cartes bancaires et vérifier que la clé soit la même à la E_{pub} donnée par l'émetteur.

Pendant la phase de personnalisation, la carte reçoit les informations suivantes:

- Le nom du porteur, le numéro de la carte ou encore la date limite de validité de celle-ci (notés Information).
- une valeur d'authentification (noté VA), signature RSA d'Informations générée avec la partie privée de la clé de l'émetteur (VA= $SigE_{priv}$(*Information*))
- le certificat de l'émetteur (E_{cert}) contenant sa clé publique signée par une autorité de certification
- le code PIN transmis au porteur de cette carte

Lors de l'utilisation

- la carte fournit au terminal Informations, le certificat E_{cert} de la banque émettrice, ainsi que la valeur d'authentification VA
- le terminal vérifie E_{cert} avec la clé publique de l'autorité de certification (CA_{pub}) et vérifie VA avec la clé publique de la banque émettrice
- le terminal demande à l'utilisateur le code PIN et le transmet (en clair) à la carte pour qu'elle le vérifie.

4.7 Améliorations

Pendant la fabrication de la carte, le client s'inscrit à la banque. Chaque client de la banque a un numéro unique comme son numéro compte bancaire et son mot de passe, il y aussi des clés construites par fabricateurs de carte. Chaque banque a des clés spéciales qui inscrites à l'intérieur de la carte, la seule comme responsable monétique connue par sa fonctionnalité.

Après l'étude précédente, on sait que la technique de sécurisation de la carte bancaire actuelle est la cryptographie proposée par RSA, mais il y a des problèmes, et aussi des inconvénients pour la clé, si la banque ont des clefs n, e et le n, d.

L'inscription : c'est la phase qu' un client est enregistré dans la base de données de la banque. On a les clés n et e, pour crypter les données concernant et n et d pour le décrypter

Les données cryptées sont inscrites dans la carte et aussi les clés n et d qui ont été mises par le constructeur de la carte. Les valeurs des clefs n et e on peut écraser on ou non

Pour cela on a alors des clés publiques n et e, les privées n et d, notre amélioration concernent à crypter une fois les clés privés n et d, car s'il y a des logiciels qui sont capables de lire à l'intérieur de la carte, on peut décrypter les données si on trouve les clés publiques disposées par la banque. Comme d' après plusieurs études des cryptographies il y aussi les techniques de forçage qui font forcer directement à calculer les valeurs de n et d à partir de n et e. Pour cette raison là qu'on intéresse de crypter une fois les clés privées n et d de la banque. On trouve également que l'un

des problèmes de cryptographie proposé par RSA est la longueur de la clé très longue, alors ici on invite celle- là on propose la longueur de la clé normale, ni trop longue ni trop courte, puisque pendant la durée d'utilisation de la carte bancaire dans le guichet automatique bancaire, il faut profiter le temps, les différentes transactions doivent- être rapides pour qu'on ne reste pas très longtemps dans le guichet, pour éviter la queue.

On peut écrire que :

- les clés publiques de la banque par : n et e
- les clés privées de la banque par : n et d
- les clés privées de la banque par : n et d et crypter par les clefs n1 et d1 ; alors les clés privées finales inscrites dans carte bancaire sont les clés n2 et d2.

4.7.1 Principe

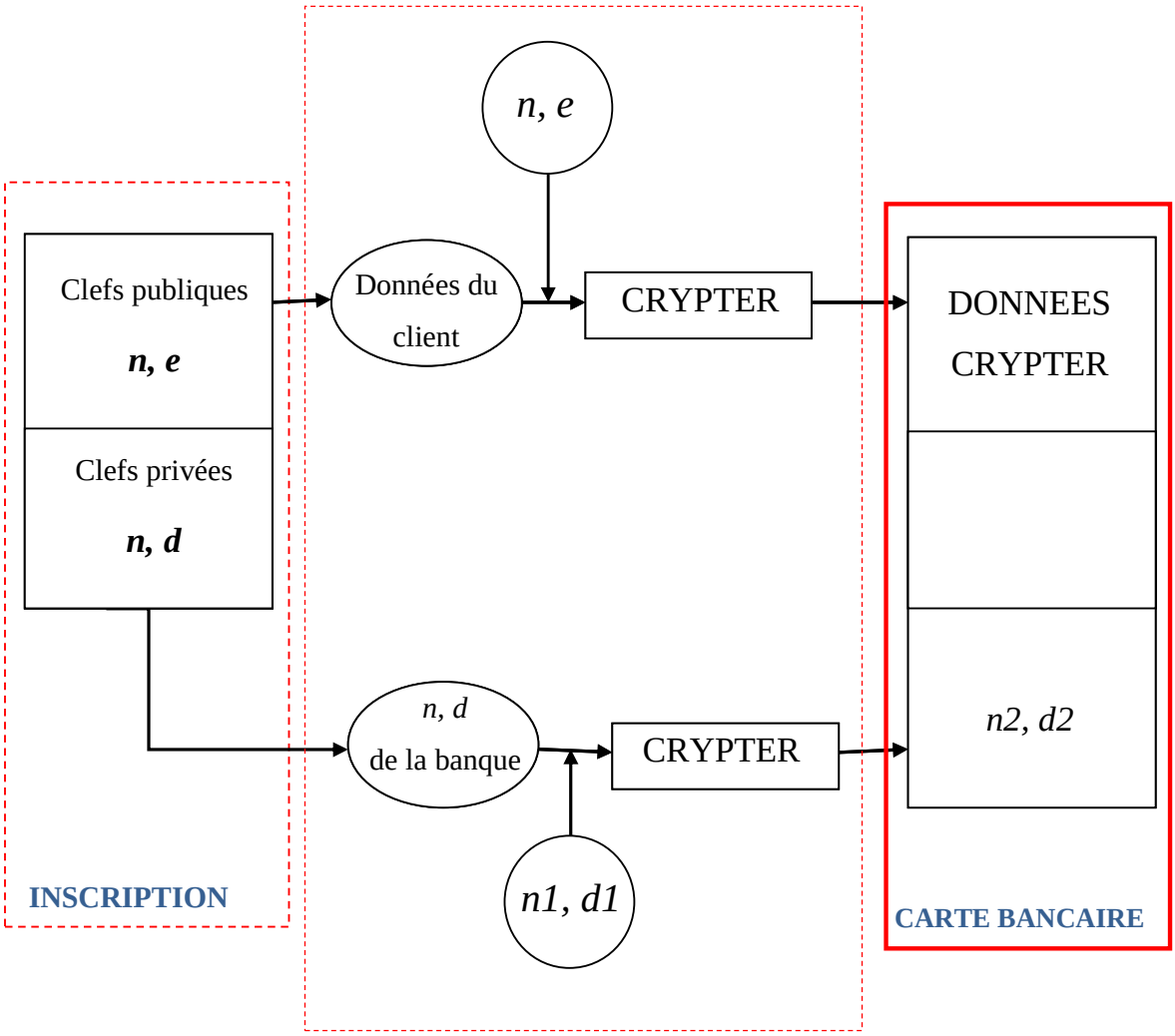


Figure 04.10 : *le passage des données vers la carte bancaire*

4.7.2 Organigramme du fonctionnement d'une carte sur le GAB

Dans cet organigramme, on trouve le passage d'une carte bancaire dans un terminal, alors on peut dire que, dans un premier temps le terminal teste est-ce-qu' il existe les deux clefs n2 et d2 ? S'il trouve ces deux clefs l'opération continue sinon il s'arrête. Puis il décrypte automatiquement la carte par sa propre clefs, notre cas il décrypte par n1 et d1 pour qu'il égalise aux données qui sont déjà inscrites à la banque. Si les valeurs contenues dans la carte sont égales il autorise les transactions.

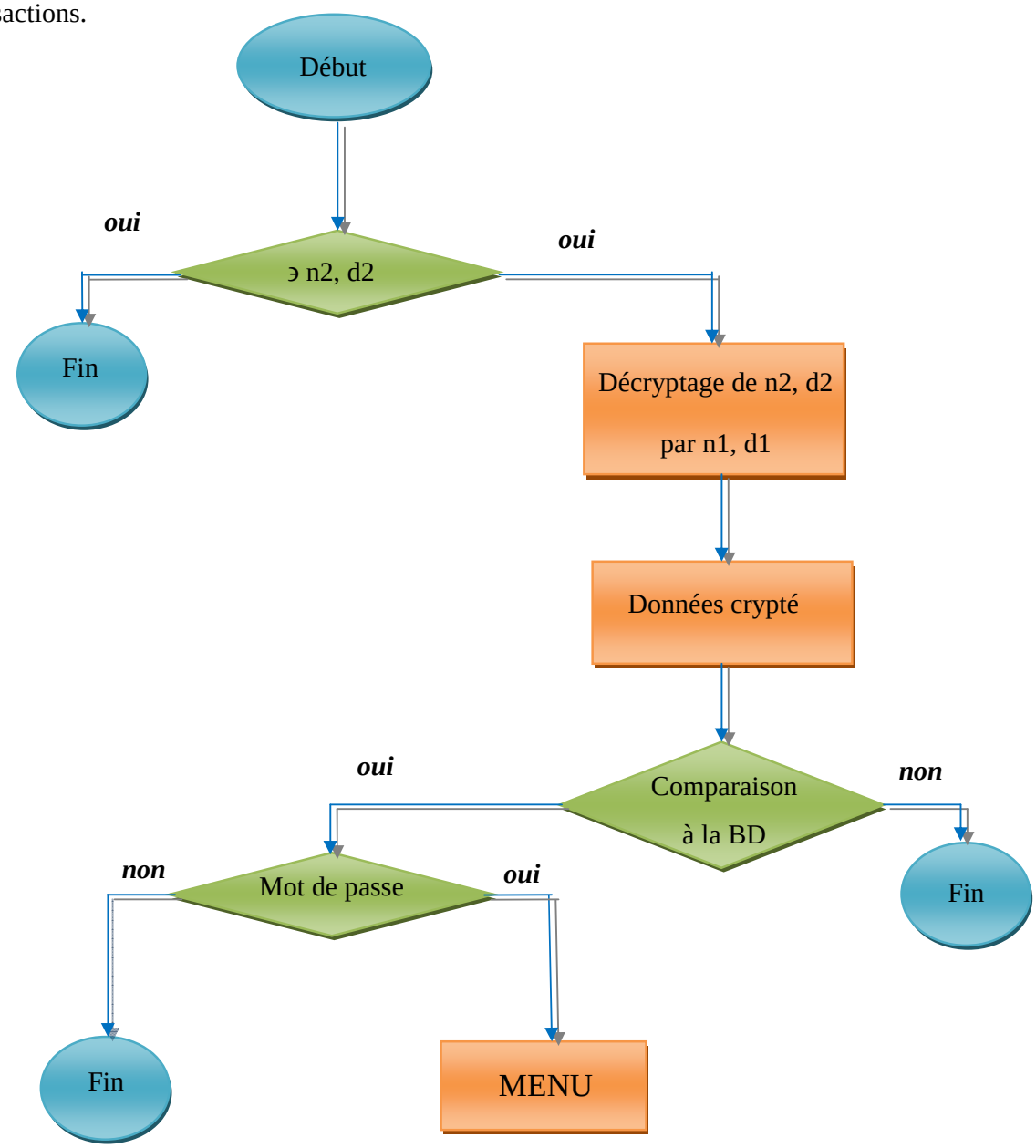


Figure 04.11 : *le fonctionnement d'une carte dans un terminal*

4.8 Conclusion

Si nous voyons, c’est très difficile de pirater une carte bancaire car si elle est perdue, il suffit d’aller chez le fournisseur de la banque et il bloque cette carte à partir des données enregistrer, or l’autre cas à l’étranger il existe de fabricateur de cette carte bancaire et pour cela on peut lire des informations à l’intérieur de la carte, puis on fait de la copie grâce les différents logicielles. Pour cette raison on propose d’effectuer un autre cryptage de la clef disposée par la différente banque, la seule responsable monétique connue la clef de leur banque mais l’autre clef c’est l’algorithme mathématiques de nombre premier fait la calcule.

CHAPITRE 5 : SIMULATION

5.1 Le mécanisme

Le but de cette simulation est de capable de connaître tous les fonctionnements de la carte bancaire sur tous les domaines de la sécurisation et les relations entre la banque et le terminale. Ce mémoire propose également aussi des améliorations des techniques de cryptage des données.

Figure 05.01 : *Le mécanisme de base du trois aspects*

5.1.1 L'inscription

Une fois que vous souhaitiez être client de la banque il faut faire des inscriptions plusieurs dossiers à fournir, et des documents à signer. Cela est très important car vos coordonnées sont stockées dans la base de données de la banque

5.1.2 Enregistrement

Vos coordonnés, votre prés d'inscription sont enregistrées à la banque aussi, puis pendant la fabrication de la carte bancaire les informations concernées sont gravées à l'intérieurs de votre carte. Après cela la banque donne le mot de passe et le numéro de compte.

5.1.3 Cryptage

Chaque carte a des clefs publiques et clefs privées suivant le numéro spécial de la banque pour différencier les types de carte bancaire. Il faut crypter par le fabricateur les informations puisque il y a fabricateur de fausse carte.

5.1.4 Décryptage

Pour pouvoir connaitre les informations contenues dans la carte il faut les décrypter. Ce décryptage se raccompagne toujours avec les bases de données de la banque car la carte est une passerelle qui ouvre les menus des montants du client.

5.1.5 Comparaison

Lorsque les informations dans la carte sont décryptées, en même temps il faut faire les comparaisons des données dans la carte avec les données inscrites de la banque

5.1.6 Menu

Une fois que vos informations dans la carte sont les mêmes à la banque, on attend juste de taper votre mot de passe pour confirmer les vérifications.

5.2 Les différentes manipulations

Figure 05.02 : *fenêtre principale*

Sur cette fenêtre l'utilisateur dispose de trois boutons aux choix :

- le bouton " A propos " contient le concert de cette application

Figure 05.03 : *Boîte de dialogue*

- le bouton " **Quitter** " lui permet de demander la validation pour quitter vraiment le programme

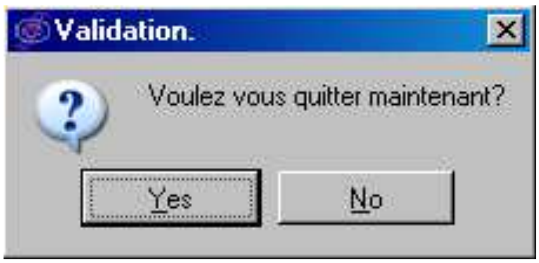


Figure 05.4 : *Boîte de confirmation*

le bouton "exécuter " permet de lancer le programme qui va faire d'inscription

Dès que l'utilisateur lance le programme, il est capable d'enregistrer au client de la banque. En inscrivant leurs coordonnées

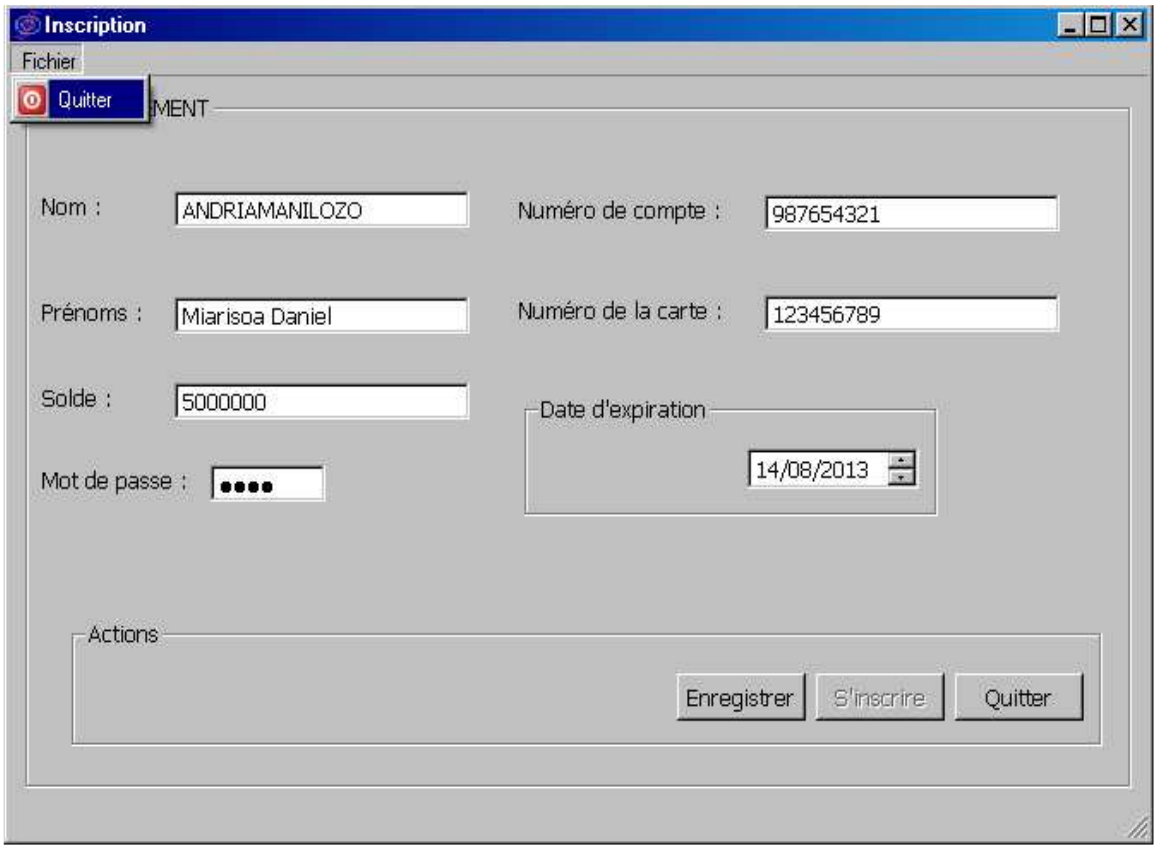


Figure 05.05 : *fenêtre d'inscription*

On voit dans le ***fichier*** une seule option **Quitter**, qui va fermer directement le programme

Il y à des plusieurs champs à remplir selon le renseignement du client.

On trouve dans un peu plus bas des trois boutons alignés "**Enregistrer", "S'inscrire", "Quitter"**

Qui ont des rôles différents/ :

- Le bouton Enregistrer qui va lancer le chemin qu'on veut souhaiter pour enregistrer vos données personnelles
- Le bouton S'inscrire est jusqu' à maintenant ne s'allume pas puisque, le client n'a pas encore enregistré dans la stockage des données de la banque.
- Le bouton Quitter fermeture de programme

Pendant la période de l'inscription, on évite de mettre des erreurs de frappe, puis les informations sont très importantes d' où s'il y a faute de frappe le programme vous guide à connaître les erreurs ;

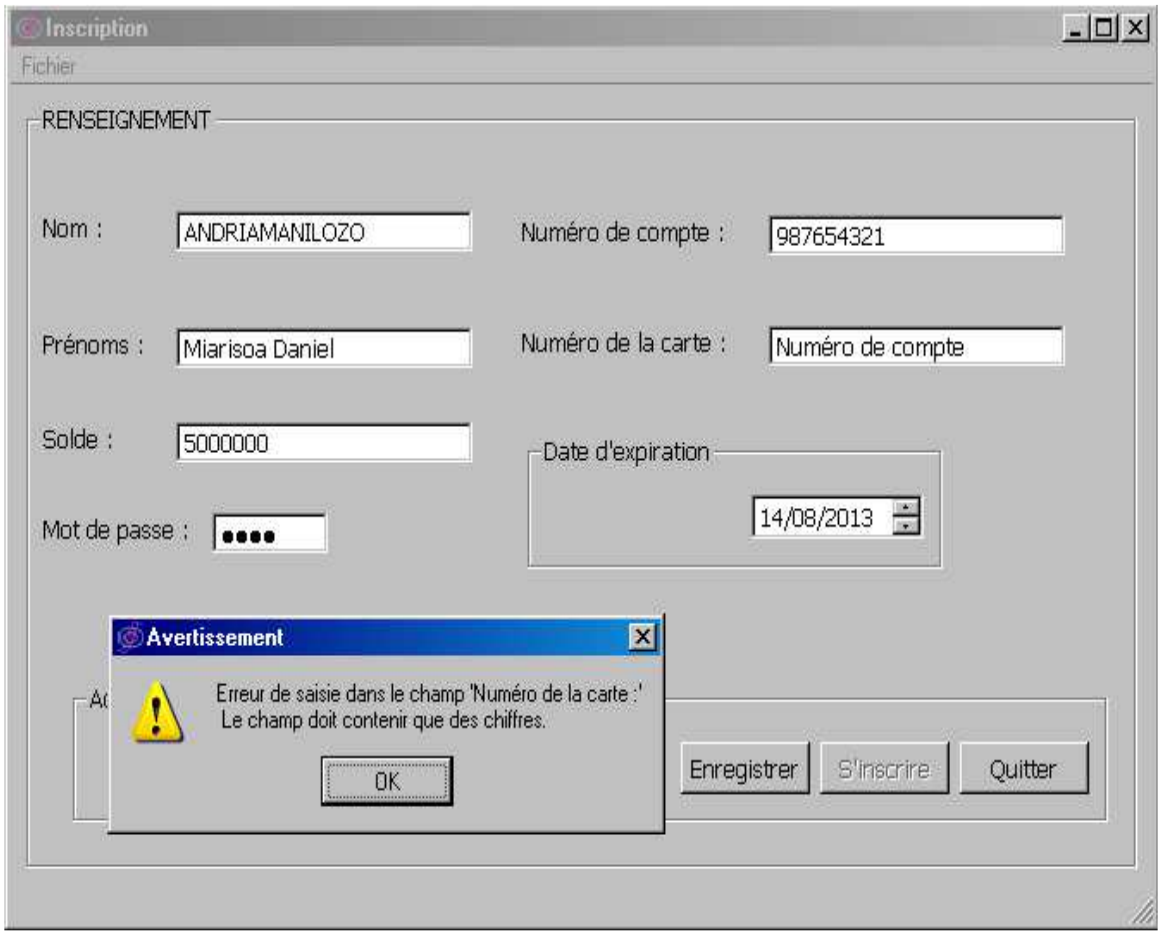


Figure 05.06 : *Boîte d'erreur*

Si le champ est vide il fait l'avertissement

Figure 05.07 : *Boîte d'avertissement*

Pourtant, tous les champs sont remplis, il suffit d'enregistrer et de designer le nom du client durant l'enregistrement.ici l'extension de ce fichier est « **.ord »** (Original Data)

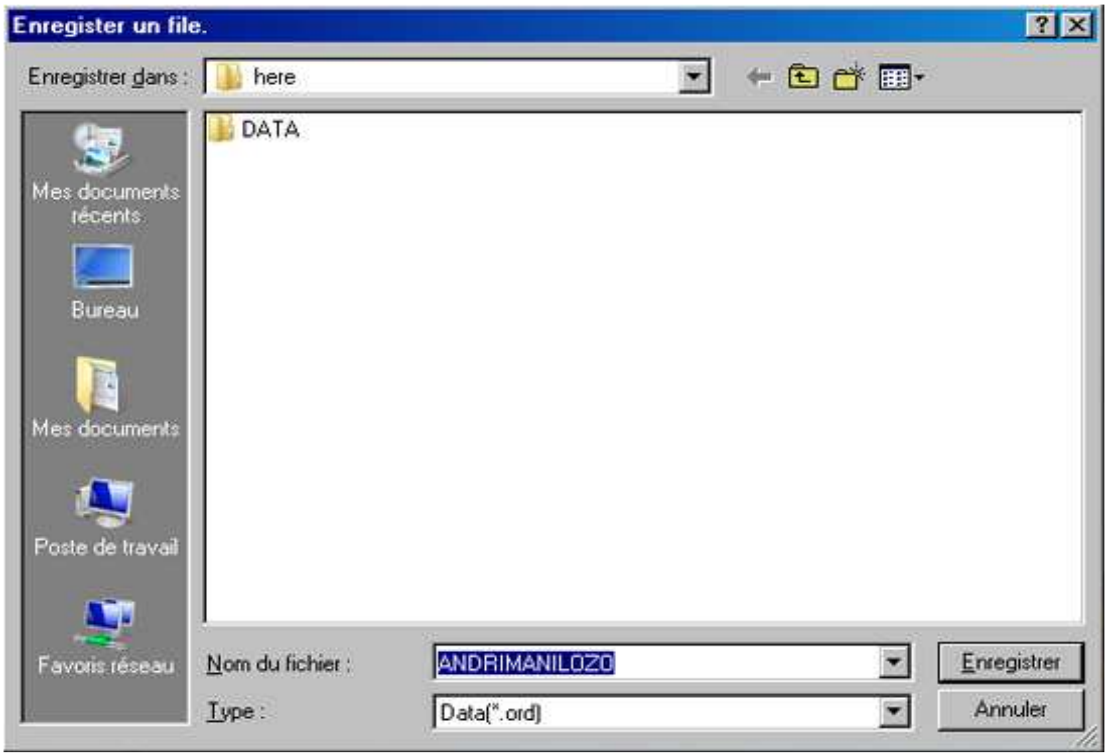


Figure 05.08 : *fenêtre d'enregistrement*

Le client est déjà dans les données de la banque, alors il est impossible d'enregistrer un nouveau pour le client précédant ; le bouton enregistrer s'apparaitre ; il ne reste que le bouton S'inscrire. La banque donne des clés pour cette personne en appuyant le bouton S'inscrire

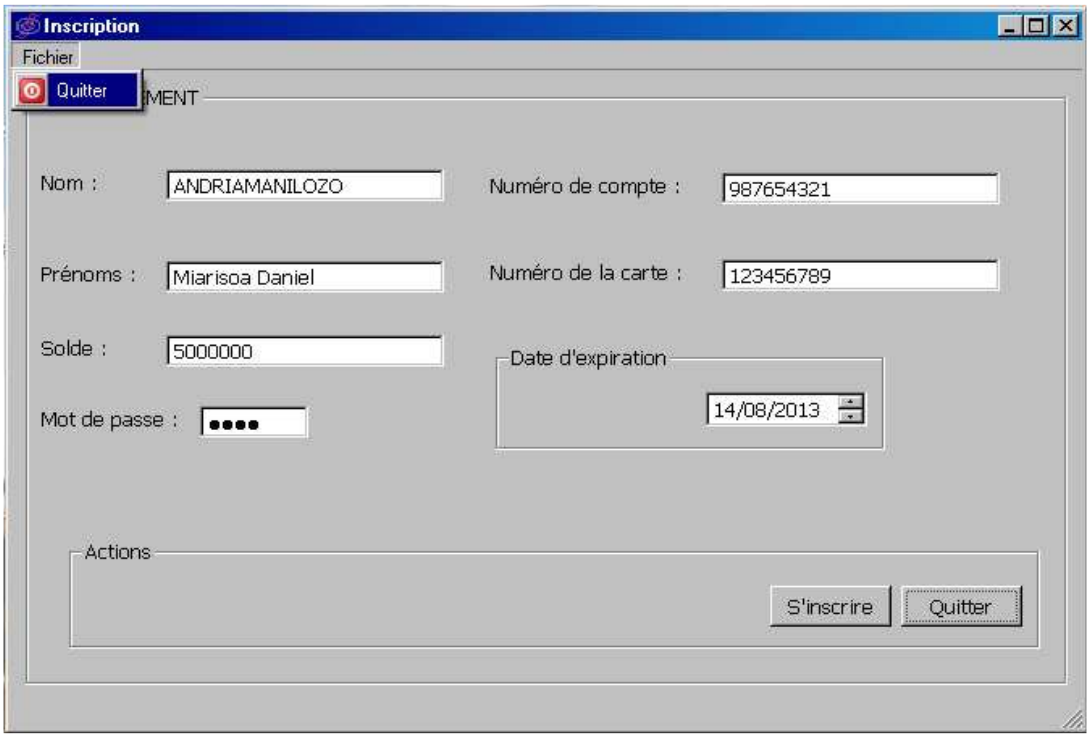


Figure05.09 : *fenêtre d'inscription*

5.2.1 Le partage des clés

Le client a des clés

Figure 05.10 : *Les différentes clés*

Apres avoir obtenu des clés le bouton S'inscrire disparaitra et dans le fichier il y a de **Nouveau** qui va indiquer, on peut faire un nouveau enregistrement

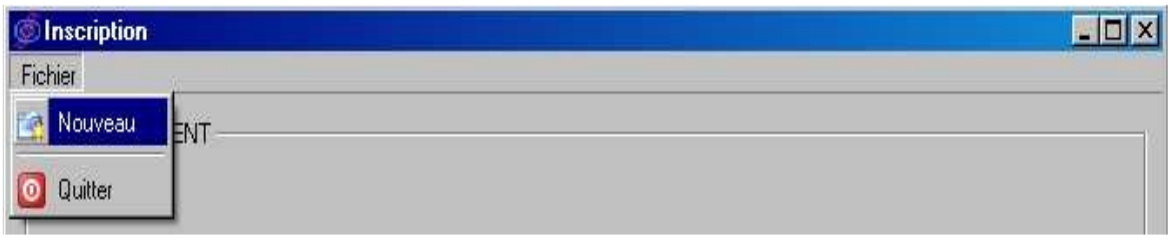


Figure 05.11 : *Nouvelle fenêtre d'inscription*

5.2.2 Cryptage des données

Durant cette inscription il y à des données confidentielles personnelles à la banque, il faut faire des fortes sécurisations, par conséquence chaque client a des clés personnelles. Donc il faut crypter les données pour les cacher.

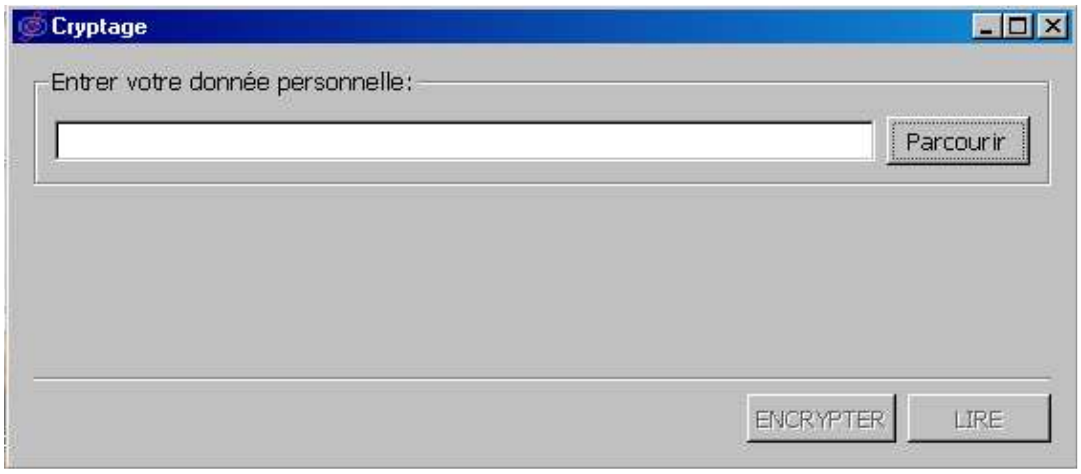


Figure 05.12 : *Parcourir les données pour crypter*

Il y a trois boutons différents :

- Le bouton **Parcourir** qui va guider le chemin que la donnée à été stockée.
- Le bouton **ENCRYPTER** et **LIRE** sont reste floues, ils attendent l'exécution de le bouton parcourir.

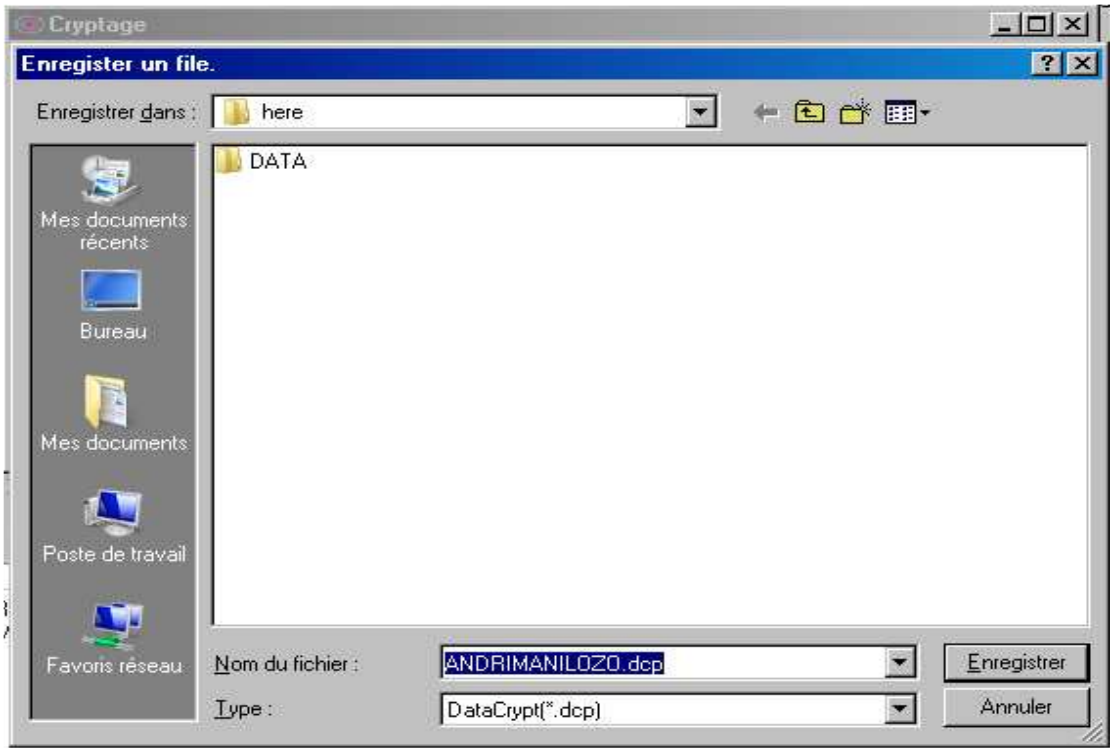


Figure 05.13 : fenêtre *d'emplacement de donnée à crypter*

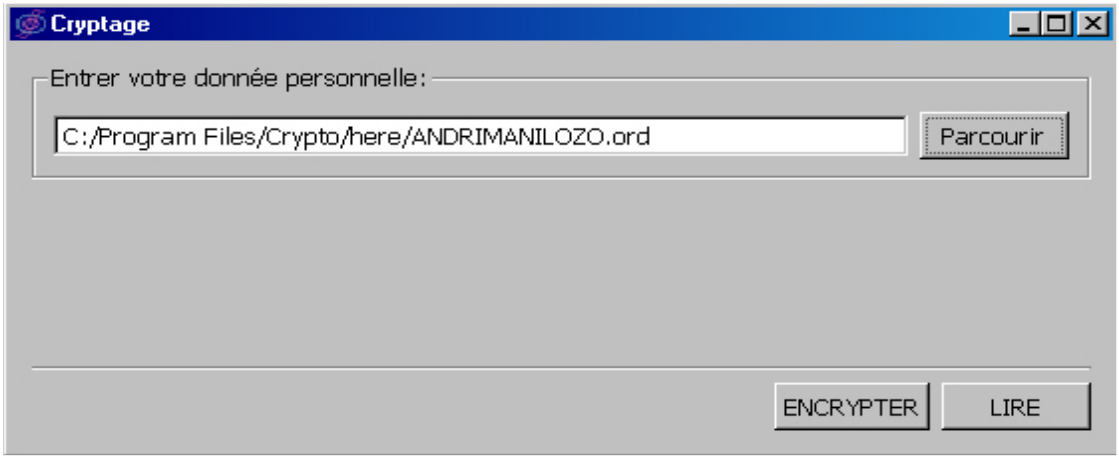


Figure 05.14 : *fenêtre pour choisir les actions*

On trouve le chemin du fichier, les deux **ENCRYPTER** et **LIRE** boutons sont activés.

LIRE lit les données qui ont été inscrites

ENCRYPTER crypte les données en saisissant de vos clés déjà partagé pendant l'inscription.

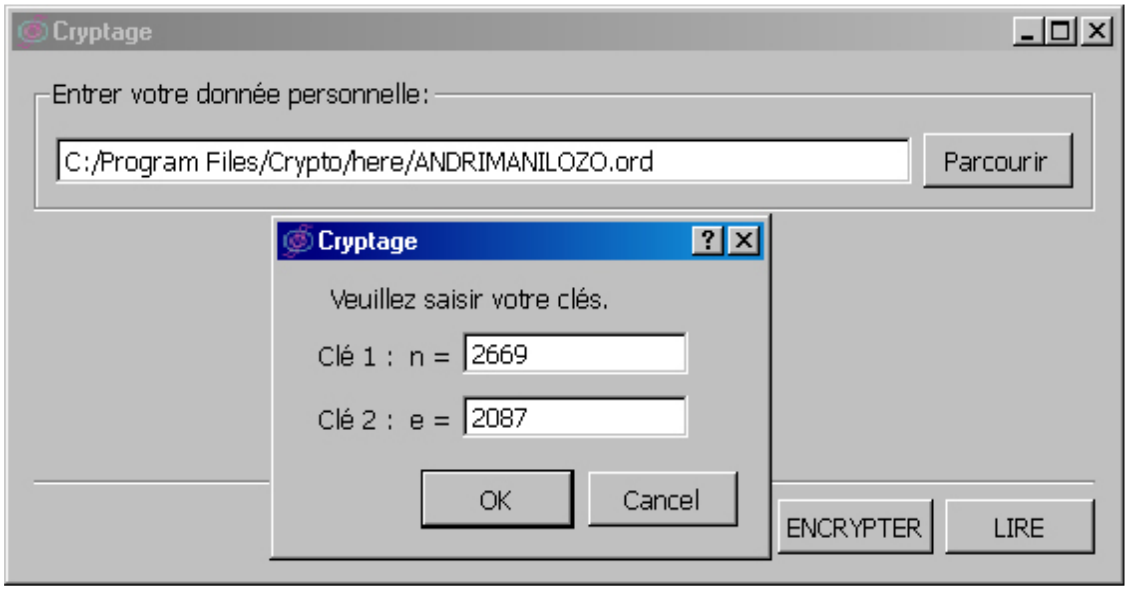


Figure05.15 : *fenêtre manquant pour choisir les clés*

Il suffit d'appuyer de bouton OK pour le crypter.

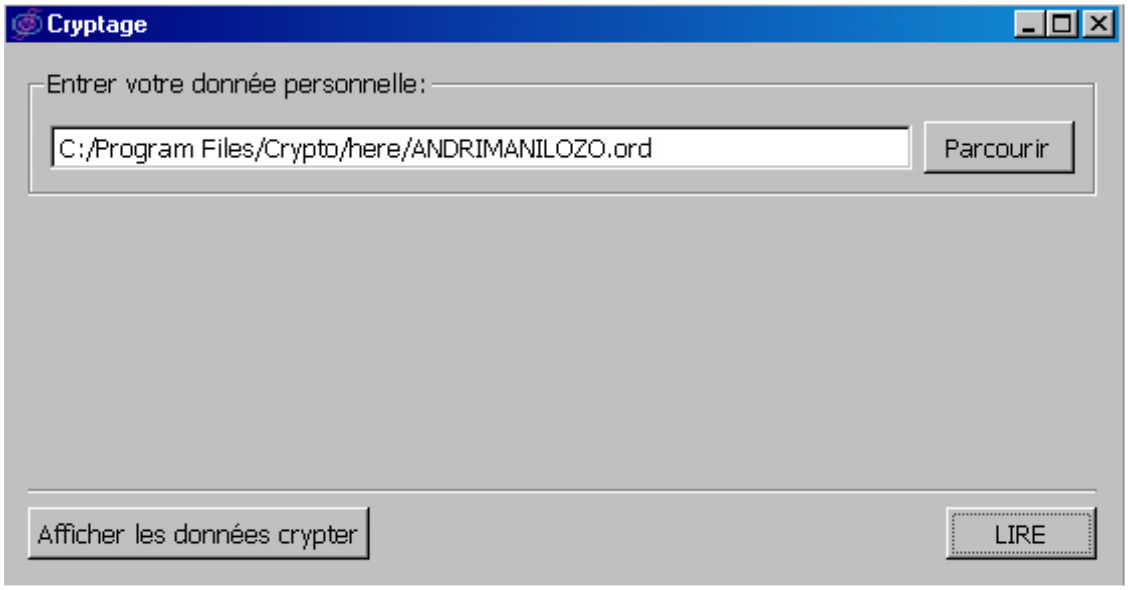


Figure05.16 : *fenêtre pour choisir les actions*

On a deux boutons de comparaison :

- l'un **LIRE** capable de lire la donnée originale
- l'autre **Afficher les données crypter**

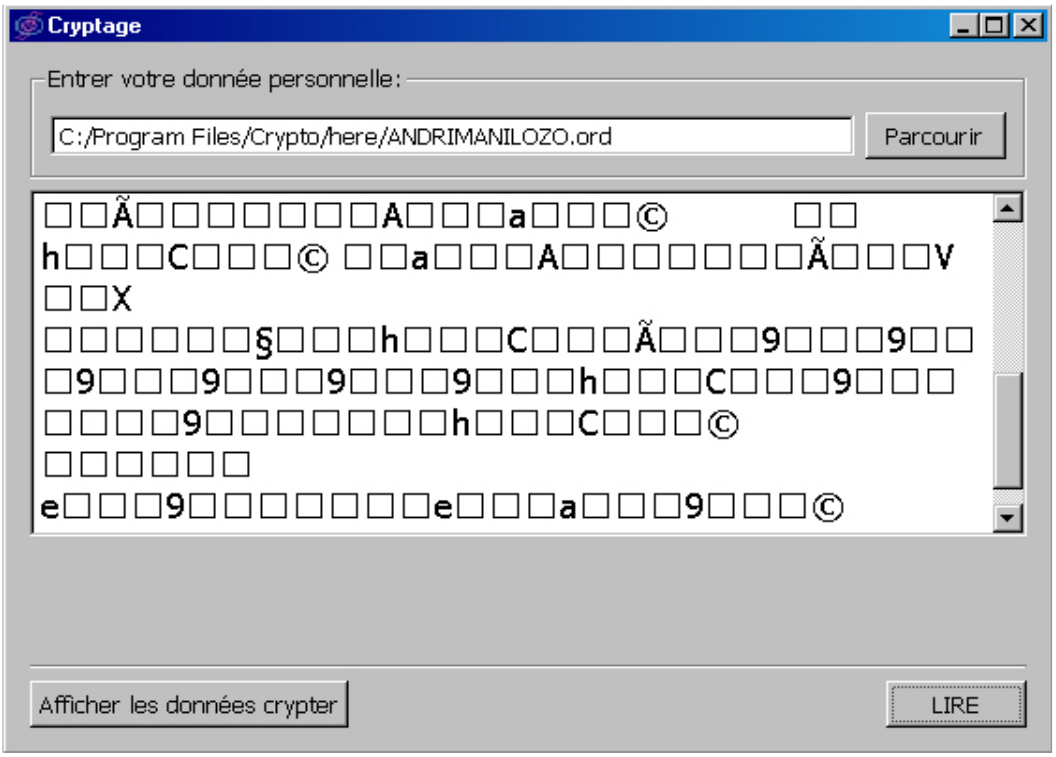


Figure05.17 : fenêtre *d'affichage de donner crypter*

On remarque que, pendant les saisies de clés il faut bine vérifier pour utiliser la vraie clé et si ce n'est pas le cas le programme exécute ou il informe

Figure05 .18 : *fenêtre d'avertissement*

5.2.3 Décryptage des données

Même cas comme le cryptage, mais on va détailler séparément

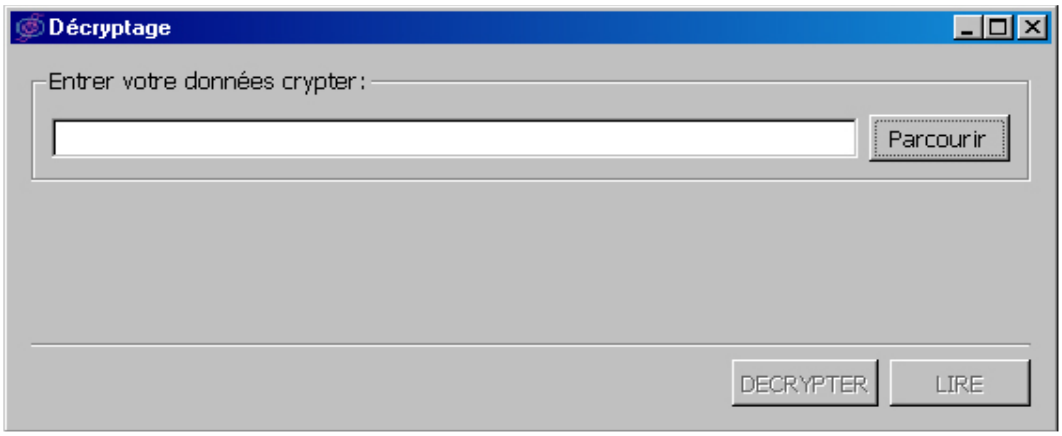


Figure 05 .19 : *fenêtre de parcours*

Les trois boutons sont équivalents au rôle des boutons Parcourir et LIRE sauf le bouton DECRYPER.

Le bouton DECRYPTER décrypte les données si on trouve l'emplacement de données crypté.

Il est activé si le chemin est placé dans le champ.

En tapant le DECRYPER, il est oblige de saisir les clés données pendant l'inscription

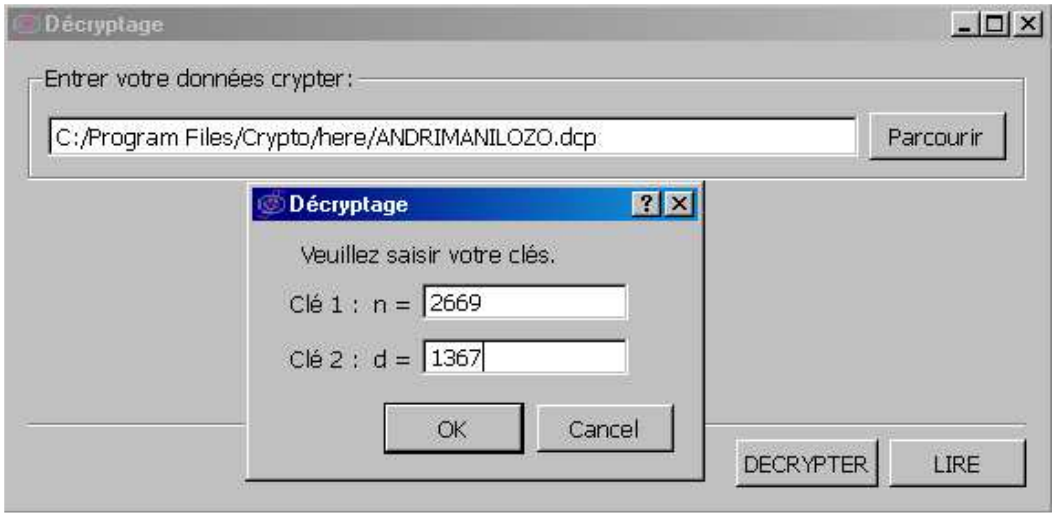


Figure 05.20 : *fenêtre manquant pour choisir des clés*

A la fin en s'appuyant sur le bouton OK on obtient la donnée équivalente à celle de la banque.

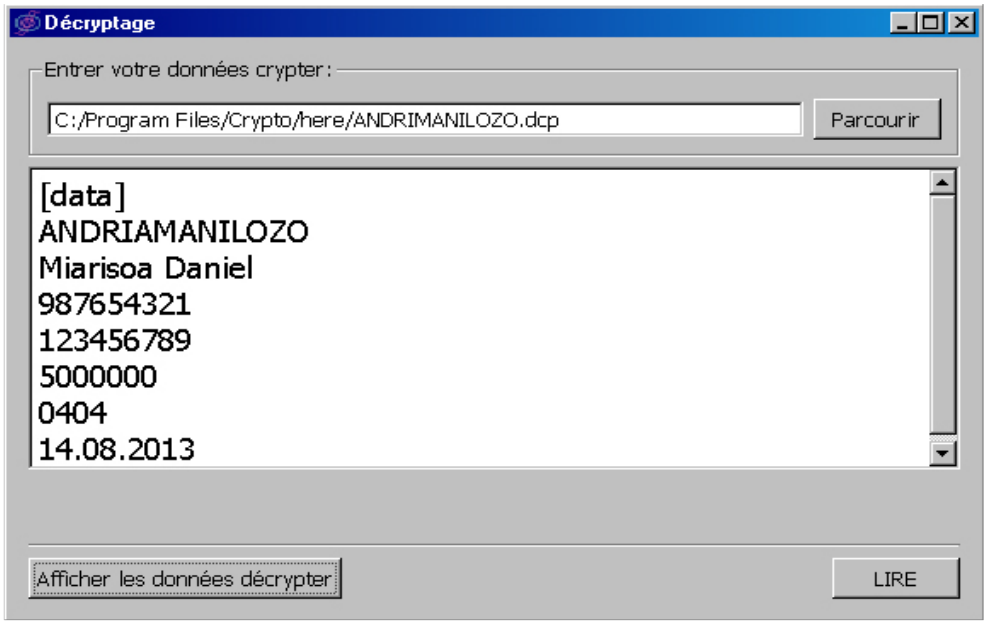


Figure05.21 : *fenêtre qui affiche la donnée personnelle*

Les données inscrites pendant l'inscription

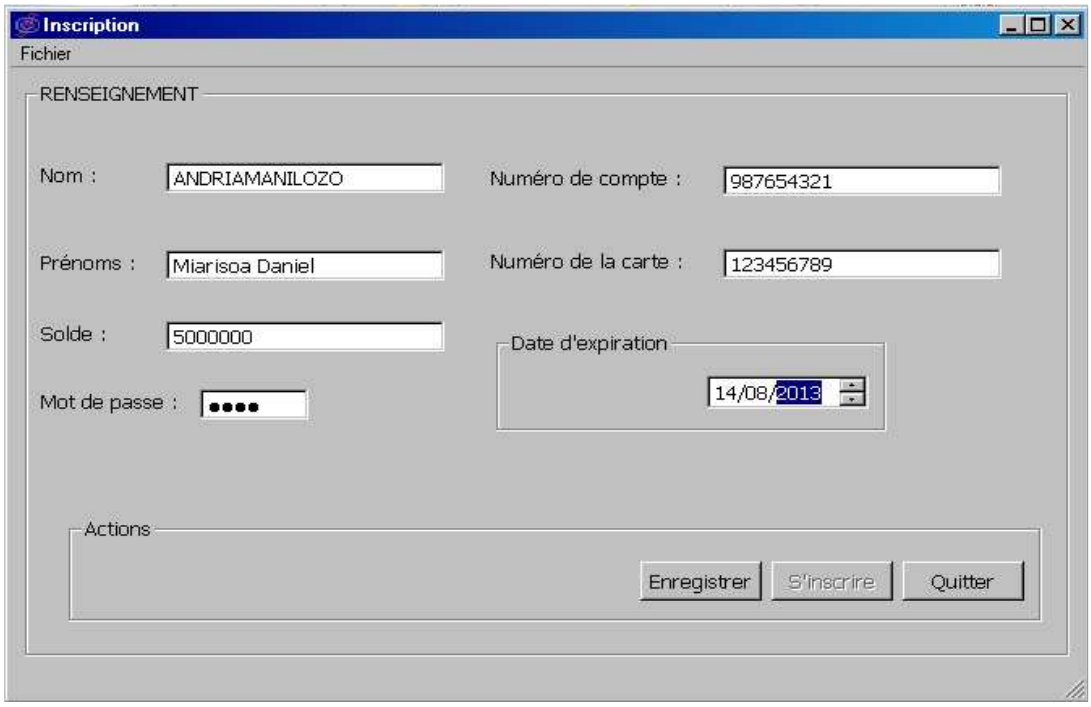


Figure05 .22 : *fenêtre qui remplit les données originales*

5.3 Conclusion

Pour connaître les différents étapes commençant à partir d'un enregistrement d'un client jusqu' à l'obtention des espèces ou de consultation d'un solde, il suffit de faire remplir les dossiers au fournisseur de chaque banque, après cette enregistrement il fabrique une carte bancaire. Crypter les informations puis le fabricateur de la carte donne une clef unique qui va faire de cryptage et de décryptage des données. Une carte bancaire est l'un des outils pour avoir des argents au guichet automatique bancaire ou de consulter les informations d'un compte, une carte dépend de la base de données d'un client dans la banque, le réseau télécommunication, et le guichet automatique bancaire.

CONCLUSION GENERALE

Pour résumer ce mémoire nous a permis de connaître tous les structures de la carte bancaire qui sont inséparables avec les fournisseurs de la banque et le réseau de la télécommunication,

Dans les chapitres, nous avons étudié les bases fondamentales de la carte, avec sa sécurisation actuelle et les différentes techniques de la cryptographie qui la concernent. Durant la réalisation de ce travail, on voit que les fonctionnements de carte bancaire sont reliés des plusieurs acteurs, et aussi de protocoles de communication. Même si on étudie la cryptologie il y a toujours des bases de données de la banque qui sont inscrites dans la carte bancaire suivante les clefs qu'il propose.

Par ailleurs c'est du principe général, or dans le premier chapitre ramène à étudier séparément de l'entourage de la carte comme, le terminal, et la banque, ils sont très importantes puisqu' une carte bancaire vit si elle est mise à jour par le fournisseur de la banque. Dans le deuxième chapitre c'est l'offre le principe de la sécurisation de la carte bancaire, le troisième permet aux techniques de la cryptographie qui sont appliquées à la sécurisation de la carte.

D'une part, dans la quatrième chapitre nous avons montré l'architecture de l'intérieur de la carte après avoir utilisé le lecteur carte ce chapitre nous a permis de connaître les relations directes entre la carte et le terminal avec les protocoles de communication, et les autres données s'écrivent en ASCII

D'autre part, sur le cinquième et dernier chapitre nous a permis d'effectuer une simulation sous langage C, pour faire le transfert de données vers de la banque avec la sécurisation de la carte bancaire.

Enfin, le but de ce mémoire nous a conduit de connaître tous les fonctionnements d'une carte bancaire provenant de la banque suit de différentes actions qu'elle subisse.

ANNEXE 1 : Fonction hachage

Fonction hachage :

La fonction de hachage est une fonction mathématique qu' à partir d'un message génère une autre chaîne permettant d'obtenir un condensé (appelé aussi haché) représentant le texte original. Il doit être associé à un et un seul texte en clair, de plus, la fonction doit être à sens unique afin qu'il soit impossible de retrouver le message original à partir du condensé.

La fonction de hachage ne chiffre pas les données, mais sert à vérifier leur intégrité. Ainsi pour qu'un certificat soit valide, il doit être signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification pour créer la signature. La clé publique ayant été préalablement et largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification.

Une fonction hachage est dite à *sens unique* si, pour essentiellement les valeurs *y* de l'espaces empreintes, il est difficile de trouver un message *x* tel que $h(x)= y$.

- *Une fonction de hachage h est dite faiblement résistante aux collisions* si, pour l'essentiellement chaque message x, il est difficile de trouver $x \neq x'$ ayant même empreinte $h(x) = h(x')$
- *Une fonction de hachage h est dite fortement résistante aux collisions* s'il est difficile de trouver deux messages de *x'* et *x* ayant même empreints $h(x) = h(x')$.

ANNEXE 2 : Certificat X.509

Un certificat X.509

Le certificat X509 fait l'objet d'une normalisation par l'ISO. Il a été réalisé par l'IETF et est identifié par un « DN»

C'est concrètement un document électronique attestant qu'une clé publique est bien liée à une organisation, une personne physique, etc.

Ce document électronique contient une clé publique, un certain nombre de champs à la norme X509 et une signature. C'est la liaison des attributs des champs et la clé publique par une signature qui constitue un certificat. Un certificat peut être un faux; c'est la signature par une autorité de certification (CA) qui lui donne une authenticité.

Globalement, la composition d'un certificat x509 est la suivante :

- Version (v3 actuellement)
- Numéro de série (unique par CA)
- Algorithme de Signature du CA
- Nom du CA (DN)
- Période de validité
- Sujet du certificat (DN)
- Caractéristiques de la clé certifiée :

· Algorithme utilisé

· Clé Publique

· Extensions éventuelles : CRL (liste de révocation), adresse mail, …

ANNEXE 3 : Rappels mathématiques

1. Division euclidienne et congruences

Théorème1 **:** pour tout *(a, b)* $\in N^2$ avec b ≠ 0, il existe (q,r) a $\in N^2$ tel que :

$$a = b\ x\ q + r\ et\ r < b$$

Definition1 : on dit alors que a est *congru* à *r* modulo b et on note $a \equiv r\ mod\ b$

Si le reste r est nul, on dit aussi que b divise a

2. pgcd et algorithme d'Euclide

Théorème2 **:** si $a = bq + r$ est la division euclidienne de a par b pour tout c : c divise à la fois a et b si est seulement si c divise à la fois b et r.

Théorème3 **:** il existe un unique plus grand entier g qui divise à la fois a et b. On le note $g = pgcd(a, b)$ et on le calcule grâce à la formule d'Euclide :

$$pgcd\ (a,b) = \begin{cases} a, & si\ b = 0 \\ pgcd(b,r) sinon \end{cases}$$

3. Théorème de Bézout et l'algorithme d'Euclide étendu

Théorème4 **:** (*théorème de Bézout*) il existe une infinité de (x, y) $\subset Z^2$ tel que

$ax + by = pgcd(a, b)$. On note *bez(a, b)* le couple (u, v) que l' on peu t calculer grâce à la formule :

$$pgcd\ (a,b) = \begin{cases} (0,1) & si\ a = bq + r \\ (u', v' - v'q)\ sinon, où\ (u', v') = bez(b,r) \end{cases}$$

Démonstration : $si\ (u', v') = bez(\ b,\ r)$, on a $u = v'\ et\ v = (u' - v'q)$ car

$pgcd\ (b,r) = bu' + rv' = bu' + (a - bq)v' = av' + b(u' - v'q) = pgcd(a, b).$ et k.

Rappel sur les nombres premiers

Définition2 : un entier p ∈ $\mathbb{Z}$ est premier si est seulement s'il a exactement deux diviseurs.

Théorème5 : pour tout entier naturel n, il existe un unique (p_1, …, p_n) de nombres premiers et unique (e_1, …, e_m) d'entiers naturels tels que : n=$p_1^{e_1}$ ... $p_m^{e_m}$ (décomposition de n en facteurs premiers)

Fonction à sens unique et factorisation

Définition3 : une fonction $f : x \to f(x) = y$ est a sens unique si est seulement si :

- Si x est donné, il facile de calculer y ;

- Si y est donné, il est infaisable de calculer x.

Soient p, q deux grandes entiers premiers tels que $n = pq$:

- Si p, q sont connus alors il est facile de calculer n ;
- Si on ne connaît que n alors il est très difficile de trouver p, q.

Rappel sur le théorème de Fermat - Euler

Définition4 : on appelle indicatrice d'Euler la fonction qui à un entier n fait correspondre le nombre d'entiers *a* premier à *n* vérifiant $1 \leq a \leq n$. On note cette fonction φ.

Si *p* est un nombre premier, alors tout entier compris entre *1 et p – 1* est premier à *p*, aussi $\varphi(p) = p - 1$. On peut également calculer assez facilement $\varphi(p^n)$, toujours pour *p* premier et $n \geq 2$ entier : les nombres premiers à p^n sont exactement les nombres non multiples de *p. Or* entre 1 et p^n, il y a exactement p^{n-1} multiples de p.

Donc $\varphi(p^n), = p^n - p^{n-1} = p^{n-1}(p-1)$

Lemme1 : soient *p* et *q* deux nombres premiers distinct. Alors $\varphi(pq) = (p-1)(q-1)$

Démonstration : pour calculer $\varphi(pq)$, il nous suffit de calculer le nombre d'entiers compris entre 1 et *p* qui ne sont pas premiers à *pq.* Ce sont bien sûr les multiples respectifs de *p* et de *q. Or* il y a exactement *q* multiples de *p* dans l'intervalle [*1 ; pq*], ainsi que multiples de q.

Notons qu'on a ainsi compté deux fois l'entier *pq.* Le nombre d'entiers non premiers à *pq* dans l'intervalle [*1 ; pq*] est donc *q + p – 1.*

Théorème6 : *(théorème de Fermat – Euler)* si a est premier avec n, alors $a^{\varphi(n)} \equiv 1$ *mod n.*

Théorème7 : si *n = pq* avec *p* et *q* premiers, alors $\varphi(n) = (p-1)(q-1)$.

BIBLIOGRAPHIE

[1] Springer-Verlag, *Canaux-de-distribution-bancaire*. Cannes, France, 2140, pp: 150-164. September 2001

[2] F. Raynal, Etudes d'outils pour la dissimilation d'information : *approches fractales, protocoles d'évaluation et protocoles cryptographies,*Thèses de doctorat de l'Université Paris, Spécialité Informatique, soutenue le 1 Mars 2002

[3] A.S. Tannenbaum - Computer Networks Prentice Hall,le 21 mars 1998

[4] B. Schneier - *Cryptographie appliqué* Thomson Publishing International France

[5] C.Chebli, Signature et chiffrement, Cours DEA en réseaux de télécommunications de l' Univérsité Libzanaise, Faculté de Génie et de Univérsité de Saint- Joseph, Faculté de d' Ingénierie ; Paru le 25 mars 2005

[6] Leroy, On-Card Byte Code Verification for Java Card, In I. Attali and T. Jensen janvier 2006

[7] Références à la biclé RSA et au masque DES de la CB relevées en http://www.bull.fr/securinews/courant/31-02_1.html, et renvoyant sur l'hebdomadaire 01 Informatique n° 1580 du 17 mars 2000.

[8] Stroob Valness, *Sécurité et Informatique*, Revue du SCSSI (Service Central de la Sécurité des Systèmes d'Informations), CNRS (A télécharger sur le site : http*://www.cnrs.fr/Infosecu/Revue.html.*
Le n° 24 d'avril 1999 contient des informations précises sur les aspects et le rôle
de la cryptographie, sur les produits de cryptologie, ainsi que sur la législation en cours.

[9]Vaness. John XX_Commission Européenne, Direction générale XII, Télécommunication, Marché de l'information et valorisation de la recherche, *Assurer la sécutité et la confiance dans la communication électronique,* Vers un cadre Européen pour les signatures Numériques et le chiffrement, 1997 EUROPE1997]

[10] D.E. Denning - *Cryptography and data security* Addison Wesley 1982

[11] VEds, *Smart card programming and security*, proceedings of E-Smart 2001, LNCS

[12] F. Arnault.*Théorie des nombres & Cryptographie*, Cours DEA de l'Université de Limoges, Faculté des Sciences, UPRESA 6090 paru le 7 Mai 2002

[13] W. Dian , *Le réseau Interbancaire Banque,* ; Paris III .2000

[14] M. C. Robert, *les opérations de chiffrement et de déchiffrement, ,* USA, 2000

[15] R. Besson, *news technologie JavaCard SMART*, 5ème édition. Edition Radio-1988

[16] http: //www.4shar.com

[18] http: //www.carc.math.uwaterloo.ca.hac.com

[19] http: //www.rsasecurity/facs/labsteamlog.com

[20] http: //www.securité.teamlog.com

[21] http: //www.secutiteinfo.com

[22] http://cedric.cnam.fr/~bouzefra/defit

PAGE DE RENSEIGNEMENTS

Nom : ANDRIAMANILOZO

Prénoms : Miarisoa Daniel

Adresse de l'auteur : Lot HTS 01

Andranomahitsy_Ambohitrimanjaka_Ambohidratrimo

Tana 105

Madagascar

Tél : +261 33 25 204 52 ; 034 99 77 355

E- Mail : *miarisoadaniel@yahoo.fr*

Titre du mémoire : « TRANSFERT DE DONNEES VIA LA BANQUE AVEC SECURISATION DE LA CARTE BANCAIRE »

Nombre de pages : 91

Nombre de figure : 67

Nombre de Tableau : 05

Mots clés : Clés – Cryptages – Décryptage – Clients

Directeur de mémoire : Mr. RAZAKARIVONY Jules

Grade : Maître de conférences

RESUME

La cryptographie est un meilleur moyen pour protéger la confidentialité et la sécurité des informations grâce à des algorithmes de chiffrement qui ne cessent chaque jour de progresser.

Toutes données sont sécurisées c'est très difficile de prendre en force les informations qui vont être s'envoyées sans restriction à cause de la rigidité du calcul mathématique utilisé, mais il y a encore des problèmes qu'on ne peut pas délaisser, nous portons des outils pour éviter les anomalies de la sécurisation enfin d'obtenir des meilleurs rendements et aussi de qualité de service pour que les données transmises soient équitables à celles des décryptés.

La détermination de la cryptologie ramène à l'évolution du développement de l'infrastructure de la télécommunication puisque nous utilisons les ressources de mathématiques, informatique et l'électronique.

ABSTRACT

Cryptography is a better means to protect the confidentiality and safety from information thanks to encryption algorithms which cease each day progressing. All data is protected it is very difficult to take in force information which will be sent without restriction because of the rigidity of calculates mathematical used, but it there with still of the problems which one cannot forsake, we carry tools to avoid the anomalies of the securisation finally obtaining better outputs and also of quality of service so that the data transmit are equitable with that of deciphered. Determinations of cryptology carry of evolution of development of the infrastructure of telecommunication since we use the resources of mathematics, data processing and the electronic ones.