**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE**
**MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE**
**UNIVERSITE M'HAMED BOUGARA BOUMERDES**


**FACULTE DE TECHNOLOGIE**

**Département Ingénierie des Systèmes Electriques**

**Filière : Electronique**

# Support de cours

**Aux Etudiants Master-M2 Electronique des Systèmes Embarqués**

# Cartes à puces

**Ecrit par :**

**Dr. BELKACEM Samia**

**Maître de conférences « A » en Electronique**

**2021/2022**

# Table des matières

# Liste des figures

## Chapitre 1



## Chapitre 2

## Chapitre 3



## Chapitre 4

# Liste des tableaux

## Chapitre 1



## Chapitre 2



## Chapitre 3



## Chapitre 4

# Liste des abréviations

**ABS** : Acrylonitrile-Budadiène-Styrène

**ACL** : Access Control List

**AES** : Advanced Encryption Standard

**AID** : Application IDentifier

**APDU** : Application Protocol Data Unit

**ASCII** : American Standard Code for Information Interchange

**ATR**: Answer to select

**CAD** : Card Accepting Device

**CAO** : Conception Assisté par Ordinateur

**CBC** : Cipher Block Chaining

**CDA** : Combined Data Authentication

**CFB** : Cipher Feedback

**CISC** : Complex Instruction Set Computer

**CLK** : CLOCK

**CMOS** : Complementary MOS

**CTR** : CounTeR

**CTS** : CipherText Stealing

**DES** : Data encryption standard

**DPA** : Differential Power Analysis

**ECB** : Electronic Code Book

**EEPROM** : Electrically Erasable PROM

**EGS** : Electronic Grade Silicon

**EPROM** : Electrically Programmable read-only Memory

**FeRAM** : ferroelectric RAM

**FIB** : Focused Ion Beam

**GSM** : Groupe System for Mobile

**IEC**: International Electrotechnical Commission

**ISO**: International Organization for Standardization

**LCD** : Liquid Crystal Display

**LED** : Light Emitting Diode

**MAM** : Microprocesseur Auto-programmable Monolithique

**MGS** : Metallurgical Grade Silicon

**MMU** : Memory Management Unit

**MOS** : Metal Oxyde Semiconductor

**MPU** : Multi-Precision Unit

**MULTOS** : MULTi-application Operating System

**NFC** : Near Field Communication

**NFCIP** : Near Field Communication Interface and Protocol

**OFB** : Output Feedback

**OMA** : Open Mobile Aliance

**OS** : Operating System

**OSI**: Open System Interconnexion

**PIN** : Personal Information

**PIX** : Proprietary Application Identifier eXtension

**PVC** : Poly Vinyl Chloride

**PC** : PolyCarbonate

**PET**: PolyesTer

**PLL** : Phase-Locked Loop

**PVC** : Poly Vinyl Chloride

**RAM** : Random Access Memory

**RID** : Registered Application Provider Identifier

**RF** : Raido Frequency

**RFID** : Radio Frequency Identification

**RFU**: Reserved for future use

**RID** : Registred Application Provides

**RISC** : Reduced Instruction Set Computer

**ROM** : Read Only Memory

**RSA** : Ron Rivest, Adi Shamir and Leonard Adleman

**SCWS** : Smart Card Web Server

**SIM** : Subscriber Identity Module

**SPA** : Single Power Analysis

**SPOM** : Self Programmable One chip Microprocessor

**SW** : Status Words

**UART** : Universal Asynchronous Receiver-Transmitter

**USB** : Universal Serial Bus

**3DES** : Triple Data Encryption Standard

# Introduction générale

Une carte à puce est une carte en plastique de dimension réduite possédant un microprocesseur permettant de réaliser un certain nombre de tâches. Elle possède généralement une ROM (Read Only Memory), une RAM et une EEPROM (Electrically Erasable Programmable ROM) de quelques kilo-octets de capacité. Certaines cartes à puces sont dotées de coprocesseur cryptographique fournissant un accélérateur de calcul pour les fonctions cryptographiques. Elle communique avec l'extérieur grâce au lecteur de carte ou via une antenne selon qu'elle soit sans contact, avec contact ou hybride.

Le polycopié de cours intitulé ‘’Cartes à puces’’ est le fruit d’enseignement de quatre ans aux étudiants de la spécialité électronique des systèmes embarqués, à l’université de Boumerdès au département Ingénierie des Systèmes Electriques (ISE).

Ce support de cours est rédigé selon le canevas proposé par le Comité Pédagogique National du Domaine Sciences et Technologies (CPND-ST) est destiné aux étudiants de l’établissement de l’enseignement supérieur en 2ème année Master LMD de la spécialité Electronique des systèmes embarqués de la filière électronique.

La carte à puce est une technologie pluridisciplinaire qui s’appuie sur trois éléments : la microélectronique, le traitement de l’information, et la cryptographie. Ces éléments ont servi à la rédaction du présent polycopié du cours, en détaillant le contenu de chaque élément en des chapitres.

Le cours est structuré en quatre chapitres comme suit :

Dans le premier chapitre on donne des généralités sur les cartes à puces, l’architecture de la carte à puce, les applications, le marché et les acteurs principaux de la carte à puce.

Le deuxième chapitre décrit la technologie de fabrication des éléments constituants la carte à puce.

Dans le chapitre trois on donne quelques notions sur la cryptographie avec un peu de détail sur les algorithmes de cryptage symétrique et asymétrique dédiés aux cartes à puces.

Le quatrième chapitre est consacré à la présentation des systèmes d'exploitation dédiés à la carte à puce ; et l'étude des modes de communication pour les cartes avec et sans contact basés sur la technologie radiofréquence.

Une annexe est insérée à la fin du polycopié constituée de deux parties. La première partie représente quelques sujets d'examen déjà proposés dans ce contexte, et la deuxième partie représente le contenu du module cartes à puces issus du canevas CPND-ST proposé en 2017/2018.

# Chapitre 1 : Généralités sur les cartes à puces

## 1.1. Introduction

Une carte à puce c'est une carte avec un circuit intégré embarqué qui a des composants pour transmettre, stocker et traiter des données. Dans ce chapitre on va donner des généralités sur les cartes à puces, leurs élements constituants, leurs domaines d'applications et les principaux acteurs du marché.

## 1.2. Composition de la carte à puce

Une carte à puce est une carte souple comportant un circuit intégré et destiné à traiter et stocker des données. Le traitement des données peut être réalisé par un microprocesseur. La carte à puce est généralement destinée à des fins d'authentification ou de paiement.

Une carte à puce est un bout de plastique de taille normalisée sur lequel est disposée une puce dont les dimensions et l'emplacement exact sont également normalisés. La puce en elle-même est invisible car cachée derrière 8 connecteurs en métal conducteur.

La carte à puce est composée des éléments présentés dans la figure (1.1) :

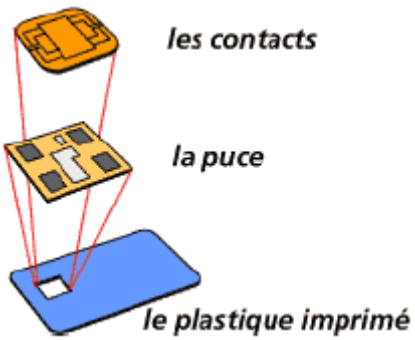


**Figure 1. 1 : Eléments d'une carte à puce**

### 1.2.1. La puce électronique

Un microcircuit (circuit intégré) est construit à partir d'une galette de silicium. Quelques modèles de cartes à puces sont donnés dans la figure (1.2) :

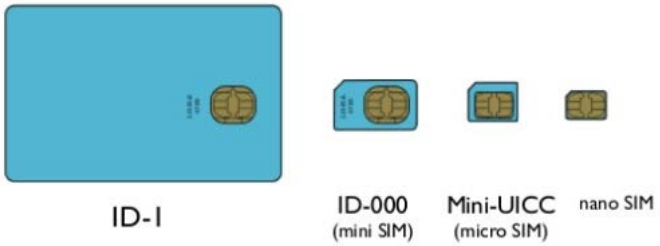


Figure 1. 2 : Taille de la puce

### 1.2.2. Le micromodule

Le micromodule c'est un circuit très mince imprimé logé dans l'épaisseur de la carte qui accueille les contacts (visibles) du connecteur sur une face et la puce (cachée sous les contacts du micromodule) sur l'autre face.

Les normes définissent la position des contacts uniquement pour assurer la compatibilité entre les cartes et les lecteurs. Les huit contacts d'une carte à puces sont montrés sur la figure ci-dessous :

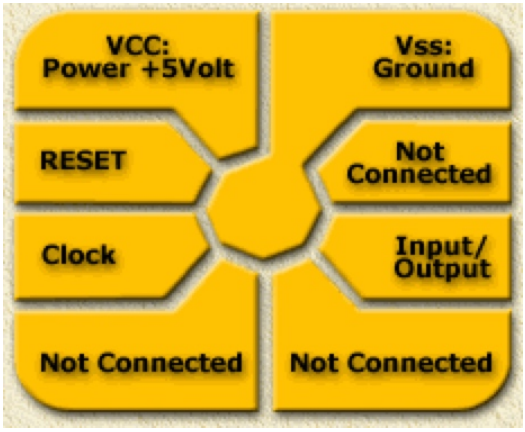


Figure 1. 3 : Les huit contacts d'une carte à puce

Sur les 8 connecteurs visibles, seuls 5 sont utilisés. Leur nom montre à quel point une carte à puce est dépendante du lecteur dans lequel on l'insère, puisque celui-ci doit lui fournir l'alimentation électrique (pattes VCC et VSS, généralement 5V) ainsi que l'horloge (patte Clock, généralement à 3.5 Mhz). Le lecteur peut également faire rebooter la puce en mettant brièvement la patte RESET à 0 (reset à chaud).

L'assignement des huit broches de la carte à puce est donné dans la figure (1.4) :

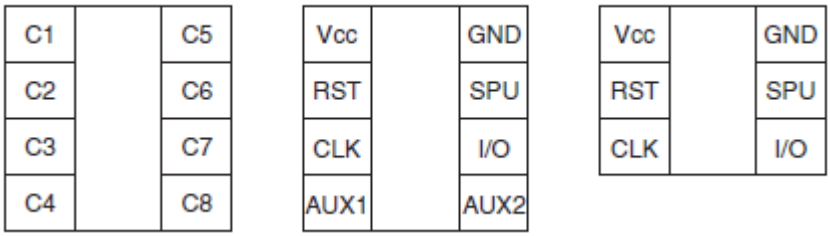


**Figure 1. 4 : Assignement des broches de la carte à puce**

La signification des contacts est résumée comme suit :

**Tableau 1. 1 : Signification des contacts**

| Contact | Signification |
|---|---|
| C1 | Vcc |
| C2 | Reset |
| C3 | CLK |
| C4 | RFU (Reserved for future use) |
| C5 | GND |
| C6 | Vpp (anciennes génération d'EEPROM) |
| C7 | I/O (bi-directionnel en mode half/duplex) |
| C8 | RFU (Reserved for future use) |

Les caractéristiques électriques de la carte à puce sont résumées sur le tableau (1.2) :

**Tableau 1. 2 : Caractéristiques électriques de la carte à puces**

| Symbole | Minimum | Maximum | Unité |
|---|---|---|---|
| Vcc | 4.75 | 5.25 | V |
| Icc | | 200 | mA |

### 1.2.3. La carte plastique

Deux principaux types de plastique sont utilisés :

- Le PVC non recyclable mais embossable
- L'ABS (acrylonitrile-Budadiène-Styrène ) non embossable mais recyclable

## 1.3. Formats de la carte à puce

Les types de cartes les plus courants actuellement utilisés ont une caractéristique commune : est d'une épaisseur de 0,76 mm. Comme l'illustre la Figure (1.5), toutes les autres dimensions peuvent différer. Ces formats ne sont pas arbitraires. Au lieu de cela, ils sont spécifiés par des normes internationales ou selon les spécifications stipulées par les principaux émetteurs de cartes.

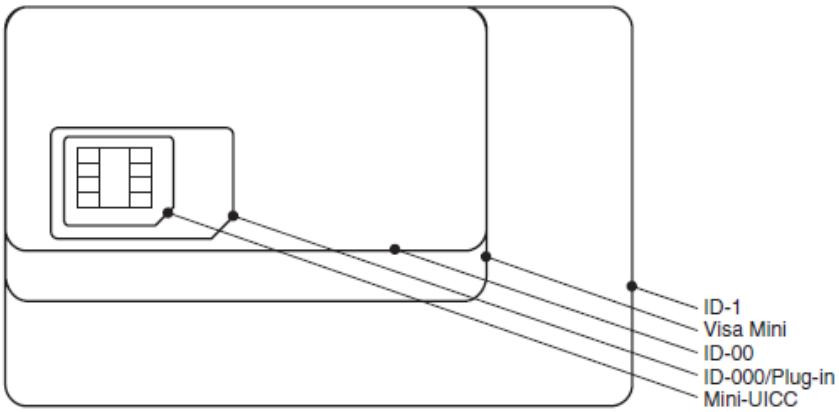


**Figure 1. 5 : Taille des cartes à puces utilisées**

Sur le tableau (1.3) nous donnons la largeur et la hauteur de la carte à puce, sachant que tous les formats possèdent la même épaisseur : 0.76mm.

**Tableau 1. 3 : Les différents formats d'une carte à puce**

| Format de la carte | Largeur (mm) | Hauteur (mm) | Utilization |
|---|---|---|---|
| ID-1 | 85.6 | 54 | Format standard |
| ID-00 | 66 | 33 | Standard pour télécommunication (n'est pas utilisée) |
| Visa Mini | 65.6 | 40 | Système de payment |
| ID-000 | 25 | 15 | Télécommunication |
| Mini-UICC | 15 | 12 | Télécommunication |

## 1.4. Histoire des cartes à puces

L'histoire des cartes à puces est intimement liée à celle de la technologie des semi-conducteurs. En 1974 Roland Moreno, met au point la carte à puce à circuit intégré. En fait, son projet n'était pas celui que tout le monde avait en tête quand on nous parlait de carte à puce, mais plutôt celui d'un porte-monnaie électronique logé sur une bague. De là naît peu à

peu le projet "Electronic Purse" qui revient avec la nouvelle technologie du "sans-contact". Mais l'idée principale est retenue : c'est la création d'une carte à mémoire. Les premières à être crées arrivent en septembre 1974 :

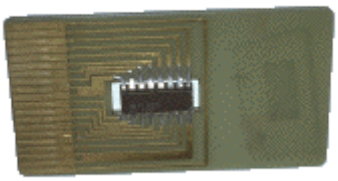

**Figure 1. 6 : Carte à puce à circuit intégré**

Roland Morénoen 1977 avait eu l'idée d'une carte mais dotée uniquement d'une mémoire protégée par des "moyens inhibiteurs"; Michel Ugon enrichit cette idée et la concrétise : la carte doit être intelligente : c'est-à-dire fonctionner comme un micro-ordinateur.

Michel Ugon dépose son premier brevet. Il s'agit d'une carte comprenant à la fois une mémoire non-volatile et un microprocesseur.

En 1978 Michel Ugon dépose cette fois le brevet SPOM (Self Programmable One Chip Micro-Computer) qui détermine l'architecture nécessaire au fonctionnement auto-programmable de la puce. Cet aspect d'auto-programmation permet à un microprocesseur quand il y a une alerte de modifier son comportement pour contrer cette alerte. Au pire, le microprocesseur peut s'autodétruire.

Michel Ugon a amélioré l'architecture de la carte à mémoire en y ajoutant l'intelligence : " J'étais convaincu que la carte devait contenir un microprocesseur auto-programmable, et non pas une simple mémoire, afin de pouvoir modifier les informations contenues à l'aide d'un dispositif pour usage externe - ", raconte Michel Ugon, aujourd'hui Directeur Projets Avancés au sein de Bull Smart Cards & Terminals.

La première carte intelligente au monde sort des ateliers Bull : La Bull CP8 en 1979. Elle est munie d'une mémoire et d'un microprocesseur (Motorola). Son schéma est donné dans la figure (1.7) :

Figure 1. 7 : Première carte intelligente

Toujours la même année, Schlumberger entre dans le capital d'Innovation et commence alors ses recherches sur la carte à mémoire : la division "Cartes à Mémoires & Systèmes" est crée au sein même de l'entreprise Schlumberger.

En 1980-85, le Groupement Carte à Mémoire est créé par un regroupement de banques françaises afin d'utiliser la carte à puce comme un nouveau moyen de paiement : ce qui deviendra la future carte banquaire. Bull, Schlumberger et Philips se lancent alors dans la conception de ces cartes, et c'est réellement en 1984 que la commercialisation des premières cartes à mémoire banquaire a lieu. En 1985 Bull livre ses premières cartes banquaires "CB" dotées de micropprocesseurs.

En 1983 la Direction générale des Télécommunications (futur France Télécom) présente la "carte télécommunications" : une carte d'abonnement qui a pour objectif de prélever chaque communication sur la facture téléphonique de l'abonné.

En 1984, c'est l'apparition de la télécarte avec la "carte pyjama" (appelée ainsi en raison de ses rayures blanches et bleues) crée par Schlumberger pour France Télécom (cartes équipées de micromodules). Une carte pyjama est montrée dans la figure (1.8) :


Figure 1. 8 : Carte pyjama

Ce sont ces cartes qui nous venaient à l'esprit quand on parlait de "carte à puce", car effectivement ce sont celles qui ont connu la plus grosse production. Peu à peu, les publiphones ont été remplacés par des cabines utilisant les cartes à puce. Les cabines ainsi que les cartes connaissent alors une croissance fulgurante : de 2 000 000 de cartes vendues par an

en 1986, on atteint vite 6 000 000 exemplaires par mois en 1991. En 1990 le mot "Télécarte" entre dans le dictionnaire.

Au début des années 90, ce même groupement a vu ses ambitions augmentées vu que la filière bancaire demande des cartes encore plus sécurisées. La nouvelle génération contient un microprocesseur et utilise la technologie de son ancêtre la SPOM (Self-Programmable One-chip Microcomputer) précédemment crée par Bull. Le résultat des essais a donné naissance à une première carte bancaire.

1991 : Lancement des premiers réseaux et services GSM, et des premières cartes SIM (Subscriber Identity Module).

1996 : Création du langage Java Card, un sous ensemble du langage Java.

2002 : La technologie de communication NFC (Near Field Communication) a été lancée par Sony et Philips. C'est une technologie de communication sans-fil à courte portée et haute fréquence, permettant l'échange de données entre un lecteur et un terminal mobile ou entre les terminaux eux-mêmes à un débit maximum de 424 Kbits/s.

2008 : l'organisation OMA (Open Mobile Aliance), a annoncé la spécification d'un serveur Web (SCWS : Smart Card Web server), destiné à des cartes SIM permettant d'exécuter des applications plus riches sur les cartes à puces, et communiquant sur le réseau.

## 1.5. Architecture des cartes à puces

Une carte à puce est composée d'une variété de modules et de composants électroniques tels qu'une mémoire morte (ROM), une unité centrale de traitement (CPU), une ROM programmable effaçable électroniquement (EEPROM), une mémoire vive (RAM) et des entrées et sorties composants (E/S) comme illustré à la Figure (1.9). La ROM est utilisée pour stocker des informations permanentes (c'est-à-dire le logiciel de base de la carte à puce et une ou plusieurs clés pouvant être utilisées pour contrôler et programmer l'EEPROM), tandis que l'EEPROM est utilisée pour stocker des données d'application (qui peuvent être écrites ou réécrites). La RAM est utilisée comme une mémoire volatile qui ne stocke que des données temporaires. Le module de traitement de la carte à puce est plus rapide qu'un ordinateur personnel (PC) de 1980. Le port d'E/S bidirectionnel est utilisé pour transférer des données (par liaison filaire ou sans fil) entre un appareil connecté et la carte à puce.

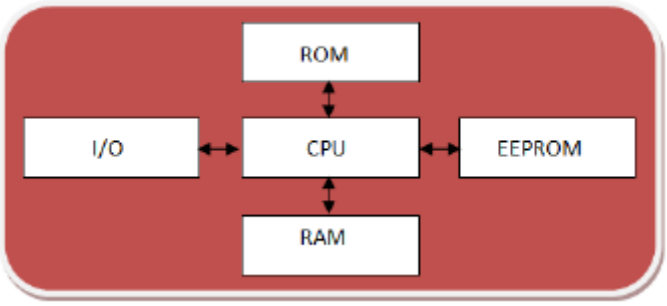


Figure 1. 9 : Architecture d'une carte à puce

## 1.6. Type de cartes

Il existe différentes familles de cartes à puces.

1) Les cartes à mémoire simple servent de simple support de stockage ;
2) Les cartes à mémoire avec logique câblée possèdent un support de stockage et sont capables d'effectuer des opérations de logique simple ;
3) Les cartes à microprocesseur sont des cartes possédant une mémoire programmable ainsi que des fonctionnalités permettant des opérations logiques avancées.

### 1.6.1. Carte magnétique

Les premières cartes ont été développées en plastique avec une bande à piste magnétique (magnetique strip card) dans les années 50. La bande magnétique représente le support de stockage des informations, elle est limitée en taille mais restait suffisante jusqu'à une certaine époque. Les cartes Diners Club sont les premières à utiliser cette technologie. Ne sont pas sécurisées, tel que plusieurs équipements peuvent lire leurs contenus. Un modèle d'une carte magnétique est donné dans la figure (1.10) :

Figure 1. 10 : Carte à piste magnétique

Quelques applications des cartes magnétiques sont citées ci-dessous :

- Paiement
- Cartes de crédit
- Cartes d'identité
- Transport

### 1.6.2. Cartes à mémoire

Il existe deux sortes de carte à mémoire, la carte à mémoire simple et la carte à mémoire à logique câblée. La plupart de leurs caractéristiques sont cependant communes :

1) Les cartes à mémoire simple

Ces cartes sont utilisées comme systèmes permettant de décrémenter des unités stockées au préalable

2) Les cartes à mémoire avec logique câblée

Les cartes à mémoire avec logique câblée sont dotées par les propriétés suivantes :

- La carte comporte un dispositif « câblé » de protection des données procurant un certain niveau de sécurité
- Ces cartes peuvent également être chargées avec une valeur non monétaire

### 1.6.2.1. 1ère génération de la carte à mémoire

La carte à mémoire est composée d'une mémoire EEPROM d'une capacité variable selon les cartes. Elle contient aussi une interface respectant la norme ISO7816 permettant la communication avec un lecteur externe.

La carte à mémoire est composée d'une mémoire EEPROM d'une capacité variable selon les cartes. Elle contient aussi une interface respectant la norme ISO7816 permettant la communication avec un lecteur externe. Au départ, Ce type de carte ne présentait aucune sécurité ou presque. La seule sécurité reposait sur la possibilité de modifier son contenu une seule fois à la phase de la personnalisation. Ces cartes ont été utilisées comme cartes téléphoniques de première génération. La Figure (1.11) présente une architecture d'une carte à mémoire de base.

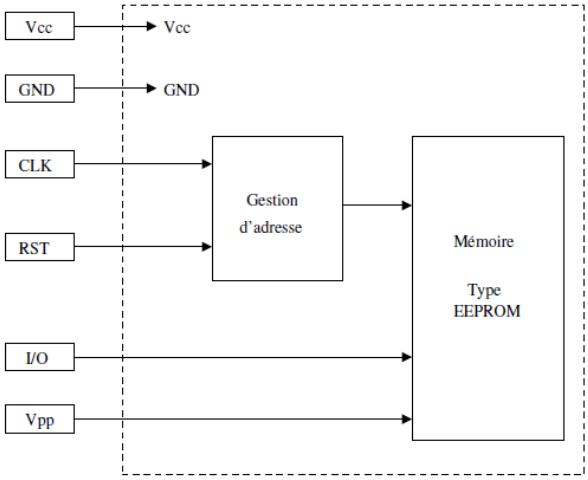


**Figure 1. 11 : Architecture de la première version d'une carte à mémoire**

### 1.6.2.2. 2ème génération de la carte à mémoire

La deuxième génération de la carte à mémoire est la carte à mémoire à sécurité câblée (carte à logique câblée sécurisée). La carte contient deux niveaux de sécurité :

Le premier niveau est utilisé pour authentifier la carte afin de différencier une carte originale d'une carte fausse et le deuxième niveau concerne la sécurité associée à chaque zone de la mémoire. Une architecture type de la carte à mémoire sécurisée est décrite dans la figure (1.12) :

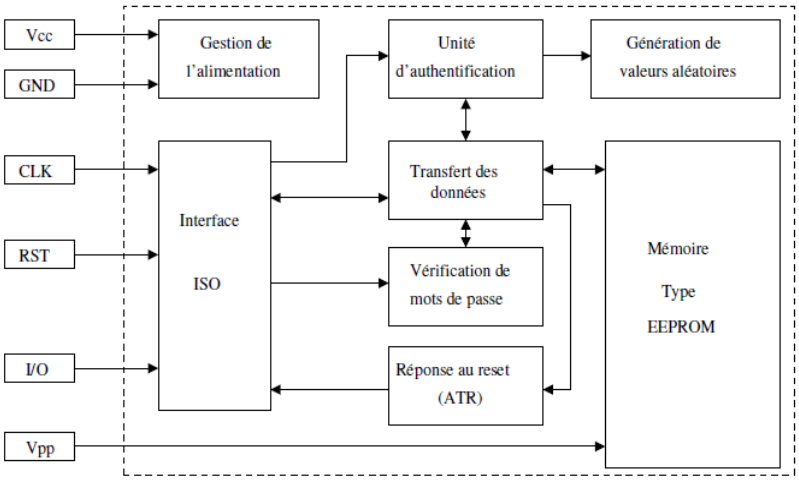


**Figure 1. 12 : Exemple de carte à mémoire à sécurité câblée**

Ce type de carte demande une authentification mutuelle au début de la communication. La mémoire de la carte est répartie en un nombre défini de zones d'une capacité spécifique et chaque zone possède un attribut lui définissant les droits de lecture et d'écriture. Afin d'accéder à la zone, une vérification d'une clé secrète ou un mot de passe est obligatoire selon son attribut.

### 1.6.2.3. Caractéristiques des cartes à mémoire

Les caractéristiques des cartes à mémoire sont résumées comme suit:

1) Elle n'a pas de processeur

   Une carte à mémoire n'a que la mémoire et l'interface d'entrée-sortie mais n'a pas de processeur

2) Pas de système d'exploitation
3) Fonctionnalités limitées

   Sur les cartes à mémoire simple les seules possibilités sont des lectures/écritures en mémoire.

Avec les cartes à mémoire à logique câblée l'accès peut être restreint avec PIN : comparaison bit à bit avec PIN stocké en ROM. Elle peut également contenir des éléments logiques simples.

La carte téléphonique a une logique câblée, ne permet que de mettre à 0 les bits donc incrémente le nombre d'unités utilisés.

4) Peu de sécurité

Il n'y a pas ou très peu de sécurité dans une carte à mémoire puisqu'il n'y a pas d'intelligence capable de réagir en cas d'intrusion malveillante ni de capacité de traitement permettant de prendre en compte des algorithmes de sécurité. Sans microprocesseur, la carte ne peut exécuter les algorithmes cryptographiques.

5) Petite

La carte à microprocesseur renferme un véritable micro-ordinateur, la taille de la puce donc nettement plus importante. La puce de la carte à mémoire (par exemple, une télécarte) a 1 millimètre de côté, la puce de la carte à microprocesseur peut atteindre 25 $mm^2$.

6) Faiblesse du standard dans ce domaine

Les contacts et l'interface électrique ne sont pas normalisés. Ceci rend les cartes difficiles à identifier lors de l'insertion dans un lecteur, ce dernier travaille par essai/erreur, essaye différents protocoles jusqu'à obtenir une réponse.

7) Faible coût

Une carte à mémoire coûte entre 0,25$ et 2,50$.

### 1.6.3. Carte à microprocesseur

Les cartes à logique câblée et les cartes à micro-processeur ont certaines caractéristiques communes : les caractéristiques physiques, de contact et de communication, qui sont d'ailleurs normalisées par l'OSI (Organisation de Standardisation Internationale).

Les cartes à microprocesseur dites aussi cartes ‘’intelligentes’’. Cette ‘’intelligence’’ vient du fait que contrairement aux cartes à mémoire les cartes à microcontrôleur peuvent être programmées pour effectuer des décisions logiques complexes.

Les deux principaux types d’architecture de microprocesseur sont appelées CISC pour Complex Instruction Set Computer et RISC pour Reduced Instruction Set Computer.

**1) Les cartes à microprocesseur CISC**

Les processeurs CISC permettent :

- L’accès à la mémoire contenant les données est sécurisé par la présence d’un circuit ‘’intelligent’’, un microprocesseur 8 bits doté de capacité de traitement de données et de calculs complexes

- La carte est programmée par un logiciel enregistré dans la ROM (c’est le système d’exploitation et les applications)

### 2) La carte à microprocesseur RISC pour JAVA

La révolution apportée par le langage JAVA consiste à ne pas affecter à une carte une tache précise, mais avec la possibilité de faire coexister plusieurs applications.

L’architecture d’une carte à puce à microprocesseur est donnée dans la figure (1.13) :

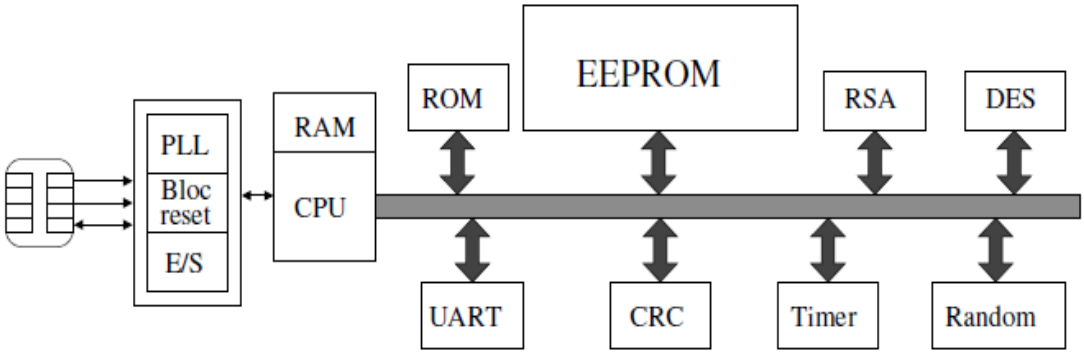


**Figure 1. 13: Architecture de la carte à puce à microprocesseur**

L'élément le plus important est le CPU ou le microprocesseur qui peut être un 8 bits, 16 bits ou 32 bits. Le deuxième élément caractéristique est la mémoire de stockage qui est l'EEPROM et qui a une taille de 1 Ko à 256 Ko. Son contenu est persistant et peut être initialisé à la phase d'initialisation de la carte et modifié en cours de son cycle de vie. La puce contient d'autres mémoires comme la ROM (Read-Only Memory) qui va contenir en général le système d'exploitation et le programme de la carte. Cette mémoire est créée et initialisée à la fabrication de la carte à puce et son contenu ne peut être changé au cours de son cycle de vie. La troisième mémoire est la RAM (Random-Access Memory) qui est utilisée par le CPU pour stocker les données de l'application et du système d'exploitation durant une session de travail avec la carte. Ces données seront perdues à la déconnexion électrique de la carte (contenu non persistant). On peut trouver également :

- L'interface de transmission de donnée en lecture et écriture sur une seule ligne comme décrit dans la partie 3 du standard ISO7816. Cette interface est intitulée UART (Universal Asynchronous Receiver-Transmitter) et elle peut fonctionner avec une vitesse de transmission adaptable

- La PLL (Phase Locked Loop) permet la génération de l'horloge interne atteignant les 20 Mhz qui est en générale différente et plus grande que l'horloge fournie qui est au maximum à 5 Mhz

- Le générateur de valeur aléatoire : Les valeurs aléatoires sont très utilisées dans le domaine de la sécurité et surtout dans l'authentification mutuelle entre la carte et le lecteur

- Le coprocesseur pour le calcul d'algorithme cryptographique : Que ce soit l'algorithme de cryptage symétrique comme DES ou l'algorithme de cryptage asymétrique comme RSA, la carte à puce a besoin de ces algorithmes pour assurer la sécurité de ces transactions. Ces calculs peuvent être confiés au microprocesseur de la carte mais un composant dédié va avoir une meilleure performance

- Le générateur de CRC : ce bloc sert à calculer une donnée qui permet de détecter des erreurs à l'émission.

- Le Timer dans une puce à microprocesseur connecté à l'horloge interne permet d'avoir un compteur programmable. Ce dernier peut avoir une capacité de 16 à 32 bits. Il peut déclencher une interruption matérielle au microprocesseur pour exécuter une tâche périodique et spécifique.

La carte à puce sans contact a la même architecture avec en plus un bloc gérant l'interface avec l'antenne. Cette interface a le rôle d'alimenter le circuit (Vcc, GND), de générer l'horloge (CLK), de communiquer dans les deux sens en lecture et en écriture (I/O) et enfin de générer le signal d'initialisation (RST).

#### 1.6.3.1. Application des cartes à puces

La carte à puce à base du microprocesseur permet :

- Le chiffrement de mail
- La signature électronique

- L’authentification forte

Une carte à microprocesseur contient un composant électronique ou puce dont l'architecture originale fait l'objet de brevets. Ce microprocesseur SPOM intègre dans une seule puce de silicium les éléments qui constituent un micro calculateur :

Un microprocesseur est constitué de l'unité de traitement et d'un coprocesseur cryptographique 8, 16, ou 32 bits (plus un coprocesseur cryptographique) SGS-Thomson, Siemens, Motorola, Hitachi, NEC, etc. et des mémoires. Une carte à microprocesseur embarque plusieurs types de mémoires, chacune d'entre elles a un usage bien spécifique :

- La mémoire volatile à accès rapide est utilisée pour exécuter le code, stockage de variables, allocations...etc : RAM (Random Access Memory), la taille de cette mémoire est réduite car très coûteuse, on peut trouver jusqu'à 2 Ko.

- La mémoire non-volatile à lecture seule contient l'OS : c'est la ROM (Read Only Memory), les plus importantes font 64 Ko.

- La mémoire non-volatile réinscriptible qui contient notamment les informations relatives au porteur de la carte et aux applications mises en œuvre. Plusieurs technologies existent, L'EPROM est devenue obsolète, on utilise plutôt de la Flash EEPROM (Electrical Erasable Programmable ROM) une mémoire électriquement effaçable ou de la FeRAM (ferroelectric RAM), une mémoire ferro-électrique à très faible consommation d'énergie particulièrement adaptée pour les cartes sans contact.

## 1.7. Familles de cartes à puces

On distingue aussi trois grandes familles de cartes qui se différencient par la technique utilisée pour communiquer avec le lecteur :

### 1.7.1. Carte à puce avec contact

Dans une carte à puce à contacts, la cadence de l’horloge varie entre 3.5 MHz et 5 MHz. L’alimentation se fait au moyen d’une source de tension de 3 à 5 volts.

La carte à contact nécessite un contact physique direct avec le lecteur au niveau du micromodule afin que l'alimentation et les commandes soient transmises.

Une carte à puce est connectée à l'ordinateur ou au contrôleur via un lecteur de carte qui obtient des informations de la carte à puce et transmet en conséquence les informations à l'ordinateur ou au contrôleur (Voir Figure (1.14)).


**Figure 1. 14 : Lecture d'une carte à puce avec contact**

### 1.7.2. Carte à puce sans contact

Carte à puce sans contact est constituée d'une puce et une antenne, elle permet la reconnaissance du porteur sans qu'il soit nécessaire d'introduire la carte dans un lecteur. La lecture se faisant à distance (quelques centimètres au plus). Encore très peu utilisée dans le cadre de programmes de fidélisation. La constitution de ce type de carte à puce est montrée sur la Figure (1.15).

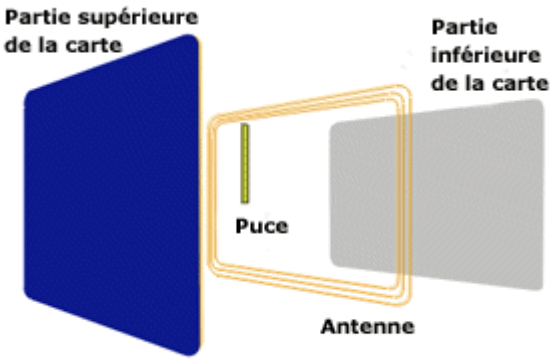


**Figure 1. 15 : Carte à puce sans contact**

Apparue en 1948 pour distinguer les avions amis de ceux des ennemis, l'identification par fréquence radio RFID (Radio frequency Identification) fut ensuite utilisée pour le suivi et la

gestion du bétail, par exemple le contrôle des moteurs réglant la quantité de la nourriture selon les caractéristiques individuelles de l'animal. Les éléments principaux sont une puce et une antenne.

L'alimentation de la puce en courant peut se faire soit à l'aide de piles, soit d'une façon passive par couplage inductif ou capacitif (Voir Figure (1.16)).

Les piles embarquées sont au Lithium, au charbon et manganèse ou exploitent l'effet photovoltaïque.

**Figure 1. 16 : Lecture d'une carte à puce sans contact**

### 1.7.2.1. Types des cartes à puces sans contact

Les deux technologies sont embarquées sur la même carte. Les types de cartes à puces sans contact sont :

- ✓ Cartes à puces à couplage très proche (quelques mm) (Close Coupling) : couvertes par les normes ISO 10536
- ✓ Cartes à puces à couplage de proximité (Proximity Coupling) (quelques cm) couvertes par les normes ISO 14 443.
- ✓ Cartes à puces à couplage éloigné ou de voisinage (Vicinity Coupling) (quelques dizaines de cm) couvertes par les normes ISO 15 693

### 1.7.2.2. Caractéristiques mécaniques des cartes à puces sans contact

Les caractéristiques mécaniques des cartes à puces peuvent se résumer comme suit :

1) La norme ISO 14 443-1 s'inspire de la norme ISO 7816-1

2) Les cartes de type ID1 (format carte bancaire)

3) L'antenne est constituée de fils qui longent le périmètre externe C

#### 1.7.2.3. Caractéristiques électriques des cartes à puces sans contact

La norme ISO 14 443-2 : Alimentation de la carte par transfert de puissance entre la carte et le lecteur au moyen d'un signal HF 13.56 MHz +/− 7 KHz  1.5 A/m ≤ le champ magnétique ≤ 6.5 A/m

#### 1.7.2.4. Avantages/Inconvénients des cartes à puces sans contact

Les principaux avantages des cartes sans contact sont :

- Absence de contacts susceptibles d'être salis ou endommagés
- Elles ne doivent pas être insérées dans un lecteur
    - Moins de possibilités de vandalisme sur les lecteurs
    - Plus rapide à manipuler, d'où un débit d'utilisateur potentiellement plus élevé

Mais ce système a aussi des inconvénients :

- Transfert assez lent
- Coût de fabrication plus élevé
- Les cartes peuvent être endommagées quand elles sont pliées (contiennent plusieurs composants répartis dans la carte
- La sécurité de transmission n'est pas assurée puisque susceptible d'être "entendue"

### 1.7.3. Les cartes hybrides

Il existe également des cartes hybrides, elles embarquent deux puces, la première reliée aux contacts, la deuxième à l'antenne. On fusionne donc deux cartes en une. Ces cartes sont le meilleur compromis car elles offrent les avantages des deux types de cartes à puces. Cependant elles héritent de leurs inconvénients en plus d'un prix beaucoup plus élevé. Un exemple d'une carte à puce hybride est donné dans la Figure (1.17) :

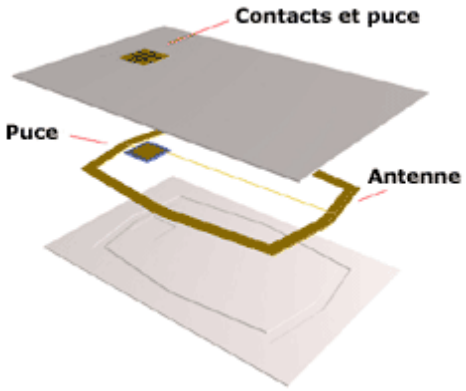


Figure 1. 17 : Carte à puce hybride

## 1.8. Applications des cartes à puces

Les applications des cartes à puces sont de plus en plus nombreuses mais elles apparaissent le plus souvent dans le classement suivant :

Les cartes de pré-paiement c'est la première utilisation des cartes à puces, aussi bien historiquement avec la télécarte que quantitativement pour l'enjeu économique qu'elles représentent. Leurs intérêts sont le paiement facile sans circulation d'argent liquide mais par unités d'achat spécifiques au service que l'on peut obtenir, et la certitude du paiement du service rendu. Bien que ces cartes soient souvent, pour des raisons économiques évidentes (faible coût de production), des cartes à logique câblée et mémoire à fusibles, donc non rechargeables, nous retrouvons ces applications dans les cartes à micro-processeur avec la possibilité supplémentaire de recharger des unités de paiement.

Les cartes de paiement sont les cartes bancaires et les porte-monnaie électroniques. Leur vente arrive en deuxième position après les télécartes. Les sommes d'argent échangées sont plus importantes et leur usage est applicable à toutes gammes de produits.

La carte à micro-processeur apporte les éléments nécessaires à l'identification et l'authentification du porteur et ajoute des contrôles plus fins comme le seuil de retrait d'argent liquide. Elle mémorise également toutes les transactions effectuées, ce qui est très important pour un fonctionnement déconnecté du système central.

Les cartes de contrôle d'accès permettent de sécuriser soit un accès physique comme l'entrée dans un bâtiment ou dans une salle, soit un accès logique tel que la connexion à un terminal d'ordinateur.

Les applications de type dossier portable commencent à se répandre. Elles consistent à mémoriser des informations concernant à la fois un individu et un domaine particulier. Nous pouvons citer les cartes Etudiant, les cartes santé et les cartes Ville de plus en plus nombreuses. Les avantages de ces cartes sont l'accès, seulement par des personnes habilitées, à des informations qui restent donc confidentielles, et la facilité d'utilisation pour le porteur. Cependant, de nouvelles générations d'applications apparaissent. Il s'agit des cartes pour la télévision cryptée et des cartes d'identification SIM (Suscriber Identifier Module) pour les téléphones mobiles GSM (Group System for Mobile).

## 1.9. Acteurs du marché

L'industrie de la carte à puce implique différents acteurs : les fondeurs fabriquent le hardware (les puces de silicium), les encarteurs fabriquent la carte proprement dite en intégrant la puce de silicium dans une carte plastique, les développeurs de système d'exploitation ou d'applets conçoivent les logiciels qui s'exécutent dans la carte à puce elle-même. Enfin, les fabricants de lecteurs fournissent aux intégrateurs et développeurs d'applications le matériel nécessaire pour s'interfacer avec la carte à puce.

STMicroelectronics est la seule société du marché à couvrir tout le cycle de production de cartes à puces, de la fabrication des plaquettes de silicium à la réalisation des cartes.

Les Acteurs en 2011 sont :

- Gemalto (Mariage Gemplus+Axalto 7 Décembre 2005)
- OberthurCardSystems
- Delarue
- Giesecke&Devrient
- Sagem Orga
- …

## 1.10. Marchés de la carte à puce

Les chiffres parlent d'eux-mêmes (source Eurosmart). En 1995, le marché des cartes à microprocesseur représentait environ 60 millions d'unités (environ 9 milliard en 2015) et le marché des cartes en logique câblées représentait environ 300 millions d'unités. Le marché français représentait alors la moitié du marché mondial en terme d'émission. C'est en 2000 que le nombre de cartes émis dans le monde est devenu supérieur à celui émis en France.

Les tendances de production des cartes à puce avec des puces de mémoire (cartes mémoire) et des cartes à puce avec des puces à microprocesseur (cartes à microcontrôleur) ces dernières années sont illustrées à la Figure (1.18).

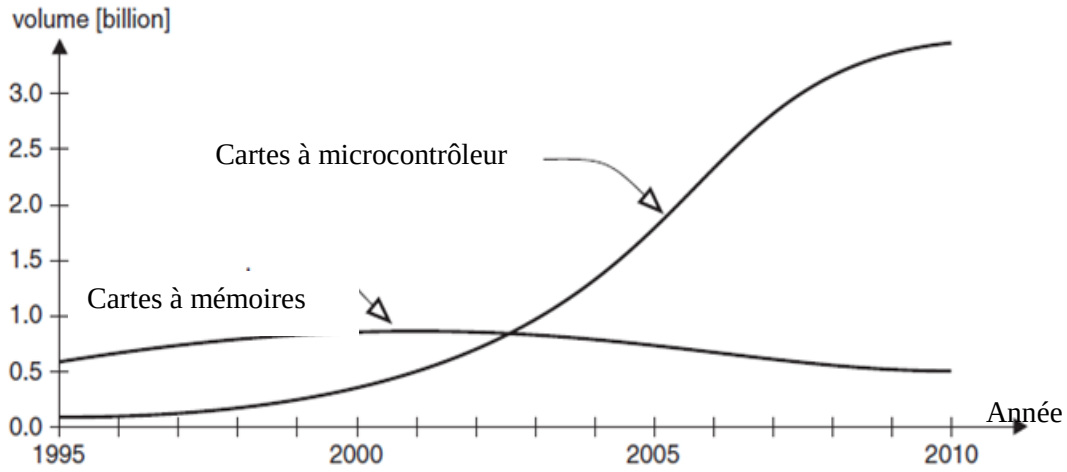


**Figure 1. 18 : Production des cartes à mémoire et carte à microprocesseur**

On remarque que, à partir de 2003 la production des cartes à microprocesseur dépassent la production des cartes à mémoires.

Le nombre de cartes à puces dans le monde en 2003, est de 2 milliards :

1) 52% de cartes à mémoire, dont 90% pour la téléphonie et 5% pour les transports
2) 48% de cartes à microprocesseur, dont 67% pour la téléphonie, 20% pour la banque, 6% pour la santé, 4%pour la télévision à péage

En 2020, l'Inde mis en œuvre des cartes à puce qui seront à la fois des cartes nationales d'identité et des porte-monnaies électroniques.

En Malaisie, depuis 2001, la carte à puce est à la fois un permis de conduire, une carte nationale d'identité, et une carte d'accès aux services de santé et des services bancaires.

L'identification des citoyens est assurée au moyen d'une photographie renforcée par le codage des empreintes digitales.

Le contrôle d'identité peut aujourd'hui s'appuyer sur de multiples preuves biologiques fournies par la numérisation des empreintes digitales, de l'image de l'iris et la reconnaissance vocale, chacune de ces techniques étant convertie en un format numérique pour l'authentification de la personne.

# Chapitre 2 : Technologie de fabrication des cartes à puces

## 2.1. Introduction

Le cœur d'une carte à puce est constitué d'un composant électronique monolithique en silicium introduit dans l'épaisseur d'une carte en plastique. Avant d'aborder les deux grandes familles de composants utilisés pour les cartes à logique câblée et celles à base de microprocesseur, nous donnons un aperçu sur les technologies qui permettent de réaliser ces puces, et nous expliquons les étapes de fabrication de ses différents éléments.

## 2.2. Technologies

Une carte à puces est constituée de trois éléments :

- Une carte en matière plastique (le plus souvent en PVC-Chlorure de Polyvinyle- ou ABS-Acrylonitrile-Budadiène-Styrène), possédant ou non une piste magnétique ;
- Un module électronique, supportant les contacts électriques ;
- Un circuit intégré en silicium.

Dans certaines applications, le circuit intégré possède une interface « sans contact », utilisant les mêmes principes que l'identification par radiofréquence (RFID). Dans ce cas, on utilise le principe de type transpondeur magnétique. Un lecteur envoie un signal radio à la carte qui elle-même contient une antenne déposée sur le substrat en plastique et connectée au circuit intégré. La puce est alors alimentée par le signal radio et va ainsi pouvoir communiquer avec le lecteur. Les intensités du champ magnétique ainsi créées sont comprises entre 1,5 et 7,5 A/m, la distance de fonctionnement entre le lecteur et la carte varie de 0 à 10 cm, la fréquence utilisée étant normalisée à 13,56 MHz. Cette technologie du « sans contact » trouve de nombreux champs d'applications tels que le paiement (y compris sur mobile), la billettique, les cartes d'identité, le contrôle d'accès, etc.

À la genèse des cartes à puces, deux filières technologiques étaient en présence selon le type de transistor utilisé pour réaliser les circuits logiques. D'un côté, la technologie dite bipolaire réalisant un effet d'amplification de courant par la diffusion de porteurs majoritaires

à travers les jonctions adjacentes de trois semi-conducteurs dopés. De l'autre côté, la technologie MOS (Metal Oxide Semiconductor) fondée sur des transistors unipolaires utilisant la conduction d'un seul type de porteurs dans un mince canal contrôlé par une électrode isolée. Suivant en cela la logique économique reprise par l'ensemble de l'industrie électronique, l'industrie de la carte à puces s'est ralliée massivement, dès l'origine, à la filière MOS. Les raisons principales sont, d'une part, des puissances consommées beaucoup plus faibles qu'en bipolaire, et d'autre part de très grandes capacités d'intégration. Au cours des deux dernières décennies, un autre avantage déterminant est l'évolution de la technologie CMOS (Complementary MOS), qui se traduit par une très faible consommation et une bonne immunité au bruit.

## 2.3. Semi-conducteurs pour cartes à puces

Les puces ne supportent pas les poussières. À l'échelle d'une puce, un grain de poussière représente un rocher qui bouche les chemins creusés pour la circulation des électrons (électricité). Pour cette raison, les lieux de fabrication des puces, les salles blanches, sont extrêmement propres. L'eau, l'air, les produits chimiques, de même que l'humidité et la température de la salle blanche doivent être rigoureusement contrôlés. Les opérateurs en salle blanche n'échappent pas à la règle. Ils portent une combinaison spéciale qui retient les particules organiques et les poussières.

Le silicium est obtenu à partir de sable blanc ou de quartz. Le sable est mélangé à du carbone en quantité appropriée. Le tout est introduit dans un four à arc. Sous l'action de l'arc, la température atteint 1600°C et la réaction suivante à lieu comme le montre la figure ci-dessous :

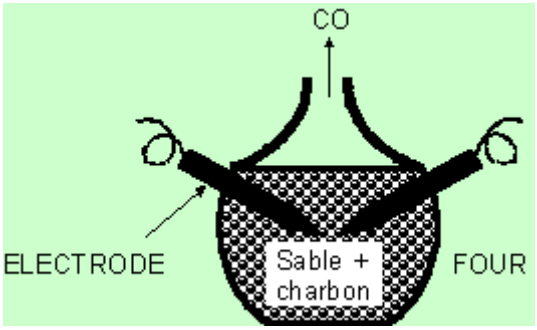


**Figure 2. 1 : Four à arc**

Le silicium ainsi obtenu s'appelle silicium métallurgique (Metallurgical Grade Silicon, MGS), sa pureté dépend du matériau de départ elle est de l'ordre de 98%. Pour obtenir du silicium de qualité électronique (Electronic Grade Silicon, EGS), il faut le purifier au point de ne plus avoir d'impuretés électroniquement actives. Ce qui veut dire qu'il faut obtenir un matériau qui contient une impureté indésirable pour un milliard d'atomes de silicium.

**Figure 2. 2 : Lingots de polysilicium**

Les composants sont réalisés par les fabricants de semiconducteurs à partir de tranches circulaires de silicium en utilisant une série de masques pour réaliser la photolithogravure des circuits. Une même tranche (ou wafer) de huit pouces de diamètre peut ainsi contenir plusieurs milliers de puces rectangulaires, qu'il faut découper à l'aide de scies diamantées. Des machines automatiques viennent ensuite prélever ces puces pour les fixer au dos des modules, dans une cavité qui a été ménagée à cet effet. C'est l'opération dite de « die bonding ».

## 2.4. Fabrication des puces

La fabrication de la puce électronique suit le même processus de fabrication d'un circuit intégré depuis le développement jusqu'à son extraction du Wafer.

Le développement de la puce est réalisé à l'aide d'outils de CAO qui permettent de générer les masques. Ces derniers servent à faire des gravures sur le Wafer pour produire la fonction souhaitée. Après avoir testé la puce sur Wafer, le processus de sciage et puis l'extraction des puces sont entamés (voir la Figure ci-dessous).

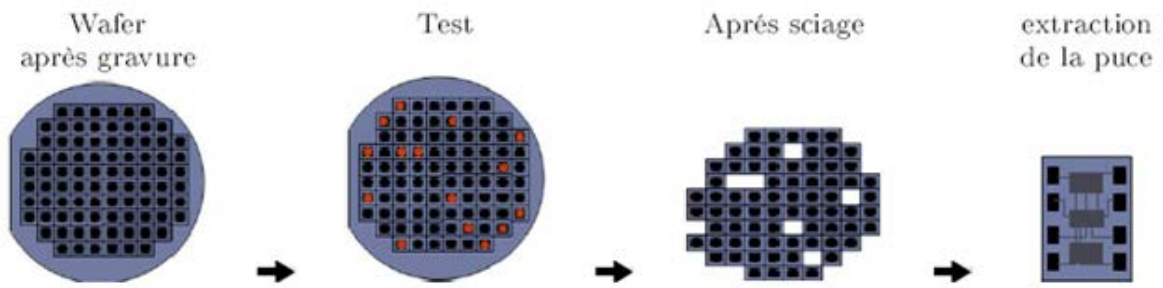


Figure 2. 3 : Etape de fabrication et extraction de la puce

Après l'extraction, chaque puce testée est intégrée dans un module de protection et de contact.

Les puces sont fabriquées sur des disques de silicium de 2 à 30 cm² et 0,2 à 0,7 mm d'épaisseur, appelés wafers.

Les phases de production de cartes à puces seront résumées dans la section suivante :

**PHASE 1 : Création des barres de silicium**

Le processus initial nécessite une graine de cristal de silicium. C'est en fait la forme la plus minuscule d'une structure cristalline qui a toutes les facettes d'un cristal complet. Elle mesure entre 1mm et 3 mm.

Ce processus de traction peut durer jusqu'à 24 heures et le diamètre du cylindre obtenu sera supérieur au diamètre nécessaire. Il sera par la suite rectifié et découpé en tranches. Ces tranches sont appelées wafers.


Figure 2. 4 : Barres de silicium a) : Les barres une fois refroidies ;b) : Découpage en wafer

**PHASE 2 : Création des masques**

Le processus de fabrication d'un semi-conducteur est basé sur l'utilisation d'un procédé photographique pour réaliser le masque de chaque couche. Selon la complexité du circuit intégré, il peut y avoir jusqu'à 24 couches ! Le masque de chaque couche est identique à un négatif photographique, il est obtenu en "taillant" au laser une couche de chrome déposée sur une plaque de quartz d'une extrême pureté. Chaque couche correspond à un schéma électronique. Plus le nombre de transistors à "graver" sur ces plaques augmente plus le temps de fabrication augmente.

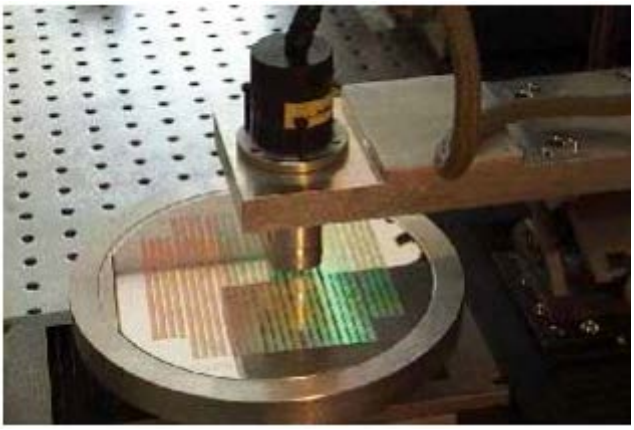

Figure 2. 5 : Gravure

**PHASE 3 : Épitaxie**

L'épitaxie est une étape consistant à faire croître du cristal sur le cristal (le silicium dans notre cas) par un apport d'éléments constituant la nouvelle couche appelée épicouche.

Figure 2. 6 : Machine pour l'épitaxie

**PHASE 4 : Oxydation et exposition**

Cette étape a pour but de créer le support des transistors. L'épi-couche est chauffée afin de développer une couche d'oxyde de silicium. Un vernis photosensible est ensuite déposé sur l'oxyde.

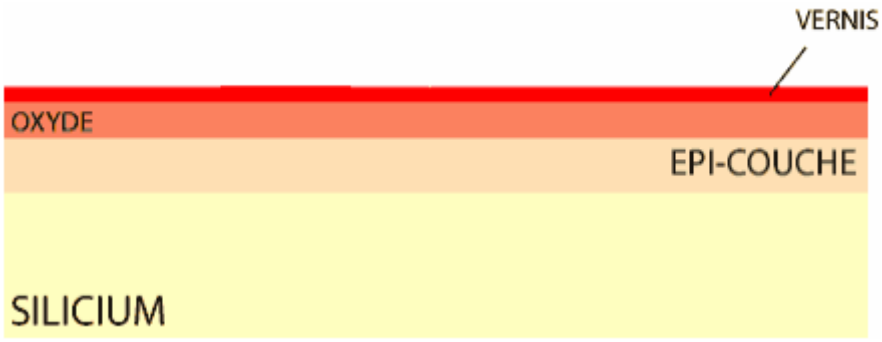


Figure 2. 7 : Oxydation

**PHASE 5 : Photolithographie**

La photolithographie est une technique permettant de projeter à l'aide d'une source lumineuse, une image sur un support photosensible afin de l'y imprimer.

Figure 2. 8 : Machine de la lithographie

Dans le cas des semi-conducteurs, la source lumineuse est un laser. Il produit un rayon invisible à l'œil humain qui se situe dans le domaine de l'ultraviolet. Ce laser projette l'image sur le wafer, marquant ainsi le vernis photosensible.

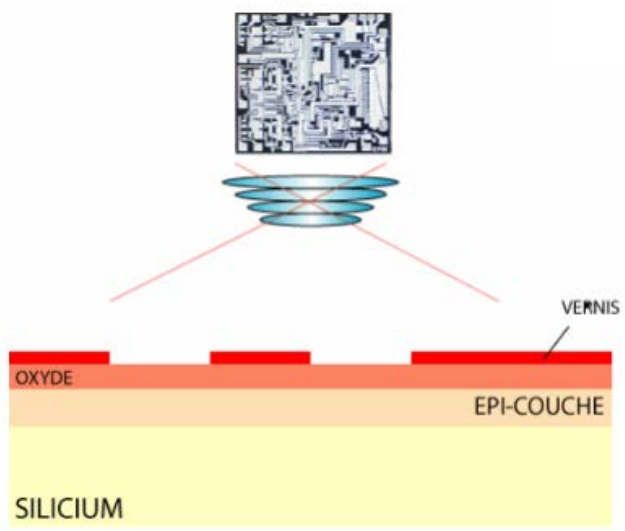


Figure 2. 9 : Projection de l'image sur le wafer

**PHASE 6 : Excavation et dépouillage**

L'excavation au plasma est une technique de creusage des zones qui ont été touchées par la photolithographie.

Ainsi, les zones où le vernis a été touché par la photolithographie permettent l'accès direct à la couche d'oxyde qui est alors creusée par le plasma. Bien sûr, les zones d'oxyde de silicium recouvertes par le vernis ne sont pas modifiées. Le profil de la couche d'oxyde devient ainsi identique à celle du vernis restant.

Figure 2. 10 : Machine d'excavation et dépouillage

**PHASE 7 : Dopage**

Cette étape a pour but de charger électriquement les zones de l'epi-couche mises à nu par la phase d'excavation. Ce procédé est connu sous le nom de "dopage", les molécules de dopant sont implantées dans la surface du silicium par un faisceau d'ions de haute intensité. Les ions

pénètrent le silicium verticalement. Ces régions sont maintenant chargées en ions, créant ainsi l'entrée et la sortie du transistor dans l'epi-couche de silicium.

Figure 2. 11 : Machine utilisée au dopage

Sur la figure ci-dessous on donne le schéma du dopage des zones de l'epi-couche.

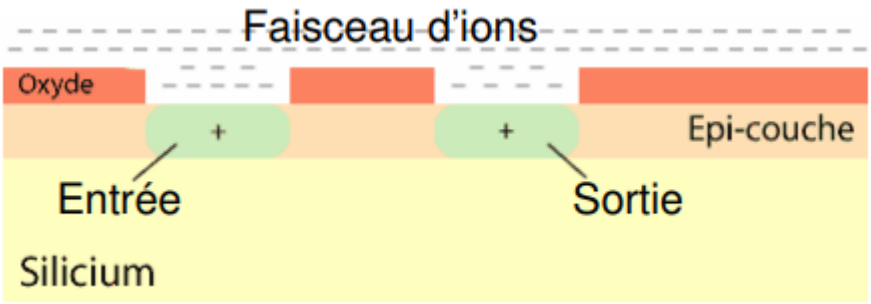


Figure 2. 12 : Dopage des zones de l'epi-couche

**PHASE 8 : Dépôt**

- Cette étape a pour but de créer la grille du transistor.
- La grille est pulvérisée sous forme gazeuse aux alentours de 1000ºC. Cette couche est fine afin de pouvoir laisser passer le champ magnétique créé par la grille du transistor. Ce champ créera le canal conducteur entre l'entrée et la sortie contrôlant le passage du courant électrique.
- Le transistor est maintenant opérationnel.

Figure 2. 13 : Machine utilisée pour le dépôt

Sur la figure (2.14) nous donnons le schéma du transistor avec dépôt de la grille.

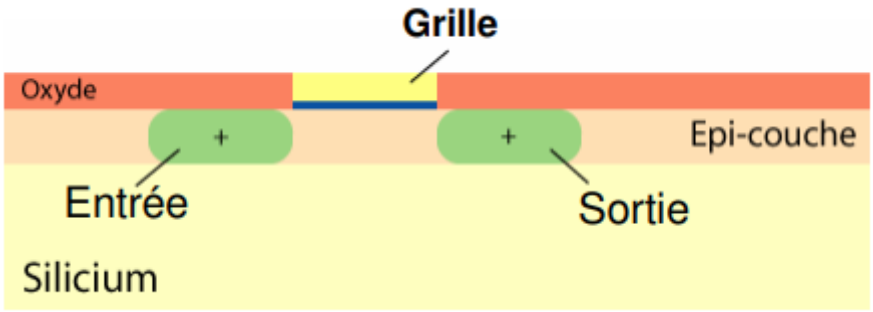


Figure 2. 14 : Dépôt de la grille du transistor

**PHASE 9 : Oxydation**

Dans cette phase il est nécessaire de :

- Pouvoir connecter ces transistors entre eux.
- Déposer une couche d'isolant pour séparer les futures couches de connections.

Sur la figure (2.15) on montre le dépôt de l'isolant.

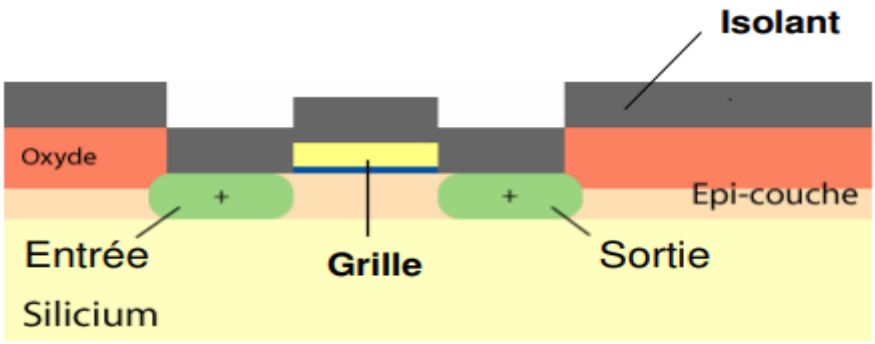


Figure 2. 15 : Dépôt de l'isolant

**PHASE 10 : Connexion des transistors**

- Cette étape permet de créer les bornes des transistors qui seront reliés aux autres transistors de la même couche. La couche d'isolant est "taillée" de la même façon que la couche d'oxyde de silicium initiale mais avec des masques différents, afin de laisser des zones creuses où l'on déposera un élément conducteur : l'aluminium.

- Il suffira ensuite de vernir l'aluminium puis de réutiliser le processus de photolithographie afin de supprimer les zones où l'aluminium n'est pas requis.

- Une couche d'isolant est ensuite déposée pour isoler cette couche de composants des couches suivantes.

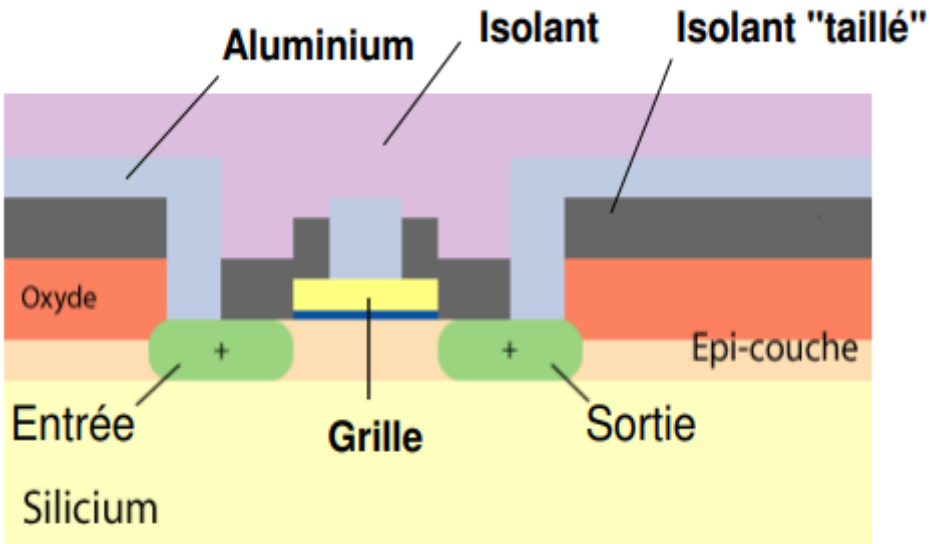


Figure 2. 16 : Création des bornes

**PHASE 11 : Polissage**

C’est un processus qui emploie un abrasif suspendu dans une boue chimique appliquée par des disques rotatifs sur la surface à traiter.

Après le polissage, la surface de l'isolant est parfaitement plane et peut accueillir une autre couche de connexion en aluminium.

Sur la figure (2.17) nous affichons la machine utilisée pour le polissage.

**Figure 2. 17: Machine utilisée pour le polissage**

Après le polissage, on obtient le wafer représenté par la figure (2.18).

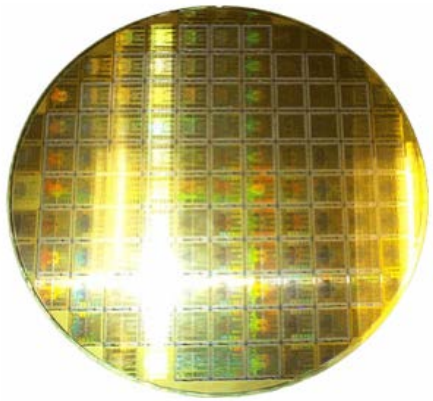

**Figure 2. 18 : Wafer**

**PHASE 12 : Interconnexion des composants**

Afin d'assurer les interconnections des différentes couches, la couche d'isolant venant d'être polie est vernie puis photolithographiée et excavée pour créer des trous qui seront remplis de tungstène ou de titane-tungstène. Ces points de connexion fournissent le moyen de raccordement électrique entre deux couches d'aluminium.

La prochaine couche d'aluminium peut être ensuite déposée, vernie puis excavée et ainsi de suite suivant le nombre de couches d'interconnexions nécessaire au wafer.

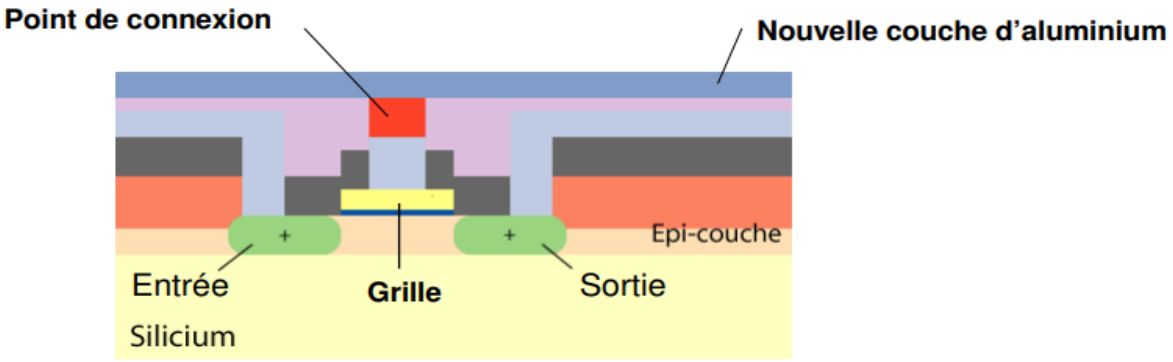


Figure 2. 19 : Interconnexion des bornes

**PHASE 13 : Inspection du wafer**

Il s'agit d'une étape critique du processus global de fabrication du wafer. En effet, il doit être inspecté minutieusement à l'aide de microscopes électroniques à balayage. Les dimensions de certaines parties du wafer descendent en dessous de 0,2 µm. L'inspection devient de plus en plus longue et complexe.

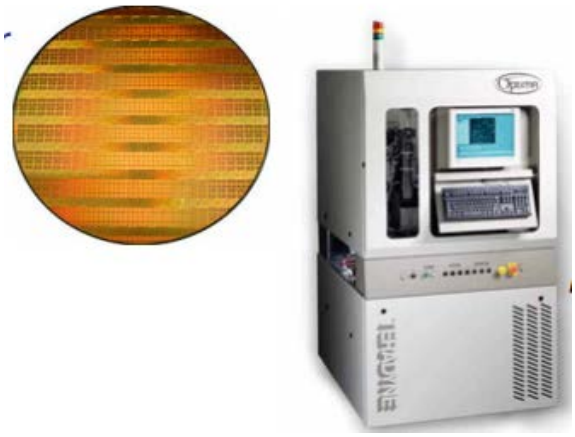

Figure 2. 20 : Microscope pour inspection

**PHASE 14 : Test**

C'est au moment du test du wafer que l'on vérifie la correspondance entre le cahier des charges initial et le fonctionnement final du composant :

– Un chariot de transport aligne le wafer avec précision sous l'ensemble de contacts constituant la carte de test.

– Une fine sonde électrique connecte les différentes entrées, sorties et modules d'alimentation à la carte de test.

– L'appareil de contrôle vérifie le fonctionnement global du circuit.

Un wafer contient plusieurs puces identiques. Les puces défectueuses sont repérées et marquées.

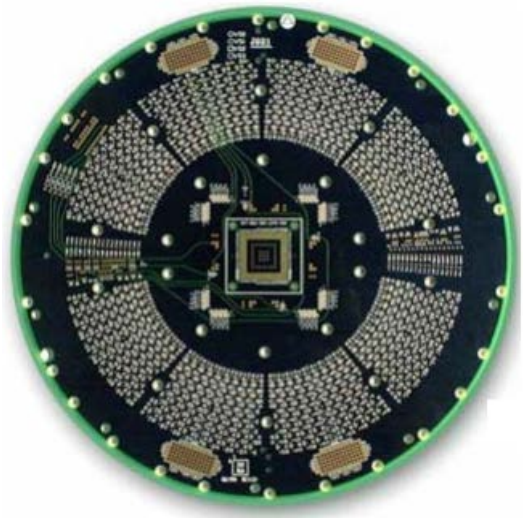

**Figure 2. 21 : Carte de test**

**PHASE 15 : Mise en place dans la puce**

- Les puces défectueuses sont tout d'abord isolées, puis les bonnes sont sciées et collées à l'armature du boîtier final.

- Chaque point de contact de la puce sera relié aux pattes externes du boîtier final par des fils d'or ou d'aluminium d'approximativement 25 µm. Ces fils sont implantés par un système qui place le bout du fil sur la zone et applique une vibration ultrasonique pour le souder.

**PHASE 16 : Qualification**

- Une fois la puce mise dans son boîtier, on procède au test final du composant.
- Cette phase est quasiment identique à la phase 14, à la différence que les puces sont testées plusieurs fois et à différentes températures.
- C'est à cette étape que l'on détermine, par exemple, que la puce qui sort de la chaîne sera un Pentium à 2.4 GHz, à 2.8 GHz ou seulement à 1.6 GHz.

## 2.5. Étapes de construction d'une carte à puce

Le processus de production de la carte à puce implique un certain nombre d'activités réalisées à l'aide de technologies de fabrication. Le processus de production est divisé en quatre étapes :

1) La première étape implique la spécification de la taille de la mémoire de la puce, la vitesse d'horloge, les types de mémoire volatile, le type de système d'exploitation et la spécification du logiciel d'application, le type, la taille et le fonctionnement de la carte.
2) La deuxième étape consiste à fabriquer des puces. Cela implique de monter la puce de silicium sur un substrat en verre époxy avec des connecteurs plaqués or, en utilisant une matrice. La puce de silicium est liée aux connecteurs en utilisant des fils de connexion (technique de liaison par fil) ou en utilisant la technologie de puce retournée (en utilisant une soudure). Le substrat de la puce est ensuite scellé à l'aide de résine époxy et collé sur le substrat de la carte. Le substrat de carte peut être une carte plastique à base de PVC ou une carte à base de polyester.
3) La troisième étape consiste à charger le code dans la mémoire en utilisant des commandes spéciales.
4) La quatrième étape consiste à charger des données dans la mémoire PROM de telle sorte que les données concernent une seule personne.

## 2.6. Fabrication du corps de la carte

La production du corps de la carte peut elle-même être divisée en plusieurs étapes, en fonction des technologies utilisées et des caractéristiques de la carte.

Le processus de fabrication du corps de carte commence par la sélection du matériau, la technologie de l'impression, la plastification ou moulage par injection du corps de carte dans la première phase et suivi de la personnalisation de la carte. Nous allons donner un aperçu de chaque étape pour fournir des connaissances de base sur le processus de fabrication de la carte à puce.

### 2.6.1. Sélection du matériau

Le choix des matériaux dépend des exigences du client. Les cartes PVC sont utilisées si le client a besoin d'un matériau recyclable à faible coût. De plus, un corps de carte en PVC est utilisé si le client exige une stabilité à haute température et une résistance mécanique élevée.

Le matériau Acrylonitrile butadiène styrène (ABS) est utilisé lorsque la stabilité de la température et le recyclage sont les principales exigences du client, avec un processus de moulage par injection. Le polyéthylène téréphtalate (PETG) est le meilleur choix si le client exige le matériau le plus respectueux de l'environnement, mais ce matériau est proposé à un prix moyen.

Le matériau de base utilisé pour les cartes est fourni sous forme de feuille pour le laminage. Le matériau classique utilisé est le PVC, mais en raison de problèmes environnementales et de conditions de vie plus longues, d'autres matériaux gagnent en importance. Sur le Tableau (2.1) nous donnons un bref aperçu sur les matériaux utilisés.

**Tableau 2. 1 : Matériaux pour la carte**

| Matériaux | Avantage (+)/inconvénients (-) |
|---|---|
| PVC | (+) Prix bas, nombreuses années d'expérience, recyclage possible<br>(-) Compatibilité environnementale, stabilité thermique limitée |
| PC | (+) stabilité à haute température et résistance mécanique, recyclage possible<br>(-) prix élevé, faible résistance aux rayures (scratch) |
| ABS | (+) moulage par injection approprié, stabilité à la température, recyclage possible<br>(-) n'est pas conforme à la norme ISO, n'est pas classé comme écologique |
| PETG | (+) meilleur matériau concernant la compatibilité environnementale, prix moyen, recyclage possible<br>(-) processus pas aussi facile et aussi connu que pour le PVC |

Ils doivent remplir de nombreux critères particuliers pour les applications des cartes. Quelques critères du choix des matériaux seront résumés comme suit :

- Possibilité de laminage et moulage par injection
- Précision à la taille
- Imprimabilité
- Qualité optique et constance des couleurs
- Fermeté mécanique
- Durée de vie
- Stabilité thermique
- Résistance à l'humidité
- Stabilité du solvant
- Anti-statique
- Physiologiquement inoffensive
- Compatibilité environnementale pendant la production et l'utilisation

### 2.6.2. Technologies d'impression

Après la sélection du matériau, vient l'étape du choix de la technologie d'impression. Il existe différents types de technologies d'impression : impression offset, sérigraphie, impression numérique, etc.

- L'impression offset est la technique d'impression la plus utilisée dans laquelle ils utilisent des plaques d'impression à quatre couleurs ou à cinq couleurs. Ces plaques sont montées sur le cylindre d'impression de la machine, qui tourne continuellement contre un rouleau amortisseur et des rouleaux encreurs, comme illustré à la Figure (2.22).
- La sérigraphie est une technologie plus ancienne et n'est pas fréquemment utilisée dans la production en raison de son taux de production plus lent.
- L'impression numérique est rarement utilisée dans la production en raison de son coût de production le plus élevé. L'impression numérique présente l'avantage de pouvoir imprimer chaque carte de manière unique.

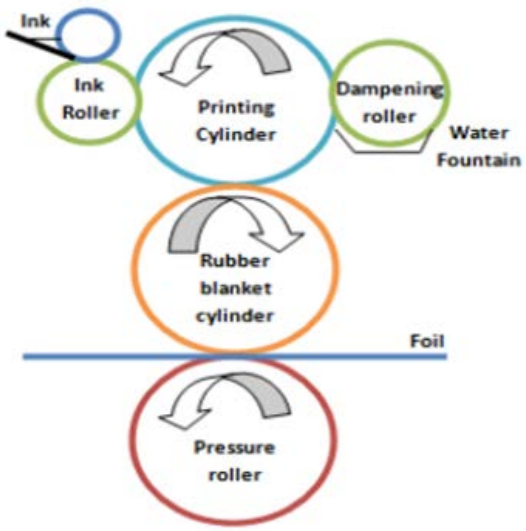


**Figure 2. 22 : Impression Offset**

### 2.6.2.1. Laminage

Les feuilles de plastique imprimées, ainsi que les couches internes des cartes, sont rassemblées et alignées dans une structure en sandwich. Les couches peuvent être de différents types et fonctions, notamment :

- Feuille extérieure sur laquelle le recto de l'illustration de la carte est imprimé
- Feuille extérieure sur laquelle le verso de l'illustration de la carte est imprimé
- Des feuilles de recouvrement transparentes, pour protéger les feuilles imprimées des égratignures et de l'abrasion, pour donner une finition brillante
- Les feuilles de noyau en plastique en PVC, ABS, Teslin ou d'autres matériaux qui ajoutent l'épaisseur requise au corps de la carte ou peuvent servir de matériau de base optimal pour la prochaine étape de personnalisation, telle que la gravure au laser.
- Feuille magnétique
- Feuilles contenant des antennes sans contact et des puces
- Films de sécurité contenant des hologrammes ou d'autres éléments de sécurité.
- Incrustation (Inlay en anglais) contenant des composants électroniques tels que batterie, LED (Light Emitting Diode), écran LCD, boutons, capteurs d'empreintes digitales ou avertisseurs sonores.

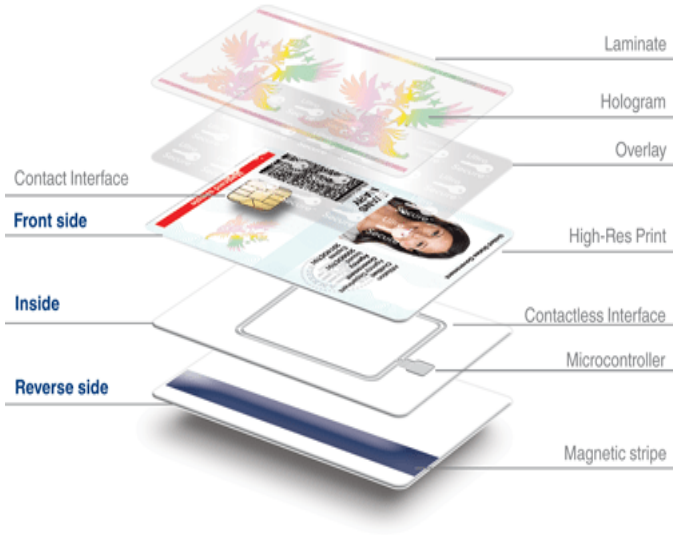


**Figure 2. 23 : Couches d'une carte à puce**

La composition la plus courante est constituée de cartes à quatre et cinq couches. Pour les cartes sans contact et les cartes d'identité, jusqu'à neuf couches sont assemblées. Quels que soient le nombre de couches utilisées, les paramètres physiques d'une carte étant définis par les cartes d'identification ISO / IEC 7810

- Caractéristiques physiques :

L'épaisseur de la feuille doit être de 0,76 mm (± 0,08 mm). Les cartes contenant des composants électroniques tels que des piles, des écrans LCD, des boutons ou des capteurs d'empreintes digitales sont généralement plus épaisses que les 0,76 mm spécifiés.

### 2.6.2.2. Fonctions spéciales / Add-ons

Il existe différents types d'add-ons qui sont utilisés lors de la création du corps de la carte, selon les besoins du client. Il existe principalement cinq types d'éléments de cartes supplémentaires : panneau de signature, bande magnétique, hologramme, microtexte et texte ultraviolet.

a) Panneau de signature

Un panneau de signature est utilisé dans toutes les cartes bancaires, car l'utilisateur doit signer sa carte avant de l'utiliser.

Les panneaux de signature sont appliqués avec deux techniques différentes : plastification ou estampage à chaud.

Les panneaux de signature en papier sont montés sur la feuille de recouvrement extérieure d'une carte et se connecteront à la surface de la carte pendant le processus de laminage. Une autre option consiste à créer des feuilles de superposition avec un panneau de signature imprimé en utilisant des couleurs spéciales dans un processus de sérigraphie. Encore une fois, cette couche sera appliquée dans un processus de stratification.

La technique de marquage à chaud fonctionne avec des éléments préfabriqués qui sont transférés d'un ruban porteur au corps de la carte par l'utilisation d'un tampon chauffé. Les éléments, tels que les panneaux de signature, sont recouverts d'un adhésif qui s'active sous l'effet de la chaleur et de la pression. Sous l'estampage à chaud, l'élément adhère à la surface de la carte et perd à son tour son lien avec le ruban porteur.

b) Bande magnétique

La bande magnétique est considérée comme l'élément principal des cartes de paiement traditionnelles. La figure suivante illustre le panneau de signature et la bande magnétique sur une carte bancaire.

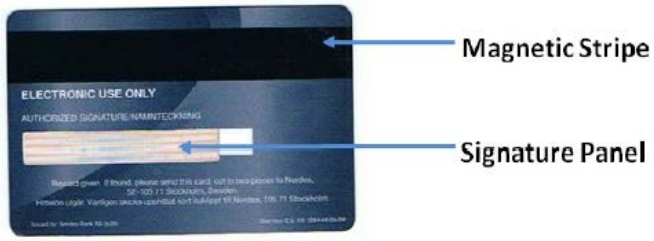


**Figure 2. 24 : Panneau de signature et la bande magnétique**

c) Hologramme

Un hologramme est utilisé comme élément de sécurité. Aujourd'hui, un hologramme est utilisé dans toutes les cartes de crédit ou de débit.

Un hologramme est une forme de photographie avancée qui permet d'enregistrer une image en trois dimensions.

Pourquoi utiliser un hologramme comme outil de renforcement de la sécurité ?

3) Il n'est pas possible de dupliquer un hologramme avec un scanner ou une photocopieuse couleur

4) Il n'est pas possible de fabriquer ou de copier un hologramme avec des procédés d'impression standard

5) Les niveaux initiaux de sécurité visuelle peuvent être utilisés pour intégrer des niveaux de contrôle supplémentaires pour une carte.

Comment intégrer un hologramme sur une carte ?

Un hologramme est appliqué sur la carte sous forme de couche transparente, grâce à un ruban spécial.

Evolis propose quatre types de rubans hologrammes :

1. Le ruban continu générique de vernis Genuine Globes pour les imprimantes à transfert thermique
2. Le ruban de vernis Globe générique enregistré pour le laminage
3. Le ruban de correction Globe générique pour le laminage

### 2.6.2.3. Guilloche

Le graphique guilloché fait référence à des motifs de ligne complexes formés de deux autres courbes lignes tracées selon des principes mathématiques. Les motifs en guillochis fournissent une protection anti-contrefaçon. Elles sont utilisées dans presque tous les billets dans le monde entier.


**Figure 2. 25 : Exemple de carte à puce à guilloche**

#### 1.2.1.1 Le microtexte et le texte ultraviolet

Le microtexte et le texte ultraviolet sont des éléments de sécurité fournis par les fabricants en complément de la demande du client. Le microtexte ne peut pas être lu à l'œil nu. Cela

ressemble à une simple ligne, donc il faut une loupe pour le lire. Pour lire le texte ultraviolet, il faut une lumière ultraviolette car cette impression utilise un type d'encre spécial qui ne peut être vu que sous une lumière ultraviolette. Un exemple d'une carte à puce à micro texte est donné sur la figure ci-dessous :


**Figure 2. 26 : Exemple de carte à puce à microtexte**

## 2.7. Fabrication de la carte à puce sans contact

La fabrication de la carte à puce sans contact suit les mêmes premières étapes que la carte à puce à contact. Cette dernière n'a pas besoin de module de contact et donc la deuxième et la troisième partie de fabrication sont différentes. Les étapes de fabrication industrielle classique sont au nombre de trois et sont décrites dans ce qui suit :

1) La réalisation de l'antenne sur un support diélectrique plastique (polychlorure de vinyle (PVC), polyesters (PET), polycarbonate (PC)...) utilisant la gravure chimique du cuivre ou de l'aluminium
2) La connexion des plots de contact de la puce sur les plots de contact de l'antenne à l'aide d'encre ou d'époxy ou de polymères conducteurs, appelée communément technique de report flip-chip
3) Le laminage sous pression à chaud des deux couches plastiques inférieure et supérieure du corps de carte (PVC, PET, PC, acrylonitrile-butadiène-styrène (ABS)...), sur le support de l'antenne afin de former une carte monobloc.

## 2.8. Interconnexion des composants

Cette opération consiste à relier électriquement les plots du composant aux contacts électriques du module. Ce câblage peut se faire selon plusieurs techniques de base :

1) Liaison filaire (Wirebonding en anglais) se fait en utilisant du fil d'or ou d'aluminium, dont le diamètre est voisin de 10µm à 20µm et dont les soudures sur les plots des composants sont réalisées par thermo compression ou ultrason. La répétition des soudures est nécessaire pour chaque extrémité du fil

2) Liaison automatisée TAB (Tap Automated Bonding) utilise un ruban continu découpé et soudé directement

3) Grille métallique semblable à celle des composants classiques avec un raccordement en fils. Les modules câblés sont protégés par une résine d'enrobage avant d'être encartés.

La Figure (2.27) montre la partie assemblage de la puce sur la partie métallique en liant les pattes de la puce avec les pattes du module de protection (face A). La connexion se fait à l'aide d'un fil de faible résistance comme l'or par exemple. Cette partie est couverte par une résine afin de protéger les connexions. La face B va servir comme support de contact externe de la puce pour se connecter au lecteur.

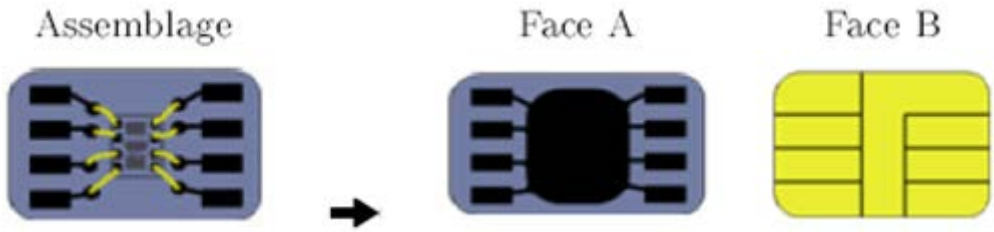


**Figure 2. 27 : Réalisation du module de la puce**

## 2.9. Encartage (chip embedding)

Une carte à puce se distingue par l'encartage d'une puce électronique cachée sous ce qu'on appelle un bouton (en général doré) qui tient lieu de connecteur vis à vis du monde extérieur.

La dernière étape de la fabrication de la carte à puce est d'insérer le module dans la carte en PVC. A partir d'une carte vierge, une cavité est creusée afin que le module de la puce soit inséré et collé (Voir Figure (2.28)). Les cartes en PVC peuvent être préparées directement avec une cavité pour faciliter l'insertion du module.

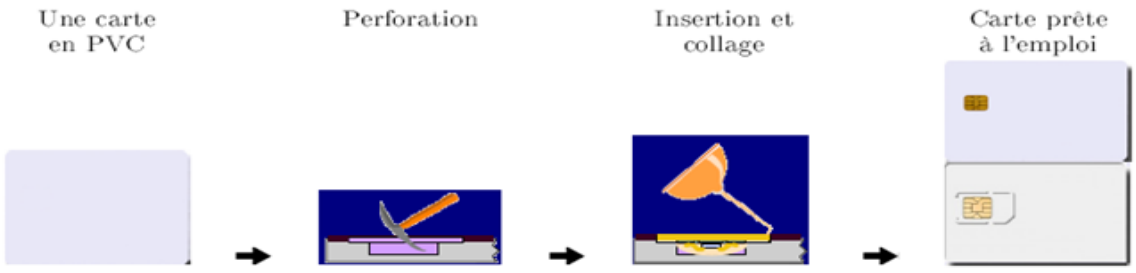


Figure 2. 28 : Procédés de préparation de la carte à puce

Les encarteurs fait l'insertion de la puce dans le plastique (encartage)

- C'est l'assemblage de la puce, du micromodule et du support plastique
- Test et pré-personnalisation (inscription du numéro de série de la carte)

4) Consiste à fixer par collage le module électronique dans la carte

5) Les modules sont encartés à l'aide de chaine industrielle robotisée

L'incorporation d'une puce semi-conductrice dans le corps de la carte est un processus très sensible.

Trois techniques sont utilisées pour intégrer la puce dans un corps de carte à puce. Ces techniques sont :

1. Enrobage par technologie de laminage,
2. L'intégration par la technologie de montage
3. Technologie dans le moule.

La technologie de montage est largement utilisée dans le processus de fabrication et est discutée plus en détail dans la section suivante :

Après la préparation du module de la carte à puce, l'étape suivante consiste à l'intégrer dans le corps de la carte ; ce qui peut être fait par un processus de fraisage (milling en anglais). Une fraiseuse est utilisée pour créer une cavité de puce dans le corps de la carte. Une machine d'implantation est ensuite utilisée pour coller le module de puce dans le corps de la carte.

Pour vérifier l'intégrité, un test de réponse à la demande (ATR) est effectué lors de l'implantation. Parfois, une imprimante à jet d'encre est utilisée pour imprimer des informations supplémentaires sur la carte, si le client demande cette impression.

## 2.10. Connectique

Le module électronique supporte les contacts qui assurent les différentes liaisons électriques avec le monde extérieur.

La qualité des contacts est liée à la conception du connecteur

1) Connecteurs frottant : peuvent entrainer des actions abrasives néfastes
2) Connecteurs à contacts « atterrissant », qui ont une fiabilité supérieure sans endommager les cartes

# Chapitre 3 : Cryptographie et sécurité de la carte à puce

## 3.1. Introduction

La sécurité et la protection de la vie privée sont des éléments clés de l'industrie. Elle a donné naissance à une importante activité économique qui touche la fabrication de composants électroniques, le développement de logiciels, les processus de personnalisation et de distribution, les machines-outils, les périphériques, le développement d'applications, les tests de conformité, les tests de sécurité, etc.

Dans ce chapitre on va donner quelques éléments essentiels à la compréhension de la cryptologie, et les méthodes principales de cryptographie utilisées pour assurer la sécurité des cartes à puces, avec un aperçu sur les attaques qui cherchent de nuire la sécurité afin d'accéder au contenu.

## 3.2. Principes de la cryptographie

La cryptographie est l'art de chiffrer et déchiffrer les messages échangés entre un émetteur et un récepteur.

Le chiffrement des messages consiste à transformer une information à l'aide d'une convention secrète. La fonction de transformation constitue l'algorithme cryptographique, dont le secret réside dans des paramètres appelés clés. Lorsque l'on déchiffre le message, on réalise l'opération inverse en connaissant ces clés. Dans les cartes à puces, la cryptographie met en œuvre divers mécanismes qui ont pour but d'assurer soit la confidentialité des informations, soit l'authentification des cartes ou des utilisateurs, soit encore la signature des messages. L'ensemble des moyens mettant en œuvre la cryptographie forme un cryptosystème. Seules les cartes dotées d'un crypto processeurs permettent de gérer le chiffrement asymétrique. II en existe trois catégories selon qu'ils sont symétriques, asymétriques ou « à apport nul de connaissance ».

1) **Symétrique** qui utilise la même clé pour le chiffrement et le déchiffrement (DES, AES)

2) **Asymétrique** avec une clé publique et une clé privée générées par une procédure mathématique comme dans l'algorithme RSA

3) **A apport nul de connaissance**

## 3.3. La cryptographie classique

Dans cette section on va aborder quelques types de la cryptographie classique :

1) Le chiffrement par substitution

2) Le chiffrement par transposition

### 3.3.1. Chiffrement par substitution

Dans la méthode de chiffrement par substitution, à chaque lettre ou groupe de lettres on substitue une autre lettre ou un autre groupe de lettres. La substitution simple (substitution mono alphabétique). Nous identifions quatre types de chiffrement par substitution.

#### 3.3.1.1. Chiffrement de César

Le chiffrement de César consiste à décaler les lettres de 3 positions.

Exemple

Texte en claire : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

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

Le message " hello wold " devient « khoorzrog »

- Il n'existe que 26 décalages possibles
- Le chiffrement de César est très vulnérable à l'analyse des fréquences

#### 3.3.1.2. Chiffrement par substitution

À chaque lettre de l'alphabet en clair, on associe une lettre au hasard.

Exemple

Texte en claire : a b c d e f g h i j k l m n o p q r s t u v w x y z

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

| a | b | c | d | e | f | g | h | i | g | k | l | m | n | o | p | k | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| U | X | O | M | P | S | N | B | E | A | Z | Q | W | D | G | V | K | H | C | R | T | Y | I | F | J | L |

Le message " hello wold " devient « BPQQG IGHQM »

### 3.3.1.3. Substitution polyalphabétique

Le principe consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prise dans ou plusieurs alphabets aléatoires associés. Par exemple, on pourra utiliser n substitutions monoalphabétiques ; celle qui est utilisée dépend de la position du caractère à chiffrer dans le texte en clair. On choisit une clé qui sert d'entrée dans la grille polyalphabétique incluant autant de symboles qu'il y a de lettres différentes à chiffrer. Chaque caractère de la clé désigne une lettre particulière dans la grille de codage. Pour coder un caractère, on doit lire le caractère correspondant du texte en clair en utilisant la grille polyalphabétique et le mot clé associé dans l'ordre séquentiel (on répète la clé si le chiffrement se fait par la méthode de VIGENERE et de BEAUFORT. L'illustration la plus simple qui corresponde à ce principe est l'utilisation d'une fonction à base de ou exclusif (XOR).

### 3.3.1.4. Substitution mono-alphabétique

Nous avons vu que le chiffrement de César présente une sécurité très faible, la principale raison est que l'espace des clés est trop petit : il y a seulement 26 clés possibles, et on peut attaquer un message chiffré en testant toutes les clés à la main.

Au lieu de faire correspondre circulairement les lettres, on associe maintenant à chaque lettre une autre lettre (sans ordre fixe ou règle générale).

Par exemple :

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

Pour crypter le message

**ETRE OU NE PAS ETRE TELLE EST LA QUESTION**

On regarde la correspondance et on remplace la lettre **E** par la lettre **X**, puis la lettre **T** par la lettre **G**, puis la lettre **R** par la lettre **K**...

Le message crypté est alors :

**XGKX DR SX OFV XGKX GXWWX XVG WF ZRXVGPDS**

Pour le décrypter, en connaissant les substitutions, on fait l'opération inverse.

Avantage : nous allons voir que l'espace des clés est gigantesque et qu'il n'est plus question d'énumérer toutes les possibilités.

Inconvénients : la clé à retenir est beaucoup plus longue, puisqu'il faut partager la clé constituée des 26 lettres.

#### 3.3.1.5. Espace des clés

Mathématiquement, le choix d'une clé revient au choix d'une bijection de l'ensemble $\{A, B, \ldots, Z\}$ vers le même ensemble $\{A, B, \ldots, Z\}$. Il y a 26! choix possibles. En effet pour la lettre A de l'ensemble de départ, il y a 26 choix possibles (nous avions choisi F), pour B il reste 25 choix possibles (tout sauf F qui est déjà choisi), pour C il reste 24 choix... enfin pour Z il ne reste qu'une seule possibilité, la seule lettre non encore choisie. Au final il y a $26 \times 25 \times 24 \times \ldots \times 2 \times 1$ soit 26! choix de clés. Ce qui fait environ $4 \times 10^{26}$ clés. Il y a plus de clés différentes que de grains de sable sur Terre ! Si un ordinateur pouvait tester 1 milliard de clés par seconde, il lui faudrait alors 12 milliards d'années pour tout énumérer.

#### 3.3.1.6. Attaque statistique

La principale faiblesse du chiffrement mono-alphabétique est qu'une même lettre est toujours chiffrée de la même façon. Par exemple, ici E devient X. Dans les textes longs, les lettres n'apparaissent pas avec la même fréquence. Ces fréquences varient suivant la langue utilisée. En français, les lettres les plus rencontrées sont dans l'ordre :

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

avec les fréquences (souvent proches et dépendant de l'échantillon utilisé) :

La répartition des lettres en français est donnée est dans le tableau ci-dessous :

**Tableau 3. 1 : Fréquence des lettres en français**

| E | S | A | I | N | T | R | U | L | O | D |
|---|---|---|---|---|---|---|---|---|---|---|
| 14.69% | 8.01% | 7.54% | 7.18% | 6.89% | 6.88% | 6.49% | 6.12% | 5.63% | 5.29% | 3.66% |

Méthode d'attaque : dans le texte crypté, on cherche la lettre qui apparaît avec un grand pourcentage, et si le texte est assez long cela devrait être le chiffrement du E, la lettre qui apparaît ensuite dans l'étude des fréquences devrait être le chiffrement du S, puis le chiffrement du A... On obtient des morceaux de texte clair sous la forme d'un texte à trous et il faut ensuite deviner les lettres manquantes.

**Exemple**

Soit à déchiffrer le message suivant par l'attaque statistique :

**LHLZ HFQ BC HFFPZ WH YOUPFH MUPZH**

On compte les apparitions des lettres :

**H** : 6 **F** : 4 **P** : 3 **Z** : 3

On suppose donc que le **H** crypte la lettre **E**, le **F** la lettre **S**, ce qui donne

***E** ES* ** ESS** *E ***SE ****E**

D'après les statistiques **P** et **Z** devraient se décrypter en **A** et **I** (ou **I** et **A**). Le quatrième mot "**HFFPZ**", pour l'instant décrypté en "**ESS****", se complète donc en "**ESSAI**" ou "**ESSIA**". La première solution semble correcte ! Ainsi **P** crypte

**A**, et **Z** crypte **I**. La phrase est maintenant :

***E*I ES* ** ESSAI *E ***ASE **AIE**

En réfléchissant un petit peu, on décrypte le message :

**CECI EST UN ESSAI DE PHRASE VRAIE**

## 3.3.2. Chiffrement par transposition

Avec le principe de la transposition toutes les lettres du message sont présentes, mais dans un ordre différent. Il utilise le principe mathématique des permutations. Plusieurs types de transpositions existent dans la littérature, nous citons :

### 3.3.2.1. Transposition simple par colonnes

On écrit le message horizontalement dans une matrice prédéfinie, et on trouve le texte à chiffrer en lisant la grille verticalement. Le destinataire légal pour décrypter le message réalise le procédé inverse.

**Exemple**

Soit le texte à chiffrer ‘’I LOVE MY ENGLISH TEACHER’’ utilise une matrice [6× 4]

| | | | |
|---|---|---|---|
| I | L | O | V |
| E | M | Y | E |
| L | N | G | I |
| S | H | T | E |
| A | C | H | E |
| R | | | |

**Figure 3. 1 : Transposition simple par colonnes**

Le texte chiffré est : IENSA RLMGH COYLT HVEIE E

#### 3.3.2.2. Transposition complexe par colonnes

Dans ce type de chiffrement, on modifie l’ordre des lettres d’un texte en clair.

Exemple

Soit à chiffrer le message « hello wold » avec la clé 213.

avec la clé 213 le message « hello wold » devient « eolhlolwd ».

| 2 | 1 | 3 |
|---|---|---|
| h | e | L |
| l | o | w |
| o | l | d |

**Figure 3. 2 : Texte chiffré avec la clé 213**

## 3.4. Le chiffrement symétrique

Les systèmes symétriques sont synonymes de systèmes à clés secrètes. Une même clé est utilisée pour le chiffrement et le déchiffrement, d’où l’obligation que celle-ci reste confidentielle.

Sur la Figure (3.3.) l’émetteur (Alice) et le destinataire (Bob) doivent se mettre d’accord préalablement sur la clé (k) à utiliser, pour ceci ils ne doivent pas utiliser le réseau de communication standard qui est susceptible d’être espionné (par Oscar). Chaque fois qu’Alice veut transmettre un message (m) à Bob, elle utilise sa clé secrète (K) et une fonction de chiffrement (E) pour chiffrer ($C = E(m)$), et elle envoie le résultat de ce chiffrement par

l'intermédiaire du même canal. Bob utilise à son tour la même clé secrète et le même algorithme public pour déchiffrer le message codé qu'il a reçu.

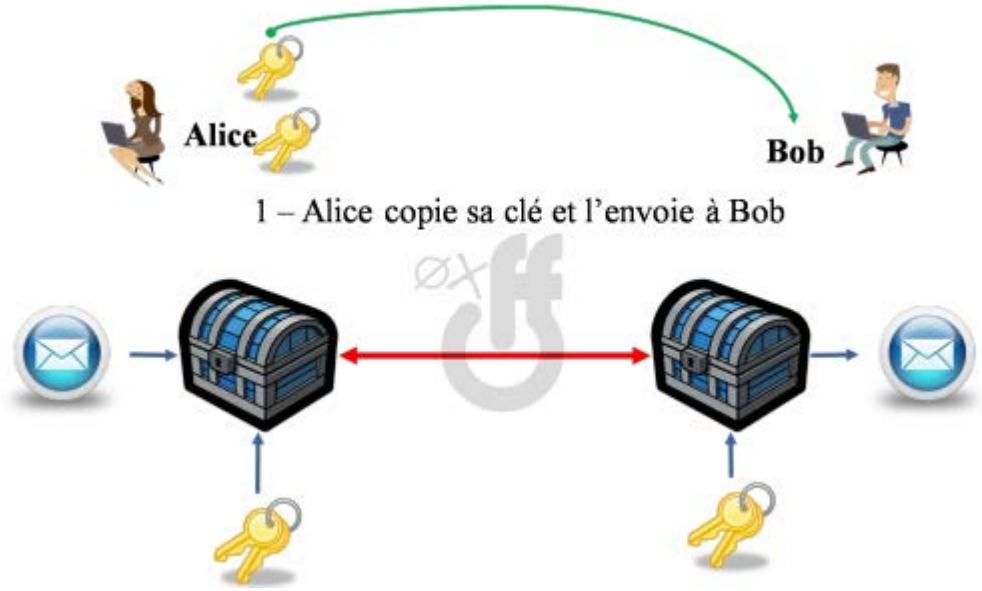


**Figure 3. 3 : Schéma illustrant Alice et Bob échangent leur message**

Les problèmes de cette technologie sont les suivants :

- Si la clé secrète est compromise (volée, extorquée, piratée, ...) par un opposant, alors ce dernier pourra déchiffrer tous les messages encodés avec celle-ci. Oscar peut même se faire passer pour Alice ou Bob.

- Les clés doivent être distribuées secrètement : c'est très difficile à l'échelle planétaire (se rencontrer, utiliser un messager sûr, etc...).

- Si une clé différente est utilisée pour chaque paire différentes d'utilisateurs du réseau, le nombre total des clés augmente très rapidement en fonction du nombre total d'utilisateurs.

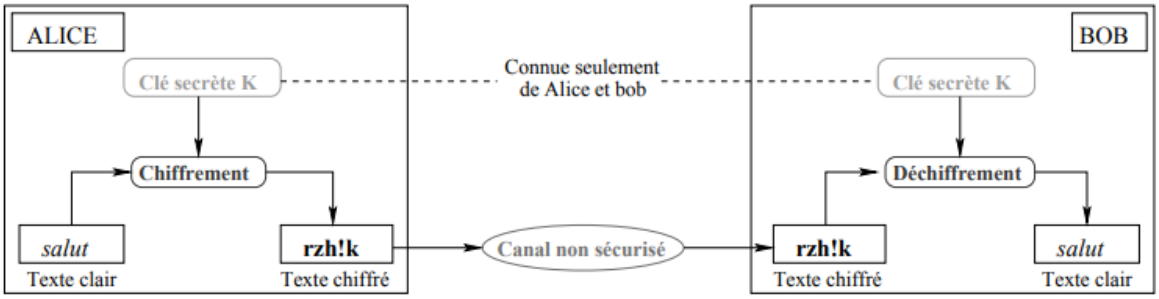


**Figure 3. 4 : Schéma illustrant le fonctionnement du chiffrement symétrique**

Cependant, en pratique, il se pose un problème majeur : comment échanger de manière sûre les clés ? C'est le principal défaut de ce système.

### 3.4.1. La cryptographie pour cartes à puces

Les algorithmes de la cryptographie symétrique les plus utilisés dans les cartes à puce sont DES (Data Encryption Standard), le triple DES, 3DES et AES (Advanced Encryption Standard).

Le DES naît en 1975 suite à une requête d'IBM en 1960 pour son programme de recherche sur le chiffrement informatique. Au début, les spécialistes de la NSA (National Security Agency, le service de sécurité intérieure américain) se cassent les dents dessus donc IBM est contraint de l'utiliser sous une forme plus simple que prévu. L'utilisation du D.E.S. se généralise alors peu à peu dans les administrations américaines. Depuis, le D.E.S. est remis à niveau tous les 5 ans environ pour faire face à la puissance croissante des ordinateurs qui le mettent en péril.

### 3.4.2. Classes de chiffrements symétriques

On distingue deux catégories de chiffrement symétrique :

#### 3.4.2.1. Les chiffrements symétriques par blocs

Le chiffrement par bloc (en anglais block cipher) est une des deux grandes catégories de chiffrements modernes en cryptographie symétrique, l'autre étant le chiffrement par flot. La principale différence vient du découpage des données en blocs de taille généralement fixe. La taille de bloc est comprise entre 32 et 512 bits, dans le milieu des années 1990 le standard était de 64 bits mais depuis 2000 et le concours AES le standard est de 128 bits.

En cryptographie, un mode d'opération est la manière de traiter les blocs de texte clairs et chiffrés au sein d'un algorithme de chiffrement par bloc. Historiquement, les modes d'opération ont été abondamment étudiés pour leurs propriétés de propagation d'erreurs lors de divers scénarios de modification de données durant le chiffrement. Les développements suivants ont considéré que la protection de l'intégrité était un objectif à atteindre par des moyens complètement différents. Mais aujourd'hui il existe des modes d'opérations qui associent chiffrement et authentification de manière efficace.

Plusieurs modes existent, certains sont plus vulnérables que d'autres :

- Dictionnaire de codes (Electronic Code Book, ECB)
- Enchaînement des blocs (Cipher Block Chaining, CBC)
- Chiffrement à rétroaction (Cipher Feedback, CFB)
- Chiffrement à rétroaction de sortie (Output Feedback, OFB)
- Chiffrement basé sur un compteur (CounTeR, CTR)
- Chiffrement avec vol de texte (Cipher Text Stealing, CTS)

Exemple d'algorithmes : DES, AES, IDEA, RC6, BLOWFISH, …

#### 3.4.2.2. Aspect technique de l'algorithme DES

- DES utilise une clé K de 56 bits utiles, qui est codée sur 64 bits et dont les bits 8, 16, 24, 32, 40, 48, 56 et 64 sont utilisés comme code de détection d'erreur et correcteur de la clé. DES est un crypto-système par blocs qui opère sur des blocs de 64 bits.

- La clé du système DES est trop courte pour les puissances de calcul actuelles. La taille de la clé secrète est de 56 bits ce qui la rend aujourd'hui vulnérable aux attaques par force brute.

Le message, au préalable converti en binaire, est découpé en blocs Bi de 64 bits. La clé K, comporte 56 bits. Pour chaque bloc Bi, on applique l'algorithme suivant :

1) On effectue une permutation initiale des bits du bloc Bi. On appelle alors G0 et D0 les parties de 32 bits droite et gauche du bloc obtenu.

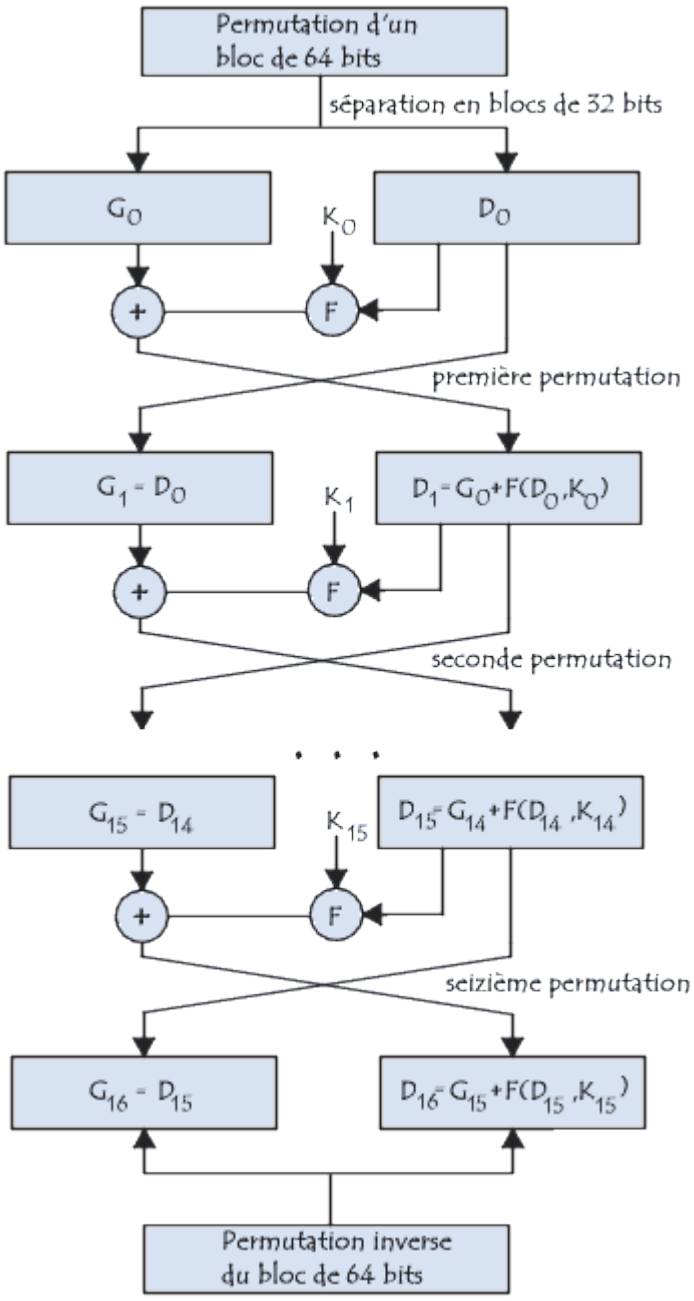


**Figure 3. 5 : Mécanisme de l'algorithme DES**

2) On répète 16 fois la procédure suivante :

$Gi = Di - 1$

Di = Gi-1 XOR F(Di-1 , Ki-1) (XOR est représenté par $\oplus$ sur le schéma de la Figure (3.5))

où Ki est un bloc de 48 bits de la clé K, et f une fonction composée successivement d'une expansion de bits, d'un XOR, d'une réduction de bits, et d'une permutation de bits.

3) On recompose un bloc B'16 en "recollant" D16 et G16 dans cet ordre.

4) On effectue la permutation inverse de la permutation initiale 1).

Le schéma résumant les différentes parties de l'algorithme est donné sur la Figure (3.5) :

Le décodage se fait en utilisant la même clé K mais en déroulant l'algorithme dans le sens inverse.

- Inconvénients

Les algorithmes de chiffrement de type DES sont fortement menacés par les puissances de calcul des ordinateurs. Il n'est en effet pas impossible de balayer la plupart des clés pour casser le code. Un nouveau système, le AES (Advanced Encryption Standard) est prévu pour le remplacer.

### 3.4.2.3. Aspect technique de l'algorithme triple DES

Le triple DES noté aussi 3DES ou TDES est un algorithme de chiffrement symétrique par bloc utilisant trois fonctions successives de l'algorithme DES sur le même bloc de données de 64 bits. L'algorithme utilise trois clé DES (K1, K2, K3), chacune de 56 bits. Deux configurations d'utilisation sont possibles qui sont : La première est 3DES avec une clé à 168 bits. Dans ce cas, les trois clés sont toutes différentes. La deuxième utilisation est 3DES avec une clé de 112 bits où les clés K1 et K3 sont identiques. Dans le chiffrement avec 3DES l'utilisation de l'algorithme DES se fait dans l'ordre suivant : DES (avec la clé K1), $DES^{1}$(avec la clé K2) et DES (avec la clé K3) comme le montre la Figure (3.6) :

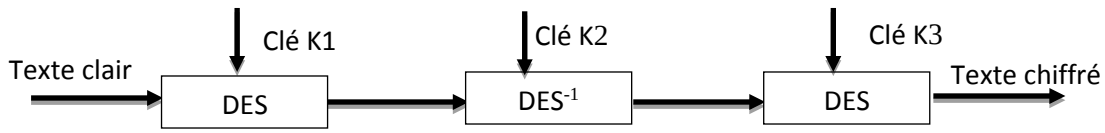


**Figure 3. 6 : Schéma global du chiffrement 3DES**

### 3.4.2.4. Décryptage DES

Le déchiffrement avec 3DES a la même structure que le chiffrement sauf que l'utilisation de l'algorithme DES se fait dans l'ordre suivant : $DES^{-1}$(avec la clé $K_3$), DES (avec la clé $K_2$) et $DES^{-1}$(avec la clé $K_1$).

### 3.4.2.5. Aspect technique de l'algorithme AES

L'Advanced Encryption Standard a fait l'objet d'un appel d'offre datant de 1997. Il s'agissait de remplacer le DES dont la taille des clés (56 bits) était devenue trop petite pour les performances des ordinateurs modernes. Les spécifications étaient une longueur de blocs de 128 bits (ou de 256 bits) et une longueur de clé paramétrable : 128 ou 192 ou 256 bits. Parmi les 15 candidats, le candidat retenu (en 2000) se nomme RIJNDAEL (mais on l'appelle simplement l'AES). Il est dù à deux chercheurs Belges, Rijmen et Daemen.

AES est un algorithme de chiffrement par blocs, les données sont traitées par blocs de 128 bits pour le texte clair et le chiffré. La clef secrète a une longueur de 128 bits, d'où le nom de version : AES 128 (il existe deux autres variantes dont la clef fait respectivement 192 et 256 bits). Le schéma illustrant le chiffrement et le déchiffrement AES est donnée sur la figure ci-dessous :

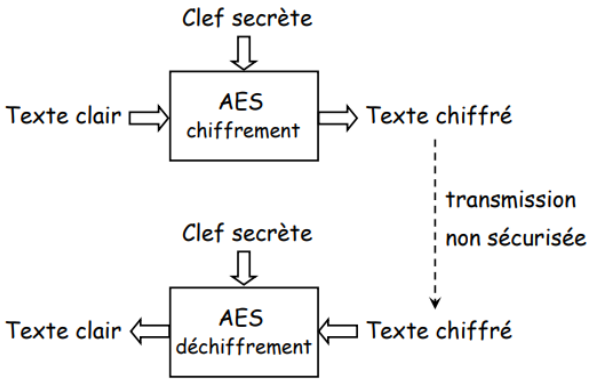


**Figure 3. 7 : Schéma illustrant le chiffrement et le déchiffrement**

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(28) (Groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours. Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs

fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.

#### 3.4.2.6. Le chiffrement symétrique par flot

Le chiffrement de flux ou chiffrement par flot (en anglais stream cipher). Un chiffrement par flot arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper. Un chiffrement par flot se présente souvent sous la forme d'un générateur de nombres pseudo-aléatoires avec lequel on opère un XOR entre un bit à la sortie du générateur et un bit provenant des données.

Exemple d'algorithmes : RC4, Bluetooth E0/1, GSM A5/1

## 3.5. Chiffrement asymétrique

Ce type de cryptographie est basé sur deux clés séparées et distinctes : l'une publique et l'autre maintenue secrète ou privée. L'algorithme asymétrique est utilisé pour assurer :

- La confidentialité : seul le propriétaire de la clé privée pourra lire le message chiffré avec la clé publique correspondante ;
- La non-altération et la non-répudiation : seul le propriétaire de la clé privée peut signer un message pour produire une signature. Cette dernière une fois déchiffrée avec la clé publique prouvera l'authenticité du message. Cette propriété est très utilisée dans les cartes à puce.

L'algorithme de la cryptographie asymétrique le plus utilisé dans les cartes à puce est le RSA. Ce dernier est nommé par les initiales de ses trois inventeurs : Rivest- Shamir - Adelman. Dans ce qui suit, la méthode d'utilisation de l'algorithme est détaillée en commençant par la méthode de la génération des clés RSA et ensuite la méthode d'utilisation de l'algorithme de cryptage et de décryptage.

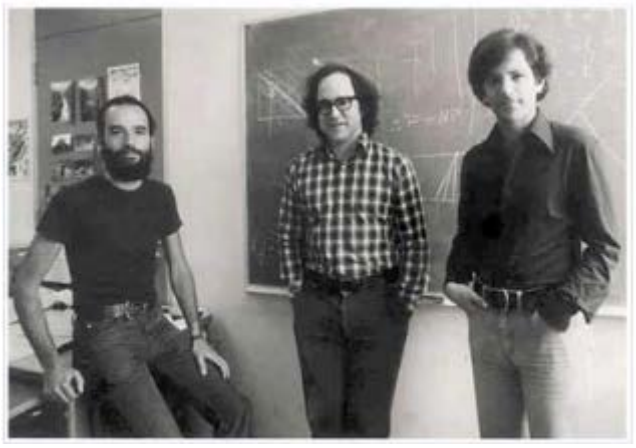

Figure 3. 8 : L'équipe RSA en 1977

Le RSA est basé sur la théorie des nombres premiers, et sa robustesse tient du fait qu'il n'existe aucun algorithme de décomposition d'un nombre en facteurs premiers. Alors qu'il est facile de multiplier deux nombres premiers, il est très difficile de retrouver ces deux entiers si l'on en connaît le produit.

Dans RSA, les blocs de message sont représentés par des entiers compris entre 0 et n-1. Pour envoyer un message m à Bob, Alice va donc chercher la clé publique de Bob et elle calcule le message chiffré c correspondant par l'utilisation de la formule : $c = m^e \bmod n$.

Lorsqu'il reçoit le message chiffré c, Bob retrouve le texte clair en calculant $c^d \bmod n = m$.

Le schéma illustrant le fonctionnement de ce type de chiffrement est donné sur la figure ci-dessous :

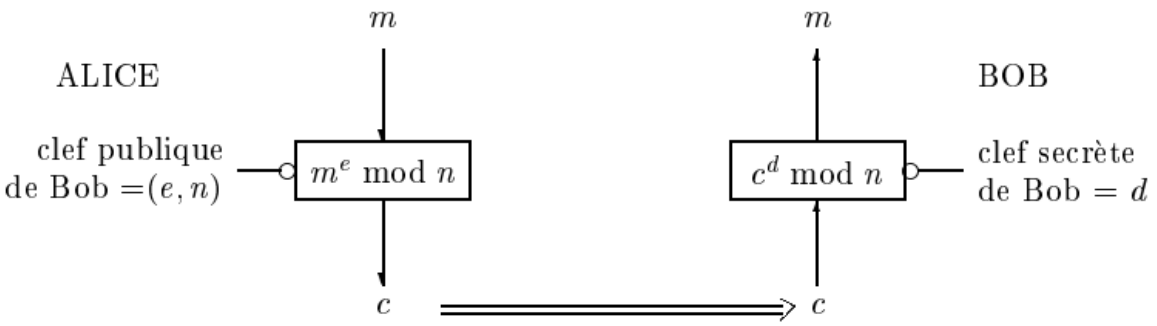


Figure 3. 9 : Chiffrement à clé publique

### 3.5.1. Comment fonctionne un algorithme RSA ?

Actuellement le chiffrement RSA est automatisé. Cependant le chiffrement peut être effectué avec les fonctions ci-après :

Petit rappel : Un nombre premier est un entier naturel qui admet exactement deux diviseurs distincts entiers et positifs (qui sont alors 1 et lui-même, par exemple 5,7,13...)

#### 3.5.1.1. Génération des clés RSA

A partir de deux grands nombres premiers aléatoirement choisis : p et q. Quatre autres valeurs sont calculées de la façon suivante :

1. Le produit $n = p \times q$, est appelé le modulo de chiffrement ;

2. La valeur de l'indicatrice d'Euler en n est définie par le produit :

$\varphi(n) = (p - 1) \times (q - 1)$ ;

3. L'entier naturel **e** est choisi premier avec $\varphi(n)$ appelé exposant de chiffrement ;

4. L'entier naturel **d** est l'inverse de **e** modulo $\varphi(n)$ appelé exposant de déchiffrement ; d peut se calculer efficacement par l'algorithme d'Euclide étendu.

Le couple $(n, e)$ définit la clé publique et le couple $(n, d)$ définit la clé privée associée.

#### 3.5.1.2. Exemple de génération de clés

Par exemple, Alice peut diffuser sa clé publique (e, n) sur Internet.

Quand Bob voudra envoyer un message secret à Alice, il cherche la clé publique d'Alice (e, n) sur Internet et crypte son message avec la clé publique d'Alice : $c = m \times e \pmod{n}$.

p, q et d constituent la clé privée d'Alice. Seule Alice connait p, q, et d.

Un tiers, Carole, ne peut pas comprendre ce que Bob a écrit à Alice car Carole n'a pas la clé privée. Quand Alice reçoit le message de Bob, elle le décrypte en utilisant sa clé privée d, n en effectuant $cd \pmod{n} = m$.

Si l'on ne connait pas d, on ne peut pas décrypter le message crypté c et connaitre le message m.

Pour connaitre d, on doit connaitre $(p-1)\times(q-1)$ pour trouver d à partir de l'équation :

$$e \times d = 1 \pmod{(p-1)\times(q-1)}.$$

Or, pour avoir $(p-1)\times(q-1)$, on doit en premier lieu être capable de factoriser le grand nombre n en p et q, tous deux premiers.

A partir du moment où tous les nombres sont de très grands nombres (100 chiffres au moins), nous pouvons dire qu'il est impossible en pratique qu'un tiers obtienne d, et puisse donc décrypter le message crypté.

**Exemple d'application**

Les variables étant données : p = 29, q = 31, e = 13, m = 123 ;

==>Nous calculons : $n = p \times q = 899$

(p-1)×(q-1) = 840

d = 517 car e×d = 13×517 = 8×(p-1)×(q-1) + 1

Pour crypter,

$c = 123^{13} \pmod{899} = 402$

Et pour décrypter, $m = 402^{517} \pmod{899} = 123$

Le chiffrement RSA est purement mathématique, tout message doit d'abord être codé par des nombres entiers (n'importe quel encodage : ASCII, Unicode, voire A1Z26).

### 3.5.2. Comment déchiffrer le RSA sans connaitre la clé privée ?

Le RSA est basé sur la théorie des nombres premiers, et sa robustesse tient du fait qu'il n'existe aucun algorithme de décomposition d'un nombre en facteurs premiers.

Pour retrouver la clé privée, un pirate doit être en mesure de réaliser la décomposition en facteurs premiers du nombre n pour retrouver ses 2 facteurs p et q.

Alors qu'il est facile de multiplier deux nombres premiers, mais il est très difficile de retrouver ces deux entiers si l'on en connaît le produit.

Remarque

La donnée de n est la clé publique : elle suffit pour chiffrer. Pour déchiffrer, il faut connaitre p et q, qui constituent la clé privée. Le problème de factorisation de grands entiers

étant très difficile, la connaissance de la clé publique n ne permet pas de retrouver les entiers p et q, qui constituent la clé secrète.

### 3.5.3. Les défauts du RSA

Le RSA présente quelques défauts qui sont :

Premièrement, sa sécurité n'a jamais été démontrée mathématiquement.

L'idée que le noyau mathématique du RSA est inviolable est une conclusion expérimentale tirée de l'échec des tentatives connues de décryptage sans la clef secrète depuis sa création en 1977.

Mais il est possible que l'on puisse casser le RSA à l'aide d'algorithmes spécifiques de factorisation, voire d'ordinateurs quantiques, et il n'est même pas sûr que casser le RSA revienne à factoriser n = p×q, peut-être est-il possible de déchiffrer un message, c'est-à-dire d'obtenir d, sans passer par p et q.

Deuxièmement, si une organisation avait réussi à casser des clés de plus de 512 bits RSA, elle le garderait certainement pour son pays et l'information ne circulerait pas forcément dans le monde. Donc la confiance qu'on lui accorde ne doit pas être une confiance aveugle.

Troisièmement, les conseils pour ne laisser transparaître aucune faille de sécurité dans le RSA se font de plus en plus nombreux avec les années (principalement pour le choix de p, q et e).

N'oublions pas que le 22 Août 1999, une clé RSA de 512 bits a été cassée : un entier n de 155 chiffres décimaux a été factorisé.

Citons enfin le cas du "RSA for paranoids" (paranoïaques) proposé par A. Shamir (un des inventeurs du RSA) en 1995, qui était censé rassurer les utilisateurs du RSA classique qui craignaient des failles de sécurité. "RSA for paranoids" permettait d'allonger la clé sans trop augmenter les coûts de codage.

Résultat : trois ans plus tard, ce prétendu renforcement du RSA est cassé.

Ainsi, un des inventeurs du RSA, croyant renforcer son système pour rassurer les paranoïaques, a, au contraire, augmenté leurs craintes.

L'algorithme de la cryptographie asymétrique le plus utilisé dans les cartes à puce est le RSA.

Ce système est beaucoup plus sûr qu'un chiffrement à simple clé de par sa conception, mais il présente quelques inconvénients. : Les temps de traitement sont plus longs, et pour un niveau de sécurité équivalent, nécessite des clés plus longues.

## 3.6. Crypto systèmes à apport nul de connaissance

Crypto système à apport nul de connaissance : Zero knowldege repose sur une idée introduite par Goldwasser, Micali et Rackoff en 1985, et optimisé par Guillou et Quisquater en 1987 pour les cartes à microcontrôleur.

Dans le système précédent, il est nécessaire qu'un secret de base soit utilisé par le vérifieur (cas de système symétrique) ou par le prouveur (cas de système asymétriques). Dans le système à apport nul de connaissance, le vérifieur n'a pas besoin de secret et le prouveur possède un secret. Il s'agit d'une méthode très puissante pour authentifier et signer des messages, sans donner la moindre information sur le secret utilisé.

## 3.7. Sécurité des cartes à puces

La sécurité est la principale qualité de la carte à puce. C'est d'ailleurs pour cette raison qu'elle a été choisie pour les transactions bancaires. Cette sécurité accrue est rendue possible grâce à un ensemble de techniques variées.

L'ISO 78 a défini 6 services de sécurité :

1) Authentification (de la source et/ou du destinataire) ;
2) Contrôle d'accès (qui nécessite une authentification préliminaire) ;
3) Confidentialité des données (les données illicitement récupérées doivent être inutilisables);
4) Intégrité des données (empêcher les modifications des données, les doublons) ;
5) Non-répudiation (un message, son envoi et sa réception ne peuvent être contestés) ;
6) Protection de l'analyse du trafic (la relation entre deux personnes doit rester secrète).

## 3.8. Les attaques

Le but d'un attaquant est de pouvoir accéder aux informations et aux secrets contenus dans la carte (code PIN, clé(s) secrète(s) cryptographique(s), etc...) ou tout simplement de nuire aux applications embarquées afin de tester le niveau sécuritaire de la carte.

Les attaques sont de deux types : physiques et logicielles. Dans cette section on va étudier les deux types d'attaques qu'il s'agit matériels et logiciels.

### 3.8.1. Attaques matérielles ou physiques

Une attaque physique est une attaque menée sur la partie électronique de la carte. En effet, les algorithmes cryptographiques sont souvent implémentés sur des modules physiques que l'attaquant peut observer, voir perturber. Ces attaques peuvent être de deux types : invasives et non invasives.

#### 3.8.1.1. Attaques invasives

Elles permettent de récupérer un ensemble d'information de la carte en se basant sur une cartographie des circuits. Ces attaques sont dites de ‘’reverse engineering’’ car l'attaquant tente de déduire les algorithmes utilisés, leurs implémentations, les systèmes de sécurité mis en place et les informations contenus dans la puce à partir de l'analyse ou la modification des circuits intégrés dans la carte. Pour pouvoir arriver à ce résultat, l'attaquant cherche à isoler les circuits de manière physique ou chimique. Le plus souvent, la puce n'est plus réutilisable après ces attaques, d'où l'aspect invasif. On peut citer comme exemple :

– La modification de circuit à l'aide du FIB (Focused Ion-Beam) permettant d'ajouter ou de retirer des nouvelles pistes conductrices sur la puce.

- Equipement **très coûteux mais possibilités énormes pour l'attaquant**

Figure 3. 10 : Equipement FIB

– La rétro-conception des blocs fonctionnels du microprocesseur dans le but de déterminer toutes les informations secrètes de la carte.

– Le sondage (probing en anglais) physique, c'est-à-dire la pose de micro-sondes sur les bus de la puce dans le but de déterminer ou falsifier l'information qui y circule.

#### 3.8.1.2. Attaques non invasives

Dans le cas des attaques non invasives, on trouve plusieurs types d'attaques qui sont :

**a) Attaques par conditions anormales**

L'attaquant fait fonctionner la carte avec des valeurs en dehors des normes acceptables de fonctionnement de la carte. Ces caractéristiques peuvent par exemple être la fréquence d'alimentation ou la tension aux bornes de la carte. Aujourd'hui, une majorité des cartes possèdent des détecteurs d'activités anormales permettant de désactiver la carte pour lutter contre ce type d'attaque.

**b) Attaques par canaux cachés**

Ce sont des attaques par observation du signal puis d'analyse statistique. Les paramètres d'observation pouvant être le temps d'exécution, la consommation du courant ou même l'émission électromagnétique. L'attaque par analyse du temps d'exécution est basée sur le temps d'exécution des instructions. L'attaquant essaie de déduire des informations sur le type d'opération, les opérandes pour avoir des informations sur un programme ou un algorithme donné.

**c) Attaques par injection de fautes**

Elles sont encore appelées attaques par perturbation. En effet, l'attaquant tente d'injecter des modifications physiques dans l'environnement de la carte (lumineuses, impulsions électriques, magnétiques, etc...) pour introduire des modifications dans le contenu des mémoires de la carte. Le but étant d'introduire des fautes lors de l'exécution d'un programme afin de provoquer des sorties erronées exploitables, d'éviter un test, d'appeler une autre sous fonction, de sauter l'appel de vérification d'un code PIN, etc... Cependant l'attaquant doit pouvoir localiser les cellules mémoires à attaquer et synchroniser l'attaque pour qu'elle coïncide avec la fenêtre d'opportunité offerte par le programme. Pour cela, l'attaquant peut observer l'activité de la carte à l'aide d'attaques par canaux cachés.

### 3.8.2. Attaques logicielles

Avec l'apparition des cartes « ouvertes » permettant de charger des applications dans la carte après émission de celle-ci, les attaques logicielles sont de plus en plus répandues. Elles utilisent des failles pour contourner les protections mises en place. Généralement, il s'agit d'une mise à défaut des mécanismes d'isolation et d'intégrité du code et des données des applications embarquées.

## 3.9. Les niveaux d'attaques

L'intrus peut effectuer quatre niveaux d'attaques, l'attaque est une tentative de cryptanalyse.

- L'attaque par cryptogramme (par message chiffré seulement) : ou le cryptanalyste ne connait qu'un ensemble de message chiffrés, il peut soit retrouver seulement les messages en clair, soit retrouver la clef. En pratique, il est très souvent possible de deviner certaines propriétés du message en clair (format ASCII, présence d'un mot particulier, …), ce qui permet de valider ou non le décryptement.

- L'attaque à message en clair connu : ou le cryptanalyste connait non seulement les messages chiffrés mais aussi les messages en clair correspondants, son but est alors de retrouver la clef. Du fait de la présence, dans la plupart des messages chiffrés, de parties connue (en-têtes de paquets, champs communs à tous les fichiers d'un type donné, …).

- L'attaque à message en clair choisi : ou le cryptanalyste peut, de plus choisir des messages en clair à chiffrer et donc utiliser des messages apportant plus d'informations sur la clef. Si le cryptanalyste peut de plus adapter ses choix en fonction des messages chiffrés précédents, on parle d'attaque adaptative.

- L'attaque à message chiffré choisi : Dans ce cas, le cryptanalyste peut choisir des messages chiffrés pour lesquels il connaitra le message en clair correspondant ; sa tâche est alors de retrouver la clef. Ce type d'attaques est principalement utilisé contre les systèmes à clef publique, pour retrouver la clef privée.

## 3.10. Comment sécuriser une carte à puce ?

Il existe de nombreuses contre-mesures pour résister à des attaques malicieuses. Ces contre-mesures peuvent être logicielles et/ou matérielles selon le type d'attaques. Pour atteindre cet objectif, tous les chemins de test doivent être irréversiblement détruites, voire inexistants. Des détecteurs d'intrusion, des alarmes et des mécanismes de protection doivent être implémentés et exploités par le système d'exploitation. Le composant doit aussi être capable d'exécuter des tâches de contrôle, non seulement dans les conditions normales de fonctionnement, mais aussi, et surtout, dans les conditions anormales.

### 1) Interdire le mode test

Tous les chemins de test doivent être invisiblement détruits. Des détecteurs d'intrusion, des alarmes et des mécanismes de protection doivent être implémentés et exploités par le système d'exploitation.

### 2) Résister aux attaques

Attaques actives ou invasives, les composants doivent résister aux tentatives de lecture des mémoires par dépassivation des couches de protection physique, lecture des bus par l'utilisation de faisceau d'ions …

Concernant les attaques passives (ne perturbant pas le fonctionnement du composant), ces types d'attaques peuvent être résumés comme suit :

- Attaque de type SPA (Single power Analysis) : fondés sur un espionnage des signaux électriques ou électromagnétiques émis par une machine.

- Attaque du temps (Timing Attack) : dans ce type d'attaque il est également possible de connaitre certaines données sensibles, comme des clés cryptographiques, en exploitant simplement le temps de traitement des différentes instructions du processeur.

- Attaque de type DPA (Differential Power Analysis) : ce type d'attaque est fondé sur une analyse statistique des variations de puissance consommée pendant l'exécution d'un algorithme cryptographique connu.

**3) Des mémoires intactes**

On doit contrôler l'intégrité des données et des programmes, ainsi que le déroulement et la reprise des diverses opérations en cas d'interruption brutale d'un processus pour une raison quelconque, comme la coupure de l'alimentation de la carte en cours de transaction (cas d'un arrachage de la carte).

**4) Conserver l'union microprocesseur-logiciel**

En termes de sécurité, le logiciel et le matériel sont inséparables. Dans les composants actuels, des dispositifs sont employés au niveau du matériel, de type ACL (Access Control List) ou MMU (Memory Management Unit), complété par des mécanismes de cloisonnement des données et des applications supervisées par logiciel. Toute tentative d'accès frauduleux à une donnée ou un programme doit être détectée et enregistrée.

## 3.11. Sécurité des communications

Les différents modes de communication (contact, sans contact) peuvent être utilisés pour tenter de compromettre les biens de la carte. Si un risque de ce type existe, il est indispensable de sécuriser les communications, en les chiffrant si on veut préserver leur confidentialité et/ou en les signant si l'on veut compromettre l'intégrité. Dans certains cas, il peut également être nécessaire d'assurer la disponibilité du canal de communication.

Pendant longtemps, le risque d'attaques sur les communications via les contacts est faible. Ainsi, les PIN des cartes étaient présentés en clair entre le lecteur et la carte. C'est encore souvent le cas mais de plus en plus, certaines applications considèrent que ce risque doit être pris en compte et qu'il faut mettre en place des contre-mesures. C'est le cas, par exemple, pour les cartes bancaires où il est prévu que le PIN puisse être présenté chiffré ou encore, que

l'intégrité des informations retournées par la carte vers le lecteur doit être assuré (mode CDA (Combined Data Authentification) en EMV par exemple).

Toutefois, en mode contact, la plupart des attaques nécessitent une intervention sur les lecteurs ou des aménagements sur les cartes elles-mêmes ce qui limite souvent leurs rentabilités ou leurs généralisations.

Les attaques applicables au mode contact sont généralement applicables au mode sans contact mais avec parfois un mode opératoire simplifié ou une plus grande discrétion. De plus, il existe des attaques que l'on peut considérer comme spécifiques au mode sans contact et qu'il est bon de rappeler, ainsi que leurs limites.

# Chapitre 4 : Systèmes d'exploitation & modes de communication

## 4.1. Introduction

Comme tout ordinateur, les cartes à microprocesseur embarqué nécessitent la présence d'un système d'exploitation faisant office d'interface pour l'accès aux ressources de la carte. Dans ce chapitre, on va décrire les systèmes d'exploitation dédiés aux cartes à puces, ainsi que les standards ISO concernant les protocoles de leurs modes de communication entre la carte à puce et son lecteur pour l'échange des données.

## 4.2. C'est quoi un système d'exploitation

Un système d'exploitation, abrégé parfois SE, (Operating System en anglais, que l'on rencontre souvent sous l'abréviation OS) représente l'ensemble des programmes qui pilote les différents composants (disque dur, écran, processeur, mémoire etc…) de l'appareil informatique et lui permet donc de fonctionner.

Il permet donc de faire l'interface entre l'utilisateur et le matériel informatique. Il est d'ailleurs chargé en premier lors du démarrage de l'appareil.

## 4.3. Les principaux systèmes d'exploitation

Les principaux systèmes d'exploitation sont :

**1)** Systèmes d'exploitation pour ordinateurs

- Windows
- Mac OS
- Linux

**2)** Systèmes d'exploitation pour smartphones et tablettes tactiles

- Android
- iOS

- Windows 10 mobile

3) Systèmes d'exploitation pour cartes à puces

## 4.4. Structure d'un système d'exploitation

Le système d'exploitation se situe entre le matériel et les autres logiciels. Afin de rendre le travail administratif possible, le système d'exploitation a une structure légèrement différente de celle de la plupart des autres programmes. On dit que les systèmes sont construits à partir de différentes couches. Dans la couche inférieure - celle qui est la plus éloignée de l'interface utilisateur - se trouve le noyau, l'élément le plus important du système d'exploitation. Ce programme est donc aussi le premier à être chargé. Le noyau est l'interface directe avec le matériel, l'initialise et transmet les commandes des programmes en cours d'exécution au matériel.

Ce noyau est ensuite utilisé comme base pour les autres couches, qui s'éloignent de plus en plus de l'interaction avec le matériel. Chaque couche communique uniquement avec la couche située au-dessus ou au-dessous d'elle. Enfin, au sommet se trouve l'interface utilisateur, l'interface entre les utilisateurs et le logiciel. Si l'utilisateur effectue une action, cette instruction est guidée à travers les différentes couches jusqu'à ce qu'elle atteigne le bon endroit, le processeur, par exemple. La structure d'un système d'exploitation est donnée sur la Figure (4.1).

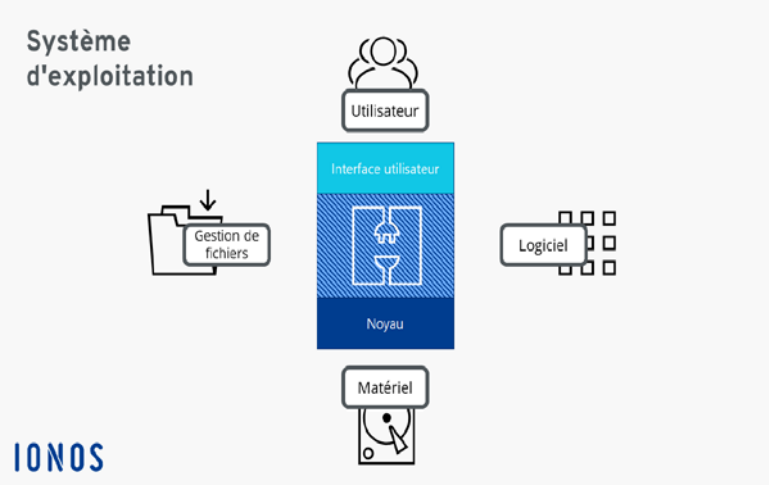


**Figure 4. 1 : Structure d'un système d'exploitation**

## 4.5. Systèmes d'exploitations pour cartes à puces

Système d'exploitation (Operating System, OS) désigne le logiciel de commande d'une carte à microcalculateur qui interprète et exécute les différents ordres élémentaires que cette carte peut réaliser. Situé dans la partie ROM du microcalculateur, il est implanté dans l'un des masques qui sert à la fabrication du circuit intégré.

L'OS réalise principalement les fonctions suivantes :

- Gestion des échanges entre la carte et le monde extérieur, notamment le protocole d'échanges ;
- Gestion des différents fichiers et des données à l'intérieur de la mémoire ;
- Contrôle des accès aux informations et aux fonctions (par exemple sélection de fichier, lecture, écriture, modification de données) ;
- Gestion de la sécurité de la carte et de la mise en œuvre des algorithmes cryptographiques ;
- Fiabilité du fonctionnement, notamment cohérence et intégrité de certaines données, ruptures de séquences et reprise des erreurs ;
- Gestion du cycle de vie de la carte dans ses différentes phases (fabrication, personnalisation, utilisation, fin de vie).

Le système d'exploitation est contenu dans la ROM dont le contenu n'est pas chiffré. La connaissance de son code, bien que difficile ne doit pas rendre possible des attaques autorisant la lecture de la mémoire non volatile.

Un système d'exploitation est réalisé par une entreprise spécialisée. Ce logiciel étant ajustée pour un composant électronique particulier, il est appelé masque.

Le masque est stocké dans la ROM du composant lors du processus de fabrication. Au terme de cette phase le fondeur de silicium écrit dans la puce une clé dite clé de fabrication et écrit dans la mémoire de cette dernière des informations telles que numéro de série du produit, date de fabrication etc.

Le wafer (plaque de silicium circulaire qui comporte un ensemble de puces) est alors envoyé à l'encarteur qui réalise sa découpe, colle les puces sur des micromodules et en réalise le micro câblage. L'ensemble est alors protégé par une substance isolante. Il est ensuite collé sur un support en plastique (PVC) dans lequel on a préalablement usiné une cavité.

L'encarteur, qui connaît les clés de fabrication, inscrit de nouvelles informations dans la puce et active un verrou de fabrication qui annule la clé de fabrication. Une nouvelle clé est inscrite dans la puce permettant de contrôler les opérations ultérieures. Cette opération est encore dénommée personnalisation.

Les cartes sont par la suite transférées vers l'émetteur de la carte qui peut inscrire de nouvelles informations. La vie d'une carte consiste à poser à verrou d'invalidation (IV) qui rend le système d'exploitation non fonctionnel.

## 4.6. Types de systèmes d'exploitation pour cartes à puces

On peut distinguer deux types de systèmes d'exploitation dédiés aux cartes à puces :

1) Les systèmes fermés ou dédiés

Généralement mono application ; dédiés à un usage unique ; par exemple les cartes bancaires, les cartes santés

2) Les systèmes ouverts

Ils ne sont pas destinés à une application particulière et il est possible de charger des logiciels après la réalisation du masque et l'encartage ;

Par exemple les JavaCards, ou le système d'exploitation Multos permettant d'installer et de désinstaller des applications.

## 4.7. Normes principales relatifs à la carte à puce

Le standard est un document établi et adopté par consensus entre différents intervenants dans un domaine bien déterminé et il est géré par une organisation spécifique comme l'organisation internationale pour la standardisation (ISO). Deux normes internationales régissent les caractéristiques des cartes à puce

- ISO 7816 pour les cartes à contact
- ISO 1443 pour les cartes sans contact

### 4.7.1. Standards relatifs à la carte à puce avec contacts 7816

La norme ISO définit :

- Les caractéristiques physiques : taille, contraintes à supporter, emplacement des contacts, et caractéristiques électriques.
- Les protocoles de communication : Par caractère (appelé T=0) et par paquet (appelé T=1).
- Les commandes applicatives : les différentes commandes/réponses suivant les applications

L'ISO 7816 « Idenfication cards – Integrated circuit cards with contacts » a été publié par l'organisation internationale de standardisation (ISO, International Organisation for Standardisation). C'est le plus important standard définissant les caractéristiques des cartes à puce qui fonctionnent avec un contact électrique. Sachant que 15 normes sont proposées pour les cartes à contact, nous décrivons brièvement ici uniquement les six premières normes.

1) ISO 7816-1

Cette norme définit les caractéristiques physiques des cartes à puces à contact : la géométrie, la résistance, les contacts, etc.

2) ISO 7816-2

Cette norme spécifie le dimensionnement physique (extérieur) des contacts de la puce. Deux des huit contacts réservés à une utilisation future (RFU) sont redéfinis pour l'utilisation USB dans la norme ISO 7816-2.

Position et dimension pour les cartes ISO 7816-2 sont montées sur la Figure (4.2).

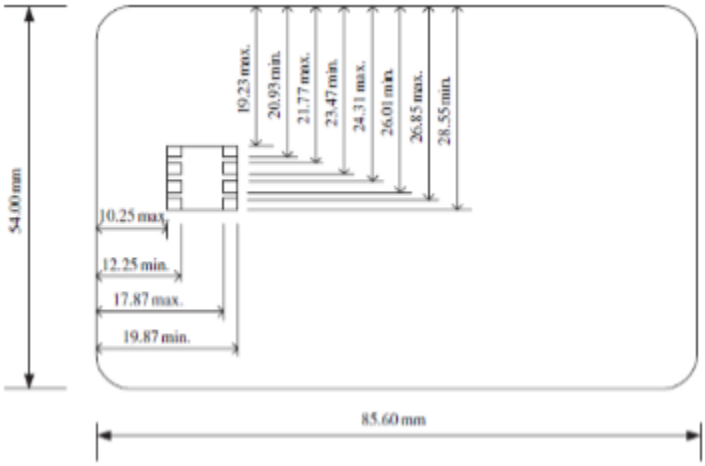


**Figure 4. 2: Position et dimension pour les cartes ISO 7816-2**

3) ISO 7816-3

Cette norme définit l'interface électrique et les protocoles de transmission :

- Les protocoles de transmission (TPDU, Transmission Protocol Data Unit) : T=0 : protocole orienté octet, T1 : protocole orienté paquet, T=14 : réservé pour les protocoles propriétaires,
- La sélection d'un type de protocole,
- La réponse à un reset (ATR, ou Answer To Reset en anglais) qui correspond aux données envoyées par la carte immédiatement après la mise sous tension,
- Les signaux électriques, tels que le voltage, la fréquence d'horloge et la vitesse de communication.

4) ISO 7816-4

Cette norme vise à assurer l'interopérabilité des échanges. Elle définit les messages APDU (Application Protocol Data Units), par lesquels les cartes à puce communiquent avec le lecteur. Les échanges s'effectuent en mode client-serveur, le terminal ayant toujours l'initiative de communication.

5) ISO 7816-5

Cette norme définit le système de numérotation et les procédures d'enregistrement et d'attribution des identifiants des applications (AID, ou Application IDentifier). Un unique

AID est associé à chaque application et à certains fichiers sur la carte. Ils sont représentés par des tableaux d'octets de taille allant de cinq à seize. Les cinq premiers octets représentent le numéro d'enregistrement du fournisseur d'application (RID, Registered Application Provider IDentifier en anglais) qui est attribué par la Copenhagen Telephone Company Ltd. Ils sont suivis par l'identifiant optionnel PIX (Proprietary Application Identifier eXtension) d'une longueur allant jusqu'à 11 octets.

L'identifiant RID est le même pour le paquetage et l'applet, mais le PIX doit être différent.

6) ISO 7816-6

Cette norme spécifie des éléments de données inter-industrie pour les échanges, tels que le numéro du porteur de carte, sa photo, sa langue, la date d'expiration, etc.

### 4.7.2. Standards relatifs à la carte à puce sans contacts 14443

Le standard ISO14443 est un standard international concernant la partie interface de la carte sans contact. Il contient les spécifications de la partie radio fréquence (RF), l'interface électrique et enfin le protocole de communication et de gestion de collision.

## 4.8. La technologie RFID

La technologie RFID (Radio Frequency Identification) est une méthode, basée sur les ondes radios, permettant d'établir un dialogue entre une étiquette RFID (tag) et un dispositif de lecture sans nécessité de contact physique. Cette technologie est particulièrement utilisée dans les secteurs du transport et de la logistique, de l'agroalimentaire, de la santé, de la grande distribution et de l'industrie pour l'identification unique d'un objet, animal ou personne.

La technologie RFID repose sur des éléments clés : la puce RFID, l'inlay, le tag, l'imprimante, le lecteur, le middleware et les systèmes d'informations type ERP, WMS, TMS, …etc.

La puce électronique est l'élément constituant, elle contient les informations d'identification. L'inlay est le support isolant sur lequel est fixé l'antenne connectée à la puce RFID. L'étape supplémentaire d'impression ou lamination permet d'aboutir à l'étiquette RFID. Le schéma général d'un système RFID est donné dans la Figure (4.3).

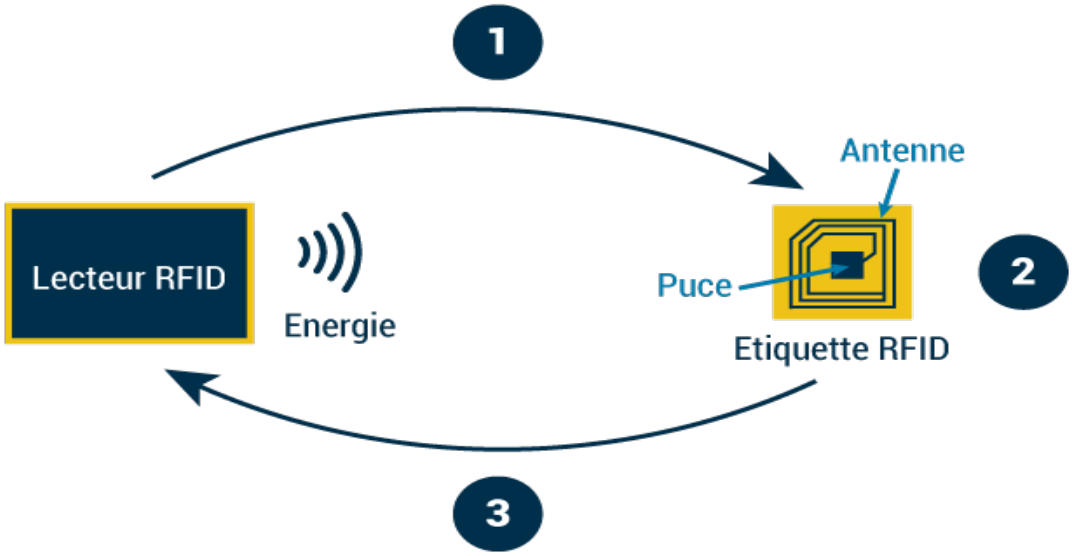


Figure 4. 3 : Schéma général d'un système RFID

La détermination de la fréquence à privilégier dépend du type d'usage que l'on souhaite en faire, les contraintes géométriques telles que la distance séparant l'interrogateur du transpondeur. Ces fréquences peuvent être classées en quatre groupes comme le montre le Tableau (4.1) :

Tableau 4. 1 : Caractéristiques de différentes fréquences de communication

| Fréquence | Dénomination | Distance | Application | Types d'étiquettes |
|---|---|---|---|---|
| 125-135 KHz | Basses fréquences | Distance<1m | Utilisées pour le contrôle d'accès ou d'identification des animaux et système d'alarme | Passive |
| 13,56 Mhz | Hautes fréquences | Quelques mètres | Utilisée notamment dans la Logistique d'objets, les cartes de crédit sans contact (technologie NFC), le transport public, le document électronique, la carte multiservices ou la logistique. | Passive |
| 433 MHz et entre 860 et 960MHz | Ultra hautes fréquences | Elles permettent d'obtenir des portées de plusieurs mètres. | Très utilisées dans le domaine la logistique industrielle, du suivi des palettes ou encore dans la gestion d'inventaires. | Passive et active |
| 2,45 GHz et 5,8 GHz. | Super hautes fréquences | Distance >100mètres | Elles se retrouvent notamment dans des applications de gestion de containers. Les péages autoroutiers ou encore les | Active |

| | | | | |
|---|---|---|---|---|
| | | | systèmes de géolocalisation. Logistique militaire. | |

## 4.9. Utilisation de la carte à puce

Afin d'utiliser une carte à puce ou sans contact, un lecteur de carte à puce est nécessaire. Le lecteur de carte à puce est un appareil électronique permettant l'écriture ou la lecture des données respectivement vers ou à partir de la carte à puce. Il est nommé aussi CAD (Card Accepting Device). Le lecteur prend plusieurs formes :

- Lecteur à interface USB pour se connecter au PC
- Lecteur de carte avec clavier pour la saisie du montant de la transaction ou du code PIN. Ce type de lecteur est en général connecté à un serveur de paiement.
- Ordinateur portable équipé d'un lecteur de carte à puce intégré.
- Lecteur de carte sans contact avec antenne.
- Des lecteurs avec acquisition biométrique comme l'empreinte ou capteur d'iris d'œil.
- Une carte à micro-contrôleur tout simple avec un petit programme qui gère la communication respectant la norme ISO7816.

Comme la carte à puce, le lecteur de carte à puce à contact doit aussi respecter une grande partie du standard ISO7816 par contre le lecteur de la carte sans contact doit respecter la spécification décrite dans la norme ISO14443.

## 4.10. Etablissement de la communication entre la carte et son lecteur

L'établissement de la communication entre la carte et son lecteur peut se faire selon le type de la carte, pour cela nous pouvons distinguer les deux cas suivants :

### 4.10.1. Cartes à puces sans contact

Lorsque la carte arrive dans la zone d'influence d'une antenne de lecteur et qu'elle se trouve donc suffisamment et correctement alimentée, elle effectue une reset interne et attend une commande de ce dernier.

Le lecteur commence par envoyer une commande appelée Request à laquelle la ou les cartes situées dans sa zone d'influence répondent par Answer To Request (ATR).

La carte sélectionnée envoie au lecteur une réponse de type (Answer To Select) qui l'informe du type de carte avec laquelle il doit s'attendre de dialoguer.

### 4.10.2. Cartes à puces avec contact

Lors de sa phase d'utilisation, une carte à microprocesseur subit des cycles de trois étapes qui constituent une connexion :

- L'introduction de la carte : lorsque la carte est insérée dans le lecteur, elle se trouve de nouveau alimentée en énergie et est réinitialisée.
- L'exécution de la commande : elle consiste en la réception d'une commande sur le port d'entrée / sortie et à l'exécution de celle-ci. Cette phase peut être renouvelée autant de fois que nécessaire pour la bonne fin de l'application.
- La déconnexion : elle correspond à une coupure de l'alimentation électrique de la carte.

## 4.11. Protocoles de liaison de niveau pour les cartes à puce

Lorsque nous parlons de protocoles de communication, nous pouvons généralement analyser la situation en termes de modèle de référence d'interconnexion de systèmes ouverts (OSI : Open system Interconnexion), qui est illustré à la Figure (4.4). Le modèle de référence OSI décrit le problème général de communication entre deux entités en termes de sept protocoles distincts qui se superposent (d'où le terme modèle à sept couches) et fournit un mécanisme complet par lequel deux modèles de référence sont la séparation stricte des couches. C'est-à-dire qu'une couche communique uniquement avec la couche immédiatement au-dessus ou en dessous d'elle via une interface bien définie, et chaque couche fournit un

ensemble spécifique de services à l'ensemble de la pile de protocoles. Sur la Figure (4.4) on donne le modèle de référence d'OSI.

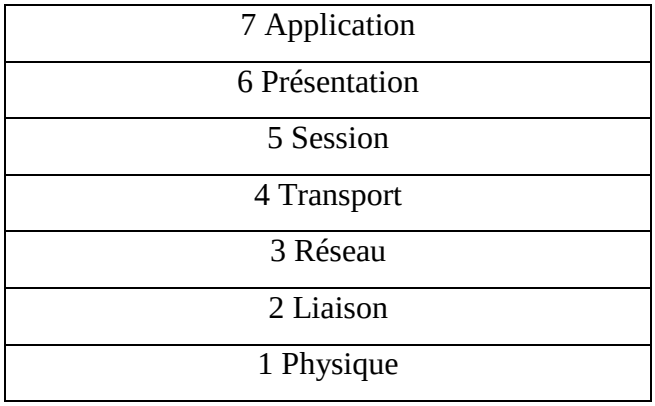


**Figure 4. 4 : Modèle de référence d'OSI**

Dans le cas des protocoles de carte à puce T=0 et T=1, le protocole T=1 s'adapte assez bien au modèle de référence OSI en tant que couche de protocole de liaison de données (ou niveau liaison), mais le protocole T=0 a tendance à mélanger les éléments de plusieurs couches de protocole différentes (telles que définies par le modèle de référence OSI).

À ce stade, il convient de rappeler que l'hôte et la carte communiquent via un protocole de commande et de réponse très strict. C'est-à-dire que le côté lecteur de la liaison envoie une commande à la carte, incluant éventuellement des données à utiliser sur la carte dans l'exécution de la commande, et la carte exécute ensuite cette commande et renvoie une réponse au lecteur.

Cette réponse peut comprendre des données résultant de l'exécution de la commande sur la carte ainsi qu'une réponse d'état concernant l'exécution de la commande. Les structures de données échangées par le lecteur et la carte dans ce protocole commande-réponse sont appelées unités de données de protocole de transmission (TPDU). Les structures TPDU utilisées dans le protocole T=0 sont assez différentes de celles utilisées dans le protocole T=1.

Une fois le protocole T=0 ou T=1 établi entre le lecteur et la carte, il est utilisé pour prendre en charge les protocoles de niveau application entre le logiciel d'application sur la carte et le logiciel d'application du côté lecteur de la liaison. Ces protocoles d'application échangent des informations via des structures de données appelées unités de données de protocole d'application (APDU). Le protocole T=0 fournit une très mauvaise séparation de couche entre le protocole au niveau liaison et le protocole au niveau application.

### 4.11.1.Protocoles de transmission des données

Dans cette section on va décrire le protocole de communication des cartes à puces avec et sans contact :

Le protocole de transmission des données définit la méthode d'envoi d'une commande du lecteur vers la carte et d'une réponse de commande de la carte vers le lecteur. Quinze protocoles de transmission ont été identifiés dans la norme ISO7816.

Deux de ces protocoles sont les plus utilisés au niveau international qui sont le T=0 et le T=1. L'élément de donnée transporté par le protocole de transmission est appelé Transmission Protocol data Units (TPDU).

Ils sont désignés par le terme T=numéro du protocole comme présenté dans la Tableau (4.2).

**Tableau 4. 2 : Sommaire des protocoles de transmissions selon la norme ISO7816**

| Protocole | Correspondance |
|---|---|
| T=0 | Asynchrone, half-duplex, orienté octets, spécifié dans la partie 3 de la norme ISO7816. |
| T=1 | Asynchrone, half-duplex, orienté blocs, spécifié dans l'amendement de la partie 3 de la norme ISO7816. |
| T=2 | Asynchrone, full-duplex, orienté octets, spécifié dans la partie 4 de la norme ISO10536. |
| T=3 | Full duplex, pas encore spécifié |
| T=4 | Asynchrone, half-duplex, orienté octets, un projet d'extension du protocole T=0. |
| T=5 … 13 | Pas encore spécifié. |
| T=14 | Utilisation spécifique (éventuellement en Allemagne), pas encore spécifié. |
| T=15 | Réservé pour une utilisation futur. |

#### 4.11.1.1. Protocole de communication pour carte à puce par contact

Les données échangées au niveau applicatif à partir d'un terminal vers une carte à puce sont appelées commandes Application Protocol Data Unit (C-APDU). Les données échangées à partir d'une carte à puce vers un terminal sont les réponses Application Protocol Data Unit (R-APDU). La carte à puce va prendre le rôle esclave dans le dialogue. La communication est

définie dans la norme ISO/IEC 7816. La structure de la communication APDU est donnée sur la Figure (4.5) :

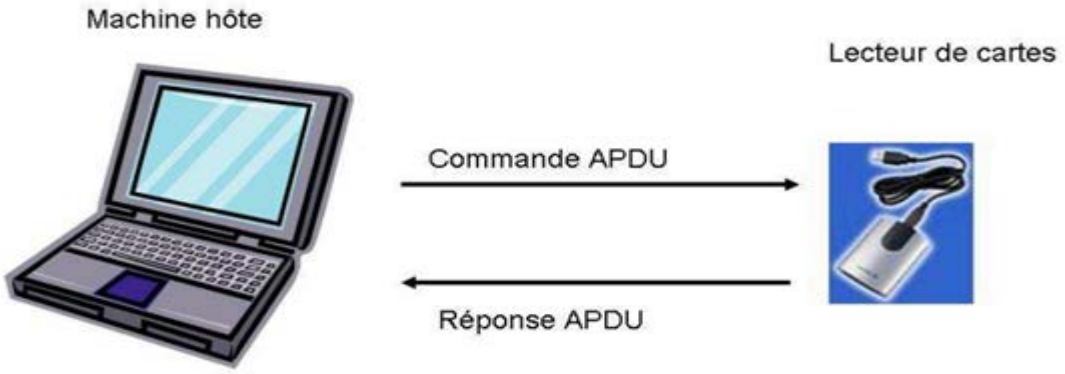


**Figure 4. 5 : Structure de la communication APDU**

#### 4.11.1.2. Format des commandes APDU

Le protocole APDU est le protocole de communication défini dans la norme ISO 7816-4, permettant à une applet s'exécutant sur une carte à puce de recevoir des requêtes émanant du terminal et d'envoyer des informations en réponse. Le dialogue entre la carte et le terminal se fait via un échange de commande et réponses APDU.

La Figure (4.6) représente les différents champs qui la composent :

| **Commande APDU** | | | | | | |
|---|---|---|---|---|---|---|
| Entête obligatoire | | | | Corps optionnel | | |
| CLA | INS | P1 | P2 | Lc | Data field | Le |

**Figure 4. 6 : Format de la commande APDU**

**CLA** : Classe de l'instruction

**INS** : Instruction

**P1** : Paramètre complémentaire

**P2** : Paramètre complémentaire

**Lc** (1 octet) : Nombre d'octets présents dans le champ données de la commande

**Le** : est le nombre maximum des octets attendus pour la donnée de l'APDU de réponse.

La longueur des paramètres (l'instruction détermine le sens, incoming si des données sont envoyées à la carte, entre 0 et 255, outgoing si des données viennent de la carte, entre 1 et 256)

**Tableau 4. 3 : Jeu d'instructions CLA**

| CLA byte | Jeu d'instruction |
|---|---|
| 0x | ISO/IEC 7816-4 instructions (files and security) |
| 10 to 7F | Reserved for future use |
| 8x or 9x | ISO/IEC 7816-4 instructions |
| AX | Application-and/or vendor-specific instructions |
| B0 To CF | ISO/IEC 7816-4 instructions |
| D0 To FE | Application-and/or vendor-specific instructions |
| FF | Reserved for protocol type selection |

Data field (octets dont le nombre est égal à la valeur de Lc) : une séquence d'octets dans le champ données de la commande. Certains d'entre eux sont résumés dans le tableaux suivant :

La norme ISO/IEC 7816-4 identifie un certain nombre d'instructions utilisées pour accéder à un système de fichiers sur carte et des fonctions de sécurité qui servent à limiter l'accès au système de fichiers et à la carte en général. Ces jeux d'instructions sont résumés dans le Tableau (4.4) :

**Tableau 4. 4 : ISO/IEC 7816-4 codes d'instructions**

| Valeur d'instruction | Nom de la commande |
|---|---|
| 20 | Vérifier (Verify) |
| 70 | Gérer la chaîne (Manage channel) |
| 82 | Authentification externe (External Authenticate) |
| 84 | Obtenez le défi (Get challenge) |
| 88 | Authentification interne (Internal authenticate) |
| A4 | Choisir le dossier (Select file) |
| B0 | Lire le binaire (Read binary) |
| B2 | Lire les enregistrements(Read record(s)) |
| C0 | Avoir une réponse (Get response) |
| C2 | Envelope |
| ca | Obtenir des données (Get data) |
| D0 | Écrire en binaire (Write binary) |
| D2 | Écrire un enregistrement (Write record) |
| D6 | Mettre à jour le binaire (Update binary) |
| DA | Mettre des données (Put data) |
| DC | mettre à jour l'enregistrement (Update record) |
| E2 | Attente d'un enregistrement (Append record) |

#### 4.11.1.3. Format des réponses APDU

La réponse APDU contient des informations sur le résultat de la commande et éventuellement des données si nécessaires. Elle est composée d'un champ de donnée et d'un mot d'état. La donnée doit respecter la taille indiquée dans le champ LE de la commande. Le mot d'état (Status Word) est codé sur deux octets : SW1 et SW2. SW1 indique si la commande a été correctement exécutée et SW2 correspond à des informations supplémentaires concernant la réponse.

Les commandes de réponses APDU sont transmises comme le montre la Figure (4.5) :

| Réponse APDU | | |
|---|---|---|
| Corps optionnel | Partie obligatoire | |
| Data field | SW1 | SW2 |

**Figure 4. 7 : Format de la réponse APDU**

Data field (longueur variable) : une séquence d'octets dans le champ données de la réponse

SW1 (1 octet) et SW2 (1 octet) : Statut Words (Mots d'état) -état de traitement par la carte.

### 4.11.2. Protocole de communication pour cartes à puces sans contact

Une distance de 10 et 20 cm de la borne de lecture suffit pour activer la puce. Une fois le contact établit, la puce et le lecteur échangent leurs données avec des débits pouvant atteindre 19,2Kbits/s. La communication occupe une de quatre bande de fréquence entre 125 KHz et 2,4 GHz selon la distance et la puissance de transmission requise ; sont utilisées en particulier la bande réservée aux applications industrielles (moins de 150KHz) ou celle des applications scientifiques et médicales (autour de 6,78MHz et de 16,56 MHz). La sécurisation de la transmission se fait selon la norme ISO/IEC 14443. Le protocole des échanges est dit d'Interface et Communication de Champ Proche NFCIP-1 (Near Field Communication Interface and Protocol).

## 4.12. Plateformes de programmation

Depuis longtemps, les cartes à puces ont été un environnement fermé. Ils ont été construits pour une seule application : le code de l'application et le système d'exploitation ont été inclus

dans la carte et masqués en permanence sur la puce. Le principal problème avec cette approche est le temps passé pour développer une carte pour chaque nouvelle application.

Aujourd'hui la technologie des cartes à puce fournit la possibilité de télécharger des multiples applications sur une seule carte, que ce soit pour cartes à puce avec ou sans contact. Les deux systèmes d'exploitation dominants et normalisés pour la multi application des cartes à puce sont JavaCard et MULTOS (MULTi-application Operating System).

Multos a été la première plateforme multi-applications des cartes à puces. De même que pour la Java Card, Multos possède aussi une machine virtuelle. Toutefois, lorsque Java Card a comme une machine virtuelle un sous-ensemble de la machine virtuelle Java, Multos a son propre langage (le langage émulateur Multos, ou MEL).

MEL est similaire du bytecode de Java dans le sens où les deux sont de bas niveau, et sont exécutées sur une machine virtuelle.

# Bibliographie

[1] A. Belhadri, Contribution à l'amélioration d'algorithmes dédiés à la cryptographie des cartes à puce, Mémoire de Magister, USTO 2011.

[2] A. C. Noubissi, A. Al-Khary Séré, J. Iguchi-Cartigny, J. Lanet, G.e Bouffard, J. Boutet, Cartes à puces : Attaques et contremesures, Conference:Majecstic At: Avignon, France, 2009.

[3] A.J. Menezes Paul, C. van Oorschot Scott, A. Vanstone, Handbook of Applied Cryptography, Edition CRC Press, ISBN :9780849385230; 0849385237, 1996.

[4] C. Tavernier, Les cartes à puce, Edition Dunod, ISBN 2100563475, 2011.

[5] D.M. Hashem Sherif, Paiements électroniques sécurisés, Presses polytechniques et universitaires romandes et groupe des Ecoles des Télécommunication (GET), 2007.

[6] J.G. Dumas, J-Louis Roch, É. Tannier, S. Varrette, Théorie des codes compression, cryptage, correction, Dunod, Paris, ISBN 9-78-210-050692-7, 2007.

[7] K. Mayes, K. Markantonakis, Smart Cards, Tokens, Security and Applications, Springer Edition, ISBN-13: 978-0-387-72197-2, 2008.

[8] L. Hacini, Cartes à puces, Polycopié de cours M1 Electronique des Systèmes Embarqués, Université de Bordj Bou Arreridj, 2020.

[9] L. Guillou, Histoire de la carte à puce du point de vue d'un cryptologue, 7e Colloque sur l'Histoire de l'Informatique et des télécommunications, p. 125-154, 2004.

[10] M. Bada, Les Problèmes De Sécurité Dans Les Systèmes Embarqués, Mémoire de Master, Université de Batna 2, 2012.

[11] M. Bahaj, R. Bahloul, Indicteurs de suivi et d'evaluation de la performance des cartes à puce et des secrets cryptographiques, Faculté des Sciences et Techniques Fès, ISBN. 978-9954-37-708-6, 2018.

[12] M. Chami, La Carte à Puce : Principes, Applications et Exercices corrigés, Sciences de l'ingénieur, 2017.

[13] M. Erritali, O.M. Reda, B. El Ouahidi, Contribution à la Sécurisation du protocole de routage « Greedy Perimeter Stateless Routing » à l'aide de l'algorithme AES et du hachage MD5, Revue Méditerranéenne des Télécommunications vol.2, n°1, janvier 2012.

[14] M. Khaldi, A. Boukoftane, Conception et implémentation du système « Radio Frequency Identification » à l'aide d'une carte Arduino et lecteur RFID, Mémoire Master, Université Djilali Bounaama Khemis Miliana, 2017.

[15] P. Urien, Introduction aux cartes à puce, Polycopie de cours, Télécom Paris, 2020.

[16] S. Ahmed Belhadj, Etude comparative entre la cryptographie à clé secrète et à clé publique appliquée aux textes arabes, Mémoire Master, Université de Tlemcen, 2014.

[17] S.A. Siddiqi, Smart Card Packaging Process Control System, Master Thesis, KTH Information and Communication Technology, 2012.

[18] S. Bouzefrane and P. Paradinas, Les Cartes à Puce, French. Hermes, ISBN: 9782746239135, 2013.

[19] T.M. Jurgensen, S.B. Guthery, Smart Cards: The developer's Toolkit, Prentice Hall, 2002.

[20] T. Peltier, La Carte Blanche : Un nouveau système d'exploitation pour objets nomades, Thèse de Doctorat, Université des Sciences et Technologies de Lille, 1995.

[21] W. Rankl and W. Effing, Smart Card Handbook, Wiley, 2010.

[22] Y. Haghiri, T. Tarantino, Smart Card Manufacturing: A Practical Guide, Wiley, 2002.

# Netographie

[1] http://www.pascalchour.fr/ressources/pccam/cours/cartes.htm#logique, Consulté en Decembre 2019

[2] http://www.smartcardbasics.com/smart-card-types.html, Consulté en Décembre 2019

[3] https://www.timcod.fr/solutions/tracabilite-technologies/rfid/ , Consulté en janvier 2020

[4] https://www.techniques-ingenieur.fr/base-documentaire/electronique-photonique-th13/cartes-electroniques-technologies-et-conception-42287210/cartes-a-puces-e3440/systemes-d-exploitation-e3440niv10005.html, Consulté en Mars 2020

[5] https://slideplayer.fr/slide/1172961/, Consulté en Mars 2020

[6] http://www.e-marketing.fr/Marketing-Direct/Article/Les-differents-types-de-cartes-3493-1.htm, Consulté en Mars 2020

[7] http://www-igm.univ-mlv.fr/~dr/XPOSE2002/puverel/contactless.html, Consulté en juin 2020

[8] https://www.ionos.fr/digitalguide/serveur/know-how/quest-ce-quun-systeme-dexploitation/, Consulté en Septembre 2020

[9] http://www.smart-webzine.com/le-marche-public-de-la-carte-a-puce-et-ses-tendances-6548, Consulté en septembre 2020

[10] https://www.techniques-ingenieur.fr/base-documentaire/electronique-photonique-th13/cartes-electroniques-technologies-et-conception-42287210/cartes-a-puces-e3440/cryptologie-et-securite-e3440niv10003.html, Consulté en septembre 2020

[11] https://www.elprocus.com/working-of-smart-card/, Consulté en Octobre 2020

[12] https://cedric.cnam.fr/~bouzefra/cours/Cartes_Intro.pdf, Consulté en Octobre 2020

[13] http://exo7.emath.fr/cours/ch_crypto.pdf, Consulté en Octobre 2020

[14] https://wakaziva.pagesperso-orange.fr/crypto/4.htm, Consulté en Octobre 2020

[15] http://www.primenumbers.net/Renaud/fr/crypto/DES.htm, Consulté en Octobre 2020

[16] http://www-igm.univ-mlv.fr/~dr/XPOSE2002/puverel/historique.html, Consulté en Octobre 2020

[17] https://www.techniques-ingenieur.fr/base-documentaire/electronique-photonique-th13/cartes-electroniques-technologies-et-conception-42287210/cartes-a-puces-e3440/semi-conducteurs-pour-cartes-a-puces-e3440v2niv10002.html, Consulté en Octobre 2020

[17] https://cartesapuce.blogspot.com/2016/07/fonctionnement-dune-carte-puce.html, Consulté en Octobre 2020

[18] https://www.techno-science.net/glossaire-definition/Carte-a-puce-page-4.html#ref_7, Consulté en Janvier 2021

[19] https://linux.goffinet.org/administration/confidentialite/chiffrement-symetrique, Consulté en Avril 2021

[20] https://www.magasin-lsa.fr/produits/10/lecteur-carte-bleue-iwl250-gpr-pN635163.html, Consulté en Septembre 2021

[21] http://perso.univ-lr.fr/gbailly/cours/chapitre5.pdf, Consulté en Septembre 2021

[22] https://www.securetechalliance.org/wp-content/uploads/CSCIP-G-Module-1-Smart-Card-Fundamentals-V5.1FINAL-0507151.pdf, Consulté en Octobre 2021

[23] http://igm.univ-mlv.fr/~dr/XPOSE2002/puverel/types_cartes.html, Consulté en Octobre 2021

# Annexe A

## Examen du module : Cartes à puces

Nom……..Prénom :……..Matricule :……..….

### Questions à choix multiple

Cocher la (les) bonne (s) réponse (s)

| | |
|---|---|
| **Q1) Le principe du chiffrement asymétrique nécessite deux clés.** | |
| | Vrai |
| | Une seule suffit |
| | Faux, il en faut 3 clés |
| | Aucune de ces réponses |
| **Q2) Les cartes magnétiques sont constituées d'un…** | |
| | processeur |
| | crypto processeur |
| | processeur et crypto processeur |
| | Aucune de ces réponses |
| **Q3) Un chiffrement à clé publique et à clé secrète sont des algorithmes de chiffrement …** | |
| | Symétrique |
| | Asymétrique et symétrique successivement |
| | symétrique et asymétrique successivement |
| | Aucune de ces réponses |
| **Q4) Les cartes à puces sans contact sont constitués du corps de la carte et d'une …** | |
| | puce seulement |
| | antenne seulement |
| | Puce et une antenne |
| | Aucune de ces réponses |
| **Q5) Le DES et RSA sont des algorithmes de chiffrement …** | |
| | Asymétrique et symétrique successivement |
| | Symétrique |
| | A apport nul de connaissance |
| | Aucune de ces réponses |
| **Q6) Dans le chiffrement symétrique …** | |
| | On encode et on décode le message avec la même clé |
| | On utilise une clé unique partagée entre les deux interlocuteurs |
| | Le problème de ce chiffrement est qu'il faut trouver un moyen de transmettre la clé unique entre les 2 interlocuteurs |

| | |
|---|---|
| | Aucune de ces réponses |
| **Q7) Le graphique guilloché …** | |
| | C’est une image 3D |
| | Fournit une protection anti-contrefaçon |
| | C’est une signature |
| | Aucune de ces réponses |
| **Q8) La norme ISO 7816 décrit les caractéristiques des** | |
| | cartes sans contacts |
| | cartes à mémoires |
| | cartes à puces à contact |
| | Aucune de ces réponses |
| **Q9) Le principe du chiffrement asymétrique …** | |
| | La clé privée n'est jamais transmise à personne |
| | La clé privée est diffusée publiquement sans problème |
| | La clé publique est diffusée publiquement sans problème |
| | Aucune de ces réponses |
| **Q10) Dans les cartes sans contact de proximité, l’alimentation en énergie se fait …** | |
| | Par couplage inductif et capacitif |
| | Par couplage inductif ou capacitif |
| | A l’aide de piles et par couplage capacitif |
| | Aucune de ces réponses |

## Question de cours

Q1). Qu’est-ce qu’une carte à puce?

Q2). Quelle est la différence entre les cartes magnétiques et les cartes à puces ?

Q3). Citer les différents types de carte à puce, et expliquer leurs modes de fonctionnement.

Bon examen !

Mme S. BELKACEM

# Rattrapage du module : Cartes à puces

Nom……..Prénom :……..Matricule :……..….

## Questions à choix multiple

Cocher la (les) bonne(s) réponse(s)

| | |
|---|---|
| **Q1). Dans un algorithme de chiffrement, …** | |
| | Les méthodes de chiffrement par substitution simple sont très fiables |
| | Le chiffrement symétrique utilise une clé différente pour chiffrer et déchiffrer le message. |
| | Le chiffrement asymétrique n'utilise qu'une clé pour chiffrer le message. |
| | DES et RSA sont des algorithmes de chiffrement symétrique. |
| | Le chiffrement asymétrique et plus rapide que le chiffrement symétrique. |
| | Aucune de ces réponses |
| **Q2). Dans une carte à puce, le processus de laminage consiste à…** | |
| | Rassembler les feuilles de plastique imprimées, ainsi que les couches internes des cartes. |
| | Imprimer sur les feuilles de plastiques |
| | Fabriquer le panneau de signature |
| | Aucune de ces réponses |
| **Q3). Les cartes magnétiques sont constituées d'une …** | |
| | Bande magnétique |
| | Antenne RFID |
| | Puce électronique |
| | Aucune de ces réponses |
| **Q4). Les cartes à puce à contact sont constituées d'une …** | |
| | antenne |
| | Puce électronique |
| | Puce électronique et une antenne |
| | Aucune de ces réponses |
| **Q5). Le processus de l'encartage consiste à …** | |
| | Fabriquer le corps de la carte |
| | Insérer la puce dans le corps de la carte |
| | Fabriquer la puce électronique |
| | Aucune de ces réponses |

## Questions de cours

Q1). Quels sont les étapes de fabrication de la carte à puce sans contact ?

Q2). Pour qu'elle objectif on fait l'intégration d'un algorithme de cryptage dans une carte à puce ?

Bon rattrapage !

Mme S. BELKACEM

# Examen du module : Cartes à puces

Nom……..Prénom :……..Matricule :……

## Questions à choix multiple

Cocher la (les) bonne (s) réponse (s)

| | |
|---|---|
| **Q1) Les cartes magnétiques sont constituées d'une …** | |
| | Bande magnétique |
| | Antenne RFID |
| | Puce électronique seulement |
| | Aucune de ces réponses |
| **Q2) Le processus de l'encartage d'une carte à puce consiste à …** | |
| | Fabriquer le corps de la carte |
| | Insérer la puce dans le corps de la carte |
| | Fabriquer la puce électronique |
| | Aucune de ces réponses |
| **Q3) Le Protocol APDU permet de …** | |
| | Recevoir des requêtes émettant d'un terminal seulement |
| | Recevoir des requêtes émettant d'un terminal seulement et d'envoyer des informations en réponse |
| | D'envoyer des requêtes à un terminal |
| | Aucune de ces réponses |
| **Q4) Les algorithmes de chiffrement AES et DES font partie des algorithmes de chiffrement …** | |
| | Symétrique |
| | Asymétriques |
| | A apport nul de connaissance |
| | Aucune de ces réponses |
| **Q5) La normalisation de la salle blanche obeit à la référence …** | |
| | ISO 14644 |
| | ISO 7816 |
| | ISO 14434 |
| | Aucune de ces réponses |
| **Q6) La technologie RFID est utilisée pour** | |
| | Carte à bande magetique |
| | Carte à contact |
| | Carte hybrid |
| | Carte sans contact |
| | Aucune de ces réponses |
| **Q7) La consommation énergétique des circuits TTL est …** | |
| | Elevée comparativement aux circuits MOS |
| | Faible comparativement aux circuits MOS |
| | Aucune de ces réponses |
| **Q8) Les circuits intégrés hybride sont construit sur un…** | |
| | Substrat isolant |
| | Conducteur |
| | Substrat semi-conducteur |

| | |
|---|---|
| | Aucune de ces réponses |
| **Q9) Le chiffrement symétrique consiste à utiliser …** | |
| | La même clé pour le chiffrement et le déchiffrement |
| | Une clé publique et une clé privée |
| | Aucune de ces réponses |
| **Q10) Les cartes à puces hybrides suit le standard ISO …** | |
| | 78816 |
| | 1443 |
| | 7816 |
| | Aucune de ces réponses |
| **Q11) La taille de la mémoire d'une carte à puce standard doit être …** | |
| | Supérieur à celle d'une java card |
| | Inferieur à celle d'une java card |
| | Aucune de ces réponses |
| **Q12) Dans une carte à puce, les systèmes d'exploitation ouverts …** | |
| | Destinés à une application particulière |
| | Permettent d'installer et désinstaller des logicielles après sa réalisation |
| | Permettent d'installer et désinstaller des logicielles avant sa réalisation |
| | Aucune de ces réponses |
| **Q13) Dans les cartes sans contact de proximité, l'alimentation en énergie se fait …** | |
| | Par couplage inductif et capacitif |
| | Par couplage inductif ou capacitif |
| | A l'aide de piles et par couplage capacitif |
| | Aucune de ces réponses |
| **Q14) Le principe du chiffrement asymétrique …** | |
| | La clé privée n'est jamais transmise à personne |
| | La clé privée est diffusée publiquement sans problème |
| | La clé publique est diffusée publiquement sans problème |
| | Aucune de ces réponses |

**Question de cours**

**Q1)** C'est quoi une carte à puce ?

**Q2)** Qu'elle est la signification des abréviations suivante : APDU, RNG, ATS, MAM ? et dans quels domaines sont utilisés.

**Q3)** Citer quelques future applications d'une carte à puce dans le monde.

Bon examen !

Mme S. BELKACEM

# Annexe B

**Semestre : 2**
**Unité d'enseignement : UED 1.2**
**Matière : Cartes à puces**
**VHS : 22h30 (Cours : 1h30)**
**Crédit : 1**
**Coefficient : 1**

**Objectifs de l'enseignement:**

Acquérir des notions techniques suffisantes sur la technologie, le fonctionnement et l'utilisation des cartes à puces en vue de son implémentation dans des projets sur les systèmes électroniques embarqués.

**Connaissances préalables recommandées :**

Architecture des systèmes à microcontrôleurs et/ou à microprocesseurs.

**Contenu de la matière :**

- Généralités, Historique, Applications et marchés de la carte à puce.
- Semi-conducteurs pour cartes à puces, Technologies, Composants en logique câblée, Microcalculateurs.
- Cryptologie et sécurité, Principes de la cryptographie, Crypto systèmes symétriques, Crypto systèmes asymétriques, Crypto systèmes à apport nul de connaissance, Sécurité physique et logique des cartes à puces.
- Principes de construction, Interconnexion des composants, Encartage, Connectique.
- Systèmes d'exploitation des cartes à puce, Généralités et mécanismes de base, Systèmes d'exploitation fermés, Systèmes d'exploitation ouverts.
- Communication par contact, Communication par radiofréquences.

**Mode d'évaluation :**

Examen : 100 %

**Références bibliographiques:**

1. W. Rankl and W. Effing, Smart Card Handbook, Wiley, 2010.
2. C. Tavernier, Les cartes à puce, Dunod, 2011.