La sécurité des cartes bancaires

Haris Coliche - Clément de Louvencourt

- - - -x

Quand on utilise sa carte bleue dans un distributeur automatique, on a souvent du mal à comprendre tout le processus de sécurité. Bien qu'il soit communément connu qu'il faut entrer son code secret pour débloquer le paiement, cela ne représente qu'un aspect de la sécurité des cartes bleues. Il est crucial de s'assurer que personne ne peut créer une fausse carte, voler votre identité bancaire et dépenser votre argent.

Sommaire

1- Introduction

Bien que nous sachions que la sécurité est au cœur de ces processus, nous avons du mal à comprendre tout ce qui se passe lorsque nous utilisons notre carte bancaire dans un terminal de paiement. Nous utilisons inconsciemment des protocoles cryptographiques.

Comment les données bancaires sont-elles sécurisées ? Comment pouvons-nous empêcher les tentatives de fraude ? En fin de compte, comment la cryptographie est-elle utilisée dans tout cela ?

Il convient de noter que nous nous concentrons ici sur un problème spécifique, le protocole de paiement par carte bancaire, mais que le sujet est en réalité beaucoup plus vaste et plus complexe à comprendre dans sa globalité, peu de ressources sont disponibles sur le sujet en ligne. Un protocole cryptographique consiste en une série d'échanges de messages chiffrés à l'aide de méthodes cryptographiques.

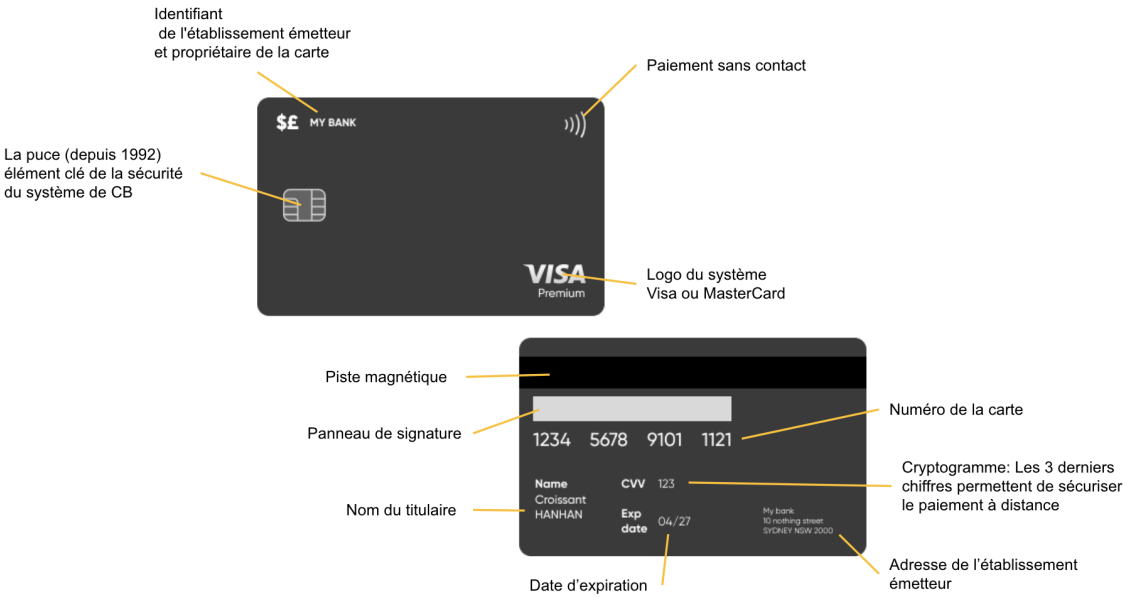
2- Histoire de la carte bancaire

En 1967, les premières cartes de paiement ont été lancées en France par six banques françaises (Crédit Lyonnais, Société Générale, Banque Nationale de Paris, Crédit Industriel et Commercial (CIC), Crédit Commercial de France (CCF) et Crédit du Nord).

Cette carte de paiement, appelée « Carte Bleue », n'était pas équipée d'une puce à cette époque (celle-ci a été créée quelques années plus tard, en 1974, par l'ingénieur français Roland Moreno). Il faut noter que ce n'est qu'en 1992 que l'utilisation généralisée de cartes à puce a commencé en France, faisant de ce pays un pionnier dans le domaine.

3- Présentation rapide

La carte bancaire est principalement constituée de ces éléments importants :



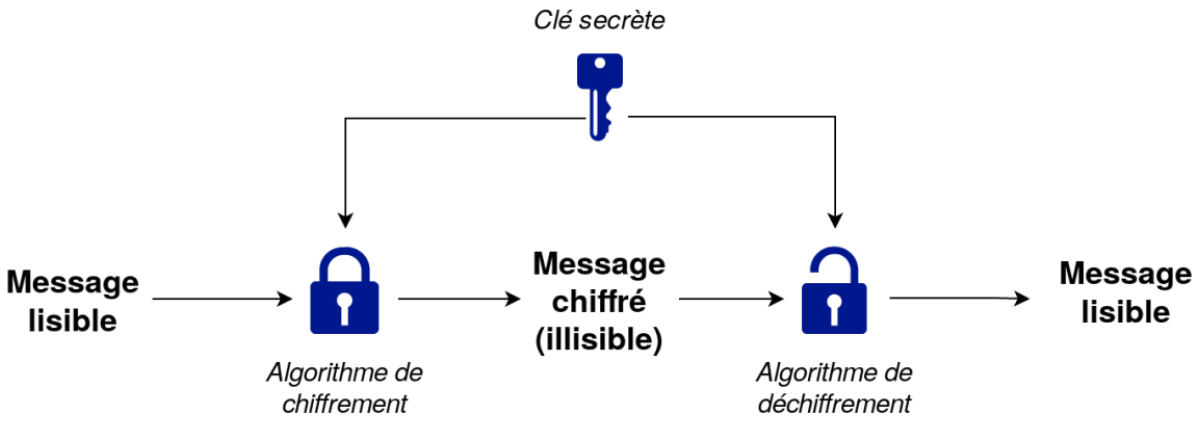
Le numéro de la carte (16 chiffres), date d'expiration, nom du propriétaire, la puce, la piste magnétique, le cryptogramme de sécurité.

La puce fonctionne comme un ordinateur, sa mémoire contient les données importantes de la carte : clés cryptographiques, le code secret ainsi que le compteur d'essai, cryptogramme, c'est l'élément essentiel de la sécurité de la carte bancaire.

Sur les anciennes cartes, il y avait un hologramme qui avait pour but de rendre la falsification plus difficile. Aujourd'hui cette sécurité est devenue obsolète devant l'ingéniosité et la créativité des faussaires pour trouver des nouvelles techniques de contre façons.

4- Méthodes de chiffrement

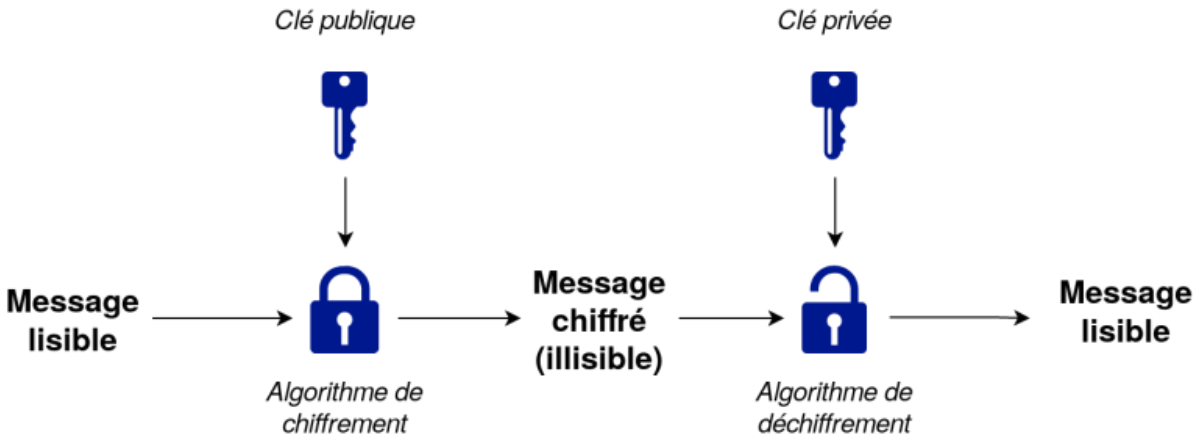
4.1- Chiffrement symétrique



Le chiffrement symétrique, également connu sous le nom de chiffrement à clé secrète ou privée, est la forme la plus ancienne de chiffrement. Ce type de chiffrement utilise une seule clé pour chiffrer et déchiffrer un message (par exemple, le Chiffre de César ou le chiffrement de Vigenère).

Pour chiffrer un message, on applique un algorithme à l'aide de la clé. En théorie, ce type de chiffrement est très sûr, car l'utilisation d'une clé de longueur au moins égale à celle du message garantit l'inviolabilité du message.

4.1- Chiffrement asymétrique



Le système de chiffrement peut être comparé à un cadenas fonctionnant avec deux clés :

- une clé publique servant de « cadenas »
- une clé privée représentant la clé du « cadenas ».

La cryptographie utilisant ce mode de fonctionnement repose sur l'existence de fonctions unidirectionnelles, c'est-à-dire des fonctions qui peuvent être facilement appliquées pour le chiffrement, mais qui sont extrêmement difficiles à inverser pour le déchiffrement.

5- Méthodes de paiement

5.1- Le paiement sans-contact / en-ligne

Ce type de paiement s'effectue couramment, lorsque l'on réalise un achat en ligne par exemple. Prenons le cas « classique ».

Ainsi, il suffit juste de donner : le numéro de la carte bancaire, la date de validité de la carte, le nom du propriétaire, le cryptogramme de sécurité.

Il est évident que ce mode de paiement est moins sûr qu'un achat "classique" nécessitant un code de carte, car si la carte est volée ou si les informations sont obtenues d'une autre manière, elles peuvent être utilisées à des fins frauduleuses.

Cependant, le cryptogramme de sécurité apporte une couche de sécurité supplémentaire, car il n'est pas stocké sur la carte.

La sécurité de ce type de paiement a été renforcée aujourd'hui. Certaines banques proposent des cartes bancaires « virtuelles » ou des cartes bancaires à cryptogramme dynamique.

On peut aussi citer le protocole 3D secure : le protocole 3D Secure a pour objectif de garantir que le titulaire de la carte effectue bien le paiement. Les détails de ce protocole peuvent varier selon les banques, mais pour finaliser la transaction, le client doit entrer un code d'authentification unique fourni par la banque, souvent par SMS. Ce protocole utilise le SSL auprès de la banque pour authentifier une requête HTTPS vers les serveurs de la banque.

Depuis peu, la directive européenne des services de paiement (DSP2) contraint les banques à valider une transaction avec non plus un, mais deux facteurs de nature distincte. Il peut s'agir d'une donnée connue (un code), détenue (une

autorisation envoyée sur un mobile), ou constitutive du client (une empreinte digitale ou le visage par exemple). Cette mesure a été prise suite au vote de la norme de sécurité votée en 2015 par le Parlement européen.

5.2- Le paiement avec un code

De nos jours, l'utilisation de la carte bancaire est devenue courante pour effectuer des achats. Cette méthode de paiement est rapide, efficace et pratique. Pendant les quelques secondes où la carte est insérée dans le terminal et que le code est entré, plusieurs opérations sont effectuées, notamment des chiffrements et déchiffrements. Le protocole utilise généralement le chiffrement asymétrique, avec l'algorithme RSA.

5.2.1- L'algorithme RSA

Le chiffrement RSA est l'un des algorithmes de cryptographie asymétrique les plus populaires et les plus utilisés dans le monde. Il a été inventé par Ron Rivest, Adi Shamir et Leonard Adleman en 1977.
Il utilise une paire de clés (des nombres entiers) composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles. Les deux clés sont créées par une personne, souvent nommée par convention Alice, qui souhaite que lui soient envoyées des données confidentielles. Alice rend la clé publique accessible. Cette clé est utilisée par ses correspondants (Bob, etc.) pour chiffrer les données qui lui sont envoyées. La clé privée est quant à elle réservée à Alice, et lui permet de déchiffrer ces données. La clé privée peut aussi être utilisée par Alice pour signer une donnée qu'elle envoie, la clé publique permettant à n'importe lequel de ses correspondants de vérifier la signature.

Le principe de base de l'algorithme est que deux nombres premiers, **p** et **q**, sont choisis et leur produit **n = p x q** est calculé. Ce nombre est utilisé comme module de chiffrement et de déchiffrement. Ensuite, deux nombres entiers e et d sont calculés de telle sorte que :

- **e** est un nombre premier avec **(p-1) x (q-1)**.
- **d** est l'inverse modulaire de **e**, c'est-à-dire que **e x d ≡ 1 (mod (p-1) x (q-1))**.

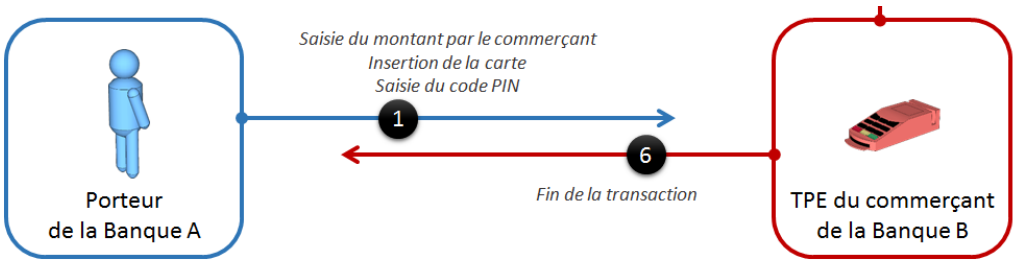
La clé publique est constituée de **n** et **e**, tandis que la clé privée est constituée de **n** et **d**.

Le chiffrement RSA consiste à prendre un message M et à le chiffrer en calculant le reste de la division de **M** élevé à la puissance e par n. Le message chiffré est donc **C = M^e (mod n)**.

Le déchiffrement RSA consiste à prendre le message chiffré **C** et à le déchiffrer en calculant le reste de la division de **C** élevé à la puissance **d** par **n**. Le message original est donc récupéré en effectuant **M = C^d (mod n)**.

La sécurité de l'algorithme RSA repose sur la difficulté de factoriser le produit **n** en ses deux facteurs premiers **p** et **q**. Si un attaquant parvient à factoriser **n**, il peut calculer les clés privées et déchiffrer les messages chiffrés. Cependant, si **p** et **q** sont suffisamment grands, la factorisation devient très difficile, voire impossible.

5.2.1- Analyse du paiement par code



{m}K, le message **m** chiffré par la clé **K**
A → B : m, l'envoi par l'agent **A** d'un message **m** à l'agent **B**

Lors de la création de la carte, un ensemble de données est inscrit sur la carte (plus particulièrement la puce) :

Un ensemble **data:{nom,prénom,numéro de carte}** en clair, et en chiffré, par la clé secrète du groupement bancaire **Kb^-1**. On l'appelle valeur de signature, **(S)={data}KB^-1** (calculée lors de l'initialisation de la carte, et stockée une fois pour toute dans celle ci). Le terminal possède la clé publique de la banque **Kb**. Le protocole peut se décrire ainsi :

T → A : « Authentification » : affichage de « authentification » sur le terminal.
C → T : Data, **{Data}KB^-1** : la carte envoie Data, **S** (valeur de signature) au terminal. Ainsi, le terminal déchiffre **S={Data}KB-1** à l'aide de la clé publique de la banque et vérifie qu'il correspond à la donnée Data. Si c'est le cas, la carte est valide.

T → A : « Code ? » : affichage de « code ? » sur le terminal.
A → T : XXXX : A envoie son code confidentiel à 4 chiffres au terminal.
T → C : XXXX : le terminal B envoie le code à la carte.
C → T : ok : la carte transmet au terminal qu'elle a accepté le code qui lui a été transmis.

6- Cas concret : faille de sécurité sur le protocole de paiement sans contact

Les progrès de la cryptographie ont permis la création de normes telles que le paiement par cartes bancaires ou en ligne, qui améliorent la sécurité lors des transactions financières. Cependant, ces normes comportent des étapes de validation, d'authentification et d'utilisation de codes, ce qui peut ralentir le processus de paiement. Dans certains secteurs où la rapidité est essentielle, comme la restauration rapide, les stations-service ou les cinémas, les transactions doivent être rapides. Pour répondre à ce besoin, les paiements sans contact ont été développés. Bien que présentant des avantages pour les commerçants et les banques, ces paiements sans contact présentent des failles de sécurité importantes.

6.1- Fonctionnement

Dans les années 2000, Visa et Mastercard ont développé ce service pour les paiements de tous les jours, et il a connu un grand succès. Le but de cette technologie est de simplifier les transactions, de réduire le nombre de paiements en espèces et d'augmenter la rapidité aux caisses. Cependant, étant donné que le paiement sans contact est destiné à des transactions de faible montant, il est limité à un montant maximum (50 € en France) et ne nécessite pas la saisie du code PIN.

Le principe de fonctionnement se base principalement sur un protocole de communication RFID (Radio Frequency Identification) / NFC(Near Field Communication). Il s’agit d’un moyen de communication de données et d’identification automatique. La puce RFID doit être collé au terminal de paiement, ce qui implique une portée très réduite.

6.2- Faille de sécurité

Renaud Lifchitz a découvert une faille de sécurité dans le paiement sans contact.

Il a démontré qu'en utilisant un simple lecteur RFID et un programme, il est possible de récupérer les informations de la carte bancaire, telles que le nom du propriétaire et la date de validité, lorsqu'on est suffisamment proche de la carte.

Les banques ont tenté de rassurer les clients en expliquant que la limite de paiement sans contact est de 20 euros (50 euros maintenant).

Cependant, en novembre 2014, des chercheurs de l'université de Newcastle ont découvert une faille encore plus importante dans le protocole, qui permettait de lancer des paiements théoriques allant jusqu'à 999 999,99 $, car la limite de 20 euros n'avait aucun effet si le paiement était effectué dans une devise étrangère.