L'ALGORITHME DE LUHN

En arithmétique modulaire, l'algorithme de Luhn est utilisé pour ses applications en cryptologie.
C'est une simple formule de somme de contrôle (*checksum*) utilisée pour valider une variété de numéros de comptes, comme les numéros de cartes bancaires, les numéros d'assurance sociale canadiens ainsi que pour le calcul de validité d'un numéro SIRET[1]. [NDLR : également pour les numéros IMEI[2]]

Elle fut développée dans les années 1960 par un ingénieur allemand de chez IBM, Hans Peter Luhn.
Sa notoriété provient de son adoption par les compagnies de cartes de crédit rapidement après sa création.

L'algorithme fait partie du domaine public et est largement répandu aujourd'hui.
Il n'a pas été conçu pour être une fonction de hachage sécurisée cryptologiquement : il protège contre les erreurs aléatoires, pas contre les attaques malveillantes. La plupart des cartes de crédit et beaucoup de numéros d'identification gouvernementaux utilisent l'algorithme comme une simple méthode de distinction de nombres valides dans des collections de chiffres aléatoires.

Source : Wikipedia

Ingénieur chez IBM, Luhn est connu pour avoir posé les fondements des sciences de l'information dans les années 1960. Il a notamment créé la méthode d'indexation par mots-clés dans le contexte (KWIC indexation) et a inventé le concept de diffusion sélective de l'information (DSI). Ce système a pour but de fournir aux chercheurs des informations actualisées, pour leur permettre de renforcer leurs capacités de recherche dans leur domaine de spécialité : cela s'est révélé indispensable pour la communauté scientifique en raison de l'explosion du nombre de publications après 1945.

1 Le Système d'identification du répertoire des établissements, ou numéro SIRET, est un code Insee permettant l'identification d'un établissement ou d'une entreprise française.

2 L'International Mobile Equipment Identity (IMEI, littéralement « identité internationale d'équipement mobile ») est un numéro qui permet d'identifier de manière unique chacun des terminaux de téléphonie mobile.
Pour l'obtenir, un utilisateur peut composer « *#06# » sur le clavier de son téléphone mobile. L'IMEI figure également sur la boîte et la facture de l'appareil, et l'opérateur peut également le communiquer à l'abonné, ce qui permet à un utilisateur d'en avoir connaissance même s'il n'a plus accès à son téléphone (perte, vol). Il permet, en cas de vol, d'interdire l'utilisation de l'appareil sur le réseau. En effet, lorsque le propriétaire porte plainte, le numéro de série se retrouve ajouté sur une liste noire et le téléphone ne sera plus autorisé à émettre des appels.

A. Numéro de carte bancaire

Cette séquence de 6 chiffres correspond à l'IIN (**Issuer Identification Number** en anglais), le numero d'identification de l'émetteur. Chaque entité (pas seulement les banques) en mesure d'émettre une carte de crédit, reçoit un numéro d'identification unique. Le mécanisme d'affectation est géré par l'ANSI (American National Standards Institute) qui a mis en place ce standard international connu sous le nom de ISO/IEC 7812.

AMEX: 34xxxx, 37xxxx
Diners Club International: 300xxx-305xxx, 309xxx, 36xxxx, 38xxxx-39xxxx
Visa: 4xxxxx
Mastercard: 51xxxx - 55xxxx

Par exemple, une carte commençant par 374960, indique une carte de crédit American Express Gold de Air France/ KLM. L'intégralité des **tables de correspondance** de tous les IIN est disponible sur le site de **l'ANSI**.

Cette séquence allant du 7ème à l'avant-dernier chiffre correspond au **numéro de compte** du détenteur de la carte. Elle a une longueur variable allant d'un minimum de 9 à un maximum de 12 chiffres selon le type d'émetteur.

Le 1er chiffre correspond au **MIN** (Major Industry Identifier), il s'agit d'un code permettant de classer les émetteurs par secteur d'activité.

1 and **2**: Compagnies aériennes,
3: Loisirs & Voyage,
4 and **5**: Banque & Finance,
6: Commerce & Banque
7: Pétrole
8: Santé, Télécom,
9: réservé aux structures étatiques

Le chiffre final est le checksum, le chiffre de contrôle. Toute carte valide doit avoir une séquence de chiffres qui obéit à l'algorithme de Luhn, ce chiffre ultime est généré au moment de l'établissement de la carte de façon à ce que la règle de Luhn soit vérifiée sur l'ensemble de la séquence. En utilisant notre **outil de vérification**, vous pouvez **vérifier la validité** de n'importe quelle carte de crédit.

Source : http://www.creditcard-validnumber.com/fr/creditcard_digits

Un numéro de carte bancaire est de la forme $\overline{a_{15}a_{14}\ldots a_2a_1a_0}$ où a_i sont des chiffres.

A chaque chiffre a_i, on associe le nombre $m(a_i)$ défini ainsi :

$m(a_i)=2a_i$ si $0\leqslant 2a_i\leqslant 9$

$m(a_i)=\alpha+\beta$ si $2a_i=\overline{\alpha\beta}$.

1. Démontrer que : $0\leqslant m(a_i)\leqslant 9$.

2. L'algorithme de Luhn consiste à vérifier que : $a_0+m(a_1)+a_2+m(a_3)+\ldots+a_{14}+m(a_{15}) \equiv 0\ [10]$.

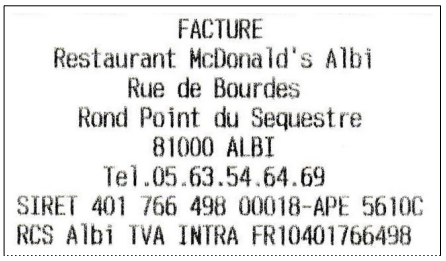
a) Vérifier que le numéro 4978 2100 3332 8381 est un numéro de carte bancaire valide.

b) Démontrer que si un seul chiffre est erroné, l'erreur est détectée.

c) Démontrer que la permutation de deux chiffres successifs distincts du numéro est détectée…
… sauf dans un cas. Lequel ?

B. Analyse d'un ticket de caisse : SIRET & TVA INTRA

Sur le ticket de caisse d'un achat au McDonald's, figure l'en-tête suivante :


FACTURE
Restaurant McDonald's Albi
Rue de Bourdes
Rond Point du Sequestre
81000 ALBI
Tel.05.63.54.64.69
SIRET 401 766 498 00018-APE 5610C
RCS Albi TVA INTRA FR10401766498

On peut y lire

SIRET 401 766 498 00018-APE 5610C

et

RCS Albi TVA INTRA FR10401766498.

Pour une fois, utilisons Internet intelligemment…

APE

Sur www.service-public.fr, on peut lire :

> *Le code APE (Activité Principale Exercée) permet d'identifier la branche d'activité principale de l'entreprise ou du travailleur indépendant. Sa fonction principale est statistique.*
> *Ce code est attribué par l'Insee lors de l'immatriculation ou la déclaration d'activité de l'entreprise, en fonction de l'activité principale déclarée et réellement exercée.*
> *Si une entreprise exerce plusieurs activités, ce qui rend difficile de déterminer son activité principale, c'est la ventilation du chiffre d'affaires ou des effectifs selon les branches qui est utilisée comme critère.*
> *Le code APE doit figurer sur les bulletins de paie des salariés.*

On peut trouver la liste des codes APE : http://www.insee.fr/fr/methodes/default.asp?page=nomenclatures/naf2008/liste_n5.htm
Quelques exemples : 01.21Z Culture de la vigne 01.47Z Élevage de volailles
11.05Z Fabrication de bière 96.02A Coiffure
20.51Z Fabrication de produits explosifs 55.10Z Hôtels et hébergement similaire
85.31Z Enseignement secondaire général 93.21Z Activités des parcs d'attractions et parcs à thèmes
Ici, pour le ticket qui nous intéresse : 56.10A Restauration traditionnelle
56.10B Cafétérias et autres libres-services
56.10C Restauration de type rapide

SIRET

Sur Wikipedia, on peut trouver, en les recoupant, les informations suivantes :

> *Le Système national d'identification et du répertoire des entreprises et de leurs établissements, couramment abrégé sous l'acronyme SIRENE, est le répertoire français géré par l'Insee qui attribue un numéro* SIREN[3] *aux entreprises, aux organismes et aux associations et un* SIRET *aux établissements de ces mêmes entreprises, organismes et associations.*
> *Le numéro* SIRET *est composé de quatorze chiffres, dont un chiffre de contrôle (le dernier) qui permet de vérifier la validité du numéro* SIRET. ***Celui-ci est calculé suivant la formule de Luhn***.
> *Les neuf premiers chiffres du numéro* SIRET *constituent le* SIREN *de l'entreprise et les cinq derniers le* NIC[4] *qui est spécifique à chaque établissement :* SIRET = SIREN + NIC.
> *Par exemple :* 732 829 320 00074 *correspond au septième établissement de l'entreprise au numéro* SIREN 732 829 320. *La clé* NIC *est le chiffre* 4.
> *Ainsi chaque établissement possède un* SIRET *unique selon l'adresse où il se trouve.*
> *Si une entreprise vient à fermer un établissement puis, par la suite, le recrée dans le même local, celui-ci aura toujours le même* SIRET.

1. Vérifier que la clé NIC est le chiffre 4 dans l'exemple ci-dessus.

2. Vérifier la clé NIC du SIRET du McDonald's qui a fourni le ticket de caisse.

3 Système d'Identification du Répertoire des Entreprises

4 Numéro Interne de Classement

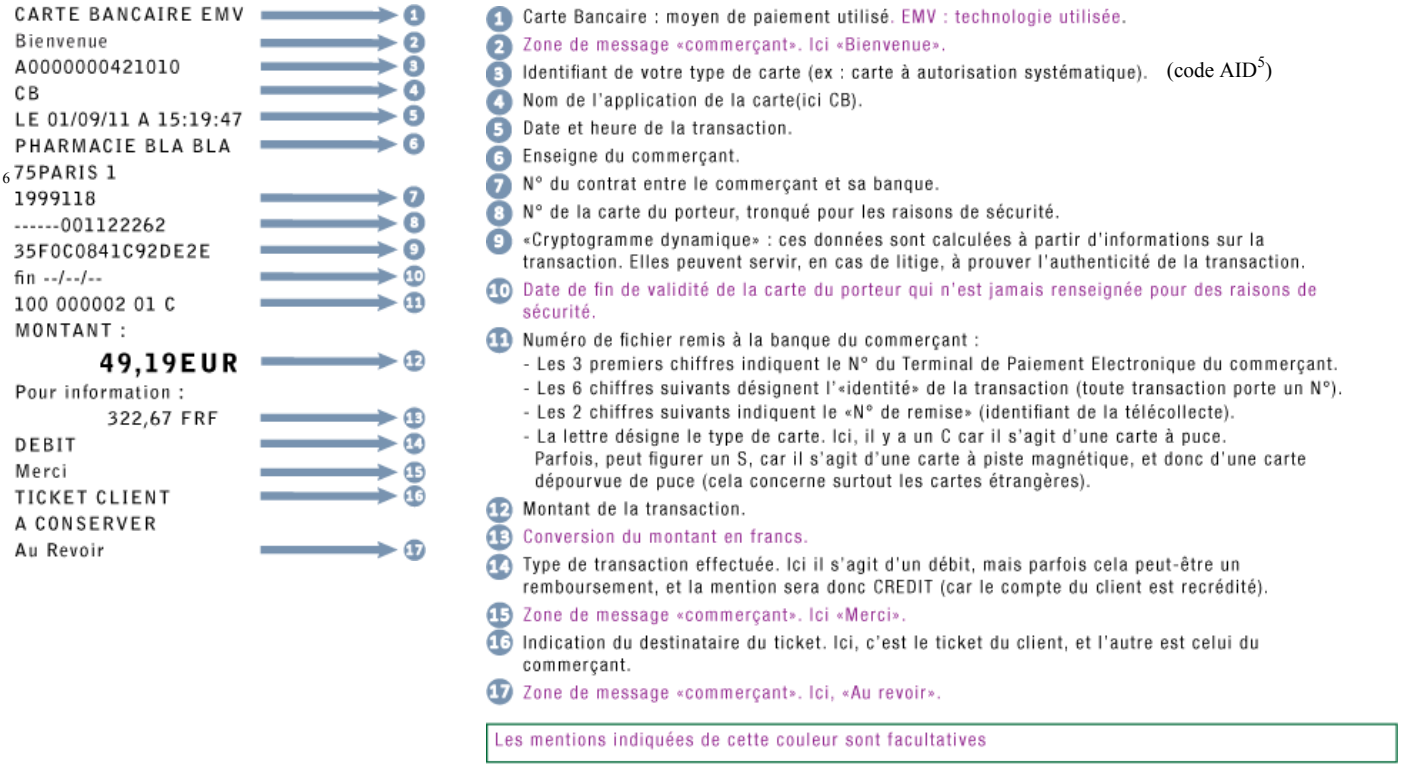
Sur Wikipedia, on peut trouver les informations suivantes :

> *Le numéro de TVA Intracommunautaire a été créé le 1er janvier 1993 pour garantir les échanges commerciaux intracommunautaires.*
> *Pour la France, il est composé des lettres FR, complétées d'une clé de deux chiffres ou lettres attribuée par le centre des impôts du lieu d'exercice de l'entreprise, et du numéro* SIREN *à neuf chiffres.*
> *La clé française suit la règle suivante :* Clé TVA = [12 + 3 × (SIREN modulo 97)] modulo 97.
> *Grâce à cette règle, il est aisé de connaître le numéro* TVA INTRA *à partir du numéro* SIREN.

3. Expliquer le TVA INTRA FR10401766498 présent sur le ticket de caisse du McDonald's.

C. Analyse d'un reçu de carte bancaire

Sur le site www.cartes-bancaires.com, on peut trouver le document suivant :



Remarque : Europay Mastercard Visa ou EMV est le standard international de sécurité des cartes de paiement (cartes à puce). L'acronyme EMV vient des 3 fondateurs qui sont Europay International (absorbé par Mastercard en 2002) ; MasterCard International et Visa International.

Voici un reçu de carte bancaire après un achat à la pharmacie Réveillon d'Albi →

On peut y lire une autre information (qui ne semble pas obligatoire) :

39358850400018

1. Conjecturer à quoi correspond ce numéro.

2. Démontrer votre conjecture.

5 *Application Identifier*

6 donnée qui peut être utile à un hacker voulant se faire passer pour le commerçant auprès de la banque de ce dernier

COMPLÉMENTS (PASSIONNANTS)

Pour en savoir plus sur la sécurité des cartes bancaires :
http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/cb

Méthodes modernes de cryptographie :
http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/index

Extraits du premier lien :

La piste magnétique et la puce ont des fonctions très différentes.
La piste magnétique comporte toutes les informations qu'on peut lire en ayant la carte en mains (nom de la banque, numéro, date d'expiration, etc.), hormis le cryptogramme de sécurité.
La puce, elle, est une sorte de petit ordinateur, avec un processeur (assez peu puissant) qui permet d'effectuer des calculs, une mémoire dont une partie est accessible en écriture (enregistrement de l'historique des transactions), une autre en lecture seule, et enfin une dernière en lecture cachée.
C'est cette puce qui gère la partie « code secret » et donc l'authentification des paiements par carte bancaire.

Les premières cartes bancaires, apparues en 1967, ne comportaient pas de puce.
La carte à puce a en effet été créée par deux ingénieurs français, Roland Moreno et Michel Ugon, en 1974.
Ce n'est qu'au début des années 1990 que les cartes bancaires avec puce se sont généralisées en France.
Aux États-Unis ou au Japon, il aura fallu attendre encore dix ans.

Jusqu'en 2001, les facturettes de cartes bancaires comportaient le numéro complet de la carte.
Autant dire que les voleurs étaient à l'affût de ces tickets souvent jetés négligemment !

L'affaire Humpich

En 1998, l'affaire Serge Humpich fait la une des journaux. Cet informaticien met en effet en évidence une faille dans le protocole décrit plus tôt. Ayant essayé de négocier, sans succès, son savoir-faire auprès du groupement des cartes bancaires, il fait une démonstration publique en achetant un carnet de tickets de métro en utilisant une carte de sa fabrication. Cela lui valut en février 2000 une condamnation à 10 mois de prison avec sursis, alors qu'il n'avait pas utilisé sa trouvaille à des fins crapuleuses.

Qui est S. Humpich ? (source : Wikipedia)

Il obtient son baccalauréat scientifique à Guebwiller en Alsace avant de poursuivre ses études à l'école d'ingénieurs INSA de Lyon.

Après l'obtention de son diplôme d'ingénieur électricien, il entre dans la finance en tant que développeur informaticien. Pendant 12 ans, il conçoit des logiciels d'aide à la décision pour gérer les ordres et les risques des traders.

Pendant son temps libre, il s'intéresse à la sécurité des appareils du quotidien et commence à travailler plus particulièrement sur la carte bancaire française vers le milieu des années 1990.
En 1997, il met en évidence une faille dans le système de sécurité des cartes bancaires.
Cette faille permet de créer des cartes acceptées par les terminaux, mais non liées à un compte bancaire.

Épaulé par un avocat, il tente – sans succès – de négocier son « savoir-faire » auprès du GIE des cartes bancaires. Pour démontrer la faisabilité de cette technique, il effectue une démonstration publique de la vulnérabilité des cartes en retirant un carnet de tickets de métro au moyen d'une carte de sa fabrication dans un distributeur automatique. Cette tentative lui vaut une perquisition, la saisie de son matériel et une mise en garde à vue.

Il est jugé le 25 février 2000, « coupable de falsification de cartes bancaires et d'introduction frauduleuse dans un système automatisé de traitement ». Et cela, malgré de nombreux soutiens envers son geste, qui a mis en évidence des failles techniques et de conception à corriger dans ces cartes bancaires.
Il est condamné à 10 mois de prison avec sursis et s'est ensuite désisté de la procédure d'appel qu'il avait lui-même engagée. À l'issue de cette condamnation, il écrit un livre, *Le cerveau bleu*, pour relater sa version de l'affaire.