Benuts

K1wy <k1wy.mail@gmail.com>

LA SECURITE DES CARTES A BANDE MAGNETIQUE

INTRODUCTION :

L'information est présente partout dans la vie, et à acquis une importance capitale dans le monde actuel. Il a donc fallut trouver des supports pour stocker ces informations à la fois petit, léger, pratique. Les cartes sont alors apparues permettant d'enregistrer plus ou moins sensible, elles ont aujourd'hui de nombreuse fonctions : carte de fidélité, carte bancaire, carte de transport, etc. Une question s'est alors posée, comment assurer la sécurité et l'authenticité des informations de la carte. La technologie ayant évoluée de nombreux types de cartes sont apparus, tel que les cartes à puce, les cartes à bande magnétique, ou les cartes avec RFID. Nous nous sommes intéressés aux cartes à bande magnétique, car ce sont les plus faciles à lire et les plus accessibles. Comment est encodée l'information sur ce type de carte et quels sont les moyens mis en place pour assurer sécurité de ces données ?

Nous allons donc voir comment les données sont stockées sur la carte magnétique et quels sont les moyens physiques puis numérique pour assurer leur sécurité.

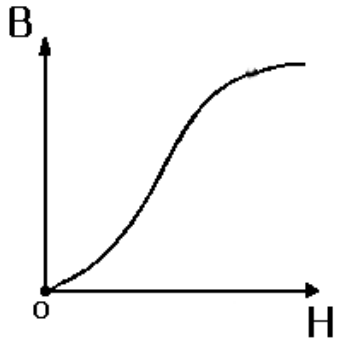
Première Partie : Stockage des données.

Principe :

Sur ce type de carte les informations de la carte sont contenue exclusivement sur a bande magnétique. Cette dernière est composée de micro particules ferromagnétiques dispersées dans un liant. Lorsqu'on applique un champ magnétique à ce mélange, les particules se comportent comme de petits cristaux aimantés qui prennent une certaine orientation selon la valeur du champ magnétique. En choisissant un champ définit on peut alors contrôler ces particules. Il existe plusieurs types de particule, mais celle retenue pour les cartes magnétiques courante est l'oxyde de fer.

Tous ces types de particules ont une certaine rémanence : cette propriété permet à un matériau magnétique d'acquérir et de conserver une aimantation permanente (même éloigner d'un champ magnétique).

Pour écrire sur cette bande il faut appliquer une excitation magnétique externe (tête d'écriture). Plus le champ magnétique appliqué à la bande sera élevé plus les particules auront une orientation similaire. Cela permet d'avoir des regroupements de particule ayant toute la même orientation



Ici H est l'intensité du champ magnétique appliqué aux particules par notre tête d'écriture. Et B l'intensité de la magnétisation induite. On voit que plus H est important plus la magnétisation induite le sera jusqu'à un certain seuil.

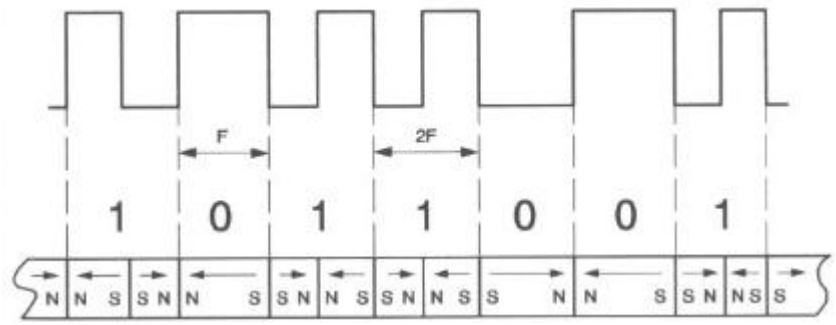
http://premiumorange.com/daniel.robert9/images/Courbe_hysteresis.gif

Lecture et écriture :

Le codage numérique (c'est-à-dire une suite de 0 et de 1) ne parait pas compliquer à mettre en place. En effet, on peut penser qu'une simple inversion de flux peut symboliser un 0 (niveau bas) ou un 1 (niveau haut). Cependant, un problème se pose : comment séparer avec précision une série de plusieurs 1 ou de plusieurs 0 à la relecture ? On utilise alors le codage F/2F.

Le codage F/2F est une technique qui permet de différencier les 0 et les 1 en se basant sur une durée (modulation de fréquence). On symbolise alors le 0 par une simple inversion de flux tandis que le 1 est codé par 2 inversions de flux consécutives. La longueur entre une inversion pour un 0 et deux inversions pour un 1 sont égales. On a donc F pour 0 et 2F pour 1. Au début de la piste, on trouve une suite de 0 permettant à l'horloge du lecteur de se synchroniser.

Pendant le défilement de la bande sous la tête d'écriture, le champ magnétique généré par cette tête va subir plusieurs inversions du à des variations d'intensités.



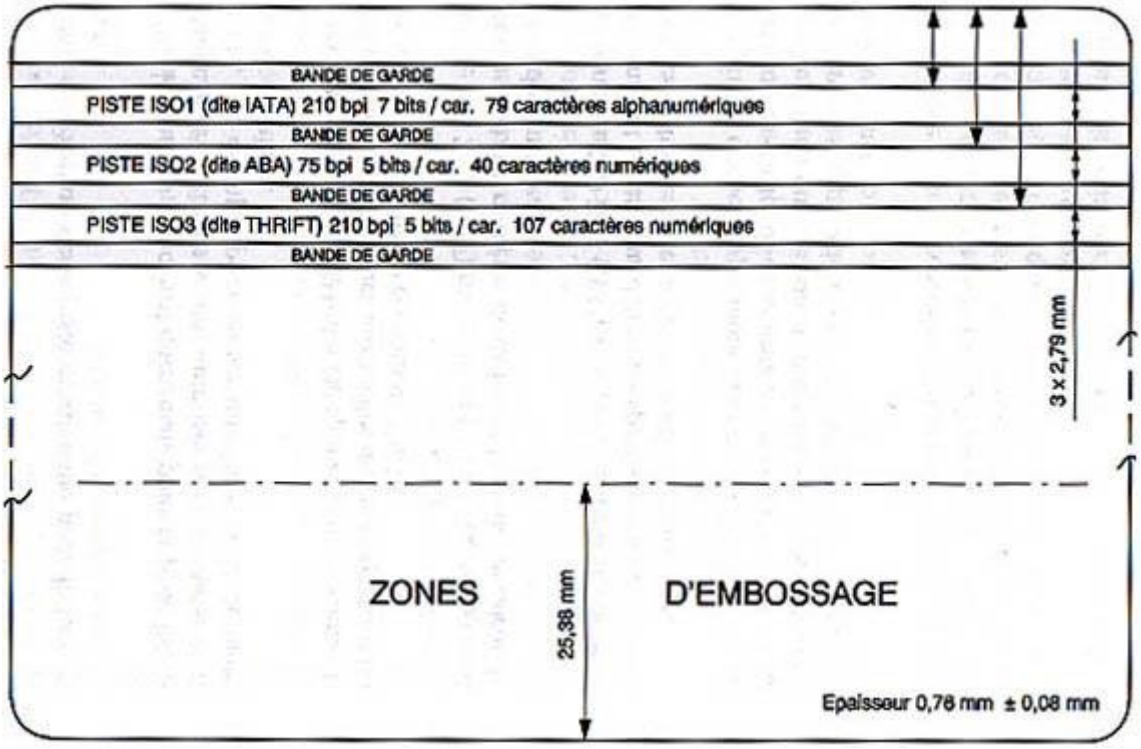
Principe du codage F/2F.

Patrick Gueulle : « Cartes magnétiques et PC »

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

Normes d'encodage :

Il existe une série de normes qui définissent différentes caractéristiques pour les cartes à bandes magnétiques. Notamment l'encodage et la répartition des informations sur la bande. Ces normes ont été définies par un organisme s'appelant ISO : International Organization for Standardization. Ces normes sont numérotés 7810, 7811 et 7813 (pour les cartes financières). Ces normes définissent 3 pistes sur la bande magnétique. Voici un schéma de la disposition de ces pistes de manière standard :



http://www.securiteinfo.com/attaques/divers/cartesmagn.shtml

- La piste ISO1, qui permet de stocker 210 bit par pouce, soit environ 82 bit par cm.
- La piste ISO2, qui permet de stocker 75 bit par pouce, soit environ 29 bit par cm.
- La piste ISO3, ayant les mêmes caractéristiques que la piste 1

Ces normes définissent aussi des codes alphanumériques faisant la correspondance entre une suite de bit et un caractère particulier. La piste ISO1 a pour codage un alphabet sur 7 bits (annexe 1) et les piste 2 et 3 un alphabet à 5 bits (annexe 2).

Ces codes contiennent aussi des caractères spéciaux de début et de fin de piste (qui encadrent l'information) et des séparateurs.

Il est à noter que ce ne sont que des standards et que les fournisseurs de cartes ne sont pas tenus de les respecter (hormis carte financière). Les tickets de tram par exemple n'utilisent que la piste 2 mais respectent quand même les dimensions qu'une carte financière au niveau du support ainsi que le même codage. Dans les cartes que nous avons tenté de décoder, il est apparu que la piste 2 est la plus utilisée.

Deuxième partie : la sécurité

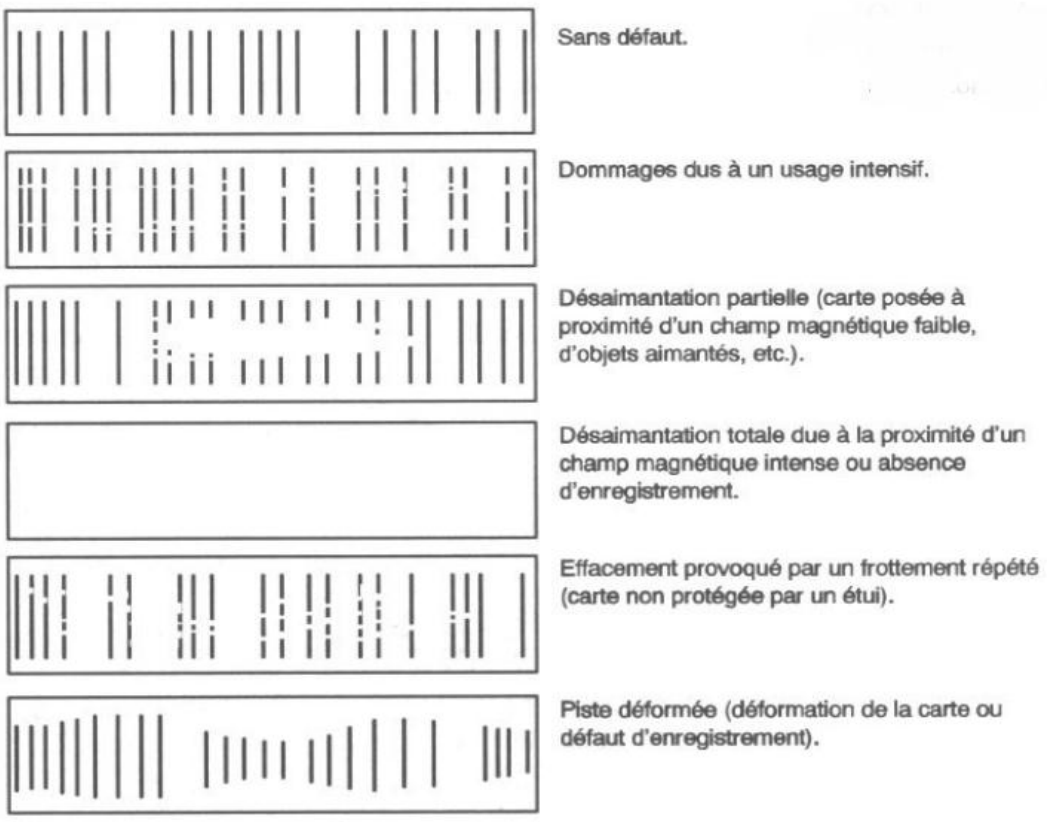
Dans cette partie nous allons traiter des différentes solutions autant physiques que numériques misent en place pour assurer la sécurité et l'intégrité des données encodés sur la carte.

Sécurité physique :

La première caractéristique importante pour éviter les erreurs et assurer la pérennité des données est d'utiliser un matériau pour la bande magnétique à haute coercitivité. La coercitivité est la capacité du matériau à garder la magnétisation qu'on lui a appliqué à l'écriture.

Lorsqu'on applique un champ magnétique extérieur sur la bande (comme on le fait à l'écriture), cette dernière doit pouvoir garder les données précédemment transmises. Elle ne doit pas s'altérer au cours du temps, ni avec une utilisation fréquente. Pour cela nous utilisons des matériaux à haute coercitivité pour les bandes magnétiques, le matériau le plus couramment utilisé sur les pistes est l'oxyde de fer. Il s'agit tout simplement de sa résistance à la désaimantation.

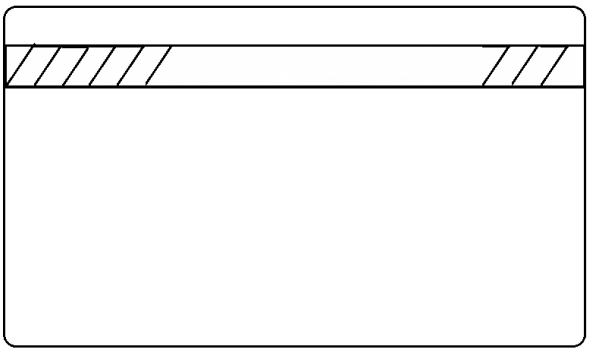
On utilise alors des matériaux à haute coercitivité pour éviter des effacements accidentels des données par des objets plus ou moins aimantés. Voici les différents types d'effacement que l'on peut retrouver (d'après doc. Thomson LCC) :



On utilise alors pour palier à ce problème d'effacements des matériaux à assez hautes coercivités. Outre le problème des effacements, il faut prendre en compte les éventuelles possibilités de réécritures. Les machines servant à réécrire sur une bande magnétique sont disponibles dans le commerce. Cependant, plus la piste a une coercivité importante, plus il faut générer un champ magnétique puissant. Le coût de ces machines augmente proportionnellement avec la coercivité de la carte à écrire. C'est un moyen de se protéger contre les tentatives de réécriture.

Un autre moyen de se protéger physiquement contre la modification d'une carte est de ne pas respecter les normes.

On peut décider d'écrire les données de façon hélicoïdale. Les données ne sont plus parallèles sur la longueur de la carte mais en biais ce qui permet d'éviter toute lecture par un lecteur non spécialisé.



Enfin, un dernier moyen de protéger la lecture et l'écriture d'une bande magnétique par un système « étranger » est de ne pas utiliser des cartes normalisées. Suivant les normes présentées précédemment, on retrouve généralement trois pistes sur la bande magnétique. Certaines cartes alors ont la bande magnétique divisées en plusieurs parties disposées à divers endroits de la carte. Voici un exemple de ces cartes :

Ceci est un passe pour une serrure électronique.

Les données sont inscrites sur la flèche.

http://www.fadini.net/prodotto.asp?language=FRA&id=90

En conclusion, même s'il existe des normes sur la disposition des pistes magnétiques et sur la façon d'écrire sur ces dernières, on retrouve de nombreux modèles de cartes magnétiques non conformes afin d'augmenter la sécurité des données contenue sur la carte. Il existe aussi des moyens numériques pour protéger ces données.

La Sécurité numérique :

La sécurité numérique est primordiale pour protéger les données de la carte magnétique et en assurer leur intégrité. Le plus important au départ est de savoir si l'information que l'on a lu sur la carte est bien valide, en effet le lecteur doit prendre en compte les erreurs qui peuvent se produire sur un bit, comme une inversion, un rajout ou encore une suppression. Mais il existe aussi des codages afin de chiffrer les informations contenues sur la carte. Pour tous ces problèmes il existe plusieurs solutions et nous allons en voir quelques-unes.

Le bit de parité :

Dans un premier temps, nous allons voir comment détecter les erreurs dans une séquence. Lorsque l'on reçoit un message binaire il est alors découper en séquence de n bits. Le contrôle par bit de parité consiste à rajouter un bit à la fin séquence. Si le nombre de 1 dans la séquence est pair alors le bit de parité sera égal à 0, et si le nombre de 1 est impair alors le bit de parité sera égal à 1.

Par exemple :

Pour une séquence 0110101 on rajoute un 0 à la fin ce qui donne 0110101***0***

Pour une séquence 0101100 on rajoute un 1 à la fin ce qui donne 0101100***1***

Bien que cette technique soit utile pour détecter des erreurs, elle ne permet en aucun cas de trouver où elle est apparue et donc de la corriger. Elle nécessite donc le renvoie du message. De plus, il existe plusieurs cas où elle est inefficace. Prenons par exemple un message original 0110101**0** et imaginons maintenant que deux erreurs se produisent sur deux bits différents. Le message devient 1010101**0**. On voit que le bit de parité n'est pas le même, bien qu'il y a eu erreur.

On peut calculer la probabilité pour le contrôle de parité de détecter une erreur :

*On suppose que chaque bit à la même probabilité **p = 1/8** d'avoir une erreur. Et l'erreur sur un bit ne dépend pas de l'erreur sur un autre bit. Les éléments sont indépendants. Soit **X** le nombre de bits erronés dans un message, et suit une loi binomiale de paramètre **n**. On a donc la probabilité pour une erreur sur **k** positions :*

$$P(k) = \binom{8}{k} p^k (1-p)^{8-k}$$

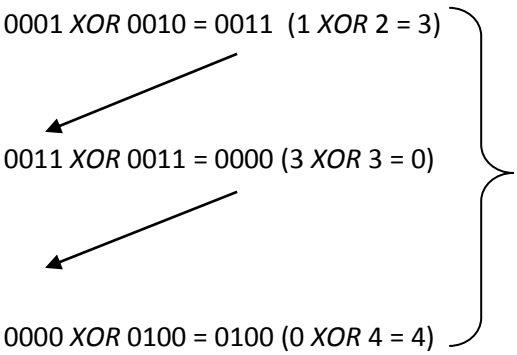
La probabilité que la transmission réussisse est P(0) = q^8

LRC (Longitudinal Redundancy Check) :

Le LRC est, tout comme le bit de parité, un contrôle pour la détection des erreurs. Il permet lui aussi de s'assurer de l'intégrité des données lues. A lui tout seul, il n'est guère plus efficace que le contrôle par bit de parité mais en combinant les deux, on obtient certes une séquence plus longue mais qui détecte un grand nombre d'erreurs.

Il fonctionne en appliquant un *XOR* (ou exclusif) « glissant » sur la totalité de la séquence. Prenons l'exemple d'une séquence : 1, 2, 3, 4 qui se représente en binaire par 0001, 0010, 0011, 0100 (bit de poids faible à droite).

Le LRC pour cette séquence donne :



La séquence avec le LRC sera donc : 0001, 0010, 0011, 0100, ***0100.***

Ensuite on ajoute à chaque bloc le bit de parité qui sera donc : 0001**1**, 0010**1**, 0011**0**, 0100**1**, 0100**1**.

Dans les cas des cartes magnétiques, le contrôle LRC est appliqué bit par bit à tous les caractères contenus entre les drapeaux *START* et *END*. Il sera donc mis à la suite du drapeau *END.*

Nature des données :

Avant tout, la sécurité qu'on apporte à des données doit être spécifique à leur nature. On évitera alors de stocker des données confidentielles sur un support lisible facilement (comme une bande magnétique), mais on favorisera l'utilisation d'un identifiant unique. Une fois la carte lue, on utilisera l'identifiant qu'elle contenait pour l'envoyer à un serveur distant et récupérer les informations confidentielles. Cela permet d'éviter tout problème de réécriture par modification des données, car seules certaines machines ayant les autorisations nécessaires pourront modifier les informations contenues directement sur le serveur, et non sur la carte.

Cryptographie :

Un autre moyen utilisé pour empêcher cette fois-ci la lecture de l'information. On se base sur quelque chose que la personne connaît (un code PIN par exemple). Avec un algorithme de chiffrement (exemple : DES utilisé par les cartes bancaires), on déchiffre les informations contenues sur la bande avec le code PIN fournit par l'utilisateur. Le lecteur vérifie ensuite la validité de la carte pour savoir si le code est correct. On peut aussi imaginer coupler plusieurs vecteurs couplés à l'utilisation d'une carte magnétique : biométrie, reconnaissance vocale ...

Exemples de cartes magnétiques :

Dans cette partie nous allons étudier deux types de cartes à bande magnétique : les tickets de bus et tram de la Semitag (Société d'économie mixte des transports publics de l'agglomération grenobloise) ; et les cartes bancaires Visa.

Les tickets de bus et de tramway :

Nous allons prendre l'exemple d'un ticket de bus/tram délivré par la semitag (transport en commun de l'agglomération grenobloise). Nous avons à notre disposition une machine permettant de lire les cartes à bande magnétique. Cet appareil nous permet de vérifier très facilement le passage du LRC et du bit de parité, puisque la machine envoie les données à l'ordinateur uniquement lorsque la séquence est valide (toutes les machines fonctionnent comme cela). Nous avons aussi développé un programme sommaire pour interpréter les données sur la carte (affichage du drapeau Start/end, reconnaissance de la piste, etc. disponible dans l'archive.

Après avoir récupéré un certain nombre de cartes, nous avons pu par rétro-ingénierie interpréter certaines données.

Sur un ticket de bus/tram, seul la piste ISO-2 est utilisée à l'exception que 43 caractères sont présents et non 40. Les données sont disposées selon ce schéma (ce ne sont uniquement que des suppositions faites par déduction) :

{Start}{Type de Carte} {Voyage Restant/Temps restant(?)} {??????} {ID de la borne : ID_BUS+IDBorne} 00002{End}

Type de Carte (5 bits) : 87401 (1 voyage), 87402 (10 voyages) 87415 (Visitag 1 jour)
Voyage restant (8 bits) : entier positif
Temps restant (8 bits) : reste à déterminer
?????? (6 bits): à déterminer
*ID_Bus/Tram (4 bits) : la ligne ou 8*00 pour une borne de tram*
ID Borne (12 bits) : l'ID de la borne qui a validé le ticket
00002 : Se finit toujours par 00002 (bits de remplissage ?)

Les différentes sauvegardes des pistes effectuées sont disponibles en annexe.

On voit alors que le nombre de voyage restant est marqué en clair sur la piste magnétique. Il est alors très facile avec une simple machine permettant d'écrire sur les cartes de rendre une carte « illimitée » !

Économiquement parlant, la solution de mettre ces données en claires est avantageuse pour la semitag. Les bornes n'ont pas besoin d'être reliées à un terminal central (ce qui est un dispositif couteux). De plus le prix d'une machine permettant d'écrire sur une bande magnétique est d'environ 225 €. Le coup de la machine est donc beaucoup plus élevé que le prix d'un ticket. Rendre un ticket « illimité » n'a donc pas de réel intérêt économique.

Cependant, d'un point de vue strictement sécuritaire, on ne peut considérer ce type de ticket comme sûr.

Les cartes bancaires VISA :

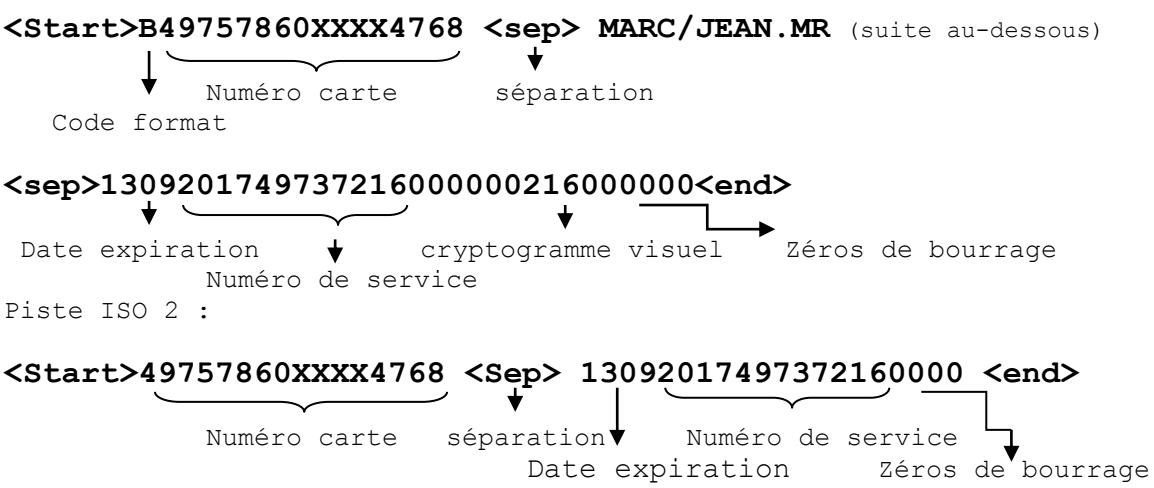
Nous allons maintenant nous intéresser aux cartes bancaires ainsi qu'à leurs données stockées sur la bande magnétique. La bande magnétique des cartes bancaires est une simple reproduction de la puce, les informations stockées sont exactement les mêmes, mais la carte à puce est maintenant beaucoup plus sécurisée et donc beaucoup plus utilisé pour les paiements.

Les informations contenues sur les différentes pistes sont aussi les nombres et les noms gravés sur la carte :

Par exemple :

- Détenteur de la carte : Mr Jean MARC
- Numéro de la carte : 49757860XXXX4768
- Expiration : 09/13

Piste Iso 1 :



Piste ISO 2 :

Contrairement a ce que l'on pourrait penser ces informations parfaitement lisible par un simple lecteur de cartes, seul les données sensibles contenue sur la carte tel que le numéro du cryptogramme visuel est crypté (ce qui est logique car on peut payer uniquement en sachant ce numéro et le numéro de la carte sur internet). Le code PIN permet alors de déchiffrer les données sur la carte.

Conclusion :

En conclusion, on peut observer que, bien qu'il existe différents moyens permettant de vérifier l'intégrité des données et de les sécuriser, la carte à bande magnétique n'est pas un moyen sûr pour stocker des informations confidentiels. En effet, bien que les bandes magnétiques soient économiquement avantageuses à produise, la possibilité de lecture et d'écriture rend la sécurité des données trop faible. D'autres moyens ont alors étaient mis en place pour le stockage des données sur une carte, comme par exemple les cartes à puces ou la technologie RFID.

Bibliographie :

- http://sysdoc.doors.ch/ASCOM/Validators_e.pdf (ticket tram)
- http://www.certu.fr/fr/_Syst%C3%A8mes_de_transports-n26/Intermodalit%C3%A9-n80/Billettique-n82/IMG/pdf/recensement.pdf (ticket tram)
- http://parodie.com/monetique/vulnerabilite.htm (info CB DES56)
- http://www.latelierweb.com/infoweb/securite/info&secuCarte/carteB.txt (Info CB)
- http://stripesnoop.sourceforge.net/devel/layoutstd.pdf (Données sur une CB)
- http://stripesnoop.sourceforge.net/devel/ (Doc sur les cartes)
- http://en.wikipedia.org/wiki/Magnetic_stripe_card (Codage de l'information sur une CB)
- Electromagnétisme théorie et application Elie Boridy - presses de l'université du Québec
- http://www.gae.ucm.es/~padilla/extrawork/magexam1.html (carte de crédit)
- Cartes Magnétiques et PC - Patrick Gueulle - Ed. Techniques et Scientifiques Françaises 1997
- Introduction aux Codes Correcteurs - Pierre Csillag - Ellipse 1990
- Codes Correcteurs d'Erreurs – Gérard Cohen, Jean-Louis Dornstetter, Philippe Godlewski – MASSON 1992
- Magnétisme : Statique, induction et milieux - Christian Garing – Ellipse 1999
- Magnétisme – Etienne du Trémolet de la Lacheisserie – EDP 2001
- http://www.cyberd.co.uk/support/technotes/isocards.htm

Annexe :

Table de caractère 7bits : (http://www.cyberd.co.uk/support/technotes/isocards.htm)

Data bits							Character	Value	Function
b1	b2	b3	b4	b5	b6	b7		(Hex)	
0	0	0	0	0	0	1	space	00	Special
1	0	0	0	0	0	0	!	01	Special
0	1	0	0	0	0	0	"	02	Special
1	1	0	0	0	0	1	#	03	Special
0	0	1	0	0	0	0	$	04	Special
1	0	1	0	0	0	1	%	05	**Start Sentinel**
0	1	1	0	0	0	1	&	06	Special
1	1	1	0	0	0	0	'	07	Special
0	0	0	1	0	0	0	(	08	Special
1	0	0	1	0	0	1	)	09	Special
0	1	0	1	0	0	1	*	0A	Special
1	1	0	1	0	0	0	+	0B	Special
0	0	1	1	0	0	1	,	0C	Special
1	0	1	1	0	0	0	-	0D	Special
0	1	1	1	0	0	0	.	0E	Special
1	0	0	1	0	0	1	/	0F	Special
0	0	0	0	1	0	0	0	10	Data
1	0	0	0	1	0	1	1	11	Data
0	1	0	0	1	0	1	2	12	Data
1	1	0	0	1	0	0	3	13	Data
0	0	1	0	1	0	1	4	14	Data
1	0	1	0	1	0	0	5	15	Data
0	1	1	0	1	0	0	6	16	Data
1	1	1	0	1	0	1	7	17	Data
0	0	0	1	1	0	1	8	18	Data
1	0	0	1	1	0	0	9	19	Data
0	1	0	1	1	0	0	:	1A	Special
1	1	0	1	1	0	1	;	1B	Special
0	0	1	1	1	0	0	<	1C	Special
1	0	1	1	1	0	1	=	1D	Special
0	1	1	1	1	0	1	>	1E	Special
1	1	1	1	1	0	0	?	1F	**End sentinel**
0	0	0	0	0	1	0	@	20	Special
1	0	0	0	0	1	1	A	21	Data
0	1	0	0	0	1	1	B	22	Data
1	1	0	0	0	1	0	C	23	Data
0	0	1	0	0	1	1	D	24	Data

1	0	1	0	0	1	0	E	25	Data
0	1	1	0	0	1	0	F	26	Data
1	1	1	0	0	1	1	G	27	Data
0	0	0	1	0	1	1	H	28	Data
1	0	0	1	0	1	0	I	29	Data
0	1	0	1	0	1	0	J	2A	Data
1	1	0	1	0	1	1	K	2B	Data
0	0	1	1	0	1	0	L	2C	Data
1	0	1	1	0	1	1	M	2D	Data
0	1	1	1	0	1	1	N	2E	Data
1	1	1	1	0	1	0	O	2F	Data
0	0	0	0	1	1	1	P	30	Data
1	0	0	0	1	1	0	Q	31	Data
0	1	0	0	1	1	0	R	32	Data
1	1	0	0	1	1	1	S	33	Data
0	0	1	0	1	1	0	T	34	Data
1	0	1	0	1	1	1	U	35	Data
0	1	1	0	1	1	1	V	36	Data
1	1	1	0	1	1	0	W	37	Data
0	0	0	1	1	1	0	X	38	Data
1	0	0	1	1	1	1	Y	39	Data
0	1	0	1	1	1	1	Z	3A	Data
1	1	0	1	1	1	0	[	3B	Special
0	0	1	1	1	1	1	\	3C	Special
1	0	1	1	1	1	0	]	3D	Special
0	1	1	1	1	1	0	^	3E	**Field Separator**
1	1	1	1	1	1	1	_	3F	Special

Table caractère 5bits :

Data bits					Character	Value	Function
b1	b2	b3	b4	b5		(Hex)	
0	0	0	0	1	0	00	Data
1	0	0	0	0	1	01	Data
0	1	0	0	0	2	02	Data
1	1	0	0	1	3	03	Data
0	0	1	0	0	4	04	Data
1	0	1	0	1	5	05	Data
0	1	1	0	1	6	06	Data
1	1	1	0	0	7	07	Data
0	0	0	1	0	8	08	Data
1	0	0	1	1	9	09	Data
0	1	0	1	1	:	0A	Control
1	1	0	1	0	;	0B	**Start Sentinel**
0	0	1	1	1	<	0C	Control
1	0	1	1	0	=	0D	**Field Separator**

0	1	1	1	0	>	0E	Control
1	1	1	1	1	?	0F	**End Sentinel**

Relevé carte Tag :

-- 10 voyages (jaune)
CODE BARRE : 3000000390016
09NOV 16h47 600 SOLDE 09
10NOV 07h00 411 SOLDE 08
12NOV 16h36 600 SOLDE 06
16NOV 07h00 411 SOLDE 05
{Start}8740200000005461220411009000100540600002{End}
SOLDE 01
{Start}8740200000001464690600013000100070400002{End}

-- 1 Voyage
12NOV 06h47 111 SOLDE 00
{Start}8740100000000455447111005000100092900002{End}

-- /!\ Bug /!\ -- 30(10) voyages (bleue)
CODE BARRE : 3000000390047
03SEP 16h57 410 SOLDE 01
{Start}8740200000000392539410014000100541600002{End}

-- 1 Voyage
03SEP 10h21 410 SOLDE 00
{Start}8740100000000354861410006000100541300002{End}

-- 10 voyages (jaune)
CODE BARRE : 3000000390016
27AOU 09h34 411 SOLDE 00
{Start}8740200000000344734411014000100540600002{End}

-- 10 voyages (bleue)
12OCT 14h05 411 SOLDE 00
{Start}8747100000000411245411014000100540600002{End}

-- 1 Voyage
{Start}8740100000000373391800005000100000900002{End}
{Start}8740100000000385552321005000100043300002{End}
{Start}8740100000000389564891005000100001900002{End}
{Start}8740100000000369324891005000100002200002{End}
{Start}8740100000000384916800005000100000900002{End}
{Start}8740100000000362128800005000100000900002{End}
{Start}8740100000000383476800005000100000900002{End}

-- Visitag 1 jour
{Start}8741500265000382036800013000100000900002{End}
{Start}8741500263000379742261015000100302800002{End}
{Start}8741500264000380596800013000100000900002{End}
{Start}8741500271000390674800013000100000900002{End}
{Start}8741500257000370536811013000100003500002{End}

-- Promo 15 Septembre
{Start}8743300258000372777810013000100003500002{End}