Les cryptogrammes visuels (CVV2 pour Visa, CVC2 pour MasterCard) sont les nombres à trois chiffres imprimés au dos des cartes bancaires. Ils contribuent à la sécurité des transactions (achats par internet, commande par courrier papier ou par téléphone…). Leur valeur statique engendre de la fraude par capture et réutilisation de cette donnée.

L'étude de ce cryptogramme temporel est une solution afin de limiter cette fraude, TVV pour dire *Time Verification Value*. Ce nouveau cryptogramme pourra être affiché sur des cartes bancaires munies d’écran (ou sur tout nouveau moyen de paiement offrant la fonction de carte bancaire : montre, smartphone, lunette, etc.) et ce TVV sera rafraîchi périodiquement. La valeur courante du TVV va être utilisée de la même façon que le cryptogramme actuel, et le gain en sécurité se trouve dans l'expiration rapide des numéros capturés.

La description de l'algorithme implanté dans les cartes est composée de trois fonctions :

1) Dérivation de la clé d'émetteur (la banque) en clé carte
2) Calcul cryptographique du TVV
3) Gestion du compteur de temps CTC (non traité dans de ce TD)

Dans ce contexte, nous allons implémenter et tester les deux premières fonctions. Cet algorithme est spécifié ainsi :

1 L’algorithme du TVV

1.1 Dérivation de clé d'émetteur en clé carte

La dérivation se fait selon la méthode suivante :

Entrées

IMK_TVV	:	clé Triple DES d'émetteur, 128 bits
PAN	:	numéro de carte, 13 à 19 digits, codage BCD[1]

1 *Binary Coded Decimal* : entier représenté sous forme hexadécimal, chaque valeur hexadécimal prenant la valeur décimale du digit.

PSN : numéro de séquence du PAN, 2 digits en codage BCD, par défaut '00'.

Sorties

MK_TVV : clé Triple DES unique par carte, 128 bits

Traitements

DIV := [$'0'^{16}$ || PAN || PSN] (-16 .. -1) // diversifiant de 16 quartets (64 bits soit 8 octets)

MKTVV_L := TDES_EDE(IMK_TVV)[DIV]

MKTVV_R := TDES_EDE(IMK_TVV)[DIV ⊕ $'FF'^{8}$]

MK_TVV := MKTVV_L || MKTVV_R

1.2 Calcul cryptographique du TVV

Entrées

MK_TVV	:	clé Triple DES unique par carte, 128 bits
PAN	:	numéro de carte, 13 à 19 digits, codage BCD
EXP	:	date d'expiration, 4 digits sous la forme MMYY, codage BCD
SC	:	Service Code, 3 digits, codage BCD
CTC	:	compteur de ticks, 6 digits, codage BCD pour ce calcul

Sorties

TVV : cryptogramme temporel, 3 digits, codage BCD ou compact

Traitements

Soit getCVV(MK,PAN,EXP,SC) cette fonction .

Le calcul des TVV réutilise cette fonction de la manière suivante:

getTVV(MK,PAN,EXP,SC,CTC) := getCVV(MK,PAN', EXP, SC') avec

PAN' = CTC(3..6) |> PAN
SC' = SC |< CTC(1..2)

// PAN': Écrasement des 4 premiers digits du PAN avec les 4 derniers digits du CTC
// SC': Écrasement des 2 derniers digits du SC par les 2 premiers digits du CTC.

Si le compteur CTC est géré comme un entier, alors
CTC(1..2) = BCD(CTC div 10000) et
CTC(3..6) = BCD(CTC mod 10000)

Cette fonction est très proche de celle définie par Visa pour le calcul des cryptogrammes dynamiques (dCVV) basés sur un compteur de transactions.

1.3 CALCUL DU CVV

Cette fonction de base est spécifiée par Visa.

Dans ce rapport, elle est notée getCVV(MK,PAN,EXP,SC).

Entrées

MK	:	clé Triple DES unique par carte, 128 bits. MK = MK_L || MK_R
PAN	:	numéro de carte, 13 à 19 digits, codage BCD
EXP	:	date d'expiration, 4 digits sous la forme MMYY, codage BCD
SC	:	Service Code, 3 digits, codage BCD

Sorties

CVV	:	cryptogramme statique, 3 digits, codage BCD

Traitements

```
m := [PAN || EXP || SC || '0'*]          // buffer de 16 octets, paddé à droite par des quartets[2] à '0'
 m1 := m(1..8)
m2 := m(9..16)                           // séparation m = m1 || m2, deux blocs de 8 octets (64 bits)
c1 := DES(MK_L)[m1]
c2 := TDES-EDE(MK)[c1 ⊕ m2]              // hachage de m sur un bloc c2 de 8 octets
c2  = q1 || q2 || … || q16               // découpage de c2 en 16 quartets.
D := {} H := {}
pour i de 1 à 16 faire
   si q(i) < 10 alors
      D := D || q(i)                     // les quartets dans 0..9 sont rangés dans un buffer D
   sinon
      H := H || q(i) – 10                // les quartets dans 'A'..'F' sont rangés comme 0..5 dans H
CVV := [D || H] (1..3)                   // le CVV est constitué des 3 digits de gauche de D || H
```

2 *Quartet* : un hexadécimal '0'..'F' (un entier de l'intervalle 0..15)

JEUX D'ESSAIS

1.1 Calcul de la clé de dérivation MK_TVV

Test de la fonction (IMK_TVV, PAN, PSN) → MK_TVV

Les données suivantes sont utilisées pour générer les vecteurs de test :

Donnée	Indice	Valeur
IMK_TVV	0	9E15204313F7318ACB79B90BD986AD29
	1	036BD4728609D4100A18FE3F99B6589F
PAN	0	0123456789874
	1	11234567898764
	2	212345678987655
	3	3123456789876547
	4	5364140000000367
	5	01234567898765437
	6	012345678987654326
	7	9123456789876543214
PSN	0	00
	1	12
EXP	0	0215
	1	0216
	2	0316
	3	1220
SC	0	000
	1	123
	2	755
	3	999

Les vecteurs sont identifiés par la concaténation décimale des indices IMK_TVV || PAN || PSN , par exemple : 031 correspond à un calcul avec l'IMK_TVV d'indice 0, le PAN d'indice 3, le PSN d'indice 1.

Le diversifiant (donnée de base à chiffrer par IMK_TVV) est également décrit.

Résultats attendus à compléter

Vecteur	**Diversifiant**	**MK_TVV (résultat)**
000	0012345678987400	ADBE 78D1 C974 EB2A 7E7E A5A3 2EF8 DC26
001	0012345678987412	7E1B 54DD B13C 91C8 FC3C 48CB 98BD 1195
010	1123456789876400	D3E7 107F 868B 8E5A EA2A 8D55 C20A 02A9
011	1123456789876412	7AB6 1196 11F7 433D D829 C588 9CDC CAE4
020	1234567898765500	A49C C81D B0EB 583E B7B9 39DE 7B2 396A0
021	1234567898765512	31B7 763D 66F3 60A2 2662 4E48 7653 89A7
030	2345678987654700	62F6 0D03 59A8 6BDF 7F21 06E9 8658 B7EC
031	2345678987654712	CD24 AA6F F283 BF7F 9CE8 42DB 0CA9 659D
040	6414000000036700	864D 29A0 20A5 0FEA 0E67 F206 E59B D002
041	6414000000036712	7295 FAFB 3C5A 6DA8 9631 0679 D82C 6F7E
050	3456789876543700	7BF2 E154 03E3 38CF D9C4 5546 FC25 5D37
051	3456789876543712	53DC 8A35 143F 7E38 35AC 14A4 3889 0DF1
060	4567898765432600	

Vecteur	Diversifiant	MK_TVV (résultat)
061	4567898765432612	CF3C 6843 4925 72E3 FED9 37EE 98C7 3F9A
070	5678987654321400	
071	5678987654321412	CEAE 745A 17A4 225C 78CE 7182 A269 A238
100	0012345678987400	
101	0012345678987412	081B 87CB 0B83 39EC BF87 C913 D552 02E8
110	1123456789876400	
111	1123456789876412	20C1 85A4 6EB5 4B30 1ADB 5691 FD31 73F9
120	1234567898765500	
121	1234567898765512	B6F2 B008 87E8 8051 6969 8307 38C3 1219
130	2345678987654700	
131	2345678987654712	4E57 82A9 619B A7B0 D097 3D41 E3E2 5231
140	6414000000036700	
141	6414000000036712	9BED 6C87 D3BD E6C7 29FF A378 35C8 2FBA
150	3456789876543700	
151	3456789876543712	0D6F DDC2 EF42 E8D0 AF63 224F 8953 F191
160	4567898765432600	
161	4567898765432612	6EAD 9DEE 6B81 D301 4FBD 56B4 16CE 2B85
170	5678987654321400	
171	5678987654321412	DB19 BF3C 12D8 DADE 52B2 2A1F 3109 83CC

1.2 Calcul du cryptogramme TVV

14 profils de carte sont utilisés :

Clé Émetteur IMK_TVV : 9E15204313F7318ACB79B90BD986AD29

Date d'Expiration : 1216

Code Service (2 valeurs) : 0 → 000, 1 → 612

PSN: 00 (utilisé dans le calcul de la clé carte MK_TVV)

PAN (7 valeurs indexées selon leur longueur, avec la clé MK_TVV correspondante) :

N°	PAN	Clé MK_TVV
3	1234567890123	83F4 2E9C B5FE 6667 C43B 56A9 C21E 4072
4	12345678901234	CAD3 AA41 9447 F80B 7A56 9D18 BC10 5D96
5	123456789012345	7C56 37D3 7D9A F792 352C CAE3 195A 080A
6	1234567890123456	6DEB E585 C940 7B28 28A7 FAB1 0FE1 E2E1
7	12345678901234567	7AC5 6A94 581F 1995 73BA 4089 1C0B 0582
8	123456789012345678	83F9 D9DF 2061 BAC7 564E 4D0A 5C0C E96E
9	1234567890123456789	907D 4A1E 56EC 9881 6206 45F2 EDB3 405E

Les profils sont notés Pij, avec i dans 0..1 (Code Service) et j dans 3..9 (rappel de la longueur du PAN)

Pour chaque profil, 12 valeurs de CTC sont utilisées :

000000 100000 020040 003000 000400 000050 000006 123456 234561 363945 589611 999999

Pour les profils P03, P13, P06, P16, P09, P19 et les valeurs de CTC 020040 et 363945, les valeurs intermédiaires suivantes sont tracées:

- Donnée à chiffrer par la clé MK_TVV
- Cryptogramme résultant de ce chiffrement

Profil – CTC	**Donnée à chiffrer**	**Cryptogramme**	**TVV**
P03 – 020040	00405678901231216002000000000000	67AF1CD58A2582B9	671
P03 – 363945	39455678901231216036000000000000	35DBE8A52AA6D918	358
P13 – 020040	00405678901231216602000000000000	48188E2B24EB0DCB	481
P13 – 363945	39455678901231216636000000000000	9A06C252961DCA7C	906
P06 – 020040	00405678901234561216002000000000	01EEED1AD1985B21	011
P06 – 363945	39455678901234561216036000000000	8215D230280C85BD	821
P16 – 020040	00405678901234561216602000000000	960334D12F861E8B	960
P16 – 363945	39455678901234561216636000000000	FD3D9A6D31B27439	396
P09 – 020040	00405678901234567891216002000000	61AB22524C336F10	612
P09 – 363945	39455678901234567891216036000000	24B9DA1C5A74BABE	249
P19 – 020040	00405678901234567891216602000000	7466291AAD17AC80	746
P19 – 363945	39455678901234567891216636000000	3B1F9718399A0A2F	319

Les TVV pour tous les profils sont à remplir dans le tableau suivant:

CTC / Pij	P03	P04	P05	P06	P07	P08	P09	P13	P14	P15	P16	P17	P18	P19
000000														
100000														
020000														
003000														
000400														
000050														
000006														
123456														
234561														
363945														
589611														
999999														