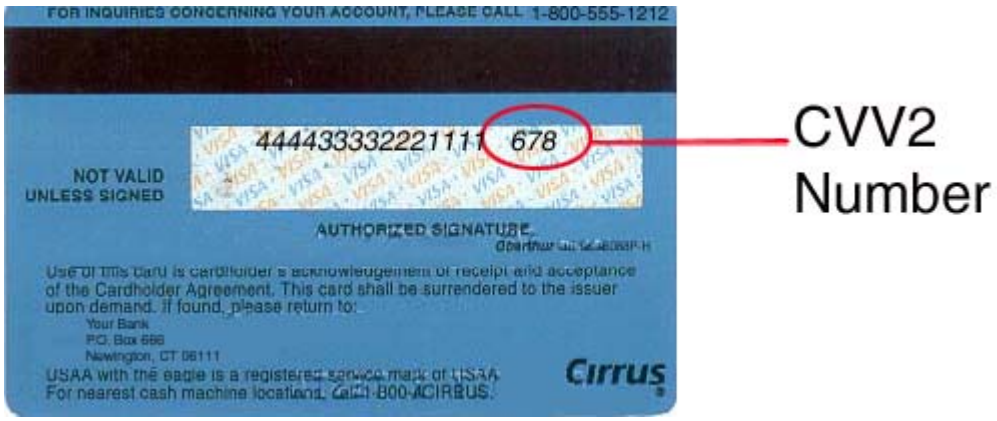
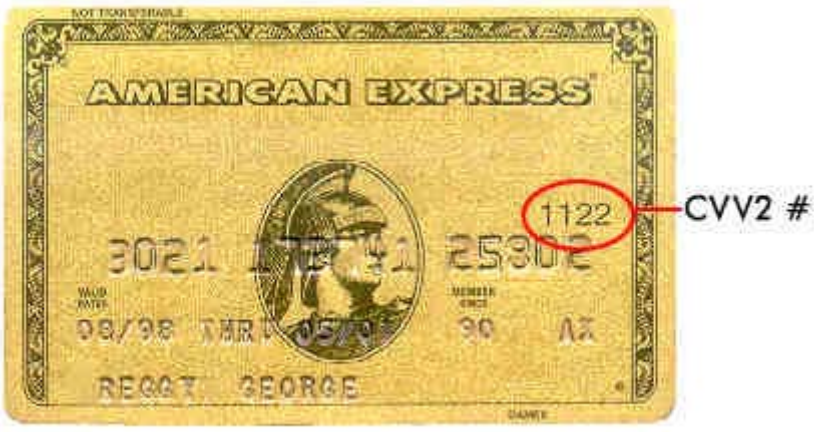
什么是 CVV2?

CVV2 是打印在你的 Visa/MasterCard 卡签名区的一个数字。它位于信用卡号后 的 3 位数字。如下图所示：



美国运通（American Express）卡将 CVV2 印刷在卡正面凸字卡号的右上角。如下图所示：



什么是 VISA CVV/MasterCard CVC?

VISA CVV（Card Validation Value）或 MasterCard CVC(Card Validation Code)是由卡号、卡有效期及服务约束代码生成的 3 位数字，一般写在卡 2 磁道的用户自定义数据区。VISA CVV 和 MasterCard CVC 生成方法一样，只是叫法不一致。

VISA 卡校验值 CVV 的计算

（一）VISA 卡校验值ＣＶＶ的计算

卡校验值即ＣＶＶ的计算方法如下：

１．将以下从第二磁道中抽取出的字符从左至右排列，产生２６个字符：

主帐号（ＰＡＮ）	１９位
卡有效期（ＥＸＰＩＲＥ　ＤＡＴＥ）	４位
服务代码（ＳＥＲＶＩＣＥ　ＣＯＤＥ）	３位

并转换为１０４　Ｂｉｔｓ（２６ｘ４），转换方法为将每一位数字转换为４位的ＢＣＤ码，即：

十六进制数字	ＢＣＤ码
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
E	1110
F	1111

２．将步骤１得出的结果的最后补上二进制“0”，使之成为１２８　Ｂｉｔｓ的字段，将该字段分为两个６４　Ｂｉｔｓ的数据，其中前６４　Ｂｉｔｓ数据为数据块１，后６４Ｂｉｔｓ数据为数据块２。

３．用ＣＶＫＡ对数据块１加密（ＥＮＣＲＹＰＴＩＯＮ）。

４．将步骤３得出的结果与数据块２异或（ＸＯＲ），并用ＣＶＫＡ对结果加密。

５．用ＣＶＫＢ对步骤４得出的结果解密（ＤＥＣＲＹＰＴＩＯＮ）。

６．用ＣＶＫＡ对步骤５得出的结果加密。

７．对步骤６得出的结果从左到右抽取出所有的数字（０～９）。

８．对步骤６得出的结果从左到右抽取出所有的十六进制字符（A～F），并对每一个十六进制字符减十进制１０，使之变为数字，例如十六进制Ｂ（十进制为１１）变为１。

９．将步骤７和８得出的数字从左至右排列，步骤８得出的数字放在步骤７得出的数字之后。

１０．步骤９得出结果的前三位数字即为卡的校验值（ＣＶＶ）。

（二）测试数据

以下数据可用于编写ＣＶＶ算法时检查程序是否正确，其中：

ＣＶＫＡ＝ 0123 4567 89AB CDEF
ＣＶＫＢ＝ FEDC BA98 7654 3210

１３位ＰＡＮ	失效日期	服务代码	ＣＶＶ
4123 456 789 012	8701	101	370
4999 988 887 777	9105	111	649
4666 655 554 444	9206	120	821
4333 322 221 111	9307	141	697

１６位ＰＡＮ	失效日期	服务代码	ＣＶＶ
4123 456 789 012345	8701	101	561
4999 988 887 777000	9105	111	245
4666 655 554 444111	9206	120	664
4333 322 221 111222	9307	141	382

以第一个十六位主帐号为例，计算卡校验值的步骤如下：

主帐号： 4123 4567 8901 2345
失效日期： 8701
服务代码： 101

步骤１： 抽取数据

4123 4567 8901 2345 8701 101

步骤２： 数据块

块１　　＝　4123 4567 8901 2345
块２　　＝　8701 1010 0000 0000

步骤３：　用ＣＶＫＡ加密

块１　　＝　4123 4567 8901 2345
ＣＶＫＡ　＝　0123 4567 89AB CDEF
结果３　　＝　B76A DDCE 71CC C6BE

步骤４：　用块２异或步骤３的结果，并用ＣＶＫＡ对异或结果加密

结果３　　＝　B76A DDCE 71CC C6BE
块２　　＝　8701 1010 0000 0000
结果　　＝　306B CDDE 71CC C6BE

ＣＶＫＡ　＝　0123 4567 89AB CDEF
结果４　　＝　A510 46A2 59A4 C467

步骤５：　用ＣＶＫＢ对步骤４的结果解密

结果４　　＝　A510 46A2 59A4 C467
ＣＶＫＢ　＝　FEDC BA98 7654 3210
结果５　　＝　90F6 DB02 A6F7 E621

步骤６：　用ＣＶＫＡ对步骤５的结果加密

结果５　　＝　90F6 DB02 A6F7 E621
ＣＶＫＡ　＝　0123 4567 89AB CDEF
结果６　　＝　5B61 4982 E03C 97DD

步骤７：　对步骤６的结果抽取数字

结果７　　＝　5614 9820 397

步骤８：　对步骤６的结果抽取十六进制字符，并转换为１０进制数字（每位减１０）

抽取结果　＝　BECD D
结果８　　＝　1423 3

步骤９：　将步骤８的结果排列在步骤７的数字后面

结果９　　＝　5614 9820 3971 4233

步骤１０：　步骤９的结果前３位数字为ＣＶＶ

结果１０　＝　561

VISA PIN 校验值 PVV 的计算

（一）VISA PIN 校验值的计算

VISA PIN 校验值的计算包括以下要素：

序号	要素	说明
1.	PVKA	Left part(64 bits) if the PIN Verification Key Pair
2.	PVKB	Right part(64 bits) if the PIN Verification Key Pair
3.	PAN	Rightmost 11 digits of the PAN exclude the check digit
4.	PVK Index	0-F
5.	Consumer PIN	First 4 digits of the consumer PIN

PIN 校验值即ＰＶＶ的计算方法如下：

1. 由 PAN 的最右 11 个数字（不包含校验位）和 PVK 索引号（一个十六进制数字）及客户个人密码的前 4 位组成 1 个 16 字节的十六进制数字串
2. 将以上 16 字节的十六进制数字串转换成 64 比特 BCD 码，用 PVKA 作 DES 加密(Encryption)运算
3. 将以上结果用 PVKB 作 DES 解密(Decryption)运算
4. 将以上结果再用 PVKA 作 DES 加密(Encryption)运算得结果
5. 对步骤 4 得出的结果从左到右抽取出所有的数字（０～９）。
6. 对步骤 5 得出的结果从左到右抽取出所有的十六进制字符（Ａ～Ｆ），并对每一个十六进制字符减十进制１０，使之变为数字，例如十六进制Ｂ（十进制为１１）变为１。
7. 将步骤 5 和 6 得出的数字从左至右排列,步骤 6 得出的数字放在步骤 5 得出的数字之后。
8. 步骤 7 得出结果的前四位数字即为 PIN 的校验值（PVV）。

（二）测试数据

以下数据可用于编写 PVV 算法时检查程序是否正确，其中：

PVKA ＝ 0123 4567 89AB CDEF
PVKB ＝ FEDC BA98 7654 3210

１３位ＰＡＮ	PVK Index	Consumer PIN	PVV
4123 456 789 012 x	0	123456	3920
4123 456 789 012 x	0	1234	3920
4999 988 887 777 x	1	234561	4045
4999 988 887 777 x	1	2345	4045
4666 655 554 444 x	2	345612	2635

4666 655 554 444 x	2	3456	2635
4333 322 221 111 x	F	456123	3421
4333 322 221 111 x	F	4561	3421

１６位ＰＡＮ	PVK Index	Consumer PIN	PVV
4123 4567 8901 2345 x	0	123456	0410
4123 4567 8901 2345 x	0	1234	0410
4999 9888 8777 7000 x	1	234561	0105
4999 9888 8777 7000 x	1	2345	0105
4666 6555 5444 4111 x	2	345612	6307
4666 6555 5444 4111 x	2	3456	6307
4333 3222 2111 1222 x	F	456123	7112
4333 3222 2111 1222 x	F	4561	7112

注：以上表中 x 为帐号之校验值，不包含在运算中。运算时，帐号只有 x 左面 11 位数字有效。

以第一个十六位主帐号为例，计算卡校验值的步骤如下：

主帐号： 4666 6555 5444 4111 x (注：x 为帐号之校验值)
PVK Index： 2
Consumer PIN： 345612

步骤 1：抽取数据组成数据块

结果 1 ＝ 555 5444 4111 2 3456

步骤 2：用 PVKA 作 DES 加密(Encryption)运算

结果 1 ＝ 555 5444 4111 2 3456
PVKA ＝ 0123 4567 89AB CDEF
结果 2 ＝ 6568 2AF5 0304 A6CA

步骤 3：用 PVKB 作 DES 解密(Decryption)运算

结果 2 ＝ 6568 2AF5 0304 A6CA
PVKB ＝ FEDC BA98 7654 3210
结果 3 ＝ 5644 6FB7 C183 CCDF

步骤 4：再用 PVKA 作 DES 加密(Encryption)运算得结果

结果 3 ＝ 5644 6FB7 C183 CCDF
PVKA ＝ 0123 4567 89AB CDEF
结果 4 ＝ 63C0 DB79 EEB3 FB9D

步骤 5：从左到右抽取出所有的数字（0～9）

结果 5　　＝　6307939

步骤 6：　对步骤 4 的结果抽取十六进制字符，并转换为１０进制数字（每位减１０）

抽取结果　＝　CDBE EBFB D
结果 6　　＝　2314 4151 3

步骤 7：将步骤 6 的结果排列在步骤 5 的数字后面

结果 7　　＝　6307 9392 314 4151 3

步骤 8：步骤 7 的结果前 4 位数字为 PVV

结果 8　　＝　6307