آشنایی با سیستم کدگذاری Viaccess (یک)

قبل از اینکه بحث وی اکسس رو آغاز کنیم ، بهتر که یه مقدار در رابطه با الگوریتم کدگذاری بیشتر آشنایی پیدا کنیم.

CSA = Common Scrambling Algorithm

نوعی سیستم رمزنگاری اطلاعات است ، که بصورت یک استاندارد DVB در آمده است.
این الگوریتم برای تمام سیستم های کدگذاری شناخته شده ، مانند وی اکسس ، ایردتو ، سکا و ... یکسان و مشترک است.
تمام الگوریتم های کدگذاری موجود مانند وی اکسس ، ایردتو ، ناگراویژن و ... ، در مقابل این الگوریتم ، یک الگوریتم ثانویه به شمار می روند. در واقع استریم Mpeg2 توسط این الگوریتم(CSA) کدگذاری شده است، و کار سایر الگوریتمهای موجود (وی اکسس ، سکا و ...) تهیه ی کلید لازم ، برای آن ، جهت رمزگشایی تصویر است.
این الگوریتم تنها از یک جفت کلید هشت بایتی استفاده می کند که توسط الگوریتمهای ثانویه ذکر شده تولید می شود. مهم نیست که طول کلید برای مثال وی اکسس 2 ، آیا 16 بایت است یا خیر ، در نهایت کار سیستمی مانند وی اکسس 2 ، تولید کلید هشت بایتی لازم (DW) جهت الگوریتم CSA است.
این مورد امکان کدگذاری سیگنال یک پرووایدر را بصورت همزمان با چندین سیستم کدگذاری فراهم می کند.
که نمونه ی آنرا برای مثال در مورد TPS ها دیده اید (همزمان بر روی وی اکسس و سکا پخش می شوند).

و اما وی اکسس ...

وی اکسس ، سیستم کدگذاری تعدادی از کانالهای ماهواره است و ذاتا از سیستم D2MAC اقتباس شده است (اما برای سیستم های دیجیتال).
لیست تعدادی از پکیجهایی که با این سیستم کدگذاری شده اند (یا شده بودند) :

008400 MCM Europe
009400 SRG Swiss
009C00 SVT Europe
007800 Canal Satellite France
007C00 TPS France
008000 FTCable
00A000 BBC Prime
00B000 TV Slovenia
&...

در لیست فوق البته تعدادی از پکیج های وی اکسس و تی پی اسکریپت با هم مخلوط شده اند. برای مثال پروایدر SRG Swiss با وی اکسس کدگذاری شده اند ، اما پکیج TPS France با سیستم TPSCrypt .
در لیست فوق ابتدا آیدی پروایدر (معروف به آیدنت) مشخص شده است ، سپس نام پروایدر.
اگر به سایت هایی که کدهای روزانه را ارائه می دهند مراجعه کنید ، کلیدها را عموما به شکل زیر نمایش می دهند:

```
009400
0B: 6A BA F5 D9 7D 2F 8B 7F
```

در مثال فوق 009400 آیدنت پروایدر SRG Swiss است. 0B اندیس کد هشت بایتی است .
و 6A BA F5 D9 7D 2F 8B 7F کد مربوط به اندیس 0B می باشد. این اعداد در مبنای هگزادسیمال (مبنای شانزده) ارائه می شوند.
نکته :
در سیستم وی اکسس به کلید با اندیس 08 ، Service Key می گویند و این کد ، تنها کدی است که هیچگاه تغییر نمی کند.
اصطلاحات :

PPUA = Program Provider Unique Address
SA = Shared Address
MK = Management Key
OP Key = Operational Key

منظور از SA همان Shared Address است که با MK یا Management Key همخوانی دارد. MK بر روی کارت اوریجینال برای باز کردن و یا از حالت کد در آوردن OP Key به کار می رود. منظور از OP Key همان Operational Key و یا کلید فعال می باشد. OP Key ها از کلید 08 تا 0F را تشکیل می دهند و قبل از این کلیدها ، کلیدهای مستر یا MK قرار می گیرند.
کلیدهای مستر از شماره 00 تا 03 در کارتهای اریجینال مختلف هستند و برای آپدیت کردن اطلاعات روی کارتِ مربوط به صاحب کارت عمل می کنند.
در این حالت PPUA و یا Program Provider Unique Address پنج بایتی اطلاعاتی نظیر نوع ، آبونمان و تاریخ مصرف کارت را نشان می دهد.
کلیدهای مسترِ از شماره ی 04 تا 07 در یک گروه از کارتها منحصر به فرد هستند و به وسیله SA چهار بایتی که توضیح داده شد ، مشخص می شوند. این گروه از کارتها معمولا تعدادشان 256 عدد است و کار این کلیدها ، آپدیت کردن OP Keys بوده و اگر بر روی کارت شما وجود داشته باشد ، دیگر نیازی به برنامه ریزی مجدد نبوده و با هر بار تغییر کدهای فعال (OP Keys) کارت از طرف پروایدر آپدیت می شود (کارت AU).
اصطلاح دیگر مربوط به CUSTWP می باشد که آخرین بایت SA است و برای دریافت کدهای آپدیت از طرف پروایدر باید حتما در کارت موجود باشد.

بطور خلاصه برای اینکه کارتی بتواند خاصیت AU یا Auto Update داشته باشد ، باید به ازای هر پروایدر ، اطلاعات MK و SA و CUSTWP را داشته باشد.

بنابراین به صورت خلاصه :

پروایدر : شرکتی که یکسری از کانالها را بصورت یک پکیج یا مجموعه نمایش می دهد. برای مثال پروایدری مانند SRG Swiss نمایش مجموعه کانالهای SF را بعهده دارد.

آیدنت : شماره منحصر بفرد هر پروایدر

UA : شماره سریال کارت است و فقط برای حالتهایی که کارت قرار است AU باشد اهمیت پیدا می کند ، در غیر اینصورت خیلی راحت آنرا 00 00 00 00 وارد کنید.

PPUA : رابطه آن با UA به این صورت است <<< UA = 00 + PPUA

این علامت + در اینجا بدین معناست که صرفا دو تا صفر سمت چپ PPUA قرار می گیرد و باز هم برای کارتهای غیر AU همان 00 00 00 00 می باشد.

MK و یا Master Key و یا Management Key :

هر کارت دارای تعدادی MK می باشد که با الگوریتم بسیار قوی کدگذاری شده است. آنها هرگز تغییر نمی کنند و برای هر کارتی متفاوت هستند. کار آنها از حالت کد خارج کردن کدهای فعال و یا Operational Keys است.

OP Keys و یا Operational Keys و یا SOK = Service Operational Keys :

این کدها بسته به نوع کانال و قیمت آن ، بین چند ساعت ، روز و یا ماه تغییر می کنند. این کلیدها کدگذاری شده اند و برای هر کارتی متعلق به یک پروایدر مشخص ، یکسان می باشند. از OP Keys برای از حالت کد خارج کردن CW استفاده می شود.

CW و یا Command Word و یا Control Word و یا Check Word :

برای رمزگشایی سیگنال بصورت بلادرنگ (Real Time) بکار می رود. بر خلاف مورد بالا که با استفاده از سیستم کدگذاری به شدت قوی ، رمزگذاری شده است ، سیگنال ویدئویی با استفاده از الگوریتمی ساده کدگذاری می گردد.

یعنی :

- سیگنال ویدئویی (که خیلی خفیف کدگذاری شده) بوسیله CW از حالت رمزگذاری شده خارج می شود . CW هر 5 تا 10 ثانیه تغییر می کند !!!
- OP Key (که به شدت و با الگوریتم قوی کدگذاری شده است) برای رمزگشایی CW بکار می رود.
- MK (که به شدت و با الگوریتم قوی کدگذاری شده است) برای از حالت کد خارج کردن OP Key بکار می روند.

UA و یا Unique Address :

در هر کارت MK های مختلفی وجود دارد ، از MK00 تا MK07 و برای اینکه EMM ها تفاوت بین کارتها را بتوانند متوجه شوند ، مفهوم UA ارائه شده است و به این صورت هر EMM فقط بوسیله همان کارت مشخص شده با آدرس منحصر بفرد قابل رمزگشایی است. EMM به کارت می گوید که به کدام MK برای رمزگشایی OP Key همراه خودش نیاز دارد و همچنین همانطور که گفته شد ، EMM به یک کارت خاص UA آدرس داده می شود. در عمل پروایدرهای بزرگ که دارای کارتهای زیادی می باشند (256 و یا 4096 کارت) دارای آدرس مشترکی هستند که به آن SA می گویند و تمام آنها MK های یکسانی نیز دارند. EMM های حاوی OP Keys جدید ، بارها و بارها قبل از تغییر کلید فعال جاری فرستاده می شوند و بنابراین هر کارت ، قبل از تغییر کلیدِ در حال استفاده ، حداقل یکبار کد جدید را دریافت می کند.

EMM ویا Entitlement Management Message :

OP Key ها توسط EMM ها به کارت فرستاده می شوند. بنابراین اگر OP Key ها حدس زده شوند بدون نیاز به تعویض کارت ، می توان آنرا تغییر داد. EMM نیز توسط سیستم رمزگذاری قوی کدگذاری شده و بوسیله MK از حالت کد در می آید. از EMM ها برای تغییر و یا حذف کلیدهای موجود استفاده می گردد.

Nano Commands :

همانطور که می دانید هر رسیوری تعدادی Instruction را به کارت می فرستد و یا داده هایی را از کارت دریافت می کند. قسمتی از این Instruction ها شامل اطلاعاتی است که برای از حالت کد خارج کردن سیگنال ویدئویی (Descrambling) بکار می رود و شامل آیدی کانال ، امضای دیجیتال و همچنین نانو کامندها است. مهمترین دلیل فرستادن نانو کامندها بدست آوردن کنترل اتفاقات رخ داده ی درون کارت است. برای مثال با یک نانو کامند خاص می توان مقدار RAM را در یک آدرس خاص درون کارت تغییر داد و یا قسمت هایی از یک آدرس خاص درون ROM و یا RAM کارت را خواند. بصورت خلاصه نانو کامندها برای آپدیت کردن کارت به آن فرستاده می شوند.

ECM و یا Entitlement Control Message :

در سیستم وی اکسس CW ها توسط ECM فرستاده می شوند.

به قسمتی از این نانو کامندها ECM هم گفته می شود و کنترل کار کردن کارت را به عهده دارند. ECM ها حاوی CW ها هستند که در ادامه توضیح داده خواهند شد. اما بصورت خلاصه ECM حاوی اطلاعاتی در مورد نوع سرویس و شرایطی که باید برآورده شوند تا بتوان از آن سرویس استفاده کرد می باشند. گاهی از اوقات پروایدرها ECM های جعلی می فرستند تا کارتهای کپی را از کار بیاندازند ، به همین دلیل به آنها Entitlement Counter Message هم گفته میشود.

بررسی ECM وی اکسس یک

برای اینکه بتوان تشخیص داد که یک کانال وی اکسس یک ، از چه آیدنتی و چه اندیس کلیدی در حال حاضر استفاده می کند ، باید یک لاگ از ECM ورودی آن کانال با استفاده از سیزن اینترفیس و یا پلاگین های کارتهای رسیور تهیه کرد ، و سپس آنالیز نمود.

این یک نمونه لاگ ECM تهیه شده توسط MD-Yankse از یکی از کانالهای وی اکسس می باشد :

00 81 70 25 00 90 03 01 1C 08 E0 01 20 EA 10 C3 DB 28 EE 3F 96 75 FA BE 00 E0 96 85 78 59 53 F0 08 9B
83 89 DA 39 8E 2F 70 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
FF FF FF FF FF FF FF FF FF FF

مفهوم آن :

81 : Table ID است.

7025 : یعنی طول ECM مساوی 37 بایت می باشد (25 هگزادسیمال مساوی 37 دسیمال است).

شمارش طول ECM فوق را اگر از 00 بعد از 7025 تا 70 آخر ، انجام دهید ، دقیقا معادل 37 بایت می شود.

00 : ؟؟

9003 : (نانو 90 به طول سه بایت) یعنی در ادامه سه بایت مربوط به آیدنت پروایدر خواهد آمد.

011C08 : یعنی پروایدر 011C00 که از کلید با اندیس 08 استفاده می کند.

E001 : نانو E0 به طول یک بایت (ECM Control که از روی آن Maturity Rating مشخص می شود)

20 : یک بایت ذکر شده فوق

EA10 : نانو EA به طول 16 بایت (10 هگز = 16 دسیمال). پس از این نانو ، CW ها ظاهر می شوند.

C3 DB 28 EE 3F 96 75 FA BE 00 E0 96 85 78 59 53 مساوی 16 بایت فوق که معادل دو ECW و یا Encrypted Control Word است. یعنی :

Encrypted Control Word = C3 DB 28 EE 3F 96 75 FA
Encrypted Control Word = BE 00 E0 96 85 78 59 53

F008 : نانو F0 به طول 8 بایت که پس از آن امضای دیجیتال ظاهر خواهد شد.

9B 83 89 DA 39 8E 2F 70 مساوی 8 بایت فوق ، یعنی امضای دیجیتال ECM مخابره شده که از روی آن هش محاسبه می شود.

بررسی یک مثال دیگر

ECM Log زیر از پروایدر SRG Swiss توسط MD-Yankse تهیه شده است :

00 80 70 27 00 90 03 00 94 0D E2 03 30 99 01 EA 10 CE ED E4 3E 53 32 F7 66 C4 0B EE 33 B8 2B CB C2
F0 08 46 FD B9 27 72 0D 73 E3

مفهوم آن :

Table ID : 80

7027 : طول کل ECM مساوی 39 بایت می باشد (27 هگز = 39 دسیمال).

00 : ؟؟

9003 : نانو 90 به طول سه بایت

00940D : سه بایت فوق و به معنای پروایدر 009400 (SRG Swiss) است که در این زمان از کلید با اندیس 0D استفاده میکند.

E203 : نانو E2 به طول سه بایت که برای ارائه تاریخ بکار می رود.

309901 : تاریخ به فرمت وی اکسس + کلاس

تاریخ 3099 یعنی : 2004/04/25

کلاس 01 : ؟

EA10 : نانو EA به طول 16 بایت (10 هگز = 16 دسیمال). پس از این نانو ، CW ها ظاهر می شوند.

Encrypted Control Word = CE ED E4 3E 53 32 F7 66
Encrypted Control Word = C4 0B EE 33 B8 2B CB C2

F008 : نانو F0 به طول 8 بایت که پس از آن امضای دیجیتال ظاهر خواهد شد.

46 FD B9 27 72 0D 73 E3 : مساوی 8 بایت فوق ، یعنی امضای دیجیتال ECM مخابره شده که از روی آن هش محاسبه می شود.

روش محاسبه تاریخ وی اکسس یک :

برای مثال 3099 (تاریخ لاگ فوق) که در مبنای هگز است ، مساوی 0011000010011001 در مبنای دو می باشد (باینری).

هفت بایت اول آن بیانگر سال ، 4 بایت بعدی به معنای ماه و 5 بایت آخر مساوی روز است.

برای مثال در مورد تاریخ فوق داریم :

0011000 (در مبنای دو) = 24 (در مبنای ده)

(که بعلاوه ی 1980 باید بشود (مبدا تاریخ در سیستم وی اکسس یک !)) = سال 2004

0100 (باینری) = 4 (دسیمال) (شمار ماه میلادی)

11001 (باینری) = 25 (دسیمال) (شمار روز)

نتیجه = 2004/04/25

همین الگوریتم در مورد تاریخ سیستم سکا یک نیز برقرار است ، البته در آنجا مبدا تاریخ از 1990 محاسبه می شود.

ی