DVD

el sistema de protección del DVD está basado en CSS[1], un estandar.

como funciona: componentes

- Clave de Disco (DK): necesaria para leer los contenidos del disco. Se ha de guardar muy bien
- Clave de Reproductor (PK): cada fabricante tiene una clave de reproductor.
- Claves de Título (TK): son las claves que mostraran realmente el contenido del disco

como funciona: proteger la información

- la DK está encriptada para que solo se pueda leer con una PK correcta
- existen 409 PK - una por cada fabricante - así que la DK está encriptada para que cualquiera de las 409 pueda leerla.
- la PK está fuertemente custodiada en un chip en el aparato, aparentemente inexpugnable

como funciona: operativa

- con la PK desencriptamos la DK, que sirve para desencrioptar las TK
- el algoritmo de cifrado se llama LFSR[2] y es un algoritmo de flujo, que realiza operaciones de cifrado bit a bit
- Utiliza la operación XOR
- Se genera un flujo de bits que parecen aleatorios, aunque en realidad no lo son (pseudoaleatoriedad).
- Esto se consigue mediante un FSR[3], pasándole una semilla (n bits iniciales) y procesando los bits, generando una cadena pseudoaleatoria. Como máximo la cadena puede tener una longitud 2 elevado a n antes de empezar a repetirse.
- El *lineal* aplicado al LFSR es porque la operación realizada es un XOR
- Con un registro de 40 bits para un LFSR podemos obtener una cadena de 128Gb
- Los LSFR son sencillos, ocupan poca memoria, es rápido y eficiente (lo que los hace ideales para sistemas de cifrado)
- En el caso del DVD se, usan 2 LFSR, uno de 17 bits y otro de 25 bits (eso da 42, pero 2 de los bits de la semilla se introducen al principio y no forman parte de la clave)
- La semilla de los LFSR proviene de la TK
- Se combinan los 2 flujos para obtener 1 de 40 bits. Se utilizaron 2 registros para hacer más complejo un análisis criptográfico.
- Pese a ello, 2 errores provocaron que se pudiesen tomar atajos:
    - en el descifrado de la TK se utiliza una técnica llamada *mangling* (exprimido) que tiene un fallo y permite averiguar 5 bits de la clave LSFR si conocemos el mensaje llano y el mensaje encriptado
    - si averiguamos los 5 bits iniciales de un LSFR combinado - como es el caso - existe una táctica que nos permitiría averiguar la clave de 40 bits
    - combinando los 2 errores, la complejidad de la clave cae de 2^40 a 2^16, reduciendo el tiempo de cálculo de 1 semana a segundos
- otro ataque, realizado por Frank A. Stevenson, permitía recuperar la DK al reducir la complejidad de la desencriptación de 2^40 a 2^25

curiosidades

- la limitación de 40 bits para la protección de los DVD fue debido a la limitación USA de exportación de cripografía de «mayor peso», (acuerdos ITAR)
- la guerra comenzó cuando la agencia encargada de dar permisos - y las claves - la DVD-CCA se negó a dar esas claves a programas Linux - por el principio de código abierto de la plataforma- lo que impedía ver DVDs a los usuarios de dichos sistemas operativos.
- el inicio del hack del sistema fue un grupo de hackers llamado MoRE [4] que obtuvieron una de las 409 claves - concretamente la de un programa llamado XingDVD.

[1]
Content Scrambling System
[2]
Lineal Feedback Shift Register
[3]
Feedback Shift Register
[4]
Masters of Reverse Engineering