# Aplicaciones para Smart Cards



## Realización de un sistema de cerradura cuya llave será una tarjeta sin contacto.

## BAJO NINGÚN CONCEPTO ESCRIBIR EN LOS Lock bytes ni en los OTP DE LA TARJETA

Se trata de realizar la simulación de un sistema de cerradura y llave para hoteles o cualquier otro tipo de dependencias con variado personal de acceso.

Utilizaremos la mifare ultralight C. Haremos uso de sus características avanzadas (autenticación, protección de lectura y escritura...etc). La clave 3DES de la mifare ultraligh-C será la que trae grabada de fábrica, por defecto.

Para simular el sistema de cerradura con llave sin contacto realizaremos dos scripts que llamaremos: **gestión y cerradura**.

**gestion**: es el script que simula la creación de las tarjetas llave para los clientes y personal del hotel. El personal del hotel tendrá una tarjeta maestra que les dará acceso a todas las habitaciones, pero cada empleado tendrá un código distinto, de tal forma que la cerradura pueda registrar quién la ha abierto en día, y hora determinada. La llave será una tarjeta mifare ultralight-C, con una serie de campos escritos según la siguiente especificación:

> Página 04: ALLD (en ASCII) (4 octetos indica llave maestra) ó ONED (en ASCII) (4 octetos indica llave de

habitación)
Página 05: Número de habitación (ASCII) (4 octetos que indican la habitación a la que pertenece la llave). Por ejemplo a 1234 en ASCII.
Página 06: Día y mes de salida del hotel en ASCII --> Ej. 26 de Febrero --> 32363032H (para los empleados su día y mes de nacimiento, el caso de maestra)
Página 07: Año de salida del hotel en ASCII --> Ej.- 1025 --> 31303235H (año de nacimiento del empleado, si la llave es maestra)
Página 08: Día y mes de entrada (4 dígitos en ASCII) igual formato que la fecha de entrada. (empleado: dia y mes de nacimiento)
Página 09: Año de salida en ASCII igual formato que el año de entrada. (empleado año de nacimiento)
Página 0A: Código del cliente y o empleado (4 dígitos en ASCII) Ej.- Se pone a C001 en ASCII. O a E001 empleado.
Página 0B: Código del hotel (4 dígitos en ASCII). Ej.- HT01
Página 0C: MAC (4 bytes). Calculado según lo siguiente:

El terminal de gestión dispone de la misma clave 3DES que tiene la tarjeta: KTL = 49 45 4D 4B 41 45 52, KTR = 21 4E 41 43 55 4F 59 46.
El terminal de gestión tendrá una clave 3DES maestra que será: KTML = 0011223344556677 , KTMR = 8899AABBCCDDEEFF.

El terminal de gestion pide el número de serie a la tarjeta que son 7 bytes, lo rellena con FFH a la derecha para que sean 8 bytes y lo cifra con 3DES y ECB y con la clave maestra; así obtendrá la clave por tarjeta.
Para calcular el MAC concatena las páginas 04|05|06|07|08|09|0A|0B, No necesita relleno. Utilizando como vector de inicialización el número de serie de la tarjeta relleno con FF a la derecha, cifra, la concatenacion de páginas 04 a 0B con la

clave por tarjeta. El MAC serán los cuatro bytes más a la izquierda de los últimos 8 bytes.

El terminal de gestion escribe en la tarjeta, en claro, las páginas 04H a 0CH, donde la última es el MAC.
El MAC se utiliza en caso de necesidad de verificación y se comprueba siempre que un cliente/empleado da la tarjeta en gestión por un problema de malfuncionamiento o cualquier otro tipo de problema.

El terminal escribe los bytes correspondientes de las páginas 2AH y 2BH (authentication configuration) para que no se pueda leer ni escribir desde la página 04 hasta el final de la tarjeta mientras no se realice la autenticación. Así la tarjeta queda protegida contra lecturas y escrituras en el caso de pérdida o robo. Así mismo será imposible duplicarla.

**puerta**: es el script que simula la función de la cerradura de la puerta de la habitación.

La cerradura dispone de la clave 3DES que tiene la tarjeta: KTL = 49 45 4D 4B 41 45 52, KTR = 21 4E 41 43 55 4F 59 46.

La cerradura autentica a la tarjeta. No verifica el MAC.
Lee la página 04 y si es ALLD abre la puerta.
Si el contenido de la página 04 es ONED lee el número de habitación, fecha y año de salida. Si el número de habitación coincide con el de la habitación donde está la cerradura y la fecha de salida de la tarjeta es posterior o igual a la fecha actual abre. En caso contrario no abre.

No es necesario implementar el sistema de registro que debería tener la cerradura, dejando constancia en un fichero de las fechas y horas de apertura o de intentos de apertura y los códigos de cliente/empleado de las tarjetas que lo han efectuado.

Subir al servidor web los script gestion y cerradura.

Disponible en: sábado, 28 de febrero de 2015, 12:00
Fecha límite de entrega: domingo, 8 de marzo de 2015, 20:00

## Borrador del envío

Aún no se han enviado archivos

Subir un archivo (Tamaño máximo: 10Mb)

Choose File No file chosen
Subir este archivo

Ud. está en el sistema como Lizandro José Ramirez Difo. (Salir)

ASC-2015