Diseño de aplicaciones RFID para seguridad y control

Espín Garcia, Roderic

Grado en Ingeniería Electrónica Industrial y Automática
EPSEVG, Departamento de Ingeniería Electrónica UPC
Av. Víctor Balaguer s/n, 08800 Vilanova i la Geltrú

Resumen

La realización de éste proyecto se ha basado en el cumplimiento de una serie de objetivos: El primer objetivo trata sobre simular una tarjeta RFID de transporte ferroviario mediante LabView, el segundo objetivo consiste en hacer seguras las comunicaciones a dicha tarjeta para evitar fraudulencias. Seguidamente, como objetivos secundarios está la creación de una máquina expendedora de comida y bebida, donde el usuario puede comprar un número determinado de productos cada día mediante la tarjeta RFID (y poder recargarla) y una aplicación que simule dos semáforos (uno peatonal y otro de carretera), si el semáforo peatonal detecta una tarjeta RFID, indicará mediante un mensaje sonoro si el usuario puede cruzar la carretera o no (está pensado para personas con problemas de vista o invidentes).

1. Introducción

En el presente proyecto se describe la realización y simulación de una serie de aplicaciones haciendo uso de la tecnología RFID. El RFID es un sistema de identificación por radiofrecuencia que nos permite enviar y recibir datos a distancia sin necesidad de contacto. El trabajo consta de dos objetivos principales: el uso de una tarjeta RFID capaz de simular una tarjeta de transporte ferroviario y que ésta sea segura a copias y modificaciones.

Toda la información que se maneja en las aplicaciones, que serán programadas mediante el software LabView, será escrita en la tarjeta RFID y tendrá una copia de seguridad (para evitar fraudulencias) en un archivo .txt guardado en una base de datos, que funciona como servidor. Todas las aplicaciones son independientes entre sí y su punto fuerte es que con solo una tarjeta se pueden disfrutar de todos los beneficios que se ofrecen en las aplicaciones, ya que la tarjeta es multifuncional e independiente.

Los datos escritos en la tarjeta estarán codificados mediante el cifrado AES, un cifrado muy potente que hoy en día todavía no se ha logrado romper su algoritmo (y romperlo a fuerza bruta, actualmente, llevaría millones de años). Así pues, el usuario no tendrá posibilidad alguna de entender los datos escritos en la tarjeta, siempre y cuando no tenga acceso a la clave adjudicada (la cual solo estará guardada en el archivo .txt situado en la base de datos del servidor y que deberá proteger el propietario).

Como objetivos secundarios, se han establecido dos aplicaciones de interesante funcionamiento: la primera consiste en una máquina expendedora en la que un usuario puede comprar un número finito de productos diariamente, con la posibilidad de recarga. La segunda aplicación es una simulación de un semáforo peatonal donde cada vez que detecte una tarjeta RFID, enviará un mensaje sonoro para que el dueño de la tarjeta sepa el estado del semáforo peatonal, la aplicación está pensada para personas con problemas visuales o invidentes.

Este artículo pretende exponer los conceptos y desarrollo empleados durante la realización del trabajo final de grado.

Primeramente, se detallarán las características de la tecnología utilizada en el proyecto: el RFID y las ventajas que ofrece y por lo cual se ha escogido como tecnología a emplear. En el siguiente capítulo, se informará de los componentes RFID utilizados en el trabajo. A continuación, se describirá el cifrado utilizado a la hora de ocultar la información al usuario de la tarjeta. Seguidamente, se detallarán las aplicaciones realizadas, una breve mención a las subrutinas más importantes y el resultado de las simulaciones realizadas.

Finalmente, se hará referencia a las conclusiones a las que se ha llegado después de la realización del proyecto.

2. RFID

El RFID [1][2] es un sistema inalámbrico que utiliza campos electromagnéticos de radiofrecuencia para transferir datos mediante *etiquetas*. La información de las etiquetas se guarda en una memoria no volátil, ya que algunos tipos de etiquetas no tienen ningún sistema de alimentación incorporado.

Así pues, todo sistema basado en RFID tiene una arquitectura específica, que puede separarse en tres elementos: Etiqueta, Antena y Lector. En la figura 1 se pueden apreciar los elementos mencionados y la interacción entre ellos:

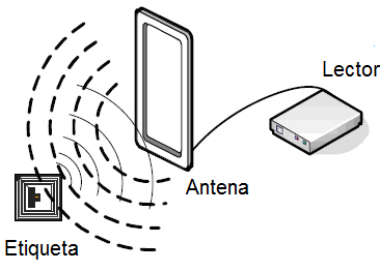

Figura 1*: *Arquitectura de un sistema RFID

Etiqueta

La etiqueta (figura 2), es un identificador por radiofrecuencia que se adhiere a un objeto para que éste sea identificado. Un transmisor-receptor llamado *lector* (o transceptor) envía una señal a la, etiqueta y capta la señal de respuesta que la etiqueta le envía.

Una etiqueta puede ser activa, pasiva o pasiva asistida por batería. Una etiqueta activa tiene una batería que periódicamente envía señal de su ID. Una etiqueta pasiva no requiere de fuente de alimentación interna ya que solo se activará cuando un lector le suministre energía cuando la propia etiqueta se encuentre en el rango del lector. El tercer tipo de etiquetas, las pasivas asistidas por batería, tienen una pequeña batería que alimenta a la etiqueta cada vez que haya un lector cerca.

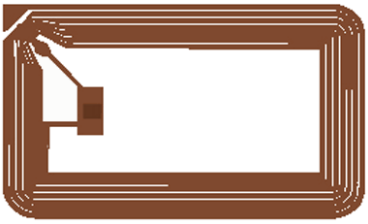

Figura 2*: *Etiqueta

Lector

El lector recibe y envía señales a una etiqueta detectada, convirtiendo las ondas de radio de las etiquetas en un formato digital para que pueda ser procesado lógicamente. Hay dos tipos de lectores: pasivos y activos, que, dependiendo de la etiqueta que haya identificado, se establecerá un comportamiento distinto entre ellos.

Si un lector pasivo encuentra a una etiqueta activa, ésta le enviará las señales al lector. Si un lector activo se encuentra con una etiqueta pasiva, será el lector quien alimente a la tarjeta mediante señales inducidas con corriente eléctrica y se inicie así la transmisión. Para un lector activo y una etiqueta activa, éstas últimas serán despertadas por una señal del lector. Las etiquetas asistidas por batería se comportan de igual manera que las etiquetas pasivas.

Antena

Las antenas son utilizadas para comunicarse entre lectores y etiquetas. Para cada frecuencia hay unas características físicas/químicas diferentes. Los tipos de antena utilizados en una etiqueta dependen de su aplicación y de la frecuencia de sus operaciones. Las frecuencias se pueden separar en cuatro grupos: baja frecuencia (LF), alta frecuencia (HF), frecuencia ultra alta (UHF) y frecuencia de microondas.

Ventajas del RFID

La tecnología RFID ofrece diversas ventajas y beneficios respecto a otras tecnologías y prácticamente no tiene inconvenientes, así pues, algunas de estas ventajas son que no se requiere línea de visión a la hora de transmitir información, puesto que con simplemente estar dentro de la distancia del rango de lectura ya es suficiente, puede funcionar en ambientes hostiles y agresivos, a largas distancias (la distancia dependerá de la frecuencia utilizada) y existe la capacidad de leer y escribir diferentes etiquetas en un rango determinado, una tras otra, gracias a una función llamada anticolisión y tiene una capacidad de lectura y escritura rápida y precisa.

Es debido a éstas ventajas que se ha escogido la tecnología RFID adecuada para transmitir la información procesada en las aplicaciones realizadas.

3. Componentes RFID empleados

Para realizar las operaciones de lectura y escritura basadas en la tecnología RFID, se ha escogido un lector/escritor de frecuencia 13’56Mhz y una tarjeta RFID de 4kb de memoria EEPROM. A continuación se mostrarán las características más importantes de estos componentes:

Tarjeta RFID: Mifare IC S70

Mifare IC S70 [4] es una tarjeta que contiene una etiqueta pasiva con un rango de funcionamiento de hasta 10cm, tiene una EEPROM de 4kb de memoria donde almacena las claves internas y los datos a almacenar. La memoria se divide en 256 bloques de 16bytes, agrupados en sectores. Para cada sector, hay una clave de acceso, la cual debes conocer si quieres leer o escribir en un bloque de memoria situado en tal sector. Así pues, para cada sector, habrá un bloque donde se guardan los valores de estas claves, que podrán ser cambiadas por el usuario, siempre y cuando conozca sus valores.

Lector RFID: YHY632A

El lector utilizado, el YHY632A[5] (figura 3), para la simulación de las aplicaciones puede leer y escribir en tarjetas RFID a una distancia máxima de 10cm de frecuencia 13’56MHz, tarda menos de 100ms en leer y escribir datos a la tarjeta, puede comunicarse bajo USB o RS232 a una velocidad de transmisión de 9600 a 115.200bps. El protocolo que utiliza es el ISO 14443A.

Figura 3*: *YHY632

Entre otras funciones, el lector/escritor escogido es capaz de leer y escribir en un bloque, permitir a la tarjeta Mifare

la función autocolisión, que el lector efectúe un pitido, cambiar las claves de un sector, etc...

4. Cifrado AES

AES (AdvancedEncryption Standard)[5][6] fue el resultado de un concurso realizado en Estados Unidos el año 1997, el objetivo del cual era encontrar un cifrado que fuese capaz de proteger la información durante el siglo XXI.

Para cifrar un texto en AES hay que seguir un orden específico que será siempre el mismo. En dicho orden actuarán cuatro cuatro procesos diferentes: *SubBytes*, *ShiftRows*, *MixColumns* y *AddRoundKey*. Por último tenemos un proceso paralelo llamado *Key Schedule* que nos servirá para expandir la clave inicial introducida.

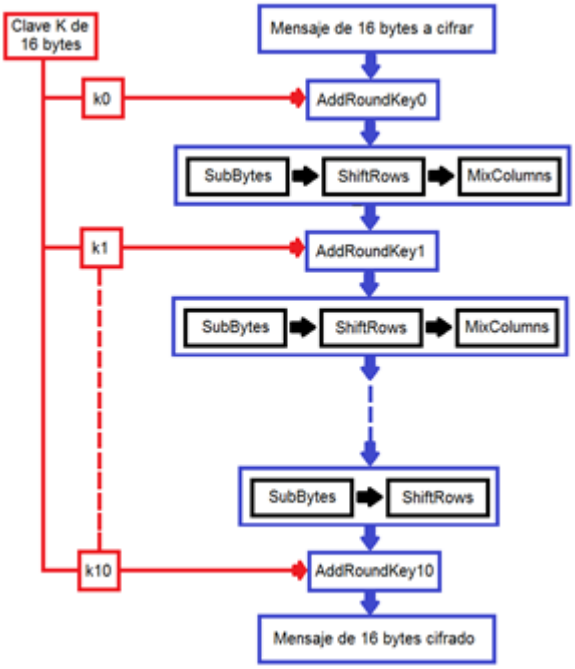

Figura 4*: *Orden del cifrado AES

La etapa SubBytes consiste en hacer una sustitución de la matriz de entrada byte a byte utilizando una tabla llamada *Rijndael S-Box* (Rijndael Substitution Box) la cual tiene propiedades no lineales. La etapa ShiftRows consiste en rotar hacia la derecha los bytes de las filas de la matriz de entrada, cada fila se le debe rotar un número conocido de bits. La etapa MixColumns consiste en multiplicar cada columna de la matriz de entrada por una matriz constante, cuyo valor dependerá de si se está cifrando o descifrando el mensaje, los resultados de estas nuevas cuatro columnas formarán la matriz de salida. AddRoundKey es una etapa que consiste en aplicar una XOR del mensaje cifrado de ronda y una clave expandida de la ronda actual. Para calcular la clave de ronda es necesario aplicar el KeySchedule, cuya función es la de expandir la clave inicial. Para descifrar los mensajes, se deben aplicar todas las etapas al revés y seguir el esquema de la figura 4 en orden invertido.

Es importante saber que a día de hoy no se ha encontrado todavía ningún método para poder romper el cifrado (siendo el ataque a fuerza bruta inviable), motivo principal por el cual se ha escogido para cifrar las aplicaciones realizadas.

5. Aplicaciones realizadas

A continuación se detallarán las cinco aplicaciones realizadas con el software LabView. Las aplicaciones han sido programadas de tal manera que eviten que el usuario pueda modificar los datos para aprovecharse, anulando así posibilidad de fraude. El único punto débil, y que ocurre con cualquier sistema de cifrado, es que la seguridad del sistema es directamente proporcional a la seguridad de la ubicación de la clave, cosa que dependerá de la seguridad de la base de datos (donde se guardarán las claves y los datos de las tarjetas).

Para poder asegurar que los usuarios no puedan saber la información guardada en una tarjeta, es necesario emplear el cifrado AES explicado anteriormente, es por eso, que la primera aplicación será la de implementar el cifrado en LabView. Así pues, el objetivo de esta aplicación ha sido el de poder cifrar y descifrar un mensaje a partir de una clave secreta. En AES, se ha escogido un tamaño de clave 128 bits, ya que éste tamaño es el mismo que el de un bloque de memoria de la tarjeta Mifare S70.

La segunda aplicación realizada en LabView es un simulador de un terminal generador de tarjetas. El objetivo de esta aplicación es la de poder escribir en la tarjeta Mifare S70 la suficiente información como para poder simular una tarjeta de viajes ferroviarios. La información que se transmita en todo el sistema RFID debe estar cifrado mediante AES para evitar que el usuario pueda conocer los datos originales que se pretendan guardar. La información también será escrita en un archivo .txt ubicado en una base de datos, que tendrá la función de servidor que almacena todos los datos y claves de las tarjetas. En lo que respecta a los datos guardados, éstos serán la fecha en que se ha creado o modificado la tarjeta de viajes, los viajes de zona disponibles, el tipo de tarjeta (tarjeta simple, tarjeta día, tarjeta mensual o tarjeta trimestral) y también si la tarjeta ha caducado. La funcionalidad de la tarjeta podrá ser comprobada en la tercera aplicación: una simulación de barreras de entrada y salida a las vías de tren. Las tarjetas caducadas o de tipo tarjeta simple podrán ser recargables por el terminal.

Ésta tercera aplicación permitirá dejar el paso a los usuarios cuyas tarjetas RFID tengan viajes disponibles. Las barreras aceptarán los cuatro tipos de tarjeta: tarifa simple, tarjeta día, tarjeta mes y tarjeta trimestre. No dejarán acceder a tarjetas sin viajes o que ya estén caducadas. Las barreras calcularán la zona en la que ha viajado el usuario y, al salir de las vías (cuando ya se haya efectuado el trayecto), se le descontará un viaje de la zona viajada a la (para tarjetas de tipo tarjeta simple). Si el usuario sale de las vías sin utilizar su tarjeta, no podrá volver a entrar con dicha tarjeta hasta que no haya efectuado el viaje completo, lo mismo ocurre

que si no se ha entrado no te dejará salir. Si el viaje realizado no corresponde a una zona disponible (o superior), las barreras tampoco te permitirán salir, y el usuario deberá recargar la tarjeta en un terminal que esté situado una vez pasadas las barreras.

La cuarta aplicación que fue pensada para empresas o centros residenciales (como ahora un geriátrico) es una máquina expendedora de comida y bebida. La función de la aplicación consiste en que, un usuario con una tarjeta RFID válida, pueda comprar de ella un número determinado de productos cada día. El usuario podrá recargar la tarjeta en la propia máquina expendedora cada día para que pueda comprar más productos, así pues cuando la tarjeta se quede sin compras permitidas, deberá esperar otro día para recargar. Toda la información será guardada también en una base de datos (como en la segunda aplicación), donde también se guardará la clave. (ya que los datos en esta aplicación también estarán cifrados).

La quinta y última aplicación está ideada para personas que sufran problemas de visibilidad o sean invidentes. Se trata de un simulador de semáforos, en la que si el semáforo peatonal detecta una tarjeta RFID, éste indique al usuario mediante un mensaje sonoro el estado actual del semáforo peatonal y los segundos restantes para cambiar de estado.

A parte de las cinco aplicaciones generales, se hace especial mención a otras subrutinas que han necesitado ser programadas también mediante LabView para poder realizar con éxito las aplicaciones anteriores. Dichas subrutinas realizan las funciones de: Leer y escribir en un archivo .txt, obtener los valores del tiempo actual, restar dos fechas con precisión de 1 minuto, detectar tarjeta, leer de tarjeta y escribir en tarjeta, creación de tablas logarítmicas, exponenciales, de S-Box y la inversa de la S-Box (utilizadas para poder cifrar y descifrar) y las diferentes etapas de cifrado.

6. Resultados de las simulaciones

Después de desarrollar las aplicaciones en LabView, se han obtenido los resultados siguientes:

El tiempo que tarda la primera aplicación en cifrar y descifrar un mensaje es de 2 milisegundos. Esta velocidad hace que el resto de aplicaciones no se vean afectadas por el hecho de tener que cifrar y descifrar la información continuamente. Así pues, en la figura 5 se muestra una captura de un mensaje cifrado en AES:

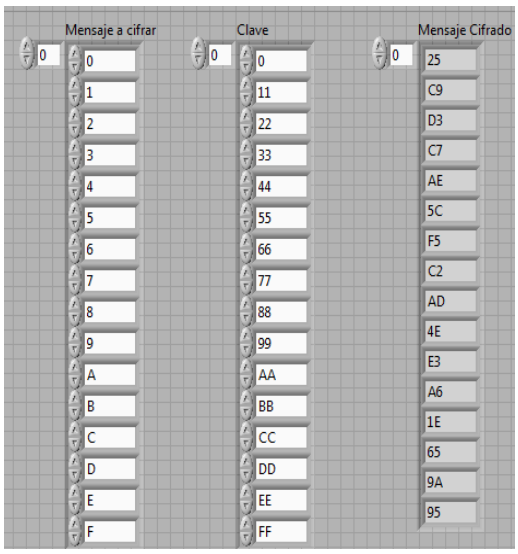

Figura 5*: *Mensaje cifrado mediante AES

En la segunda aplicación, se ha simulado un menú HMI para poder realizar la generación de tarjetas para viajar en tren, la figura 6 se muestra la interfaz cuando el usuario está en la selección de viajes y zonas a comprar:

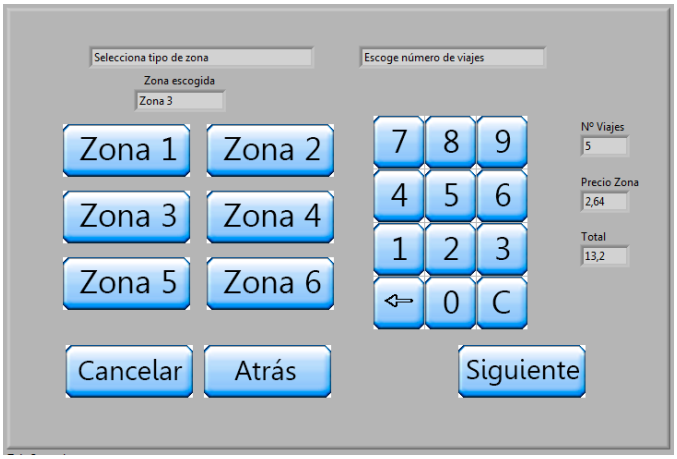

Figura 6*: *Interfaz de selección de viajes

Después de efectuar el pago, se ha creado una página extra para que se puedan observar los datos más interesantes, aunque hay que tener en cuenta que en una aplicación real, estos datos NO deben ser visibles para nadie, ya que los datos de la clave generada será guardado en el archivo .txt y el array a escribir se escribirá cifrado para que el usuario no pueda entender los datos escritos.

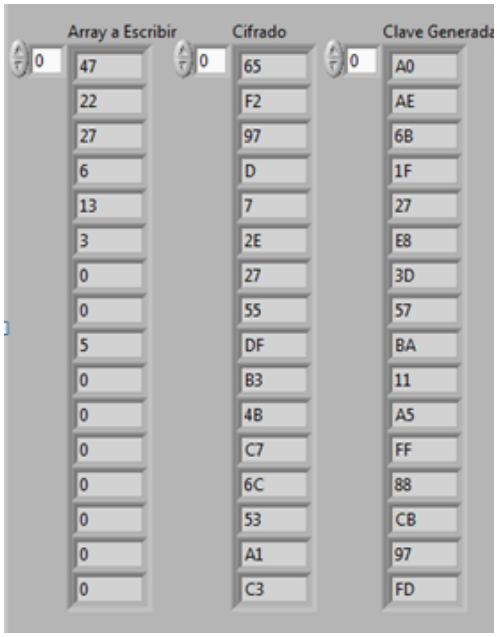

Figura 7*: *Datos a escribir en la tarjeta

En la figura 8 se muestra la base de datos creada a partir de la generación de diferentes tarjetas RFID y una muestra de la información que contiene una de ellas. El nombre de cada archivo es el mismo que el de la ID de cada tarjeta (en valor decimal):

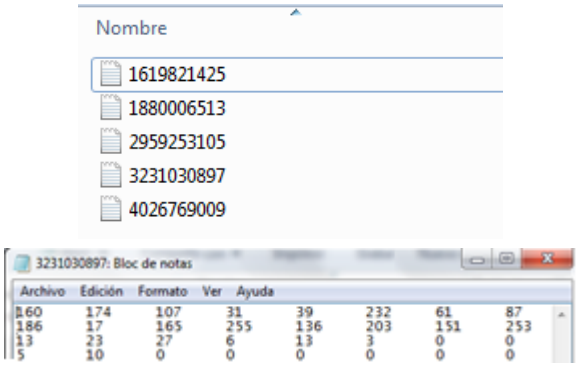

Figura 8*: *Base de datos generada

La tercera aplicación simula dos tipos de barreras: las de entrada y las de salida. Generamos una tarjeta con 5 viajes de zona 1 y recargamos 2 viajes de zona 3 y nos dirigimos a una barrera de entrada, aparece una animación de las barreras abriéndose:

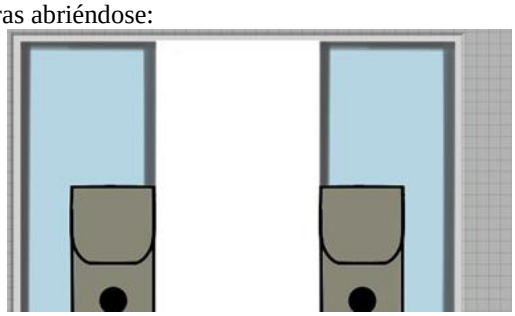

Figura 9*: *Barreras abiertas

Si la tarjeta impide la entrada o salida de las barreras, éstas permanecen cerradas.

En la cuarta aplicación se ha creado el interfaz de la figura 10 para poder simular una máquina expendedora:

Figura 10*: *Máquina expendedora

En la figura anterior se puede observar que se ha encendido un LED identificador donde se sitúa el producto seleccionado (en este caso un bocadillo) y también se muestra el precio por si el usuario prefiere pagar el producto en metálico. La luz roja indica que no se ha detectado ninguna tarjeta. Cuando intentamos comprar un producto podremos ver si se ha realizado la transacción con éxito mirando el LED identificador, si pasa a verde significa que la transacción se ha realizado (siendo el valor 2 los productos de bebida disponible y 1 el de comida):

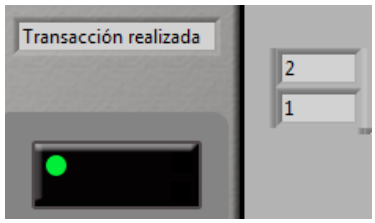

Figura 11*: *Transacción realizada

En cambio, si compramos más comidas de las permitidas nos encontraremos con lo siguiente:

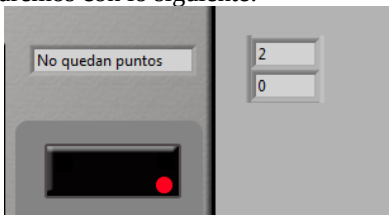

Figura 12*: *Transacción no realizada

En la quinta aplicación, se obtienen como resultados una satisfactoria detección de la tarjeta y mensaje de respuesta,

como ejemplo la siguiente captura indica lo que ocurre justo cuando se detecta una tarjeta RFID:

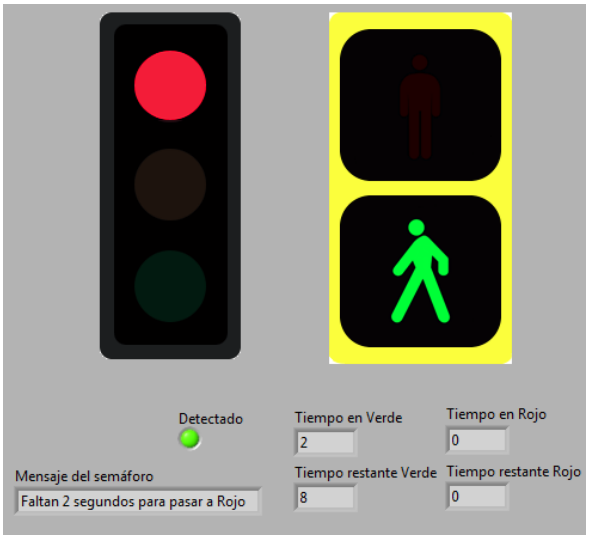

Figura 13*: *Semáforo peatonal en verde

7. Conclusiones

Con este proyecto se ha conseguido transferir datos con una tarjeta RFID libre de modificaciones no permitidas, si bien se ha diseñado específicamente para las aplicaciones realizadas, los métodos utilizados se puede extrapolar a otras aplicaciones en las que se empleen también tarjetas RFID y se necesite que estén protegidas.

También hay que tener en cuenta, que las aplicaciones realizadas son muy flexibles y permiten la capacidad de añadir funciones extras con relativa facilidad, por ejemplo, añadir diferentes tipos de comida o restricciones en la máquina expendedora, crear un sistema jerárquico en lo que a permisos se refiere, poder utilizar el mismo sistema realizado en el semáforo pero para otras aplicaciones donde los invidentes hoy en día sigan necesitando información, etc.

Mencionar también la independencia que hay en las diferentes aplicaciones, pero que pueden ser utilizadas en una misma tarjeta, esto es importante pues con sólo una tarjeta se pueden hacer múltiples actividades, ahorrando así espacio en el monedero u otro contenedor.

Personalmente, gracias también a la realización del proyecto, he adquirido los conocimientos necesarios para poder cifrar y descifrar con un cifrado muy poderoso (y que seguirá siéndolo durante años), además de entender y comprender una tecnología que cada día está siendo más popular y está sustituyendo a tecnologías que se están quedando obsoletas.

8. Referencias

[1] Weis, Stephen A, *RFID (Radio Frequency Identification): Principles and Applications*, MIT CSAIL, 2007

[2] Sen, Dipankar; Sen Prosenjit; Das, Anand, *RFID For Energy and Utility Industries, PennWell*, 2009

[3] NXP Semiconductors, MF1S703x, Diciembre 2010

[4] Beijing易火眼, *YHY632User Manual*, Junio 2009

[5] J. Daemen and V.Rijmen, *AES Proposal*: Rijndael, Septiembre 1999

[6] National Institute of Standards and Technology (NIST), *AES*, Noviembre 2001