**Citar este artículo como**: Gómez Collado, C.O., & Suárez Marina, P.A. (2019). Sistema de control de acceso con encriptación AES a 128 bits. *Revista Utesiana de la Facultad de Arquitectura e Ingeniería*, *4(4)*, 34-43.

# SISTEMA DE CONTROL DE ACCESO CON ENCRIPTACIÓN AES A 128 BITS

**Cristhian O. Gómez Collado**[6]
Universidad Tecnológica de Santiago

**Paul A. Suárez Marina**[7]
Universidad Tecnológica de Santiago

**RESUMEN**: Este artículo presentará con detalle el funcionamiento del sistema de control de acceso con encriptación AES a 128 bits. Este producto debe controlar, monitorear y registrar los eventos que ocurren en un portal mediante el uso un software de computadora. Todo control de acceso básico está compuesto por un identificador de usuario que en el caso de este sistema es un lector de RFID, cerradura electrónica en este caso se utilizó electromagnético. En cuanto a los aspectos de comunicación del servidor, los controles de acceso convencionales utilizan el estándar Ethernet, sin embargo este producto le ofrece la opción al cliente de comunicarse con el servidor médiate de manera inalámbrica mediante el protocolo WIFI.

**Palabras clave**: sistema control de acceso, encriptación AES, computadora, software.

**ABSTRACT**: This paper will present in detail the operation of the access control system with AES 128-bit encryption. This product must control, monitor and record the events that occur in a portal through the use of computer software. All basic access control is composed of a user identifier that in the case of this system is an RFID reader, electronic lock in this case electromagnetic was used. Regarding the communication aspects of the server, the conventional access controls use the Ethernet standard, however, this product offers the option to the client to communicate with the server mediated wirelessly through the WIFI protocol.

**Key words**: access control system, AES encryption, computer, software.

[6] Estudiante de la carrera de Ingeniería Electrónica de la Universidad Tecnológica de Santiago. Autor para correspondencia: crishtiangomez1@alumno.utesa.edu
[7] Estudiante de la carrera de Ingeniería Electrónica de la Universidad Tecnológica de Santiago.

## INTRODUCCIÓN

El presente artículo desglosara de manera detallada todos los procesos realizados durante la asignatura de diseño electrónico. Este trabajo busca explicar el procedimiento utilizado para convertir un prototipo en un producto. El prototipo el cual se analizara a lo largo de esta asignatura es el sistema de control de acceso con encriptación AES a 128 bits. Un control de acceso es un dispositivo que identifica una entidad o persona, es decir, que autentifica mediante clave, tarjetas, huellas digitales y otros dispositivos de identificación que la persona es quien dice ser. Dado a que es un sistema, es lógico asumir que existen más elementos o mecanismos que lo componen.

## DESCRIPCIÓN DEL DISEÑO

Este sistema busca controlar y monitorear la entrada y salida de personal de una o más sucursales de manera electrónica a través de 2 módulos de comunicación, donde uno se comunicará con los servidores mediante vía ETHERNET y el otro se comunicará vía WIFI. Dicha información será cifrada bajo el estándar AES (Encriptación Estándar Avanzada, por sus siglas en inglés) con un tamaño de 128 bits.

## NORMATIVAS

- Norma ISO/IEC JTC 1/SC 25: estándar para sistemas de microprocesadores, microcontroladores protocolos, interfaces, redes, entradas, salidas y construcción eléctricas.
- Norma ISO / IEC JTC 1 / SC 22: estándar para el uso de lenguajes de programación.
- IPC-2518: estándar para la inclusión del listado de piezas que componen un diseño.
- IPC-2221B: estándar del diseño de PCB.
- EIA-485, ANSI/TIA/EIA-485-A-1998: estándar de especificación de características eléctricas que debe poseer la comunicación entre dispositivos.
- IEEE 802.11: estándar para la comunicación inalámbrica WIFI.
- IEEE 801.11: estándar para la comunicación alámbrica Ethernet.
- FCC: estándar que regula que los dispositivos no pueden crear interferencia o señales no deseadas en otros sistemas.
- SSC/PCI/PA-DSS: estándar que regula la seguridad de datos.
- IPC-D-279: Instrucciones de diseño para montaje en superficie Impreso.
- ISO / IEC 25030: proporciona requisitos y recomendaciones para la especificación de los requisitos de calidad del software.
- ISO/IEC 15504: es un modelo para la mejora, evaluación de los procesos de desarrollo, mantenimiento de sistemas de información y productos de software.

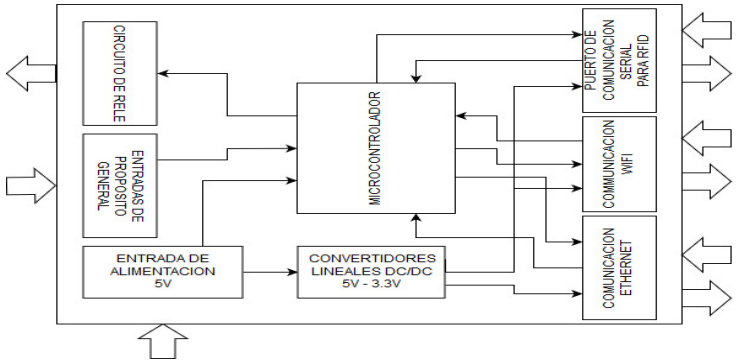
- ISO/IEC 27001: normativa que regula la implementación de seguridad de la información.
- ISO/IEC 7816: estándar que regula las tarjetas de identificación electrónicas.
- ISO/IEC/IEEE 42010: norma que regula la descripción de la arquitectura de un sistema.
- ISO/IEC 14598: regula la calidad y estructura de software de computadora.
- La Norma ISO 924: es la norma enfocada a la calidad en usabilidad y ergonomía tanto de hardware como de software, fue creada por la ISO y la IEC.

## ESPECIFICACIONES DEL DISEÑO

- Estándar avanzado de encriptación (AES) a 128 bits.
- Interfaz Ethernet RJ35.
- Comunicación WIFI 2.4 GHz.
- Protocolo de red TCP/IP.
- 2 salidas de 125VAC-30VDC.
- Software de monitoreo en tiempo real.
- Control de portal.
- Asignación de usuarios maestros.
- Modificación de llave de encriptación.
- Registro de usuarios.
- Capacidad para 20 usuarios normales.
- Capacidad para 3 usuarios maestros.
- Lector de tarjetas RFID de 125kHz.
- Switch de selección de comunicación con servidor.
- Botón de reinicio.
- Voltaje de entrada 5 Vdc.
- LED indicador de transmisión de datos Wifi.

## DIAGRAMA DE BLOQUES Y DE FLUJO

Figura 1. Diagrama de bloque del MCC.




Fuente: elaboración propia.

A continuación, se definen las etapas:

- Etapa de alimentación: En esta etapa tenemos un circuito con un LM 317 que regulará el voltaje de entrada de 5v a 3.3v. Este circuito tendrá un puerto de alimentación hembra de 5.5mm que alimentará el regulador. Este circuito se necesita para alimentar el controlador de la comunicación Ethernet (USRTCP232) y el módulo de comunicación WIFI (ESP8260).
- Etapa de salida de portal: El Prototipo manejará 2 salidas relé que son necesarios para la activación de los dispositivos electromecánicos que se encargaran del cierre y la apertura de los portales.
- Etapa de entrada de portal: A través de entradas de propósito general se detectará el estado de las puertas.
- Etapa de comunicación Wifi: Para poder transmitir información a la red de manera inalámbrica se utilizó un módulo esp8266.
- Etapa de comunicación Ethernet: Se utilizó el módulo USRTCP232 que convierte la información serial UART RS232 en paquetes de datos TCP.
- Etapa de lectura de datos de RFID: Se utilizará una la lectora ID12LA, para recibir los datos desde las tarjetas de 125 Khz. Este módulo envía los datos mediante el protocolo UART RS232.
- Etapa de procesamiento de datos: Para este prototipo utilizaremos un micro controlador PIC18f25k22 creado por la empresa microchip de arquitectura tipo RISC que por su siglas en ingles significa computador de conjunto de instrucciones reducidas. Este se encargará de recibir, encriptar y enviar la información de la tarjeta de RFID hacia el servidor.

**PROGRAMADOR DE SOFTWARE**

- Inicio: Inmediatamente se le subministra alimentación al módulo de comunicación y control Ethernet/wifi, el software iniciará automáticamente el programa o firmware.
- Inicialización de fusible/bits de configuración:En la familia de los micros controladores PIC existen a nivel de programación unos bits de configuración que necesitan ser inicializados para que el micro pueda operar de manera correcta; también se le conocen como fusibles. La mayoría de estos fusibles poseen de manera predeterminada una configuración y no necesitan ser inicializados.
- Configuración de puertos: En este segmento declaramos los puertos que se utilizaran como entrada y salida.
- Inclusión de librerías: En esta parte procedemos a incluir las librerías que se necesitan para manejar de manera más prácticas algunos elementos del microcontrolador ,como pueden ser el manejo de los módulos Ethernet, WIFI y encriptación AES128 bits.

- Declaración de variables globales y funciones: En esta parte del programa declaramos todas las variables globales que estarán presentes en varios de los procesos a realizar y también las funciones.
- Inicialización de comunicación uart (rs232): En esta parte del programa procedemos a enviar la información de configuración para habilitar los tipos de comunicación que vamos a utilizar. Para el módulo wifi necesitamos comunicación rs232 y para el modulo Ethernet y rfid necesita comunicación uart.
- Inicialización de módulos Ethernet & wifi y verificación de comunicación: En esta parte a inicializamos lo módulos utilizando librerías, y enviamos los parámetros de configuración que se necesitan para que comience la comunicación. Mediante un método de verificación detectaremos cual módulos está conectado; dependiendo de esto inicializamos uno de los 2; en el caso de que ninguno esté conectado se le enviará una señal al usuario que le indicará error en la conexión de los módulos.
- Establecer comunicación con servidor: En esta etapa del programa, una vez que se confirme que medio de comunicación, se utilizará y se establecerá comunicación entre el software de la computadora y el módulo de comunicación y control. En el caso de que la comunicación con el servidor sea negativa se le indicará al usuario que hay en error en la comunicación con el servidor.
- Verificar estado de portales:E n esta parte del programa utilizaremos una entrada análoga y una entrada digital para verificar el estado de las puertas y de estar abierta se mandará un dato de notificación al servidor.
- Leer puerto rfid: En esta parte del programa entra en un bucle infinito donde siempre se mantendrá leyendo el registro del puerto serial de donde proviene la información de la lectora rfid. En caso de que se detecte la presencia de datos, el programa ejecutará una sub rutina a la que hemos llamado “sub-proceso a”.
- Verificar estado del botón: En esta parte del programa se verifica a través de una entrada digital si el botón de salida fue pulsado. En el caso de que el caso positivo entraremos en una sub rutina a la que hemos llamado “sub-proceso b”.
- Lectura de datos desde el servidor para apertura de puerta: En esta parte del programa se mantendrá leyendo el registro del puerto serial para verificar si alguna información llega desde el servidor. En el caso de que la señal que llega desde el servidor , luego de ser desencriptado, si se verifica que es el dato para abrir la puerta de manera remota desde el servidor se enviara la señal para abrir la puerta.
- Verificación de estado de portal: En esta parte del programa utilizaremos una entrada análoga que nos indicará si el estado de la puerta está abierto y cerrado y en el caso de se detecte que este abierto el programa el programa entrara en la sub rutina “sub-proceso b”.
- Encriptar datos: En esta parte de la sub rutina se le aplicará una serie de procesos lógicos y matemáticos al mensaje proveniente desde la

lectora rfid. La particularidad de este tipo de encriptación requiere de una clave definida por el diseño y que se mezclan con el mensaje procesado.

- Enviar datos al servidor: Esta parte de la sub rutina se envían los datos encriptados al servidor a través del puerto serial cuyo protocolo de comunicación va a depender del módulo que esté conectado que previamente fue detectado.
- Verificación de datos desde el servidor: En esta etapa de la sub rutina el programa espera la respuesta de confirmación de que el mensaje llego de manera exitosa. En caso de que no reciba una respuesta del servidor, el micro notificará al usuario y buscará la información en la memoria eeprom del micro. En el caso de que la información del usuario este en la memoria, se enviará la señal para la apertura de la puerta. De lo contrario terminara la sub rutina.
- Esperar respuesta del servidor: Para el caso de que la confirmación del mensaje sea exitosa, el programa se quedará esperando respuesta del servidor. En el caso de que el servidor confirme que la información subministrada coincide con la base de datos, se envía la señal de apertura de puerta. Para el caso contrario, termina la sub rutina.
- Encriptar datos: En esta parte de la sub rutina se le aplicará una serie de procesos lógicos y matemáticos al mensaje proveniente desde la lectora RFID. La particularidad de este tipo de encriptación requiere de una clave definida por el diseño y que se mezclan con el mensaje procesado.
- Enviar datos al servidor: Esta parte de la sub rutina se envían los datos encriptados al servidor a través del puerto serial cuyo protocolo de comunicación va a depender del módulo que esté conectado, que previamente fue detectado.
- Verificación de datos desde el servidor: En esta etapa de la sub rutina el programa espera la respuesta de confirmación de que el mensaje llego de manera exitosa. En caso de no recibir la confirmación del servidor, notificará al usuario y terminará la sub rutina. En el caso de que se reciba la confirmación del servidor simplemente termina la sub rutina.

## VERIFICACIÓN Y PRUEBAS PRELIMINARES

- Definición de prueba de encriptación y desencriptacion de datos del módulo de comunicación y control: En esta prueba se busca cifrar y descifrar datos utilizando el estándar americano de encriptación (AES por sus siglas en inglés) a un tamaño de 128 bits.
- Definición de prueba de comunicación con red Ethernet a otros dispositivos: En esta prueba se busca enviar y recibir datos desde el módulo de comunicación y control hacia una computadora vía Ethernet utilizando un cable RJ45 y mediante el protocolo de comunicación SPI en el firmware. El mismo será visualizado utilizando el

programa HÉRCULES UTILITY que permite ver el tráfico de información presente en la red local.

- Definición de prueba de lectura valida de tarjeta RFID: En esta prueba se busca recibir datos de una tarjeta RFID utilizando el módulo ID12LA mediante el protocolo de comunicación serial UART por software. El dato recibido por el módulo de comunicación y control será enviado nuevamente a través del puerto serial nativo del PIC hacia una tarjeta de arduino que hará el papel de monitor serial.
- Definición de prueba de comunicación en red wifi con otros dispositivos: En esta prueba se busca establecer conexión y enviar datos a un ordenador, desde el módulo de comunicación y control, utilizando el módulo ESP8266. Dichos datos deberán ser visualizados en un software que actuará como monitor serial del puerto que se seleccionará para recibir estos datos. También requieren que se le proporcione una dirección de IP con la que el módulo ESP8266 establecerá la conexión.
- Definición de prueba de encriptación de información de tarjeta RFID: En esta prueba se busca integrar la lectura de la tarjeta RFID utilizando el módulo ID12LA y la encriptación de esa información mediante el algoritmo AES a 128 bit. Dicha información será enviada de manera serial al servidor mediante el protocolo UART nativo del microcontrolador; el servidor deberá mostrar el dato encriptado de la tarjeta.
- Definición de prueba de distancia máxima de operación comunicación wifi: En esta prueba se busca determinar cuál es la distancia máxima que debe haber entre el módulo de comunicación y control y el ordenador para que el sistema pueda operar correctamente utilizando la comunicación wifi. Esta prueba se realizará solo para determinar la distancia, por lo que no deberá haber obstáculos entre ambos.
- Definición de prueba de comunicación wifi entre modulo y ordenador: Lo que se hará es leer el valor de varias tarjetas de RFID 125 kHz utilizando el módulo ID12LA; una vez se tenga la información se enviará hacia el ordenador y se visualizará a través de un software que muestra el tránsito de paquetes TCP.
- Definición de prueba de desencriptacion del servidor: En esta prueba se busca visualizar a través del software del servidor la desencriptacion de los datos provenientes del módulo de comunicación y control. Dichos datos serán proporcionados por el modulo lector de RFID ID12LA y se transmitirán mediante vía WIFI mediante el protocolo TCP, utilizando el dispositivo ESP8266.
- Definición de prueba de comunicación entre servidor y módulo de com. Y control: En esta prueba se busca establecer comunicación entre el módulo de comunicación y control y el software servidor. Lo que se hará primero es establecer comunicación para luego enviar un paquete de datos utilizando el protocolo TCP mediante módulo wifi ESP8266. El IP del módulo de comunicación y control será 192.168.43.54, mientras que el del servidor será 192.168.43.109 y se comunicaran a través del puerto 80001. Por otro lado, el dato que se enviará será ID de la tarjeta

encriptado, luego se le enviara un dato al módulo de comunicación y control para que accione los relés.

Tal y como se demostró en un ensayo realizado en la herramienta proteos, se espera que el momento de iniciar la prueba el microcontrolador auxiliar comience a enviar datos no cifrados de manera serial (UART), y que el módulo de comunicación y control aplique el algoritmo de encriptación AES, que sin importar el tamaño del dato de origen, el dato resultante debe ser de 128 bits.

Durante una simulación emulamos el comportamiento de la lectora de tarjeta RFID utilizando un micro controlador que se encargará en enviar datos a través del puerto serial de la misma manera en que el módulo trasmite la información de la tarjeta, resultado en la recepción correcta de datos. Por lo que se espera que al momento de aproximar la tarjeta RFID se pueda visualizar el valor de la tarjeta en el monitor serial, Se espera recibir de 16 a 32 caracteres debido a experiencia con otros lectores de RFID.

Los primeros ensayos con el módulo ESP8266 fueron escribirle directamente desde la terminal de un ordenador. Luego de que la información llega al ordenador, se visualiza a través del programa WILDSHARK el dato encriptado y a través del software servidor se visualiza el dato de la tarjeta RFID. Se espera que en el ensayo 3 que tendrá una distancia de 20 metros haya deficiencia en la comunicación causando un retraso en el tiempo de respuesta. Los resultados de las muestras revelan como el software servidor es capaz de desencriptar los datos recibidos desde el módulo de comunicación y control.

Luego de llevar a cabo esta prueba podemos decir que el módulo de comunicación y control es capaz de encriptar y desencriptar datos mediante el uso del estándar americano de encriptación (AES) a un tamaño de 128 bits. Sin importar el tamaño del mensaje origina,l el módulo envía un dato encriptado de 128 bits, lo que sugiere que no hay ningún error en la traslación en el algoritmos de encriptación.

## RESULTADOS

- Luego de que pasaran 60 segundos no se encontró el dispositivo en la red local.
- Al momento de leer el puerto UDP (10001) y la dirección de IP asignado al módulo a través del firmware, no se recibieron datos de parte del mismo.

Resultado de prueba de lectura valida de tarjeta rfid:

- Al momento de realizar la prueba con la tarjeta identificada como "cristhian" obtuvimos a través del monitor serial su valor

correspondiente, donde el primer carácter es una información redundante teniendo un así el siguiente código valido: 5500849084C5.

- Se recibió un dato desde el IP (192.168.43.65) con un tamaño de 16 bytes por el puerto 8001. Y también se tiene que desde el ordenadorcuyo IP es 192.168.43.109 no envió respuesta hacia el módulo de comunicación y control.
- Análisis de prueba deencriptación de información de tarjeta RFID: Tomando en cuenta los resultados de esta prueba y de las pruebas preliminare,s podemos decir que el módulo de comunicación y control es capaz de llevar a cabo el algoritmo de encriptación AES a 128 bits.
- Análisis de prueba de comunicación wifi entre modulo y ordenador: Según las pruebas realizadas, se comprobó que el módulo de comunicación y control es capaz de conectar y enviar paquetes de datos encriptados usando el protocolo TCP a través del módulo ESP8266; y que también somos capaces de confirmar si dicha información coincide con la de la tarjeta RFID.
- Análisis de prueba de desencriptacion del servidor: Durante las pruebas se pudo observar que el dato encriptado por el módulo de comunicación y control no coincide el que encriptar el software, debido a la manera en que el visual estudio maneja la librería de criptografía.
- Análisis de prueba de comunicación entre servidor y módulo de com. Y control: Basado en los resultados obtenidos, podemos concluir que el sistema tiene la capacidad de comunicarse entre sus componentes, pudimos confirmar que el servidor es capaz de encriptar y desencriptar datos; también que el módulo de comunicación y control es capar de encriptar datos y enviarlos inalámbricamente vía wifi.

## PRUEBAS DE FIABILIDAD

El sistema de control de acceso con encriptación AES a 128 bits, es un producto cuyas etapas no son reparables por razones económicas; el mantenimiento del dispositivo es enteramente de software y firmware, es decir, que el módulo de comunicación y control no está constituido por componentes que se degraden a corto plazo.

## CONCLUSIONES

El sistema de control de acceso con encriptación AES a 128 bits es un producto dedicado a entidades bancarias y financieras que necesitan monitoreo constante de las personas que entran a un área determinada, y que esta información llegue al servidor de manera segura.

Durante el proceso de desarrollo de este producto se han realizado modificaciones importantes como fueron el cambio de la lectora de tarjetas de RFID, el cual en un principio era un módulo RC522 de la compañía

Microchip, que utiliza una comunicación SPI. Este fue remplazado por el módulo ID12LA por motivos de capacidad de memoria de programa.

También se cambió el módulo de comunicación Ethernet ENC28J60, por el USRTCP232 para agilizar el tiempo de respuesta entre el módulo de comunicación y control y el servidor. Esta modificación implicó el rediseño de la tarjeta, lo cual altera el costo de producción que representa un aumento en los precios final del producto.

El estudio económico indica que se necesita de una inversión total inicial de RD$ 889,296.33 para cubrir los gastos legales y de infraestructura que se necesitan para arrancar y también para sostener el proyecto durante los primeros 5 meses.

*Recibido: 21/04/2019*
*Reenviado: 27/04/2019*
*Aceptado: 28/04/2019*
*Sometido a evaluación de pares anónimos*