



Parcial 1

Desafío

**Jackh Emmanuel Narvaez Guerra,
Santiago Alejandro Palacio, Juan Pablo
Davila Bedoya**

Departamento de Ingeniería Electrónica y
Telecomunicaciones
Universidad de Antioquia
Medellín
Febrero de 2022

Índice

1. Introduccion	2
2. Abstrac	2
3. Marco teorico	2
4. Conexiones	3
5. En que consiste la incryptacion	4
5.1. Metodo de cifrado	4
6. como se incrypta los datos	4
7. Diseño	4
8. Visualizacion.	4
9. complicaciones	5
10.Conclusión	6

1. Introduccion

En este informe se va a presentar un analisis de un diseño de un sistema el cual genera un trama de informacion encriptada, la envia a un arduino de forma serial, éste la manda y en la recepcion esta informacion se convierte en forma paralela para poder desencriptarla. para recibir la informacion serial y mandarla como paralela se estudia el funcionamiento del integrado 74HC595 y se implementa un ejemplo con arduino para comprobar que con las entradas de control (serial) se envíe informacion de forma paralela hacia el otro arduino.

2. Abstrac

se va a realizar un sistema de incriptacion para cifrar datos entre los sistemas de computo usando 2 computadores usando el arduino junto al integrado 74HC595 y una protoboart.

3. Marco teorico

El SHIFT REGISTER ó 74HC595 posee tres puertos indispensables para su uso, el SHCP, que corresponde a el reloj del componente, el STCP, que le corresponde la tarea de capturar el valor que se ingresa por un puerto digital, y el DS, cuyo trabajo es reflejar o emitir los datos almacenados en STCP. El puerto SHCP es el responsable de captar si se recibe un cero o un uno, estando en estado high o no, es decir, si el puerto digital al cual esta conectado manda una señal, se recibirá un cero o un uno en función de si está o no en high el SHCP. Por otro lado, tenemos el puerto STCP, tendrá la función de almacenar los ceros o unos recibidos por el SHCP. Por último tenemos el puerto DS, este puerto es el encargado de mostrar la cadena almacenada de STCP de unos y ceros. Realmente las posibilidades son infinitas, en principio la solución más rápida al problema es intercambiar los ceros por unos y viceversa, este caso por ejemplo se haría así: 1. Recorrer la cadena de bits que se desea desencriptar e identificando que posiciones de esa cadena corresponde a un cero o a un uno. 2. Luego poniendo en high el puerto SHCP en caso de que halla un cero, y poniéndolo en low cada que haya un uno. 3. Enviar dicha señal poniendo el puerto DS en high, la señal iría al sitio que se desee transmitir, ya sea un servidor, una fila de leds, etc. Con estos tres simples pasos podemos desencriptar o encriptar cualquier byte con el método de cambiar unos por ceros y ceros por unos de manera muy sencilla.

- Integrado 74HC595 ¿Que es? es un registro de desplazamiento que cuenta con 1 entrada en serie y salida en paralelo de 8 bytes, es de gran ayuda cuando se requiere ampliar la cantidad de salidas digitales ya que por ejemplo se pueden conectar 8 leds con tan solo 3 pines del arduino. cuenta con 8 pines de salida de datos paralela pin a tierra, pin en serie que permite la conexion en cascada, un pin para resetear (reset), un pin de reloj para el desplazamiento de los datos, un pin para cargar los datos, un pin de

enable, un pin de entrada de datos y un pin de alimentacion.

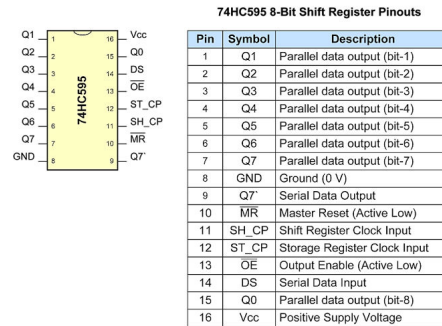


Figura 1: Integrado 74hc595

- Arduino Es una placa con todos los elementos necesarios para conectar perifericos a las entradas y salidas de un microcontrolador que puede ser programado tanto en windows, Linux en Mac Os

4. Conexiones

Para la conexión Usaremos los pines estándar de comunicación serie de Arduino:

- 0: RX (pin por el que se RECIBE los datos serie)
- 1: TX (pin por el que se ENVIA los datos serie)

Para comunicación en 2 direcciones: los 2 pueden enviar / recibir. Las conexiones TX/RX se intercambian (lo que uno envía -TX- tiene que entrar en el otro -RX-). Cualquiera de las 2 puede ser Maestro o Esclavo. **IMPORTANTE:** Conectar ambas GND de las placas. [?]



Figura 2: Arduino

5. En que consiste la incriptacion

La criptografía o el cifrado designan a un procedimiento que traduce un texto sin formato (plain text o texto plano) en una secuencia ininteligible de caracteres mediante una clave. El objetivo es que el contenido del texto secreto resultante o criptograma (texto cifrado) solo sea accesible para aquellos que disponen de la clave para descifrarlo. Aunque expresiones tales como "texto plano." "texto cifrado" provengan de la estrategia militar, los métodos criptográficos pueden ser también aplicados a otro tipo de información electrónica como mensajes de voz, archivos de imagen o códigos de programación, además de a mensajes de texto. [?]

5.1. Metodo de cifrado

- En el cifrado por transposición, las permutaciones suelen llevarse a cabo a partir de una matriz (matriz de transposición) que ha de conocerse o poderse reconstruir.
- El cifrado por sustitución se basa en una ordenación tabular de caracteres y cifras en forma de código secreto.

6. como se incripta los datos

Un método de cifrado se compone fundamentalmente de dos elementos, un algoritmo criptográfico y una o más claves secretas. Mientras que el algoritmo describe el método de encriptado (p. ej., "desplaza cada letra a lo largo de la secuencia del alfabeto"), la clave proporciona el parámetro ($C = \text{tres posiciones}$). Esto es lo que permite definir al cifrado como un procedimiento por el cual se entrega un texto en claro y una clave al algoritmo criptográfico y se obtiene un texto cifrado.

7. Diseño

Implementacion de nuestro circuito se conecto una led para ver que si llegaba el mensaje en paralelo se conectaron a los puertos seriales

8. Visualizacion.

Para el ensamble del sistema utilizamos 2 arduinos, un integrado, 8 leds y un pulsador esto con el fin de poder visualizar como se llevaría la información de un arduino maestro a un esclavo. introducimos el codigo que implementamos para poder encender los leds `int pindata=7;//Pin de entrada de datos int pinlatch=8;//Pin de segunda etapa de registros(salida) int pinclock=9;//Pin de primera entrada de registros (entrada)`

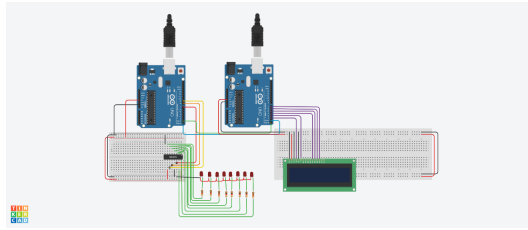


Figura 3: Diseño

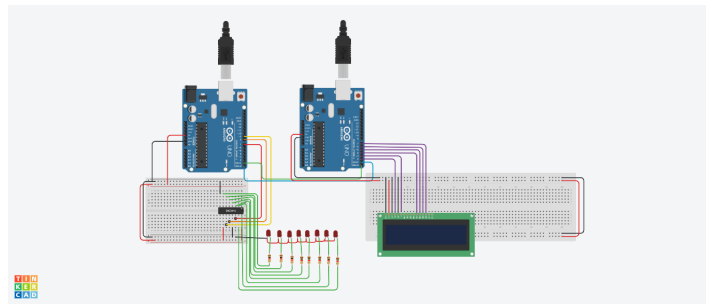


Figura 4: comunicacion serial a paralela

```
void setup() pinMode(pindata, OUTPUT); pinMode(pinlatch, OUTPUT); pin-
Mode(pinclock, OUTPUT);

digitalWrite(pindata,0); digitalWrite(pinlatch,0); digitalWrite(pinclock,0); en-
cender(); void apagar() for (int x=0;x<8;x++)//Comprobar 8 leds

digitalWrite(pindata,0);delay(100); // digitalWrite(pinclock,0); digitalWrite(pinclock,1);
digitalWrite(pinclock,0); // digitalWrite(pinlatch,0); digitalWrite(pinlatch,1); di-
gitalWrite(pinlatch,0); void encender() for (int x=0;x<8;x++)//Comprobar 8
leds

digitalWrite(pindata,1);delay(100); // digitalWrite(pinclock,0); digitalWrite(pinclock,1);
digitalWrite(pinclock,0); // digitalWrite(pinlatch,0); digitalWrite(pinlatch,1); di-
gitalWrite(pinlatch,0); void loop() apagar(); encender();
```

9. complicaciones

A medida de que fuimos desarrollando el desafio nos encontramos con el primer problema que fue la conexión del integrado solo basto estudiarlo un poco mas para poder comprender como usar sus 8 pines de salida junto con sus registros y poder conectarlo para que no quedara en corto. entender muy bien el concepto de entrada serial y salida paralelo para implementar la encriptacion. -a la hora de comunicar los dos arduinos nos falto conectar los GND(tierra) entre ellos lo cual

no permitia que la informacion fuera recibida por parte del arduino ESCLAVO

10. Conclusión

de acuerdo a las necesidades de enviar más bytes se pueden usar más integrados usando las mismas tres entradas de control para cumplir con el objetivo de este desafío tuvimos que investigar bastante sobre como funciona un integrado y como poder manipularlo junto con la idea de si era posible conectar 2 arduinos lo cual pense que no se podia y fue mas facil de lo pensando

Referencias