DESCRIPCIÓN DE LOS PINES

Gabriel Omar García Salazar
Leslie Martínez Bello
Lorette Mora Hernández
Miranda García Ugalde

Ramiro Rafael Fomperoza Guerrero (Profesor)

Pines de entrada (16 pines)

8 pines - 8 bits de entrada

El código utilizará 8 pines de entrada, donde cada pin recibirá un bit de la representación binaria de un carácter de la contraseña. En otras palabras, significa que cada carácter será convertido a su forma binaria de 8 bits y procesado en paralelo y cada carácter será asignado a un pin diferente.

Ejemplo:

Pin	Carácter	Código Binario
Pin 1	5	00000101
Pin 2	2	00000010
Pin 3	4	00000100
Pin 4	8	00001000
Pin 5	1	00000001
Pin 6	6	00000110
Pin 7	9	00001001
Pin 8	5	00000101

Fig 1. Funcionamiento de los 8 pines de entrada iniciales por carácter, convirtiendo el número decimal a binario.

En el ejemplo presentado anteriormente se demuestra como los caracteres introducidos, los números naturales, serán traducidos a código binario y en este formato serán asignados al pin necesario.

8 pines del valor a desplazar

DESCRIPCIÓN DE LOS PINES

La operación del cifrado se realizaría mediante el uso de 8 pines de entrada, a través de los cuales se ingresarán en paralelo el texto original y la clave, teniendo la capacidad de manejar un carácter a la vez. Estos serán procesados en cada pin para realizar la suma binaria, a través de la compuerta lógica XOR (operación aritmética de suma).

Pin 1	Procesa bit 0 de texto original y bit 0 de clave
Pin 2	Procesa bit 1 de texto original y bit 1 de clave
Pin 3	Procesa bit 2 de texto original y bit 2 de clave
Pin 4	Procesa bit 3 de texto original y bit 3 de clave
Pin 5	Procesa bit 4 de texto original y bit 4 de clave
Pin 6	Procesa bit 5 de texto original y bit 5 de clave
Pin 7	Procesa bit 6 de texto original y bit 6 de clave
Pin 8	Procesa bit 7 de texto original y bit 7 de clave

Fig 2. Asignación del procesamiento paralelo (texto original y clave) para cada uno de los carácteres que serán cifrados en Código César.

Ejemplo: Los pines de entrada de desplazamiento realizarán la siguiente función si el código 122 (*01111010 en código binario)* se quiere desplazar 4 lugares (*00000100, Cesar Cipher para 4 en código binario)*.

A (texto original) = 01111010
B (clave) = 00000100

Pines	A XOR B
Pin 1	0 XOR 0
Pin 2	1 XOR 0
Pin 3	1 XOR 0
Pin 4	1 XOR 0
Pin 5	1 XOR 0
Pin 6	0 XOR 1

A	RB	B	RB
A0	0	B0	0
A1	1	B1	0
A2	1	B2	0
A3	1	B3	0
A4	1	B4	0
A5	0	B5	1
A6	1	B6	0
A7	0	B7	0

Pin 7	1 XOR 0
Pin 8	0 XOR 0

Fig 3. Procesamiento de caracteres (A, texto original y B, clave) mediante su definición en representación binaria (RB) y su entrada por pin al pasar por la operación XOR.

Pines de salida (9 pines)

El sistema diseñado cuenta con 2 partes principales en su funcionamiento, uno el cual consta de un sumador de 8 bits, y el otro un módulo de cifrado basado en un algoritmo tipo Cesar, ambos son dependientes el uno del otro, es decir que comparten la misma cantidad de pines de salida. A continuación se explica en detalle el funcionamiento de los pines de **salida.**

- **Suma (8 pines):** El sumador de 8 bits, consta en un sistema el cual representa el resultado de la suma en binario de cada bit individual, es decir, cada bit de un dígito representado en el sistema binario, se le agrega el bit correspondiente al desplazamiento establecido.

  Ejemplo:
  Número de entrada: *122 (01111010 en representación binaria)*
  Desplazamiento: *4 (0000100 en representación binaria)*
  Suma: 01111010 + 0000100 = 01111110 (126 en representación decimal)

En total existen 8 pines de salida que tienen que ser representados a la hora de realizar esta operación:

Suma [7]	0 + 0 = **0**
Suma [6]	1 + 0 = **1**

Suma [5]	1 + 0 = **1**
Suma [4]	1 + 0 = **1**
Suma [3]	1 + 0 = **1**
Suma [2]	0 + 1 = **1**
Suma [1]	1 + 0 = **1**
Suma [0]	0 + 0 = 0

Fig 4. Salida para la operación de suma, resultados al pasar por la compuerta XOR.

**Evidentemente, la suma se basa directamente en una suma de tipo binario, en caso de ser necesario en la misma suma, podrá producirse un acarreo al valor del siguiente nivel binario, el ejemplo previamente abordado coincide involuntariamente con una suma de tipo aritmética.*

- **Acarreo de salida (1 pin):** El acarreo de salida consta de un pin único, el cual se activa al producirse un desbordamiento en caso de exceder *26* como valor al cifrar, esto directamente relacionado a la cantidad de letras en el abecedario español, con el fin de preservar una traducción dentro el mismo, al excederse *26* como valor, el pin reinicia el conteo la cantidad de ciclos necesario para cumplir el desplazamiento.

  Ejemplo:
  Número de entrada: *122 (01111010 en representación binaria)*
  Desplazamiento: *4 (0000100 en representación binaria)*
  Suma: *01111010 + 0000100 = 01111110 (126 en representación decimal)*
  Acarreo: 126/26 ≈ 4.8
  El acarreo nos indica que el ciclo se repetirá 4.8 veces con el fin de entregar un valor dentro de los parámetros de 0 a 26.