Nombre: Ortega Silva Jorge Eduardo

Como ejecutar los programas

El archivo con el código fuente se llama S-DES.c, solo es necesario la ejecución de este para generar las dos subclaves de salida de la clave de entrada.

Funciones realizadas

```
void SDES(unsigned char *llave, unsigned char *subllave1, unsigned char *subllave2){
    unsigned char auxKey[10];
    unsigned char bloqueKey[10];
    int i=0;
    int p10[10]={3,5,2,7,4,10,1,9,8,6};
    int p8[8]={6,3,7,4,8,5,10,9};
    ////////Subllave 1//////
    /////////P10////////////
    for(i=0; i<10; i++){
        auxKey[i]=llave[p10[i]-1];
    }
    /////Corrimiento//////
    corrimiento(auxKey, bloqueKey);
    /////////P8////////////
    for(i=0; i<8; i++){
        auxKey[i]=bloqueKey[p8[i]-1];
    }
    //asignacion primera subllave
    for(i=0; i<8; i++){
        subllave1[i]=auxKey[i];
    }
    ////////Subllave 2//////
    /////Corrimientos//////
    corrimiento(bloqueKey, auxKey);
    corrimiento(auxKey, bloqueKey);
    /////////P8////////////
    for(i=0; i<8; i++){
        auxKey[i]=bloqueKey[p8[i]-1];
    }
    //asignacion segunda subllave
    for(i=0; i<8; i++){
        subllave2[i]=auxKey[i];
    }
}
```

Se definen el orden de las permutaciones en P10 y P8 en un arreglo de enteros, para después recorrer el toda la cadena de la llave y reacomodarla con el orden que se proporciona en P10, seguido se llama a la función corrimiento, donde se pasa como parámetro la cadena de 10 bits a la que se le aplicará corrimiento y otra cadena del mismo tamaño en donde se guardará el corrimiento, este función simula lo que hace el método, dividir la cadena en dos y hacer un corrimiento a la izquierda a cada una y volverlas a unir; cumplido lo anterior, al resultado se le hará la permutación en el orden de P8, para después asignar la primera subclave a la cadena pasada como parámetro.

Para la segunda llave se hace algo similar, con la llave resultante del primer corrimiento, solo que para este caso se llevan a cabo dos corrimientos más, para después aplicar P8 y por último asignar la subclave a la cadena pasada como parámetro.

Capturas de pantalla de pruebas