Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Arquitectura de Computadores y Ensambladores 1
Sección A

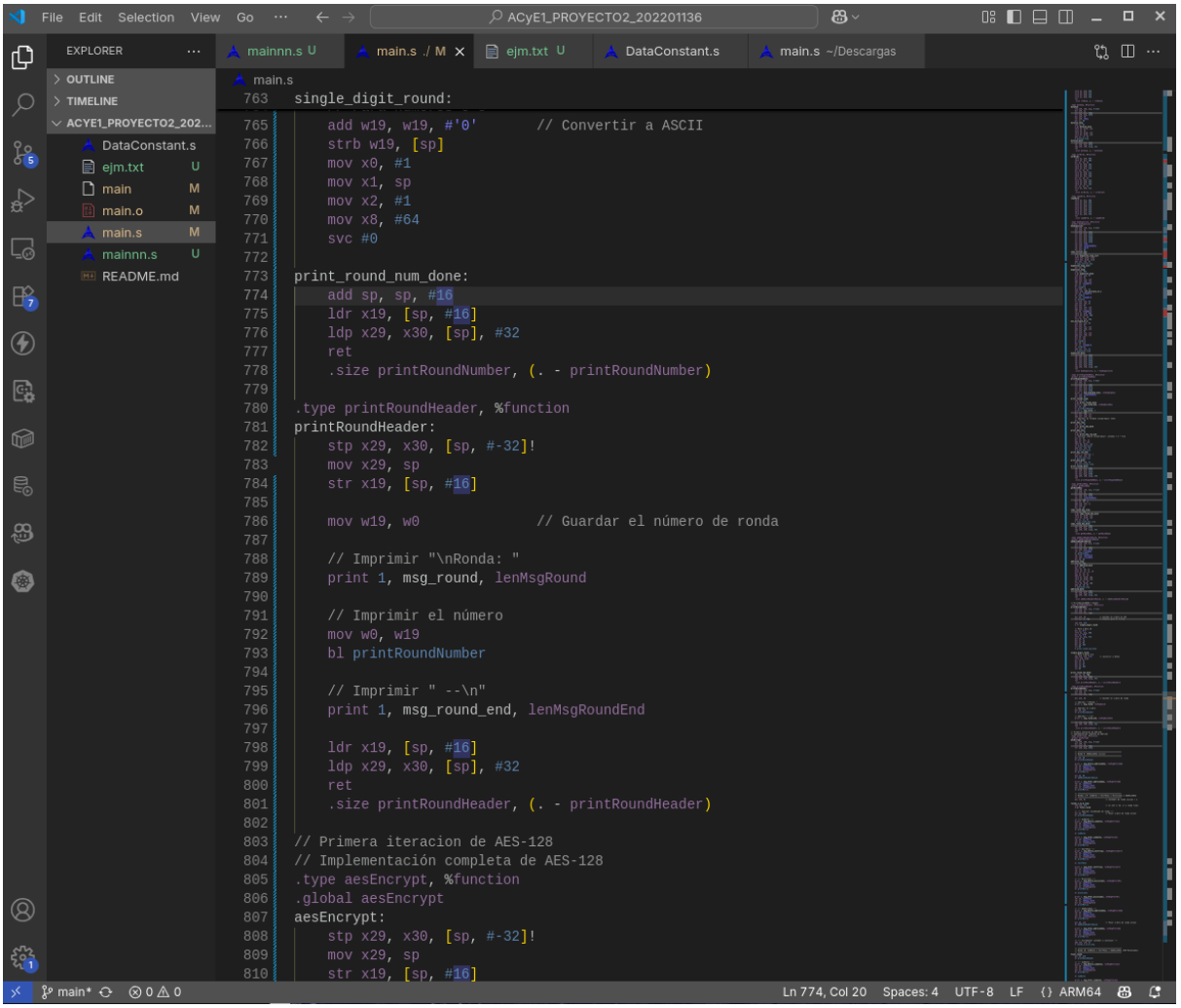
PROYECTO 2

MANUAL DE USUSARIO

Andrea Alejandra Pérez Sandoval – 202201136

MANUAL DE USUARIO

1. Abrir Visual Studio COde.



2. Colocar los siguiente código:

```
alejandra@alejandra-300E4C-300E5C-300E7C:~/ARQUI/ACyE1_PROYECTO2_202201136$ aarch64-linux-gnu-as -o main.o main.s
main.s: Mensajes del ensamblador:
main.s: Aviso: final de fichero no está al final de una línea: se insertó línea nueva
alejandra@alejandra-300E4C-300E5C-300E7C:~/ARQUI/ACyE1_PROYECTO2_202201136$ aarch64-linux-gnu-ld -o main main.o
alejandra@alejandra-300E4C-300E5C-300E7C:~/ARQUI/ACyE1_PROYECTO2_202201136$ qemu-aarch64 ./main
```

3. Colocar el texto a cifrar y la clave:

```
Ingrese el texto a cifrar (maximo 16 caracteres): Two One Nine Two
Matriz de Estado:
Matriz de Estado:
54 4F 4E 20
77 6E 69 54
6F 65 6E 77
20 20 65 6F

Ingrese la clave (32 caracteres hex): 5468617473206D79204B756E67204675
Matriz de Clave:
Matriz de Clave:
54 68 61 74
73 20 6D 79
20 4B 75 6E
67 20 46 75
```

4. AL darle enter se crearán y subirán todas las matrices y el mensaje encriptado.

```
SSubclaves Expandidas:

Subclave Ronda 0:
54 73 20 67
68 20 4B 20
61 6D 75 46
74 79 6E 75

Subclave Ronda 1:
E2 91 B1 D6
32 12 59 79
FC 91 E4 A2
F1 88 E6 93

Subclave Ronda 2:
56 C7 76 A0
08 1A 43 3A
20 B1 55 F7
07 8F 69 FA

Subclave Ronda 3:
D2 15 63 C3
60 7A 39 03
0D BC E9 1E
E7 68 01 FB

Subclave Ronda 4:
A1 B4 D7 14
12 68 51 52
02 BE 57 49
C9 A1 A0 5B

Subclave Ronda 5:
B1 05 D2 C6
29 41 10 42
3B 85 D2 9B
33 92 32 69

Subclave Ronda 6:
BD B8 6A AC
3D 7C 6C 2E
C2 47 95 0E
87 15 27 4E
```

```
Subclave Ronda 7:
CC 74 1E B2
96 EA 86 A8
ED AA 3F 31
16 03 24 6A

Subclave Ronda 8:
8E FA E4 56
51 BB 3D 95
EF 45 7A 4B
21 22 06 6C

Subclave Ronda 9:
BF 45 A1 F7
E2 59 64 F1
BF FA 80 CB
90 B2 B4 D8

Subclave Ronda 10:
28 6D CC 3B
FD A4 C0 31
DE 24 A4 6F
F8 4A FE 26

Ronda: 0 --
Estado antes de AddRoundKey:
Matriz de Estado:
54 4F 4E 20
77 6E 69 54
6F 65 6E 77
20 20 65 6F

Estado después de AddRoundKey:
Matriz de Estado:
00 3C 6E 47
1F 4E 22 74
0E 08 1B 31
54 59 0B 1A


Ronda: 1 --
Estado antes de SubBytes:
Matriz de Estado:
```

```
Estado después de SubBytes:
Matriz de Estado:
01 3A 8C 21
33 3E B0 E2
3D B8 8E 04
BC 4D 1C A7

Estado antes de ShiftRows:
Matriz de Estado:
01 3A 8C 21
33 3E B0 E2
3D B8 8E 04
BC 4D 1C A7

Estado después de ShiftRows:
Matriz de Estado:
01 3A 8C 21
3E B0 E2 33
8E 04 3D B8
A7 BC 4D 1C

Estado antes de AddRoundKey:
Matriz de Estado:
01 3A 8C 21
3E B0 E2 33
8E 04 3D B8
A7 BC 4D 1C

Estado después de AddRoundKey:
Matriz de Estado:
29 57 40 1A
C3 14 22 02
50 20 99 D7
5F F6 B3 3A

Texto Cifrado: Matriz de Estado:
29 57 40 1A
C3 14 22 02
50 20 99 D7
5F F6 B3 3A


Texto Cifrado: 29C3505F571420F6402299B31A02D73A
```