



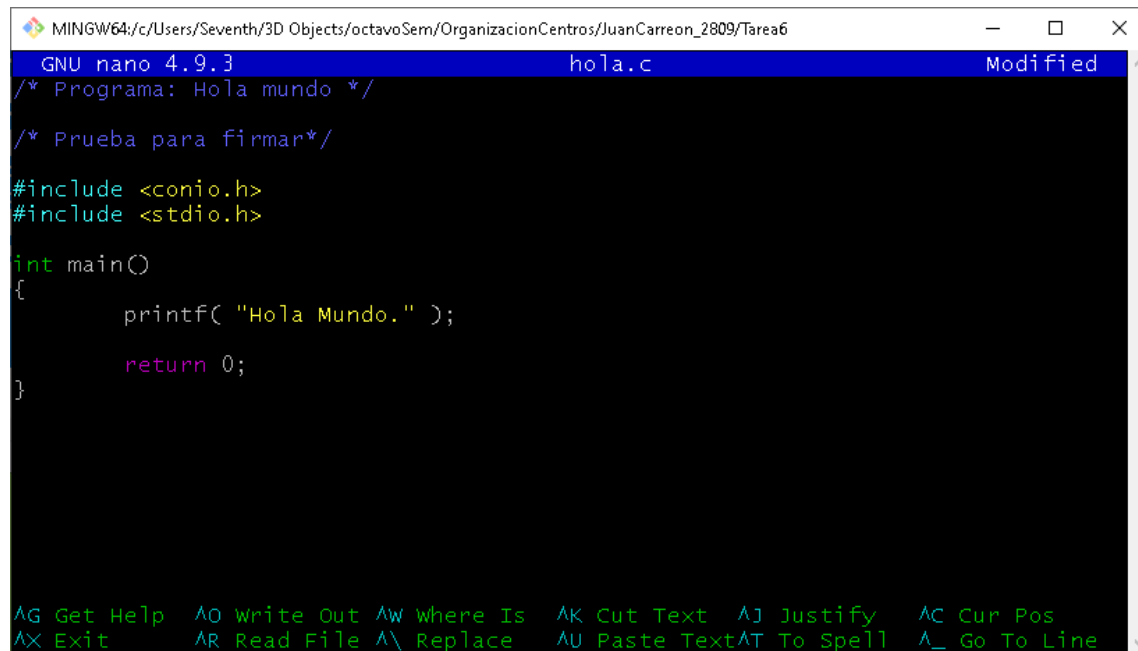
UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO **FES ARAGÓN**

TAREA6.- Firma Digital

VELASCO AGUSTION AARON
ORG. Y ADM. DE CENTRO DE COMP.
CARREÓN CHÁVEZ JUAN MANUEL

Tarea 6.- Realizar el ejercicio de Firma Digital encontrado en las diapositivas

1.-Creamos el archivo hola.c



```
MINGW64:/c:/Users/Seventh/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6
GNU nano 4.9.3 hola.c Modified
/* Programa: Hola mundo */

/* Prueba para firmar*/

#include <conio.h>
#include <stdio.h>

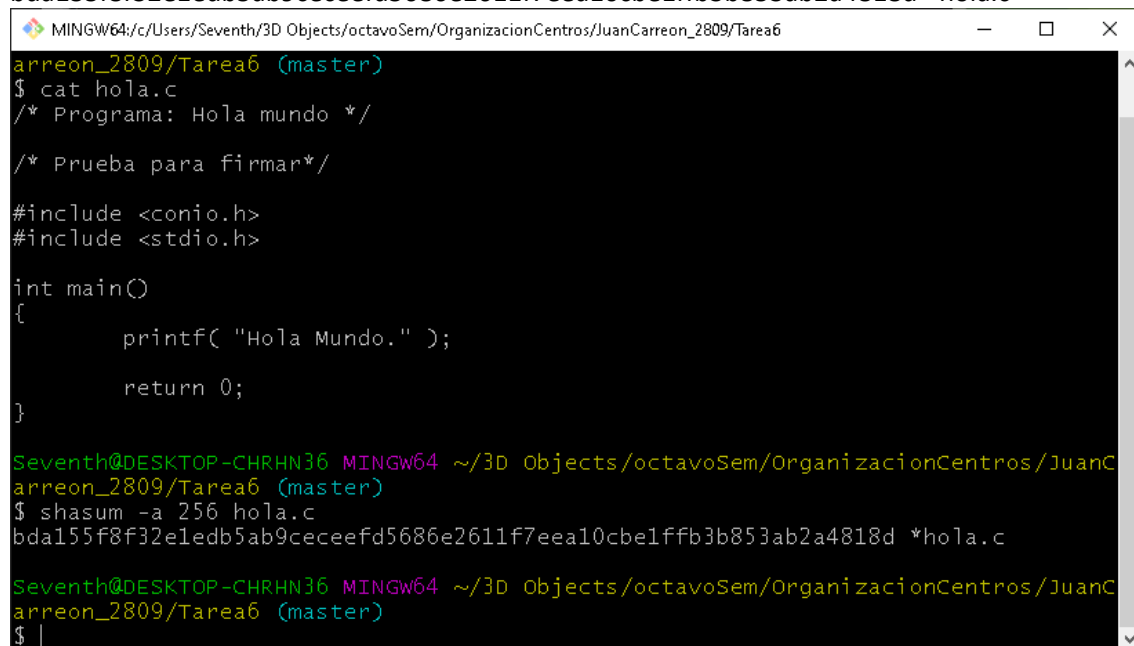
int main()
{
    printf( "Hola Mundo." );

    return 0;
}

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text^T To Spell ^_ Go To Line
```

2.-Creamos la firma del archivo original obteniendo la siguiente firma.

bda155f8f32e1edb5ab9ceceefd5686e2611f7eea10cbe1ffb3b853ab2a4818d *hola.c



```
MINGW64:/c:/Users/Seventh/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6
arreon_2809/Tarea6 (master)
$ cat hola.c
/* Programa: Hola mundo */

/* Prueba para firmar*/

#include <conio.h>
#include <stdio.h>

int main()
{
    printf( "Hola Mundo." );

    return 0;
}

Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ shasum -a 256 hola.c
bda155f8f32e1edb5ab9ceceefd5686e2611f7eea10cbe1ffb3b853ab2a4818d *hola.c

Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ |
```

3.-Guardamos la firma original en un archivo

```
MINGW64/c/Users/Seventh/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6
bda155f8f32e1edb5ab9ceceefd5686e2611f7eea10cbe1ffb3b853ab2a4818d *hola.c
Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ AC
Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ shasum -a 256 hola.c > firmaOriginal.txt
Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ cat firma original
cat: firma: No such file or directory
cat: original: No such file or directory
Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ cat firmaOriginal.txt
bda155f8f32e1edb5ab9ceceefd5686e2611f7eea10cbe1ffb3b853ab2a4818d *hola.c
Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$
```

4.-Modificamos el programa y guardamos la firma del archivo modificado

```
MINGW64/c/Users/Seventh/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6
cat: firma: No such file or directory
cat: original: No such file or directory
Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ cat firmaOriginal.txt
bda155f8f32e1edb5ab9ceceefd5686e2611f7eea10cbe1ffb3b853ab2a4818d *hola.c
Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ nano hola.c
Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ shasum -a 256 hola.c > firmaCambiada.txt
Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ cat firmaCambiada.txt
437842f7edd08dadf9b6036830408714decfbda75cd20a982d62e7f3833934bd *hola.c
Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$
```

5.-Con el archivo cambiado revisamos las firmas para comprobar que el archivo esta cambiado aun y la firma responde a la firma cambiada

```
MINGW64:/c/Users/Seventh/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6
$ shasum -c hola.c
shasum: hola.c: no properly formatted SHA checksum lines found

Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ shasum -c firmaOriginal.txt
hola.c: FAILED
shasum: WARNING: 1 computed checksum did NOT match

Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ shasum -c firmaCambiada.txt
hola.c: OK

Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ shasum -c firmaCambiada.txt firmaOriginal.txt
hola.c: OK
hola.c: FAILED
shasum: WARNING: 1 computed checksum did NOT match

Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$
```

6.-Regresamos el archivo a su estado original

```
MINGW64:/c/Users/Seventh/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6
GNU nano 4.9.3 hola.c Modified
/* Programa: Hola mundo */

/* Prueba para firmar*/

#include <conio.h>
#include <stdio.h>

int main()
{
    printf( "Hola Mundo." );
    return 0;
}

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

7.-Y por último verificamos la firma y vemos que de nuevo coincide con la firma original

```
MINGW64:/c:/Users/Seventh/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6
$ shasum -c firmaCambiada.txt firmaOriginal.txt
hola.c: OK
hola.c: FAILED
shasum: WARNING: 1 computed checksum did NOT match

Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ nano hola.c

Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ shasum -c firmaCambiada.txt firmaOriginal.txt
hola.c: FAILED
shasum: WARNING: 1 computed checksum did NOT match
hola.c: OK

Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ shasum -c firmaOriginal.txt
hola.c: OK

Seventh@DESKTOP-CHRH36 MINGW64 ~/3D Objects/octavoSem/OrganizacionCentros/JuanCarreon_2809/Tarea6 (master)
$ |
```