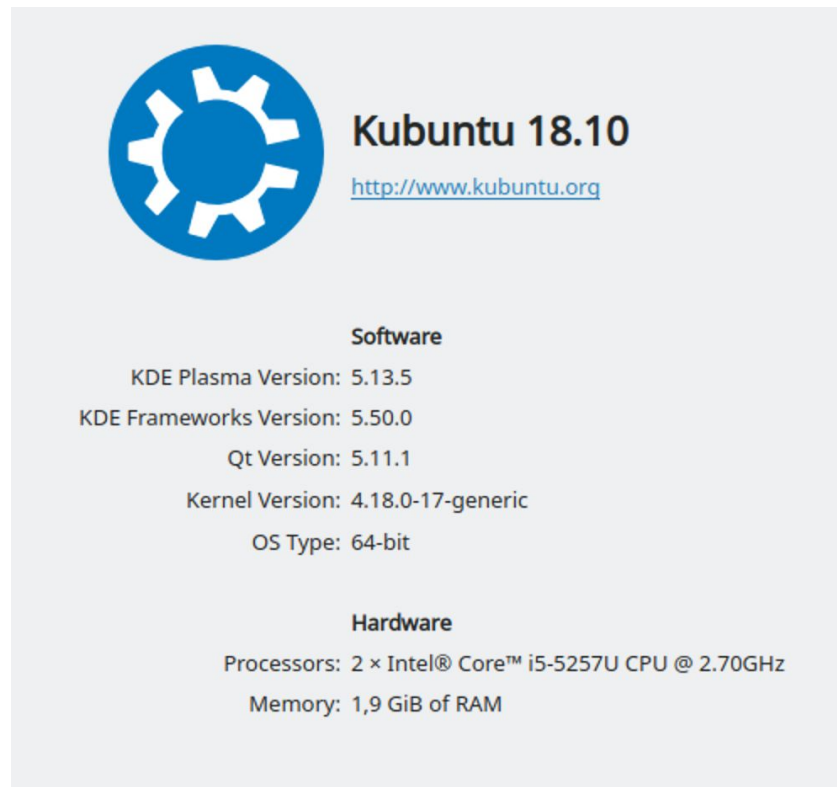


To run this project, you will need Linux 64 bit OS, it was created and tested with Kubuntu 18.10 with the following hardware:



This project was made possible with the SASM IDE using x86_64 architecture. SASM IDE requires the following dependencies been installed priorly:

1. NASM assembler
2. gcc-multilib

Above dependencies can be easily installed with apt-get. Follow the given bellow steps:

1. `sudo apt-get update`
2. `sudo apt-get -f install`
3. `sudo apt-get install nasm`
4. `sudo apt-get install gcc-multilib`

Then download the .deb distribution with the following command:

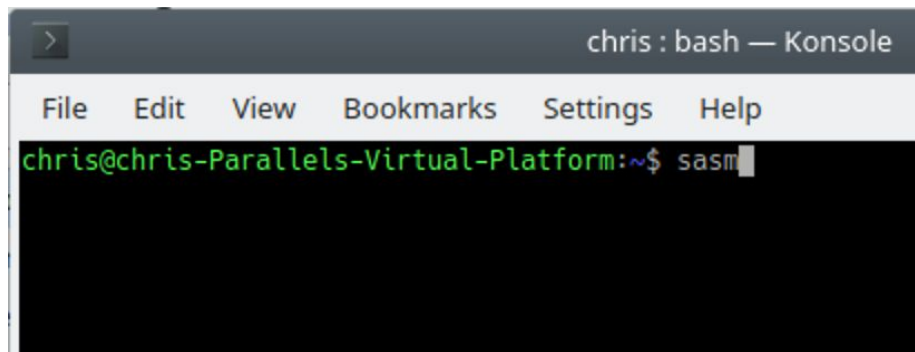
```
wget http://download.opensuse.org/repositories/home:/Dman95/xUbuntu_18.04/amd64/sasm_3.10.1_amd64.deb
```

then install the debian package with dpkg using the following command:

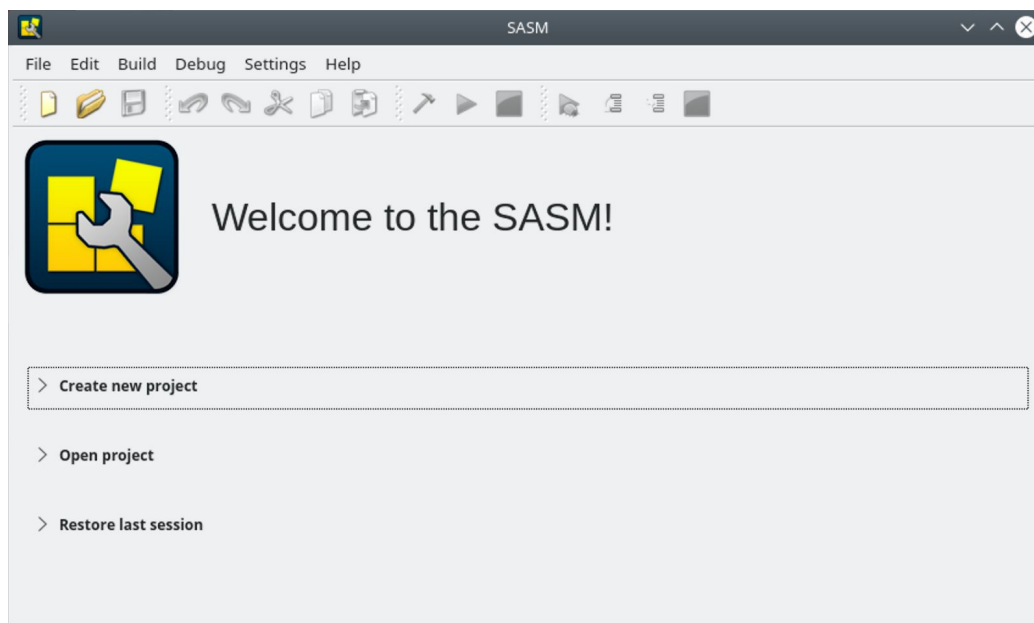
```
sudo dpkg -i asm_3.10.1_amd64.deb
```

Once the installation is completed, run the following command to start the IDE:

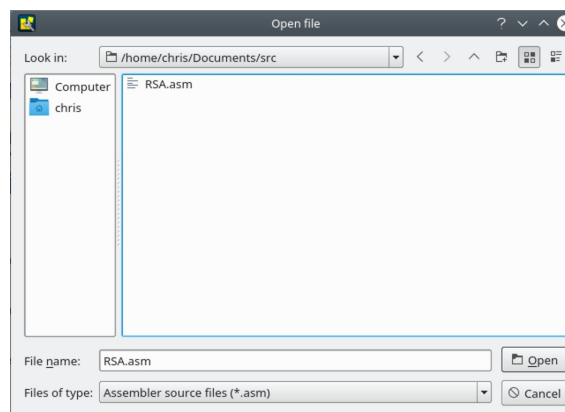
sasm



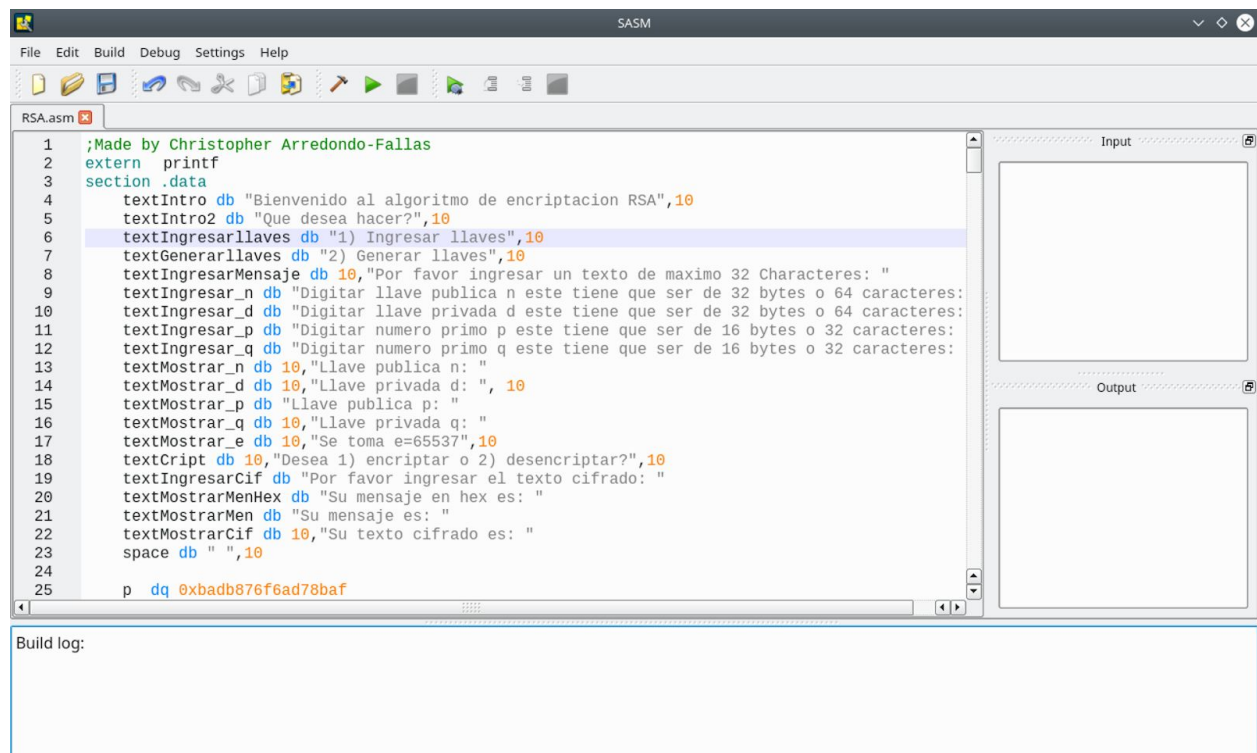
The following window should appear:



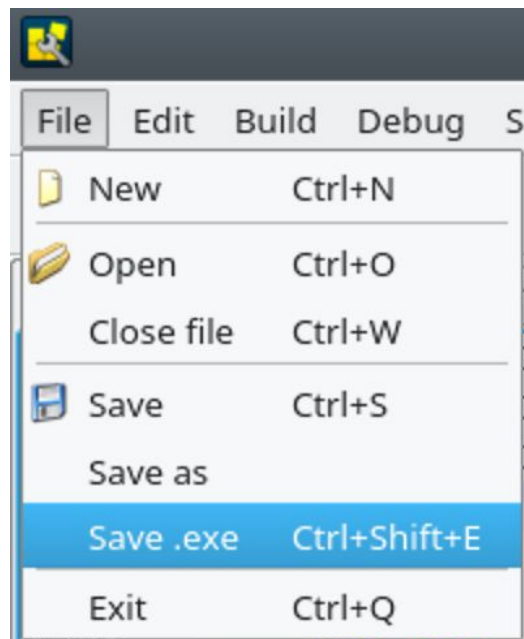
After that look for the project file name RSA.asm in the folder src and open it with the open project button.



You should see the following screen:



If you want to save as a executable, go to file > save as .exe, and pick the src folder



To run the program, put the src file in your desktop and run:

```
chris : bash — Konsole
marks Settings Help
chris@chris-Parallels-Virtual-Platform:~$ cd Desktop/src
```

After that, run:

```
src : bash — Konsole
marks Settings Help
chris@chris-Parallels-Virtual-Platform:~$ cd Desktop/src
chris@chris-Parallels-Virtual-Platform:~/Desktop/src$ ./RSA
```

After that you will see the following menu:

```
> src : RSA — Konsole
File Edit View Bookmarks Settings Help
chris@chris-Parallels-Virtual-Platform:~$ cd Desktop/src
chris@chris-Parallels-Virtual-Platform:~/Desktop/src$ ./RSA
Bienvenido al algoritmo de encriptacion RSA
Que desea hacer?
1) Ingresar llaves
2) Generar llaves

```

You see two options:

- Insert keys (n,d)
- Generate keys from prime numbers (p,q)

If you decide to Insert Keys, you will see the next screen:

```
src : RSA — Konsole
File Edit View Bookmarks Settings Help
chris@chris-Parallels-Virtual-Platform:~$ cd Desktop/src
chris@chris-Parallels-Virtual-Platform:~/Desktop/src$ ./RSA
Bienvenido al algoritmo de encriptacion RSA
Que desea hacer?
1) Ingresar llaves
2) Generar llaves
1

Se toma e=65537
Digitar llave publica n este tiene que ser de 32 bytes o 64 caracteres: █
```

After that, all you have to do is insert the key of your election, you can obtain keys from the following page:

https://www.mobilefish.com/services/rsa_key_generation/rsa_key_generation.php

In this case I used:

- n = bd431ca095becf48de7dfdf3cd2c7ec65fc8e0d30d668f79388cdaa94725bdd1
- d = 8b285c552aa5788dd0a1fce694f661633e4d7770fc2906612d0661ec92323f51

```
src : RSA — Konsole
File Edit View Bookmarks Settings Help
chris@chris-Parallels-Virtual-Platform:~$ cd Desktop/src
chris@chris-Parallels-Virtual-Platform:~/Desktop/src$ ./RSA
Bienvenido al algoritmo de encriptacion RSA
Que desea hacer?
1) Ingresar llaves
2) Generar llaves
1

Se toma e=65537
Digitar llave publica n este tiene que ser de 32 bytes o 64 caracteres: bd431ca095b
bdd1
Digitar llave privada d este tiene que ser de 32 bytes o 64 caracteres: 8b285c552aa

Llave publica n: bd431ca095becf48de7dfdf3cd2c7ec65fc8e0d30d668f79388cdaa94725bdd1
Llave privada d: 8b285c552aa5788dd0a1fce694f661633e4d7770fc2906612d0661ec92323f51
Desea 1) encriptar o 2) desencriptar?
█
```

After that you have two options

- Encrypt
- Decrypt

If you pick Encrypt:

```
src : RS
File Edit View Bookmarks Settings Help
chris@chris-Parallels-Virtual-Platform:~$ cd Desktop/src
chris@chris-Parallels-Virtual-Platform:~/Desktop/src$ ./RSA
Bienvenido al algoritmo de encriptacion RSA
Que desea hacer?
1) Ingresar llaves
2) Generar llaves
1
Se toma e=65537
Digital llave publica n este tiene que ser de 32 bytes o 64 caracteres:
bdd1
Digital llave privada d este tiene que ser de 32 bytes o 64 caracteres:
Llave publica n: bd431ca095becf48de7dfdf3cd2c7ec65fc8e0d30d668f79388d
Llave privada d: 8b285c552aa5788dd0a1fce694f661633e4d7770fc2906612d06
Desea 1) encriptar o 2) desencriptar?
1
Por favor ingresar un texto de maximo 32 Caracteres: Tecnologico
```

You have the option of entering a word of maximum 32 letters or 256 bits
After that you will receive your ciphered text:

```
src : bash — Konsole
File Edit View Bookmarks Settings Help
Bienvenido al algoritmo de encriptacion RSA
Que desea hacer?
1) Ingresar llaves
2) Generar llaves
1
Se toma e=65537
Digital llave publica n este tiene que ser de 32 bytes o 64 caracteres: bd431ca095becf48de7dfdf3cd2c7ec65fc8e0d30d668f79388d
bdd1
Digital llave privada d este tiene que ser de 32 bytes o 64 caracteres: 8b285c552aa5788dd0a1fce694f661633e4d7770fc2906612d0661ec92323f51
Llave publica n: bd431ca095becf48de7dfdf3cd2c7ec65fc8e0d30d668f79388cd
Llave privada d: 8b285c552aa5788dd0a1fce694f661633e4d7770fc2906612d0661ec92323f51
Desea 1) encriptar o 2) desencriptar?
1
Por favor ingresar un texto de maximo 32 Caracteres: Tecnologico
Su mensaje en hex es: 000000000a6f6369676f6c6f6e636554
Su texto cifrado es: 16d2fb92393b69ceb04bd575b55b71ec4792a709a32daae9574e767aba7725a
chris@chris-Parallels-Virtual-Platform:~/Desktop/src$
```

You will get your ciphered text.
If you pick decrypt:


```
src : RSA — Konsole
File Edit View Bookmarks Settings Help

Por favor ingresar un texto de maximo 32 Caracteres: Tecnologico
Su mensaje en hex es: 00000000a6f6369676f6c6f6e636554
Su texto cifrado es: 16d2fb92393b69ceb04bd575b55b71ec4792a709a32daae9574e767aba7725a
chris@chris-Parallels-Virtual-Platform:~/Desktop/src$ ./RSA
Bienvenido al algoritmo de encriptacion RSA
Que desea hacer?
1) Ingresar llaves
2) Generar llaves
1
Se toma e=65537
Digitar llave publica n este tiene que ser de 32 bytes o 64 caracteres: bd431ca095becf48de7dfdf3cd2c7ec6
Digitar llave privada d este tiene que ser de 32 bytes o 64 caracteres: 8b285c552aa5788dd0a1fce694f66163
Llave publica n: bd431ca095becf48de7dfdf3cd2c7ec65fc8e0d30d668f79388cdaa94725bdd1
Llave privada d: 8b285c552aa5788dd0a1fce694f661633e4d7770fc2906612d0661ec92323f51
Desea 1) encriptar o 2) desencriptar?
2
Por favor ingresar el texto cifrado: 16d2fb92393b69ceb04bd575b55b71ec4792a709a32daae9574e767aba7725a
```

You can enter the ciphered text obtained in the previous iteration.

```
src : bash — Konsole
File Edit View Bookmarks Settings Help

Que desea hacer?
1) Ingresar llaves
2) Generar llaves
1
Se toma e=65537
Digitar llave publica n este tiene que ser de 32 bytes o 64 caracteres: bd431ca095becf4
Digitar llave privada d este tiene que ser de 32 bytes o 64 caracteres: 8b285c552aa5788
Llave publica n: bd431ca095becf48de7dfdf3cd2c7ec65fc8e0d30d668f79388cdaa94725bdd1
Llave privada d: 8b285c552aa5788dd0a1fce694f661633e4d7770fc2906612d0661ec92323f51
Desea 1) encriptar o 2) desencriptar?
2
Por favor ingresar el texto cifrado: 16d2fb92393b69ceb04bd575b55b71ec4792a709a32daae95
Su texto cifrado es: 16d2fb92393b69ceb04bd575b55b71ec4792a709a32daae9574e767aba7725a
Su mensaje es: Tecnologico
chris@chris-Parallels-Virtual-Platform:~/Desktop/src$
```

Finally you will obtained the decrypted text.

If you pick Generate keys you will be asked to enter prime numbers(p,q) and then you will get the same menu as explained before.

```
chris@chris-Parallels-Virtual-Platform:~/Desktop/src$ ./RSA
Bienvenido al algoritmo de encriptacion RSA
Que desea hacer?
1) Ingresar llaves
2) Generar llaves
2

Se toma e=65537
Digitar numero primo p este tiene que ser de 16 bytes o 32 caracteres: fa5085d90131fd4b0adfe6b2ca2d8f6d
Digitar numero primo q este tiene que ser de 16 bytes o 32 caracteres: c18f981e1324c357aaff6a7e4a045575
Llave publica p: fa5085d90131fd4b0adfe6b2ca2d8f6d
Llave privada q: c18f981e1324c357aaff6a7e4a045575
Llave publica n: bd431ca095becf48de7dfdf3cd2c7ec65fc8e0d30d668f79388cdaa94725bdd1
Llave privada d: 8b285c552aa5788dd0a1fce694f661633e4d7770fc2906612d0661ec92323f51
Desea 1) encriptar o 2) desencriptar?
```