Kingdom of Saudi Arabia
Ministry of Education
Taibah University
Faculty of Computer Science and Engineering
Department of Computer Science

المملكة العربية السعودية
وزارة التعليم
جامعة طيبة
كلية علوم وهندسة الحاسب
قسم علوم الحاسب

Class project

Group member:

Asma Abdulsamad Abdulaziz 3950013
Randa Mohammed Al Hashmi 3550402
Sereen Abdullah Hakami 3656414

Section: C9A

A project submitted for Computer Security course – CS 433

Instructor: Dr. Maher Wasl Alharby

Spring 2022

Submitted on May 14, 2022

- **Steps to open the project**

1- Unzip the folder.

2- Open the NetBeans program, then go to:

File -> Open Project -> select path of unzip (filetest) Project

3- Now the project is ready for implementation.

- **Project run steps**

A menu appears to choose whether the user wants encryption (assymmetric encryption (RSA) or hashing

If the user presses:

1- Selects encryption, a new menu appears:

1.1 - encryption option

1.2 - Decryption option

In each menu appears 1 to encrypt/decrypt a .txt text file, such as all.txt 2 to encrypt/decrypt an entire folder, such as test_RSA

After choosing the option that the user wants, he enters the file name .txt / folder name

Note: The file/folder must be within the project file

Two keys will be generated, a public key and a private key

The public key is used in encryption as public1.pub

The private key is used to decrypt as private1.key

We will enter the name of the public key file when encrypting, and private when decrypting

When encrypting the file name.txt

When decrypted the input: file name.encrypted, the output file name.decrypted

****

If user select hashing:

The program asks to enter the file name, for example, test_hash.txt, then the user chooses the algorithm SHA-256, SHA-512, and the output is test_hash.msgdigest.

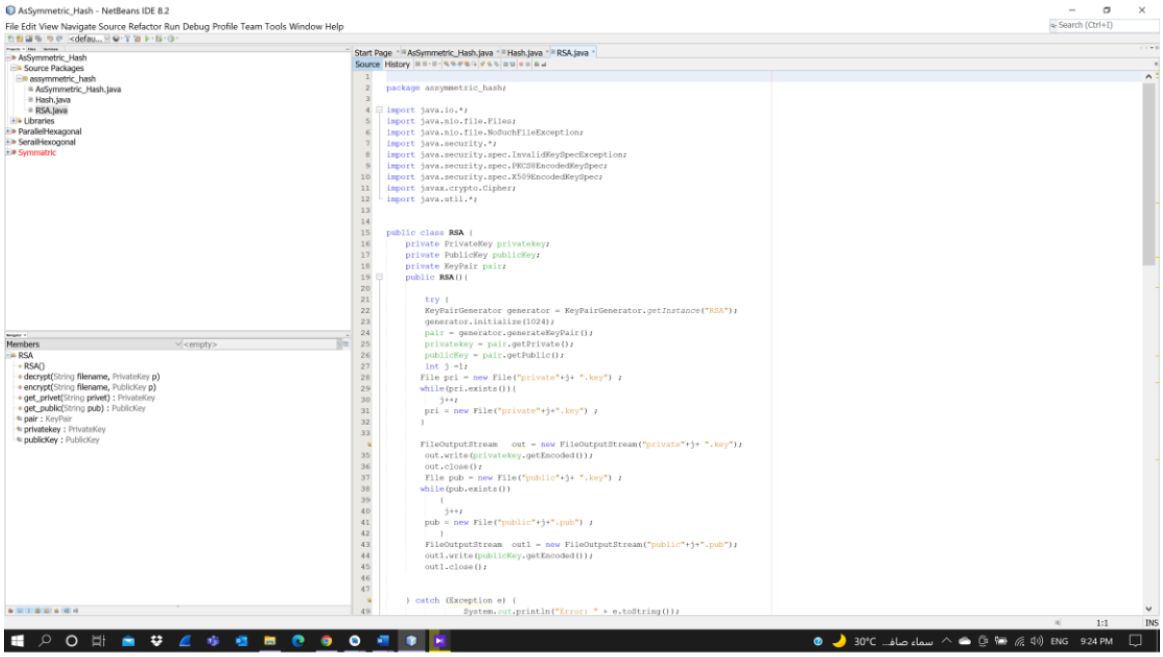
Notes:

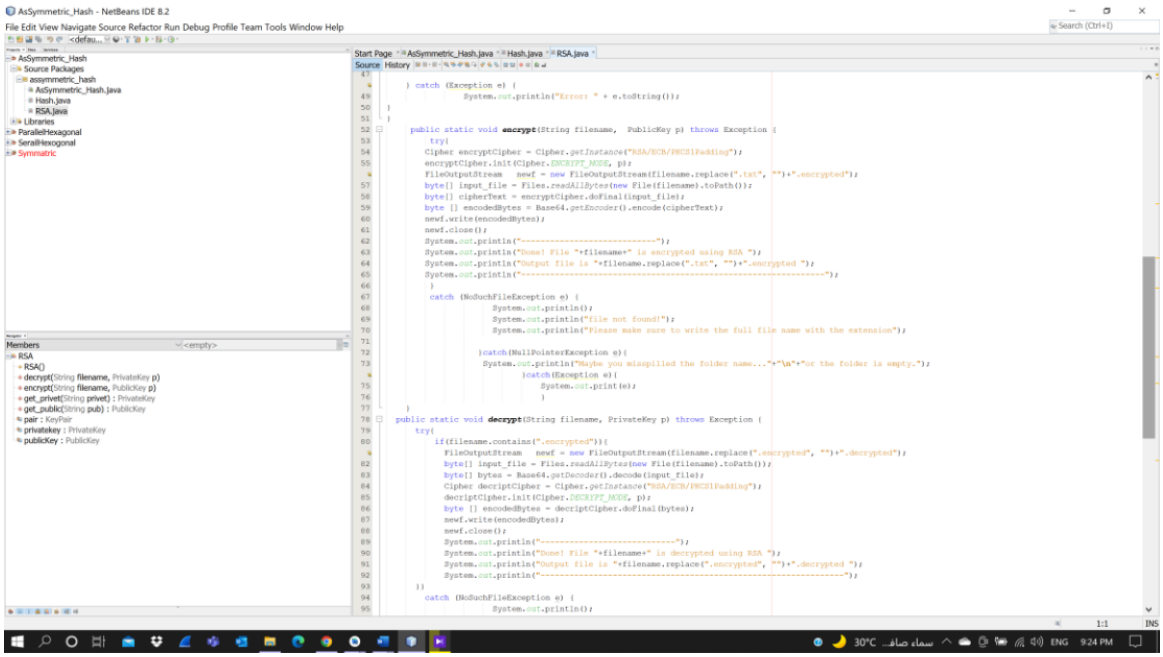
- The two algorithms work in the same principle, but the difference between them is the number of bytes.

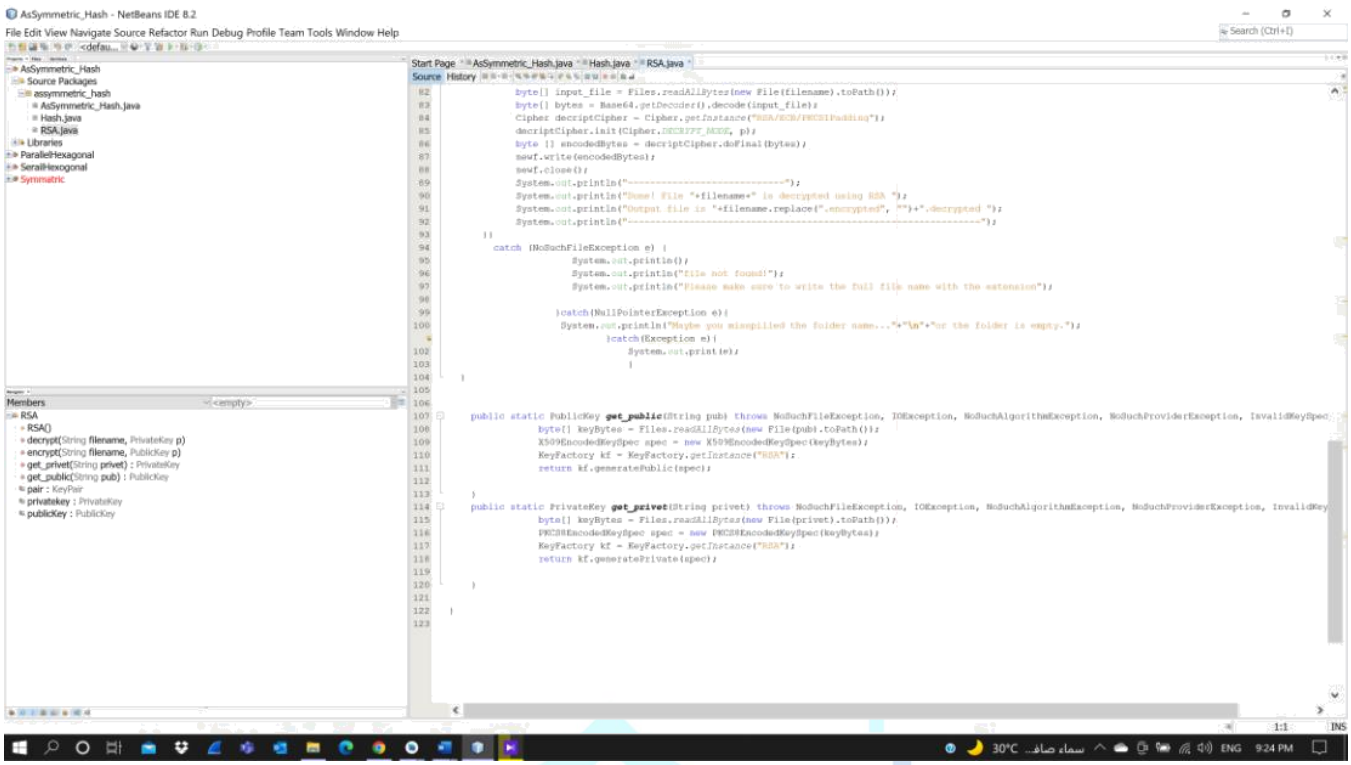
- Hashing is one-way encryption (encryption only).

Screenshots for run project

First: RSA code:

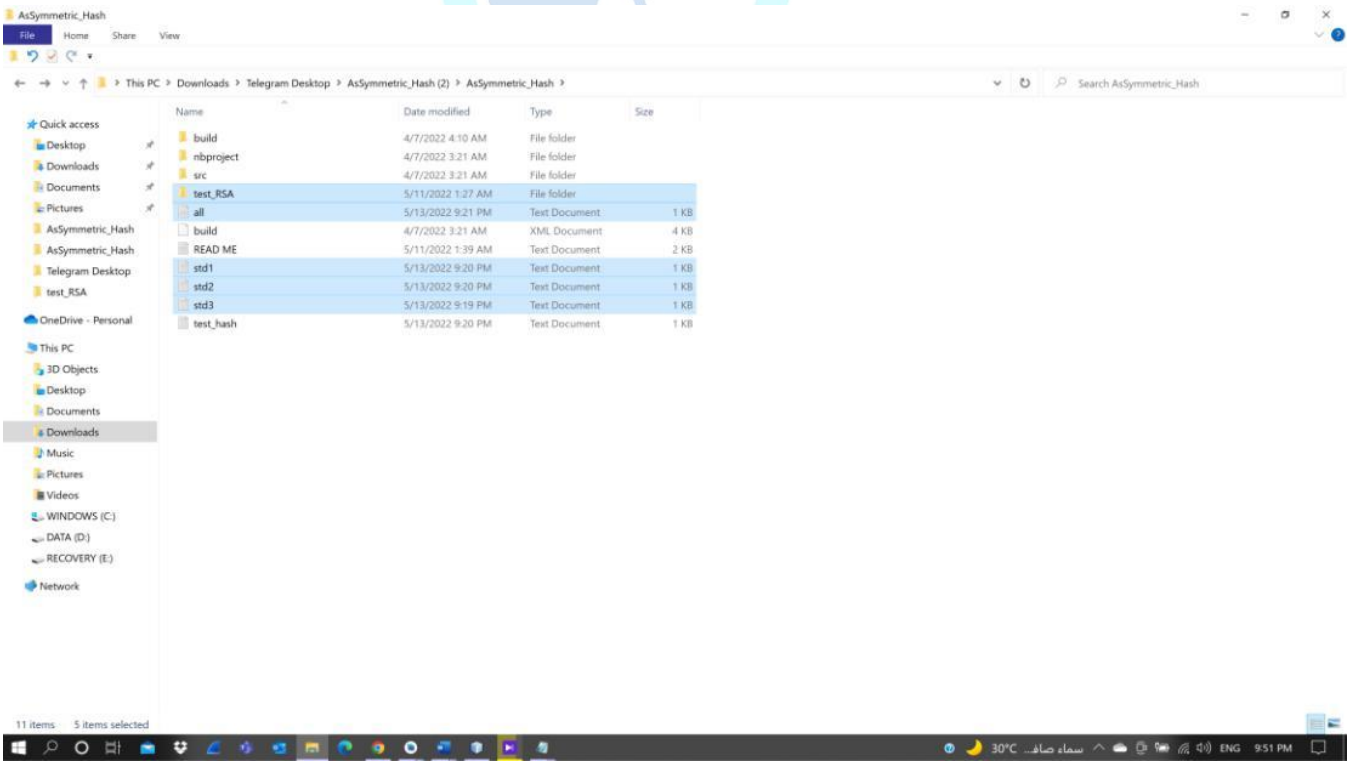




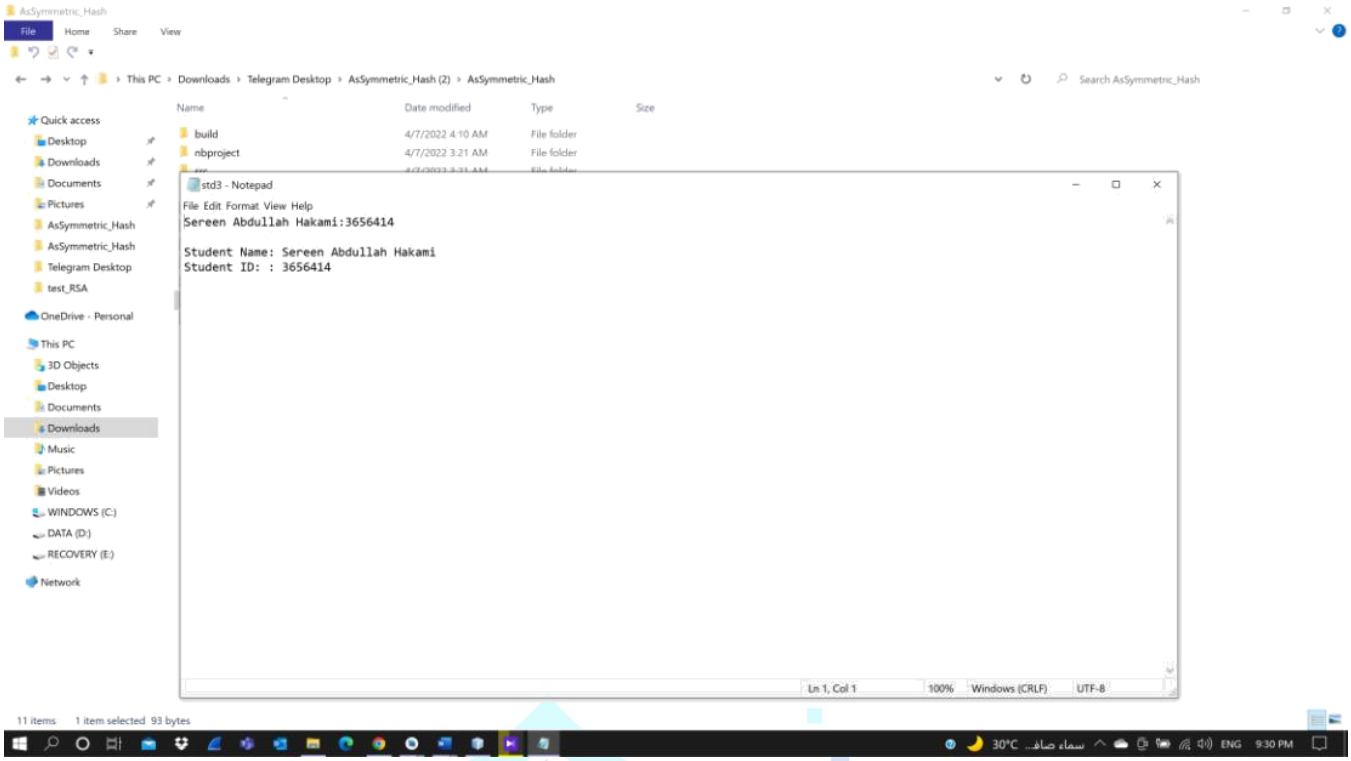


Run code:

Before RSA Algorithm running:

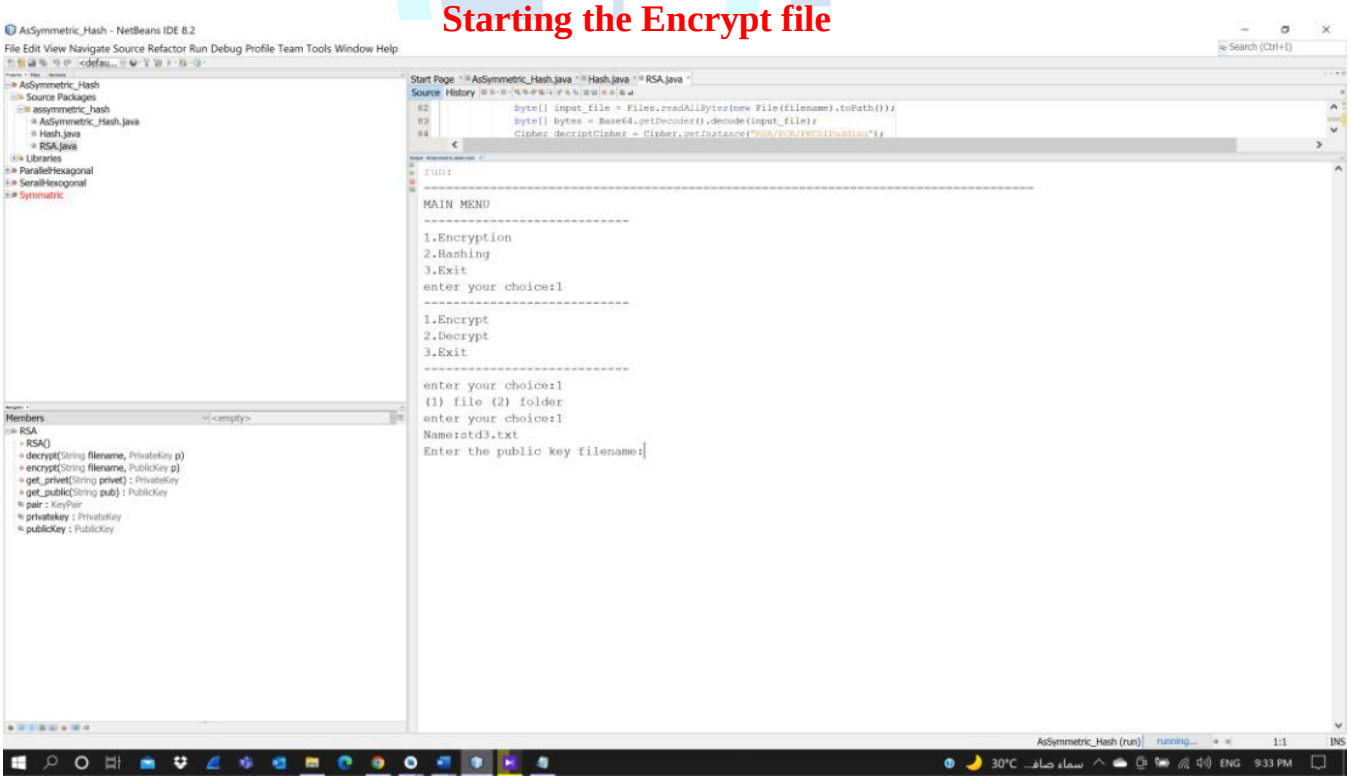


These are the files and the folder to which we will apply the encryption and decryption algorithm

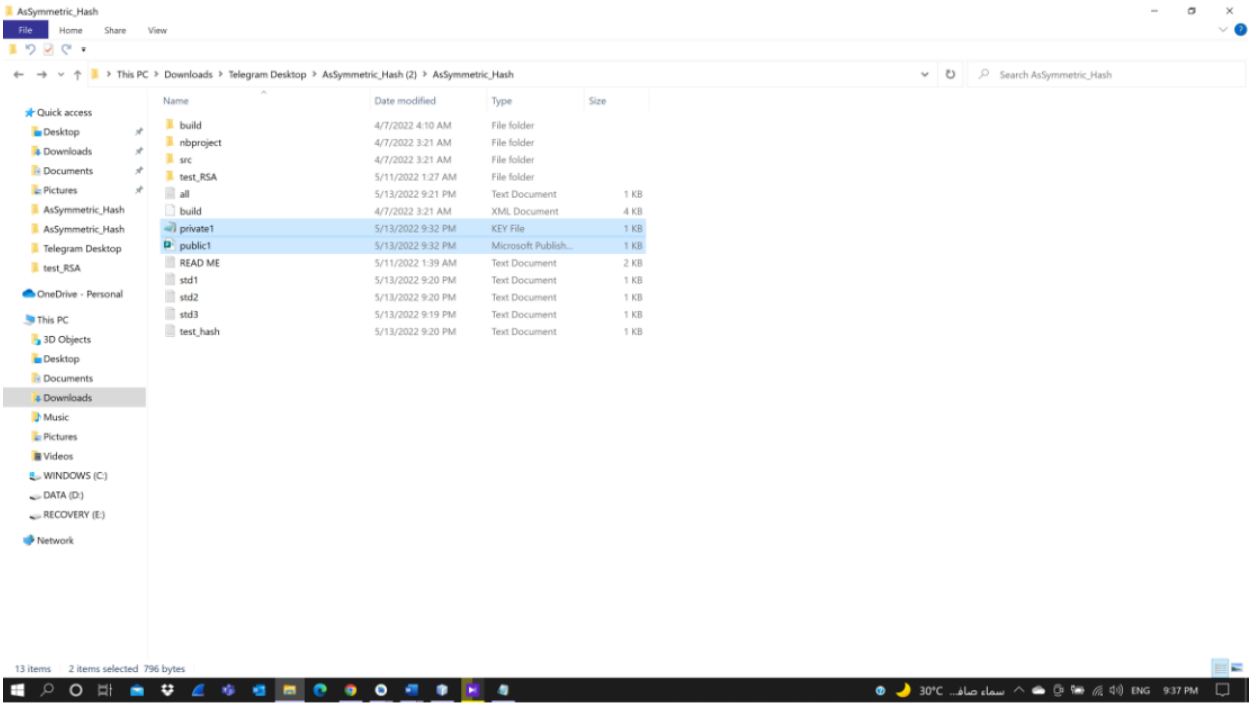


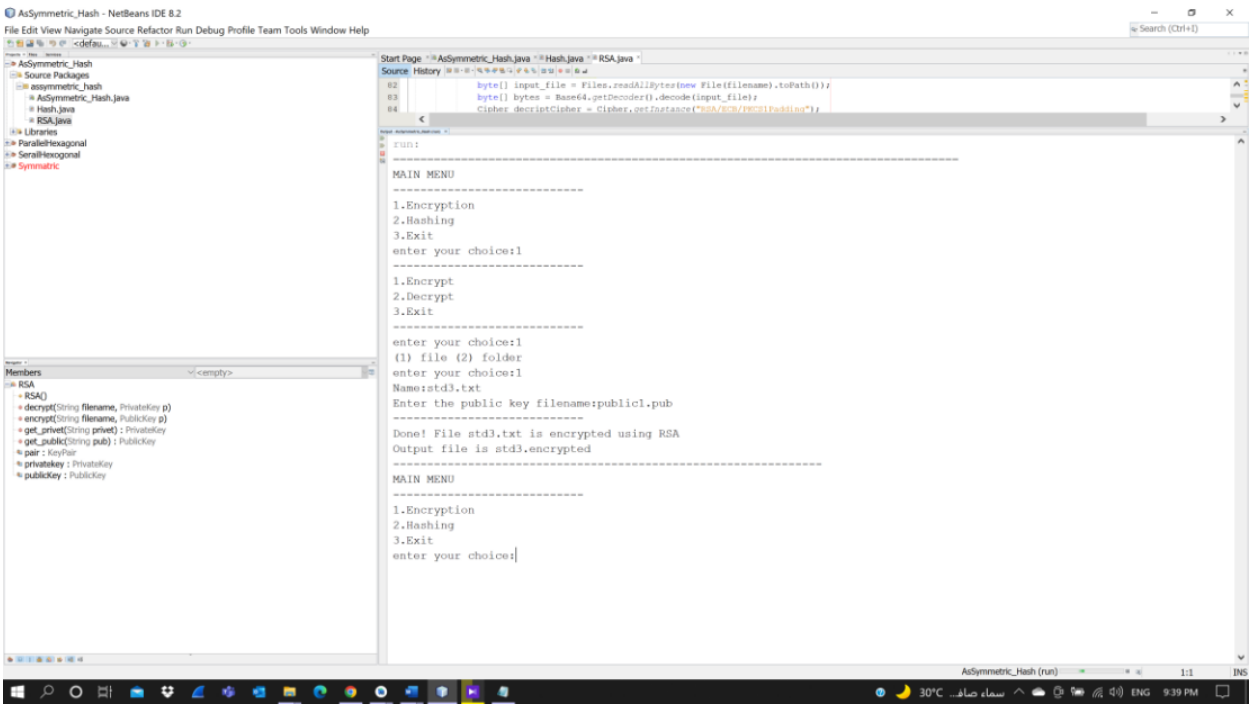
We will apply encryption and decryption to a file named <u>std3</u>

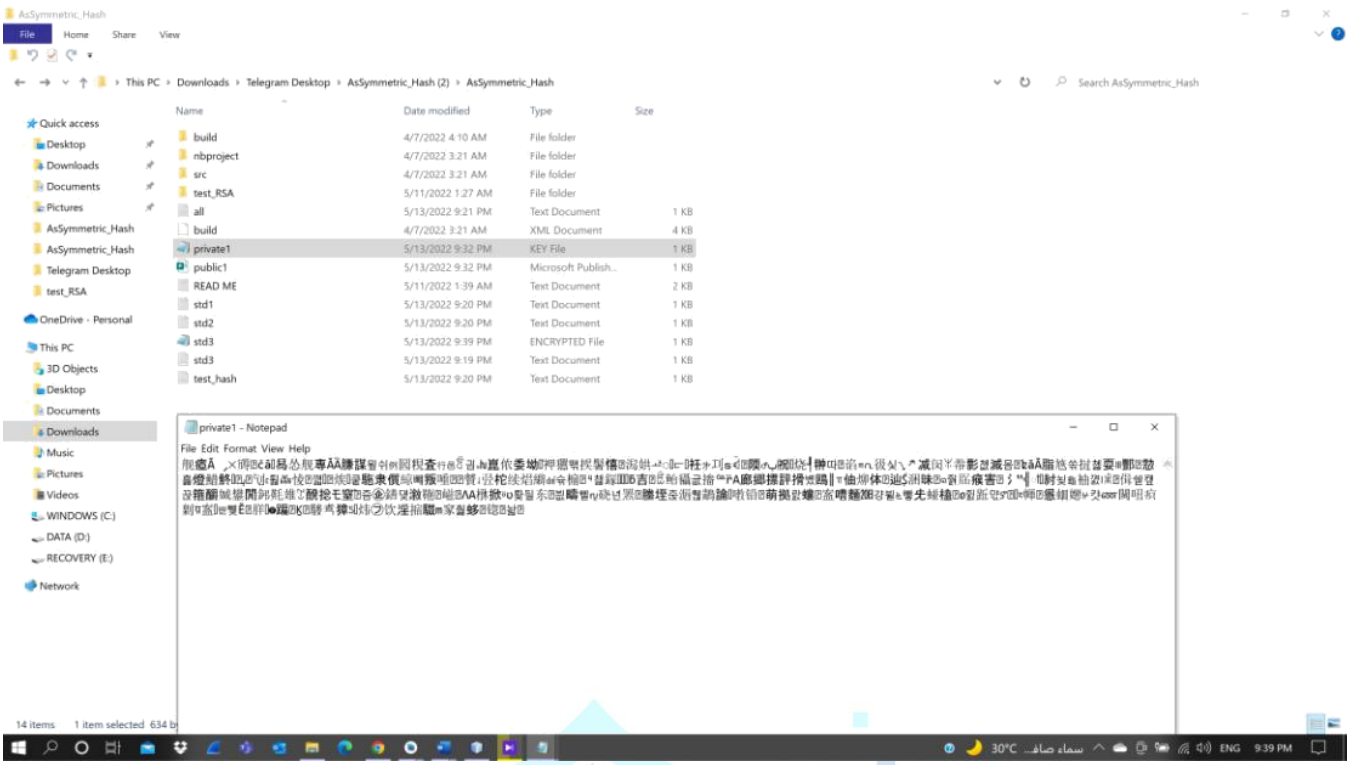
Starting the Encrypt file



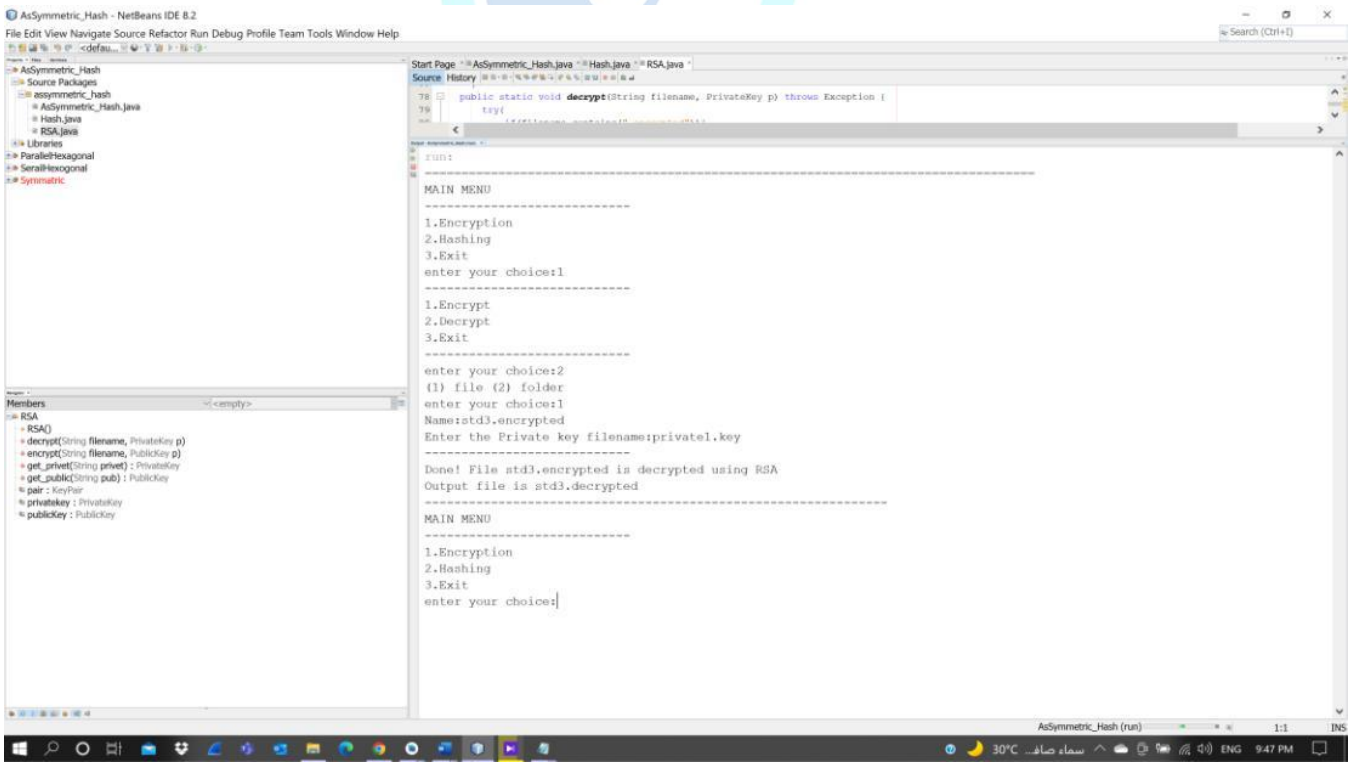
When encrypt the file we can see it has created a key file name <u>(Private key and public Key)</u>


AsSymmetric_Hash
File Home Share View
This PC › Downloads › Telegram Desktop › AsSymmetric_Hash (2) › AsSymmetric_Hash
Search AsSymmetric_Hash
Quick access
Desktop
Downloads
Documents
Pictures
AsSymmetric_Hash
AsSymmetric_Hash
Telegram Desktop
test_RSA
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
WINDOWS (C:)
DATA (D:)
RECOVERY (E:)
Network
Name
Date modified
Type
Size
build 4/7/2022 4:10 AM File folder
nbproject 4/7/2022 3:21 AM File folder
src 4/7/2022 3:21 AM File folder
test_RSA 5/11/2022 1:27 AM File folder
all 5/13/2022 9:21 PM Text Document 1 KB
build 4/7/2022 3:21 AM XML Document 4 KB
private1 5/13/2022 9:32 PM KEY File 1 KB
public1 5/13/2022 9:32 PM Microsoft Publish... 1 KB
READ ME 5/11/2022 1:39 AM Text Document 2 KB
std1 5/13/2022 9:20 PM Text Document 1 KB
std2 5/13/2022 9:20 PM Text Document 1 KB
std3 5/13/2022 9:19 PM Text Document 1 KB
test_hash 5/13/2022 9:20 PM Text Document 1 KB
13 items 2 items selected 796 bytes
9:37 PM

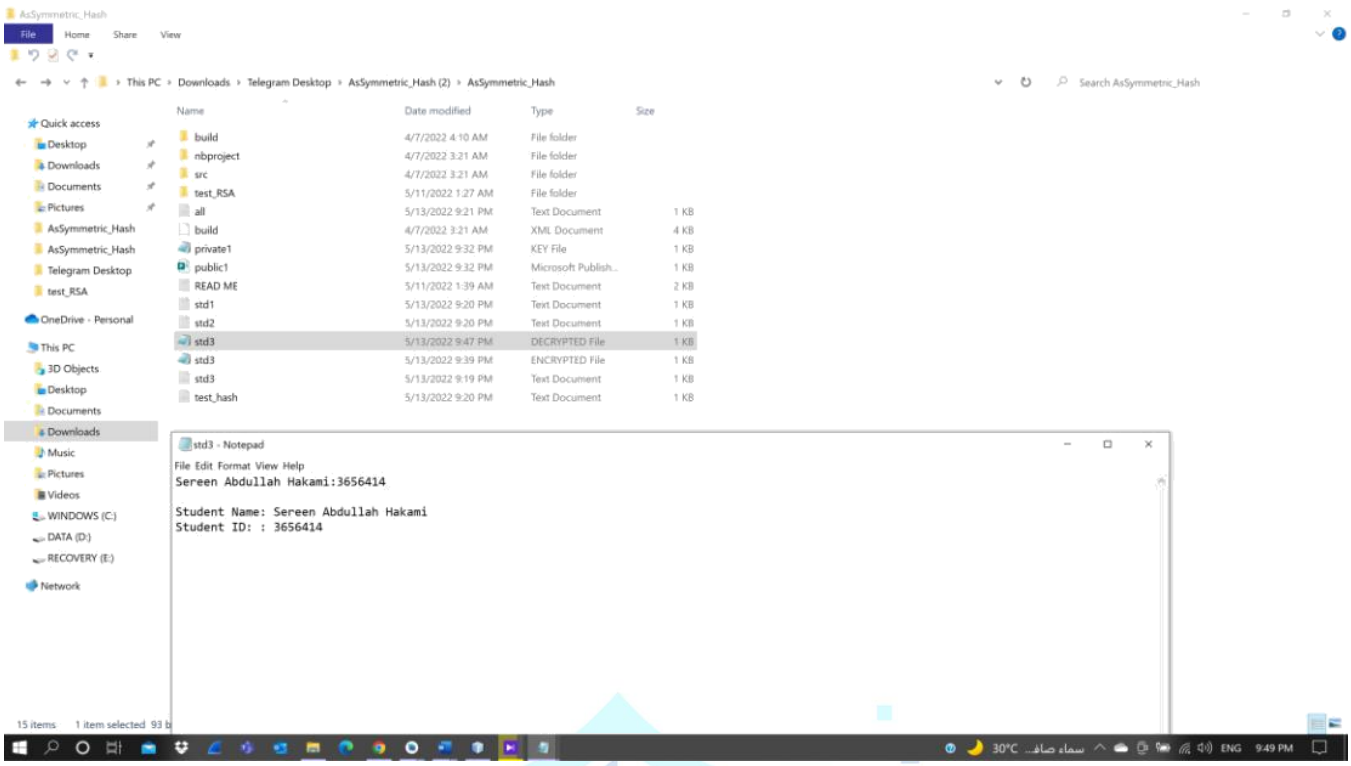

AsSymmetric_Hash - NetBeans IDE 8.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
AsSymmetric_Hash
Source Packages
assymmetric_hash
AsSymmetric_Hash.java
Hash.java
RSA.java
Libraries
ParallelHexagonal
SerailHexogonal
Symmatric
Start Page
AsSymmetric_Hash.java
Hash.java
RSA.java
Source History
run:
MAIN MENU
1.Encryption
2.Hashing
3.Exit
enter your choice:1
1.Encrypt
2.Decrypt
3.Exit
enter your choice:1
(1) file (2) folder
enter your choice:1
Name:std3.txt
Enter the public key filename:public1.pub
Done! File std3.txt is encrypted using RSA
Output file is std3.encrypted
MAIN MENU
1.Encryption
2.Hashing
3.Exit
enter your choice:
Members
RSA
RSA()
decrypt(String filename, PrivateKey p)
encrypt(String filename, PublicKey p)
get_privet(String privet) : PrivateKey
get_public(String pub) : PublicKey
pair : KeyPair
privatekey : PrivateKey
publicKey : PublicKey
AsSymmetric_Hash (run)
9:39 PM



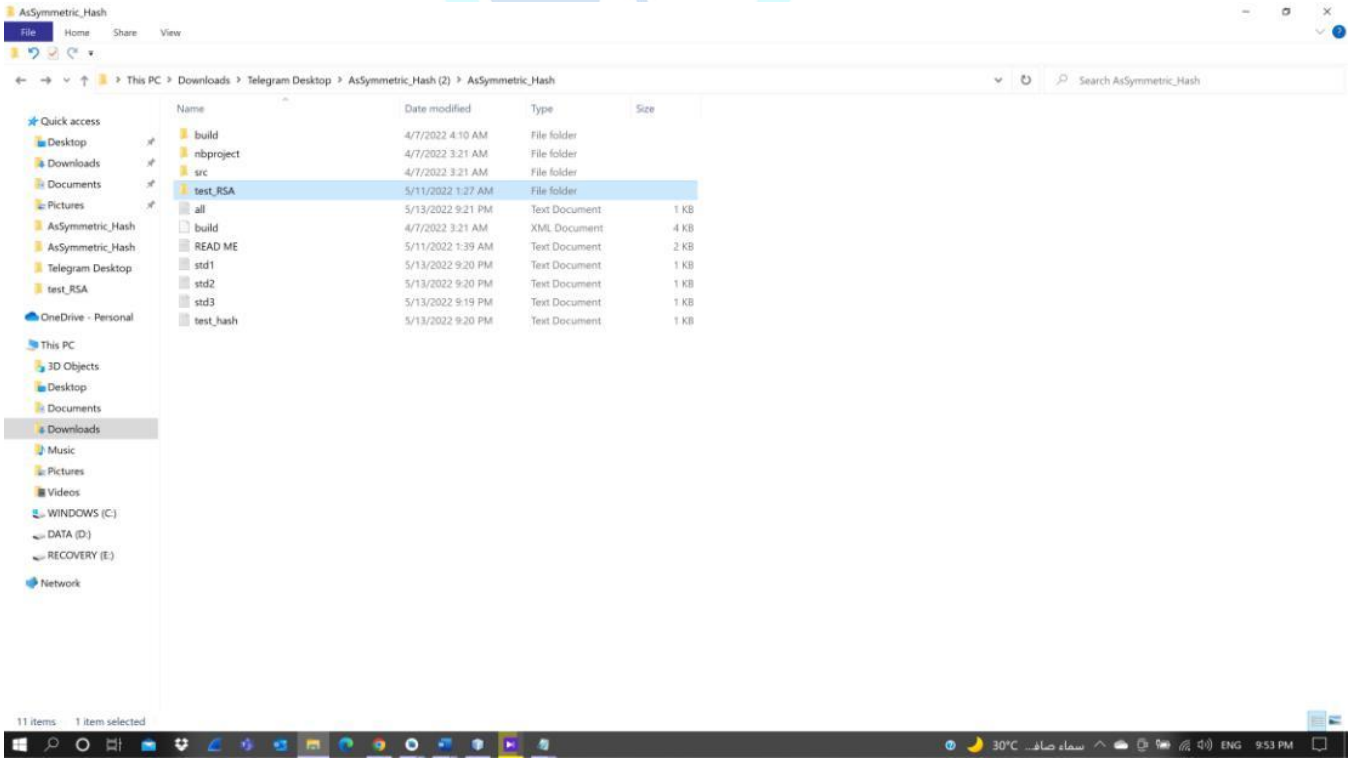
After doing the encryption using the public key, we notice that the text in the file has been encrypted

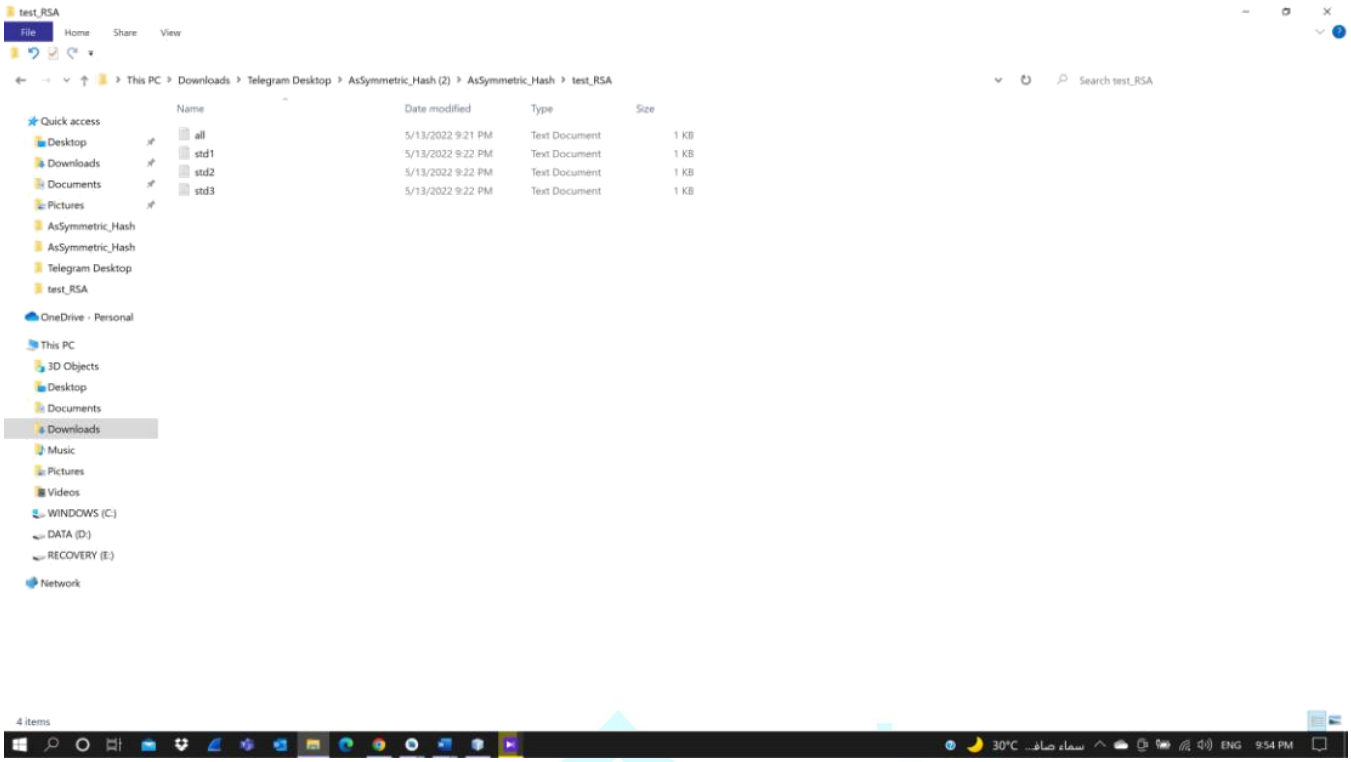


Now we are using the decrypt with the private key to open the encrypted file

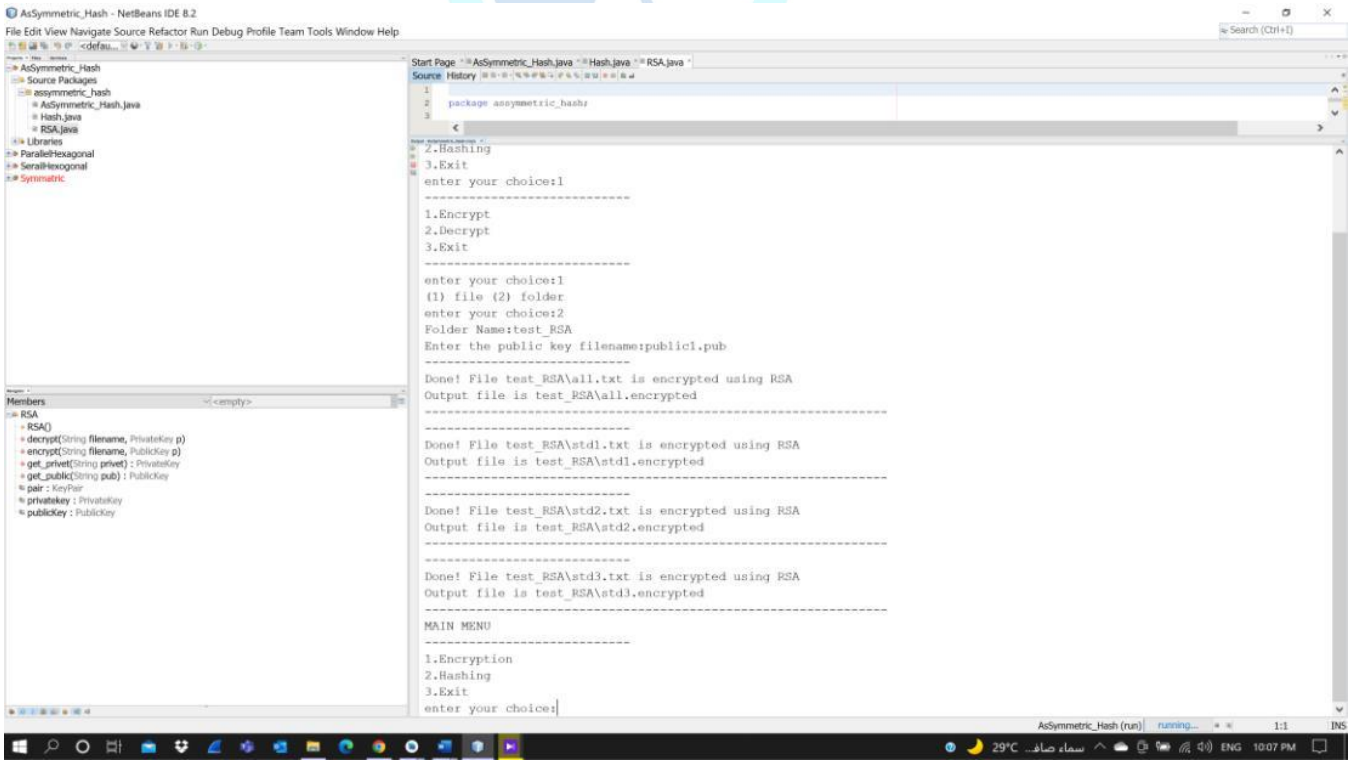


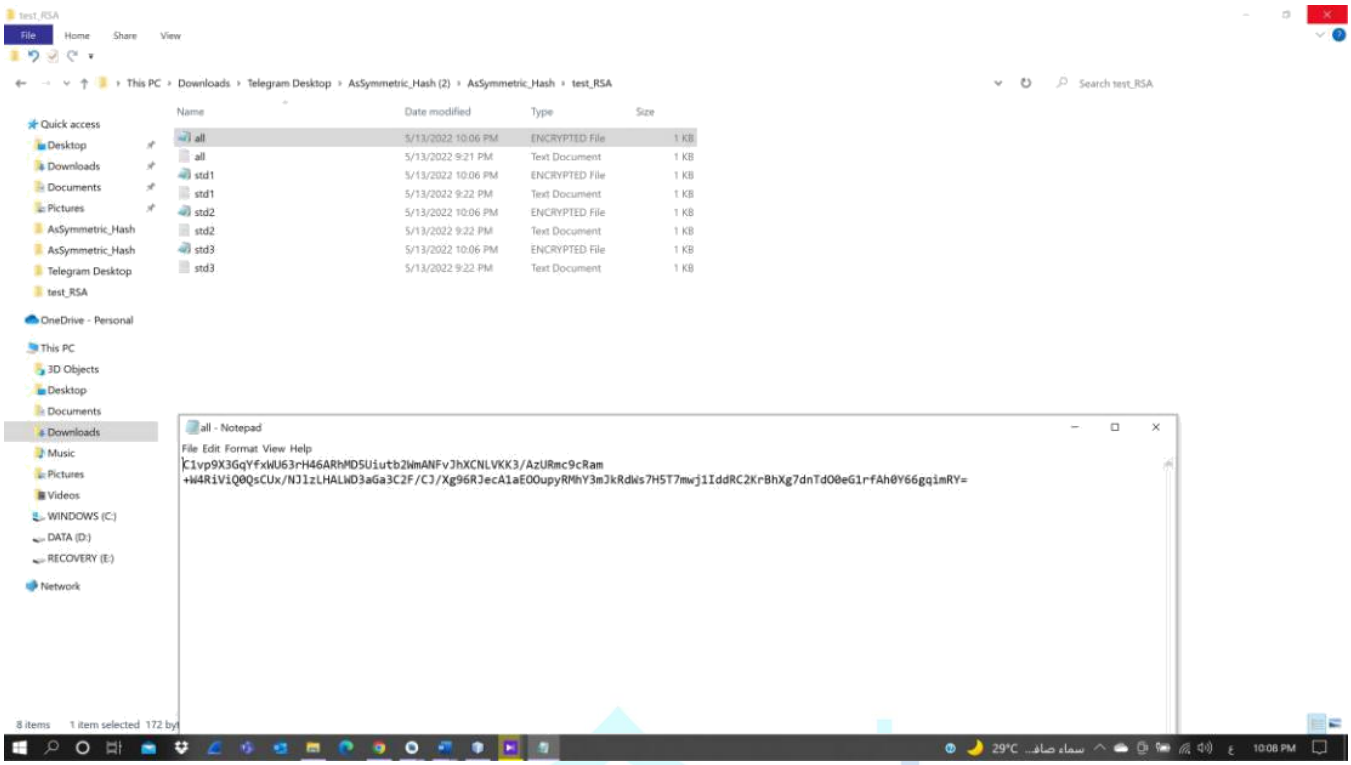
Starting the Encrypt folder



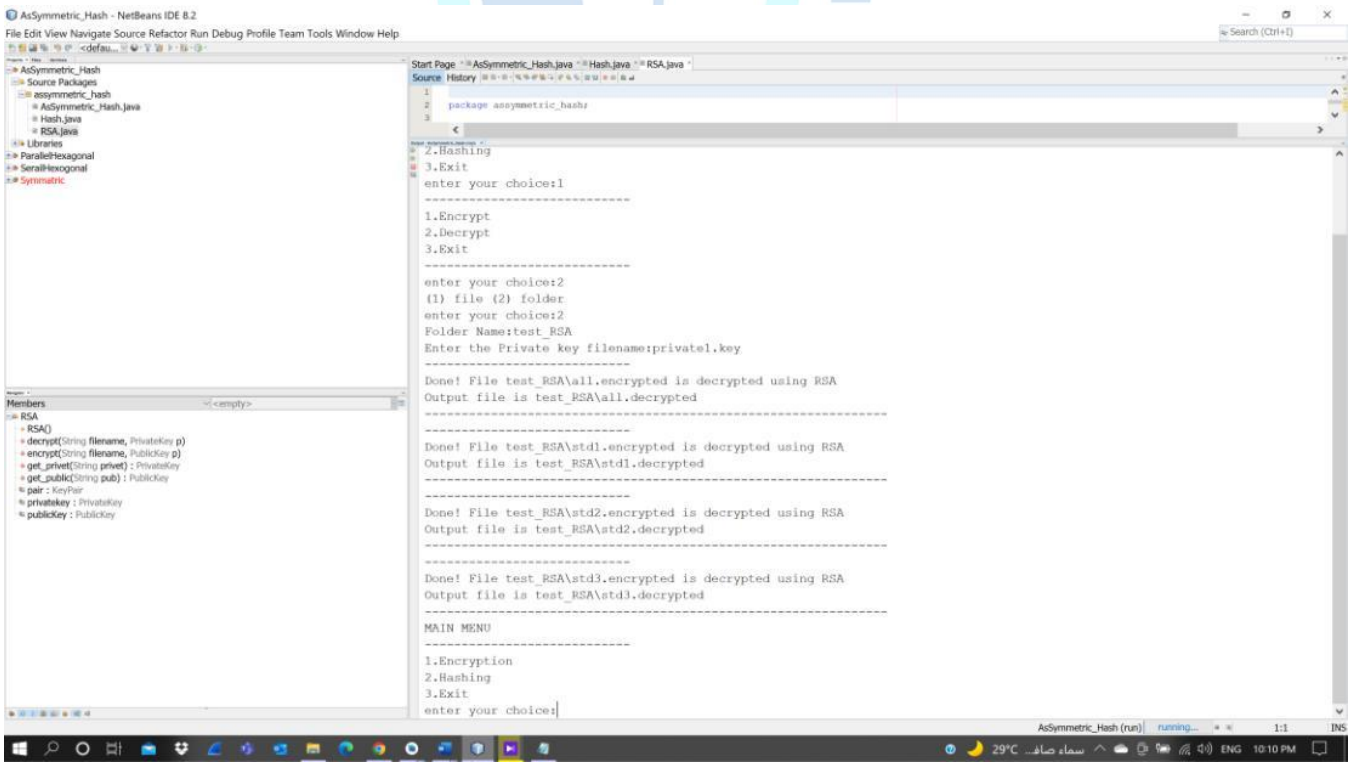


We will now encrypt and decrypt the folder named (test_RSA), which contains 4 files inside

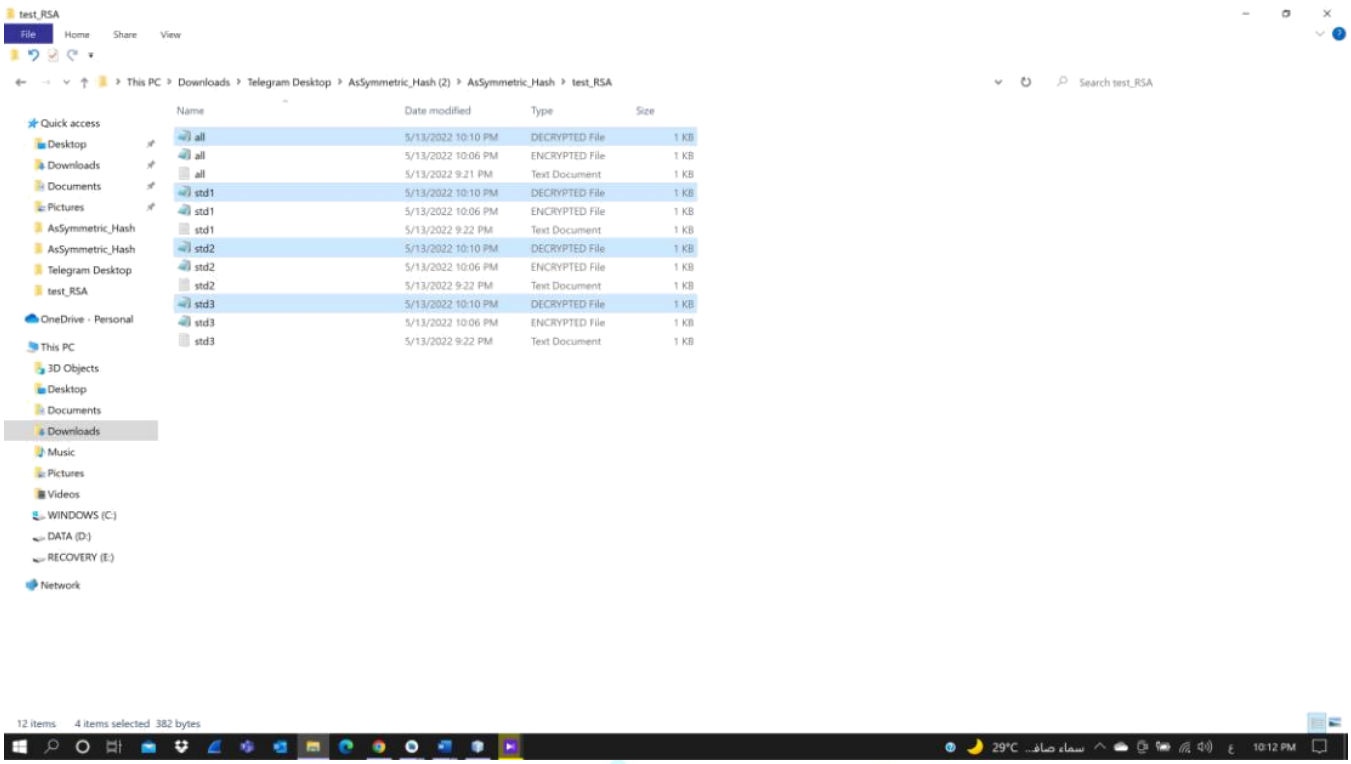




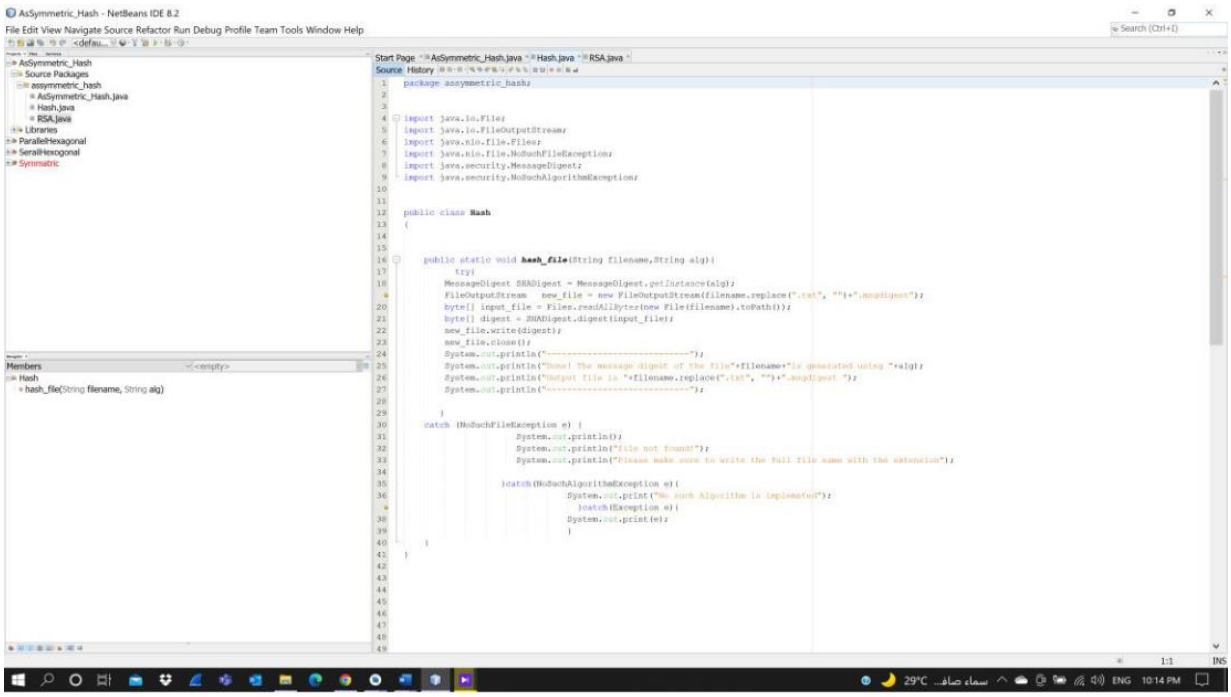
We can see that all the files inside the folder have been encrypted

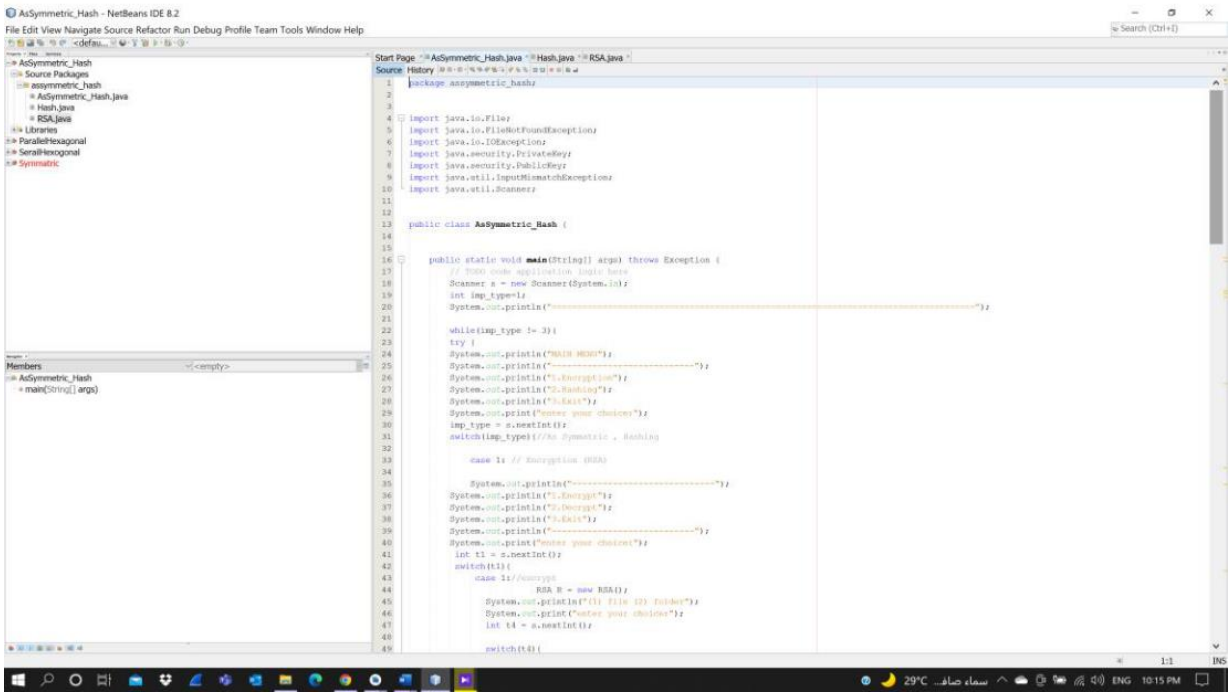


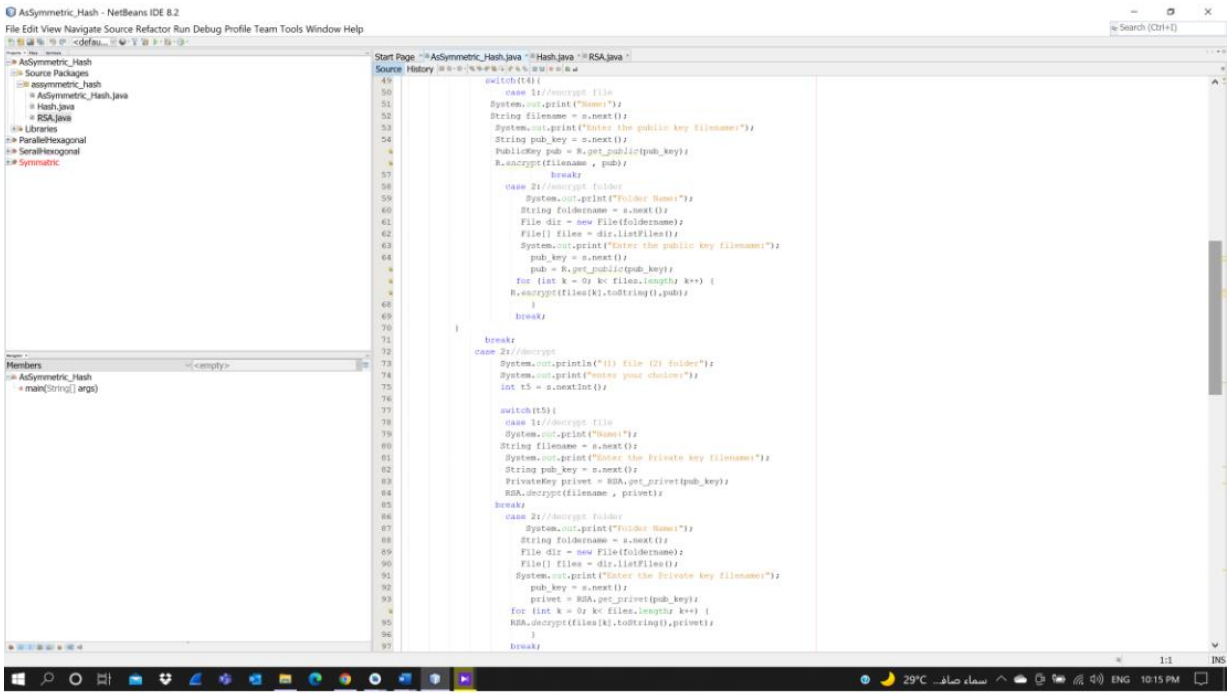
Now we take the opposite step, decryption

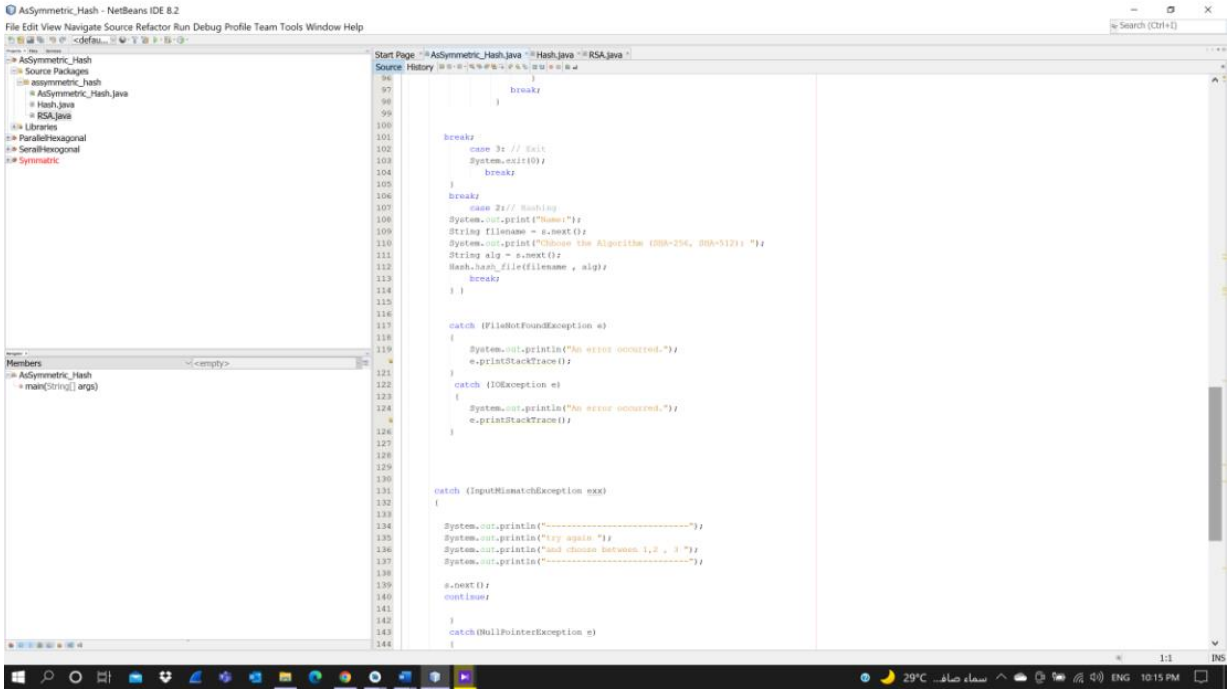

test_RSA
File
Home
Share
View
This PC > Downloads > Telegram Desktop > AsSymmetric_Hash (2) > AsSymmetric_Hash > test_RSA
Search test_RSA
Quick access
Desktop
Downloads
Documents
Pictures
AsSymmetric_Hash
AsSymmetric_Hash
Telegram Desktop
test_RSA
OneDrive - Personal
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
WINDOWS (C:)
DATA (D:)
RECOVERY (E:)
Network
Name
Date modified
Type
Size
all 5/13/2022 10:10 PM DECRYPTED File 1 KB
all 5/13/2022 10:06 PM ENCRYPTED File 1 KB
all 5/13/2022 9:21 PM Text Document 1 KB
std1 5/13/2022 10:10 PM DECRYPTED File 1 KB
std1 5/13/2022 10:06 PM ENCRYPTED File 1 KB
std1 5/13/2022 9:22 PM Text Document 1 KB
std2 5/13/2022 10:10 PM DECRYPTED File 1 KB
std2 5/13/2022 10:06 PM ENCRYPTED File 1 KB
std2 5/13/2022 9:22 PM Text Document 1 KB
std3 5/13/2022 10:10 PM DECRYPTED File 1 KB
std3 5/13/2022 10:06 PM ENCRYPTED File 1 KB
std3 5/13/2022 9:22 PM Text Document 1 KB
12 items
4 items selected 382 bytes
29°C
10:12 PM

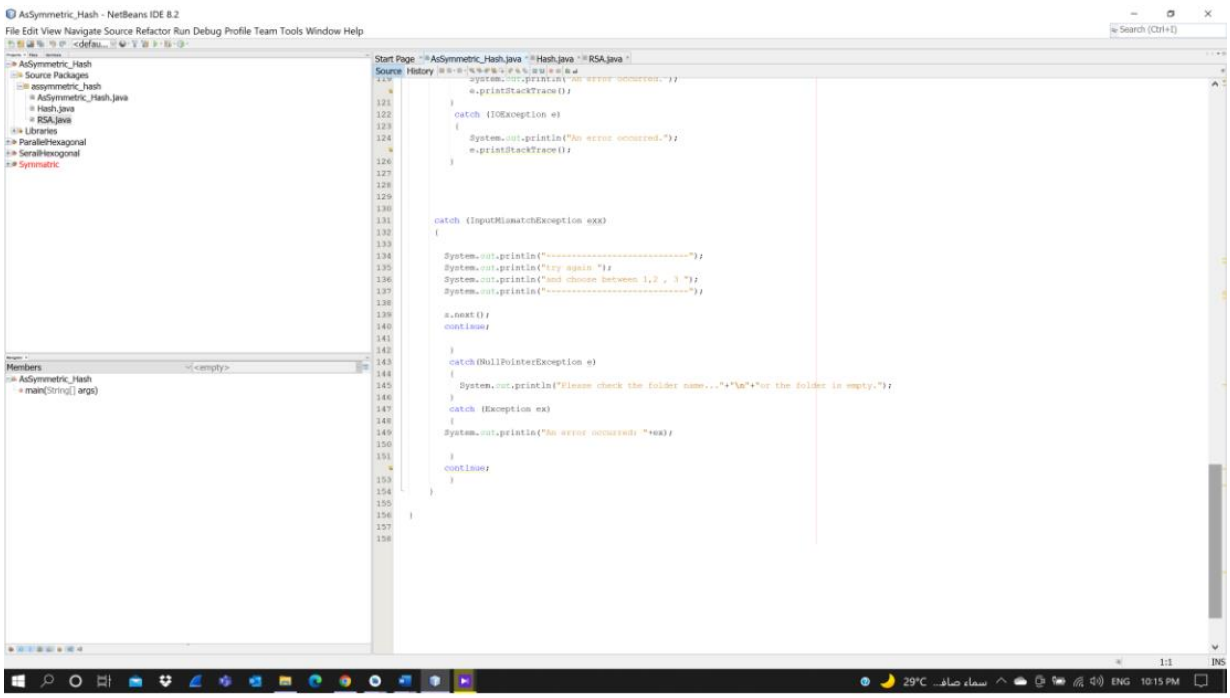
Second: hashing code

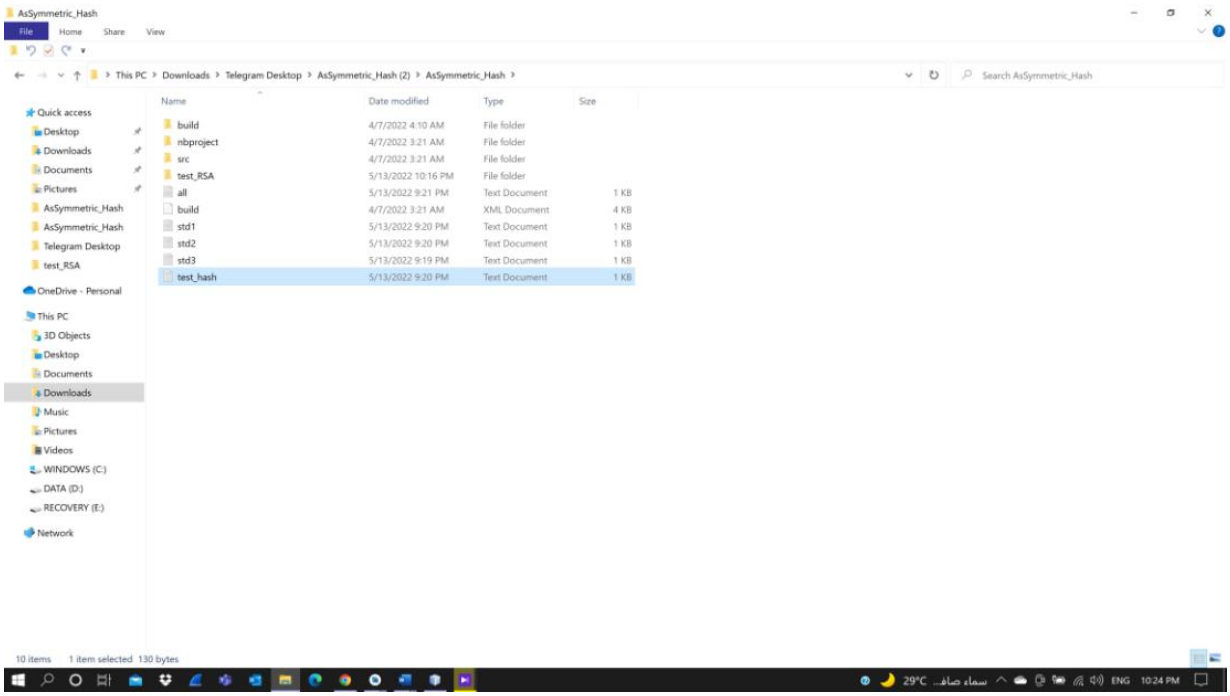






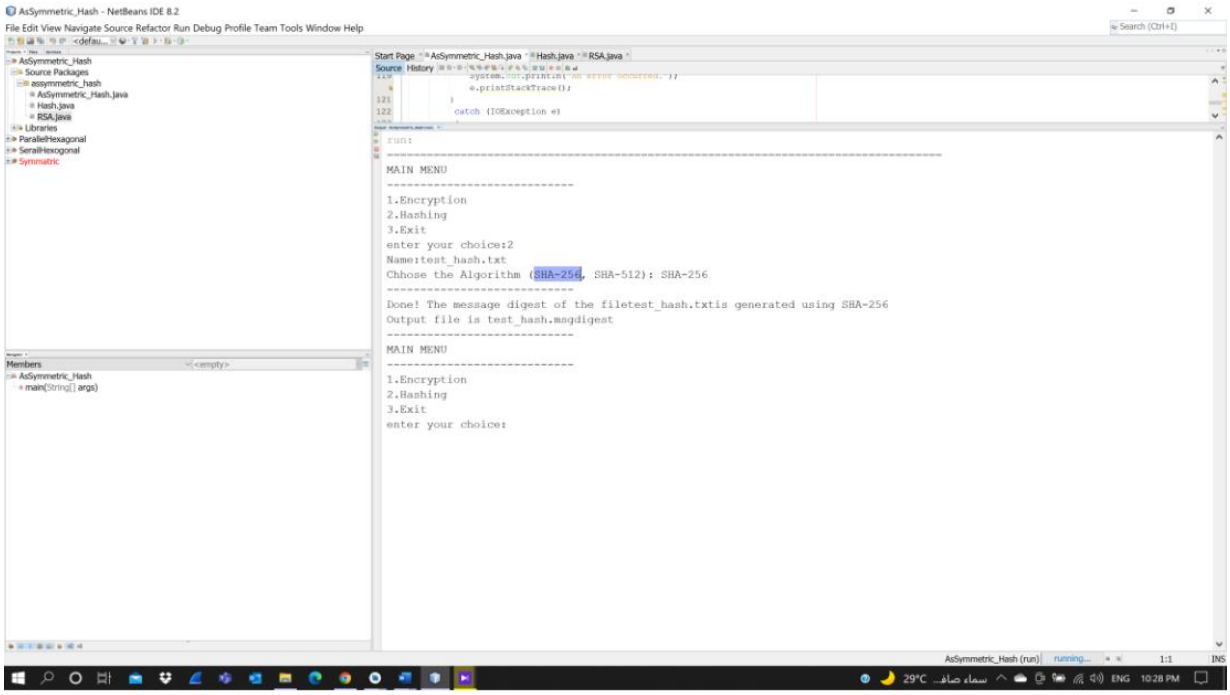


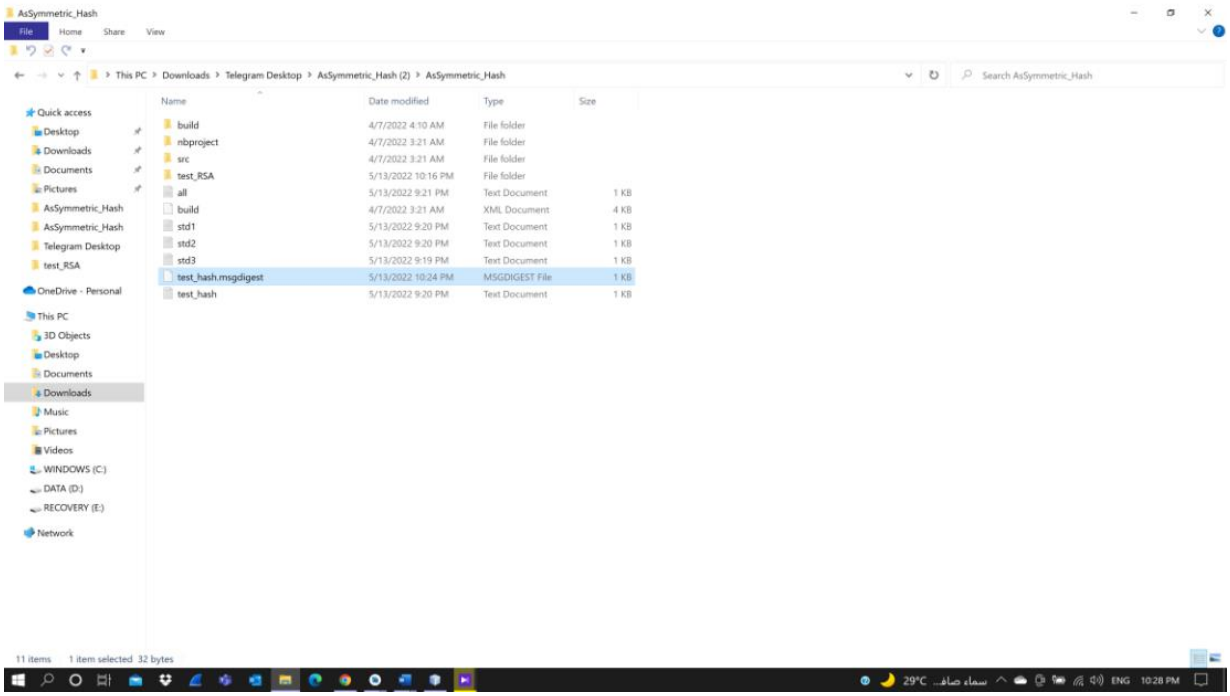


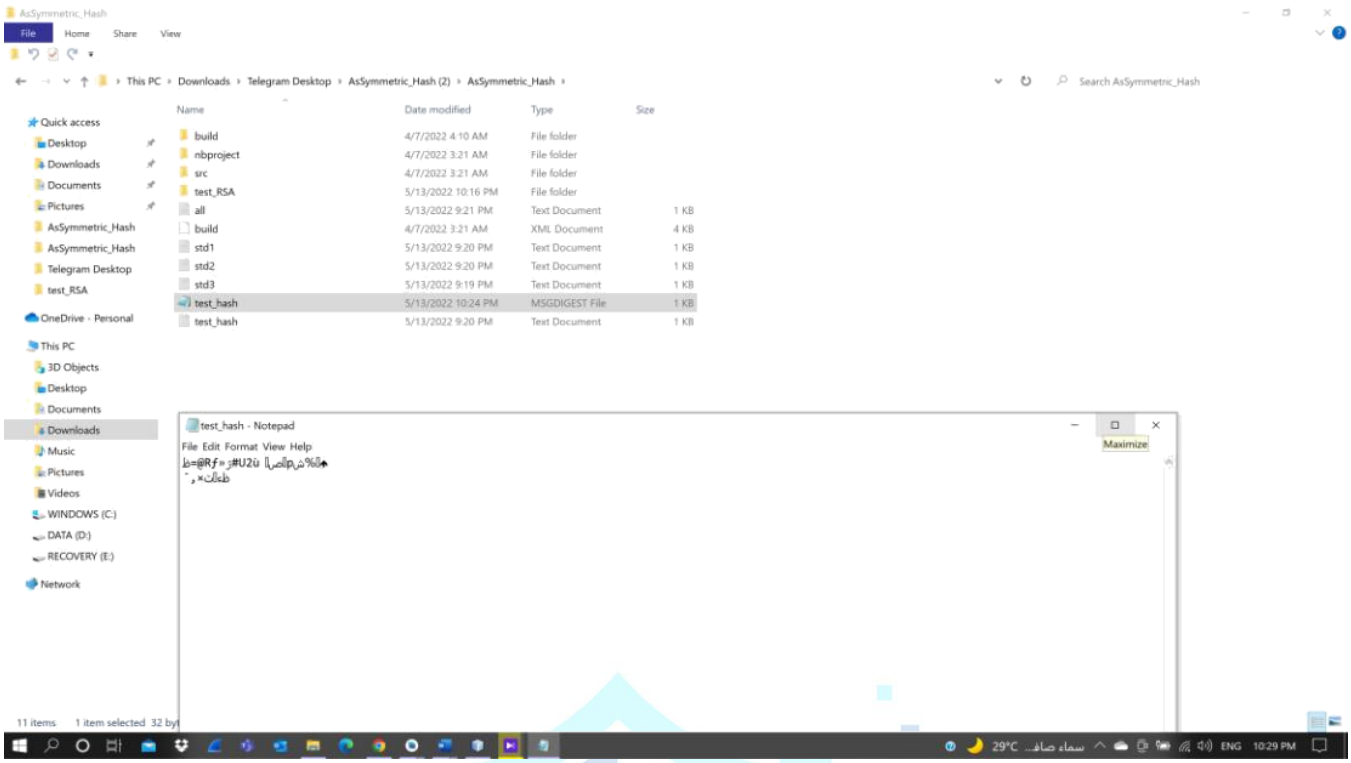


Now we will encrypt this file using the hashing algorithm.

We will be using first Algorithm (SHA-256)


AsSymmetric_Hash - NetBeans IDE 8.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
Start Page
AsSymmetric_Hash.java
Hash.java
RSA.java
run:
MAIN MENU
1.Encryption
2.Hashing
3.Exit
enter your choice:2
Name:test_hash.txt
Chhose the Algorithm (SHA-256, SHA-512): SHA-256
Done! The message digest of the filetest_hash.txtis generated using SHA-256
Output file is test_hash.msgdigest
MAIN MENU
1.Encryption
2.Hashing
3.Exit
enter your choice:


AsSymmetric_Hash
This PC > Downloads > Telegram Desktop > AsSymmetric_Hash (2) > AsSymmetric_Hash
build
nbproject
src
test_RSA
all
build
std1
std2
std3
test_hash.msgdigest
test_hash



Now we will use the second Algorithm (SHA-512)