Organized by:

POORNIMA

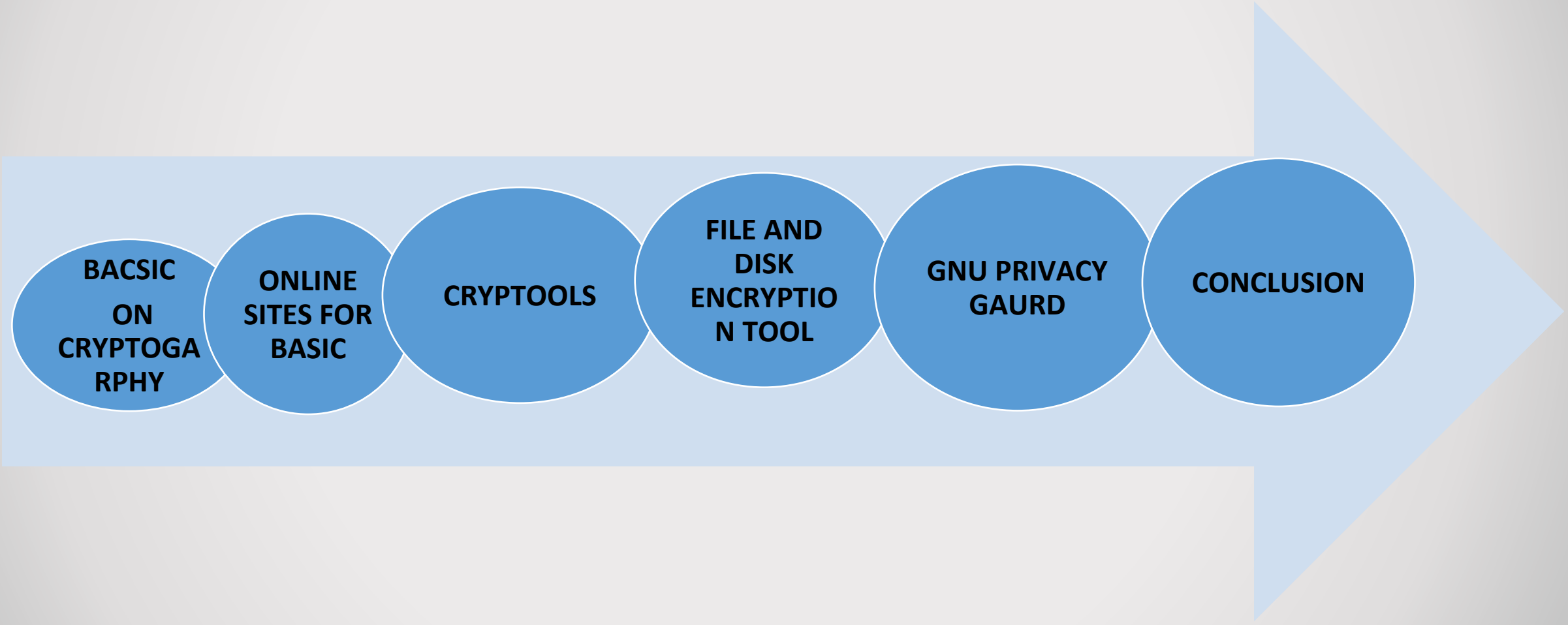
INSTITUTE OF ENGINEERING & TECHNOLOGY

Affiliated to RTU, Kota • Approved by AICTE & UGC under 2(f) • Accredited by NAAC and NBA

OPEN SOURCE CRYPTOGRAPHY TOOLS

Presented by : -
Dr.Anil Kumar
Associate Professor
Department of Computer Engineering
Poornima Institute Of Engineering & technology, Jaipur
Contact : +91-9896017351

CONTENTS


BACSIC ON CRYPTOGARPHY
ONLINE SITES FOR BASIC
CRYPTOOLS
FILE AND DISK ENCRYPTION TOOL
GNU PRIVACY GAURD
CONCLUSION

introduction

120201311 by Dawn. So can you guess what it is ?

1-A

20-T

20-T

1-A

3-C

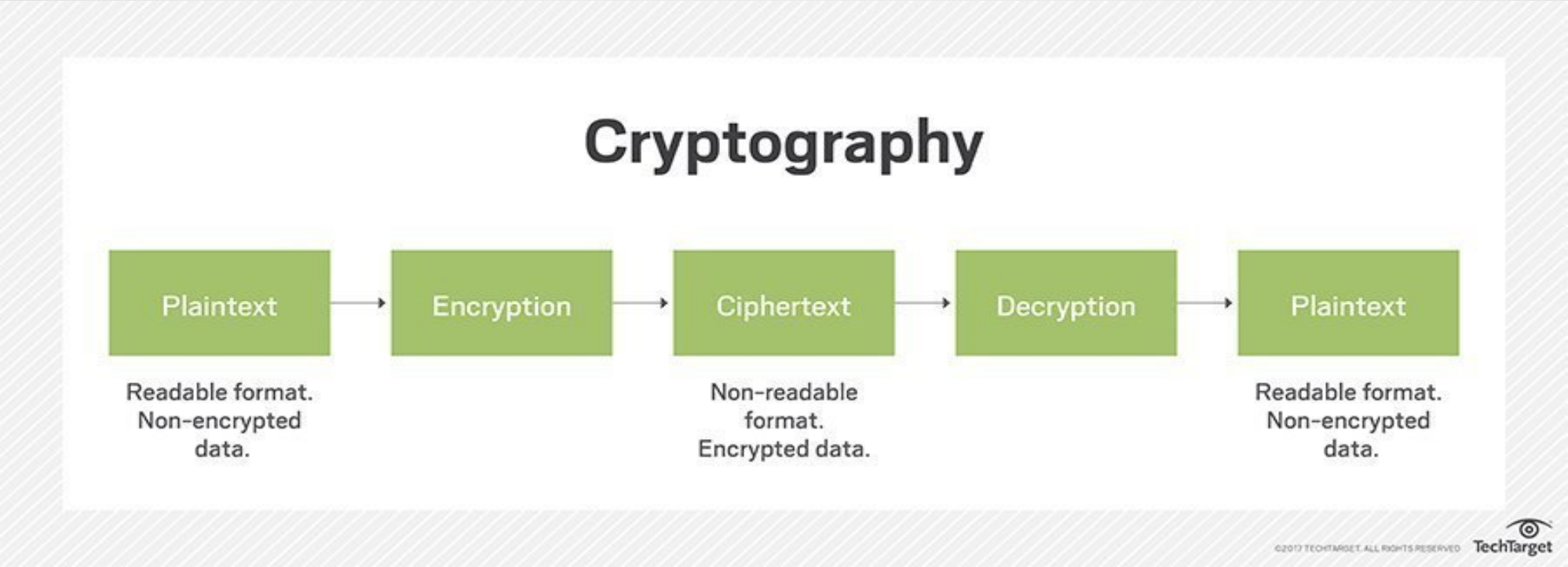
11-K

BY DAWN

SO THE ANSWER IS – ATTACK BY DAWN

What is cryptography

- Cryptography means creating an unreadable format of message to protect the original message from attack.
- Cryptography is the process or implementation of different protocols or algorithm to protect the message or data or information from the influence of third parties or adversaries.



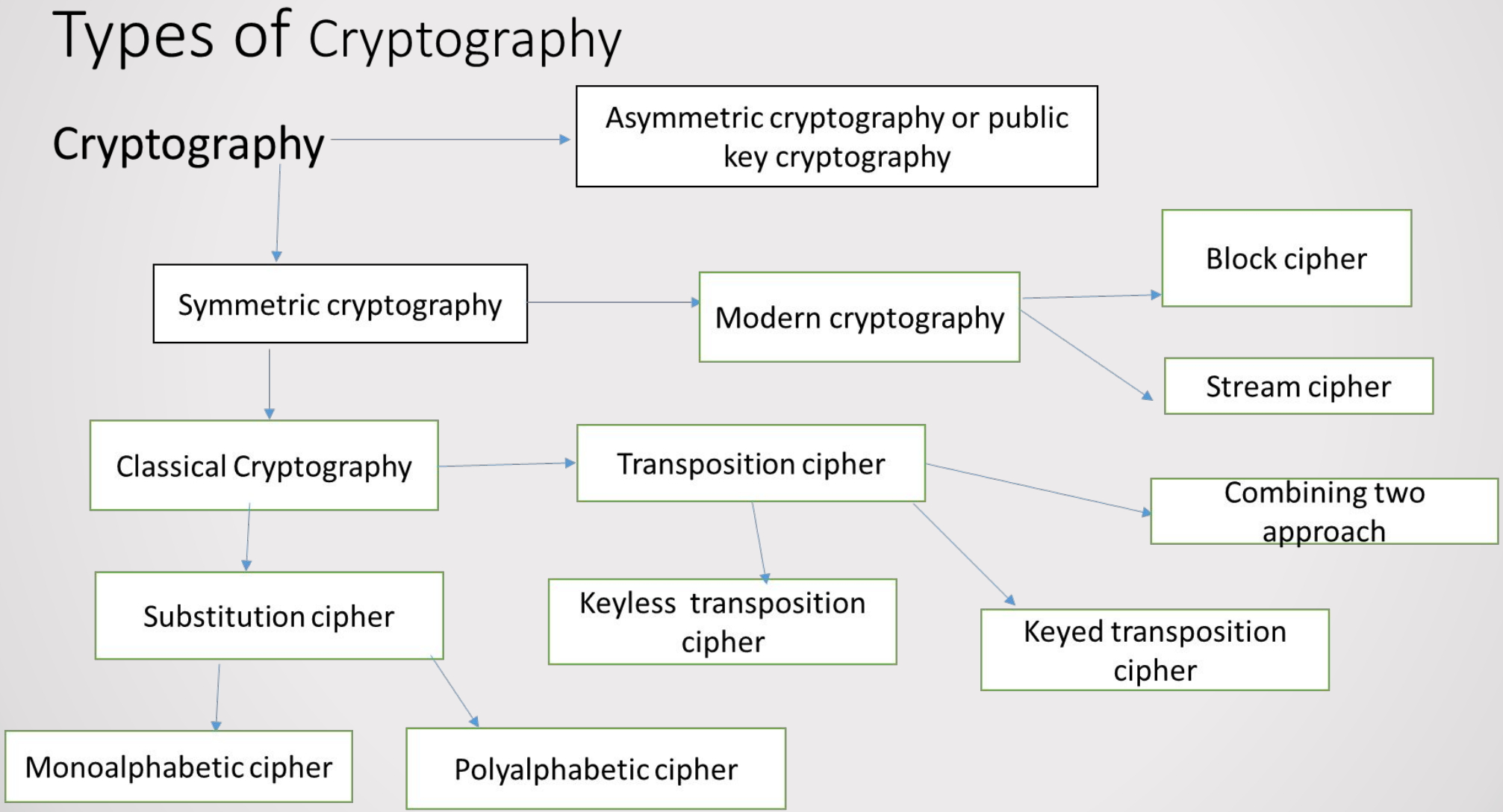
history

- The history of cryptography starts from the ancient era when it was practiced by secret societies or by troops in battlefields.
- The roots of cryptography are found in Roman and Egyptian civilizations.
- Back to 1900 B.C the Egyptians used to communicate by messages written in hieroglyph.
- During World War-I cryptography was highly implemented but mathematically it was used during World war -II.

basic terms

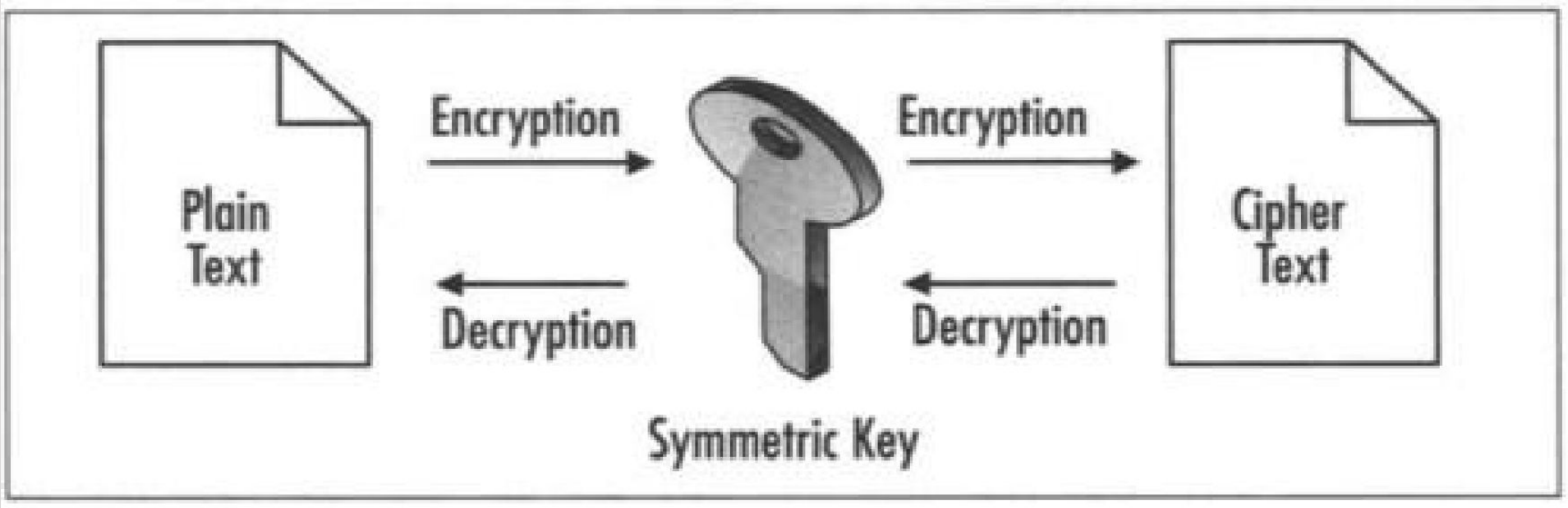
1. **Plain text:-** The readable format of message or the original message.
2. **Cipher text : -** The scrambled or the unreadable format of the message created after the process used called encryption.
3. **Encryption:-** The method used convert the plain text to the cipher text.
4. **Decryption:-** It is the process of converting the cipher text to the plain text.
5. **Key:-** Key is the information used to encrypt or decrypt the plain text or cipher text.
6. **Crypt-analysis :-** Study of deciphering or breaking codes.
7. **Cryptology :-** It is the field that includes both cryptography and cryptanalysis

Types of cryptography

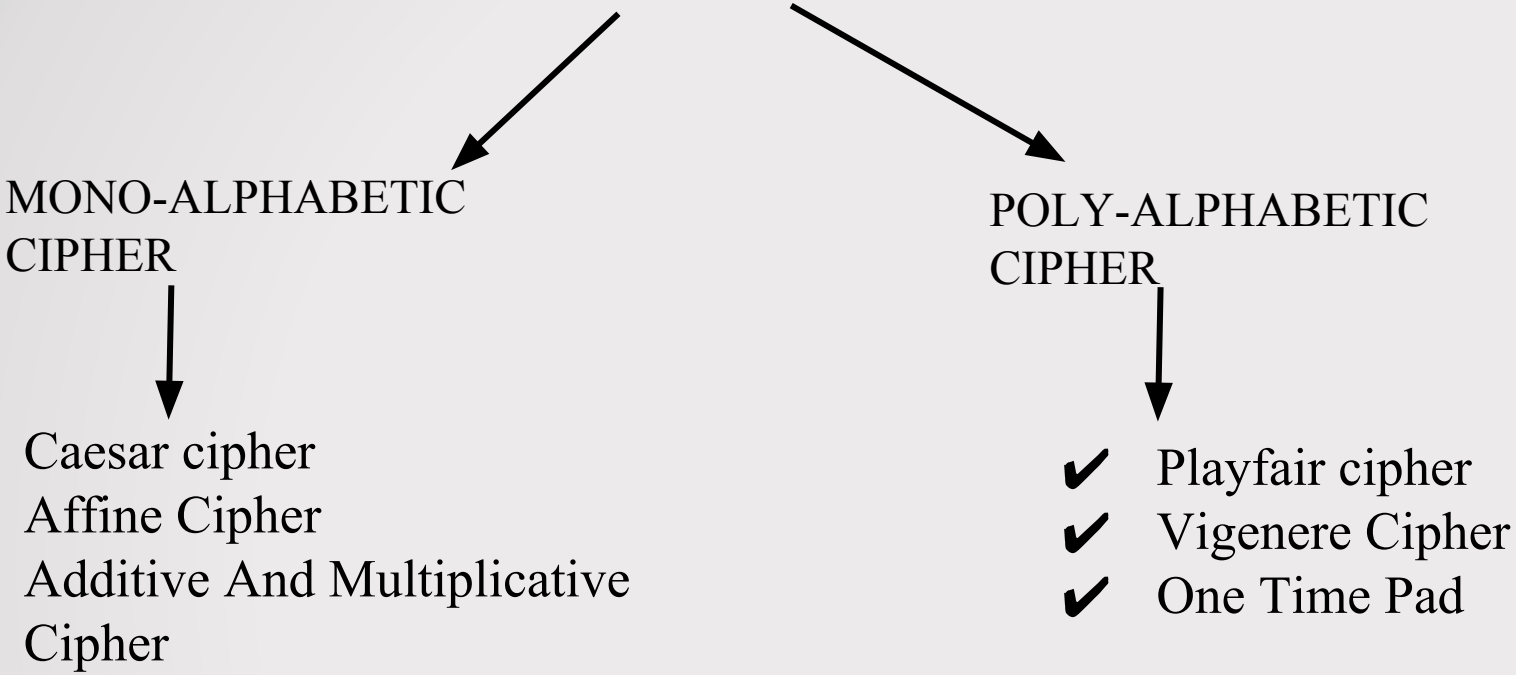


Symmetric key

- Symmetric key cryptography is named as it uses same key for encryption and decryption.



- Substitution cipher: - A Substitution cipher replaces one symbol with another.

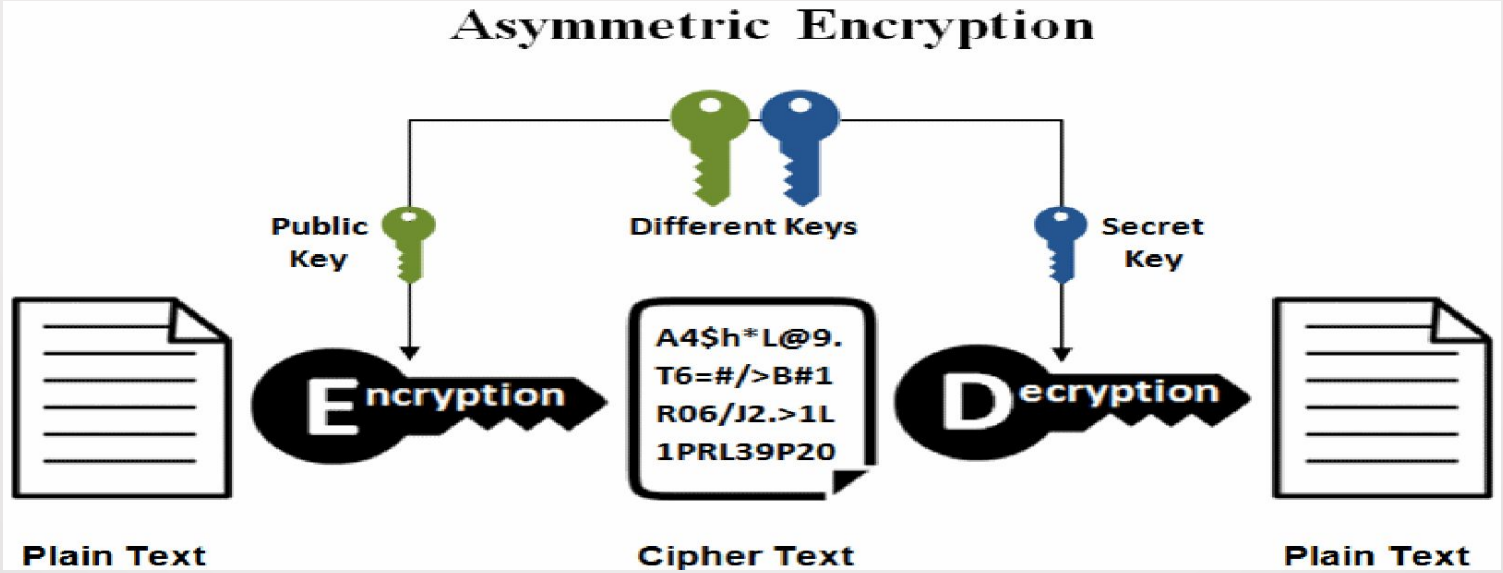


- Transposition cipher:-

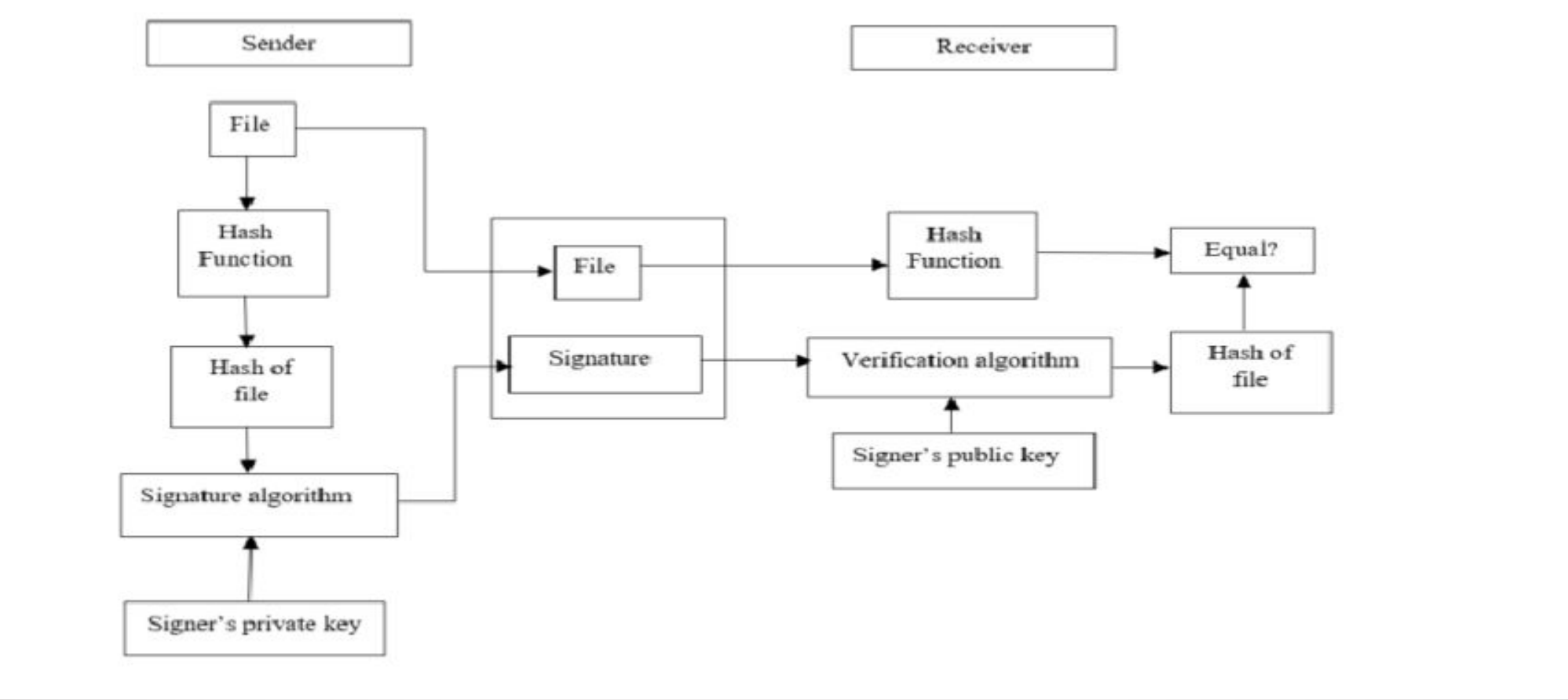
✔ Rail fence Cipher
✔ Columnar cipher
✔ Double columnar Cipher
✔ Route Cipher

ASYMMETRIC KEY CRYPTOGRAPHY

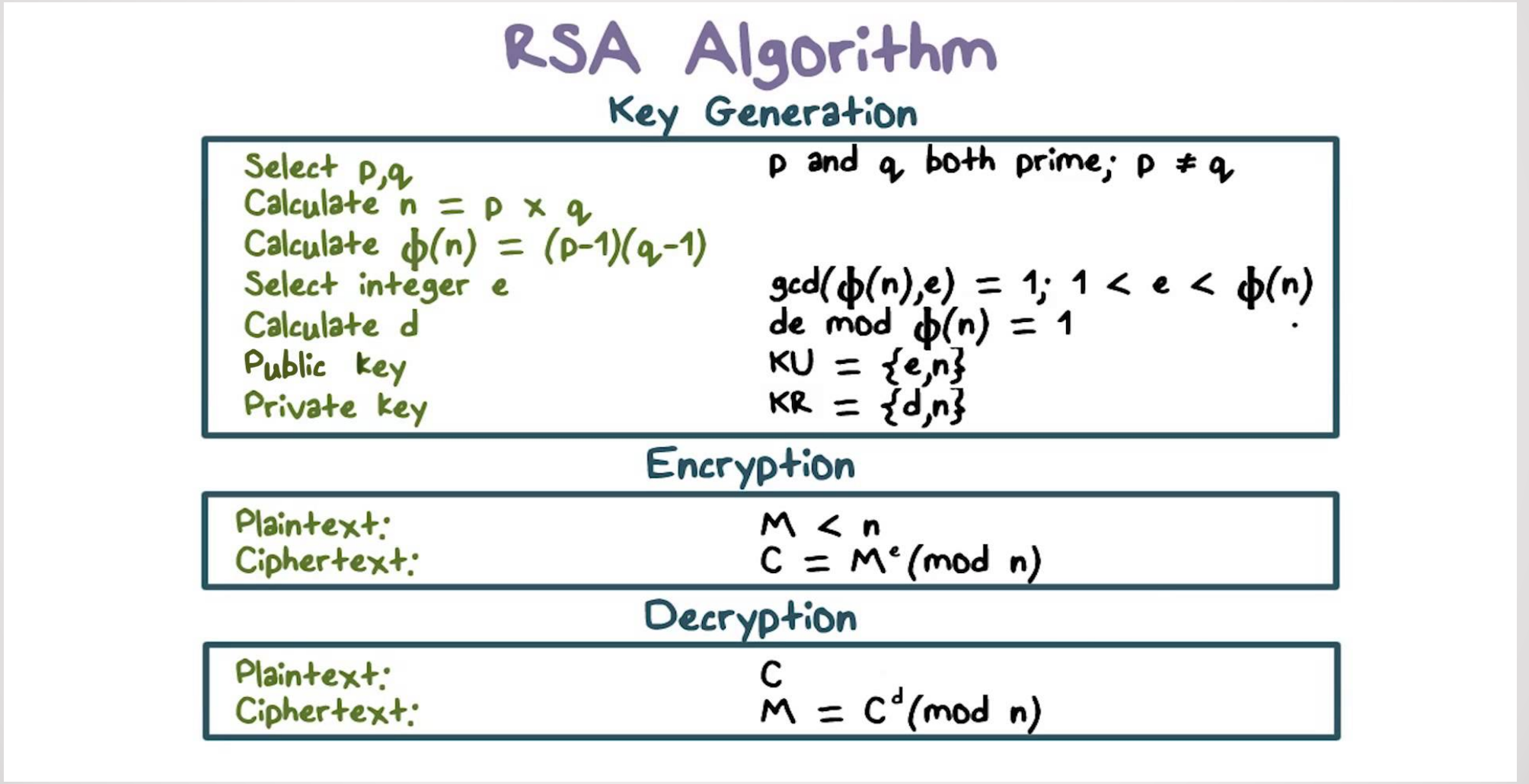
- Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data.
- Asymmetric encryption algorithms use a mathematically-related key pair for encryption and decryption; one is the public key and the other is the private key.



DIGITAL SIGNATURE

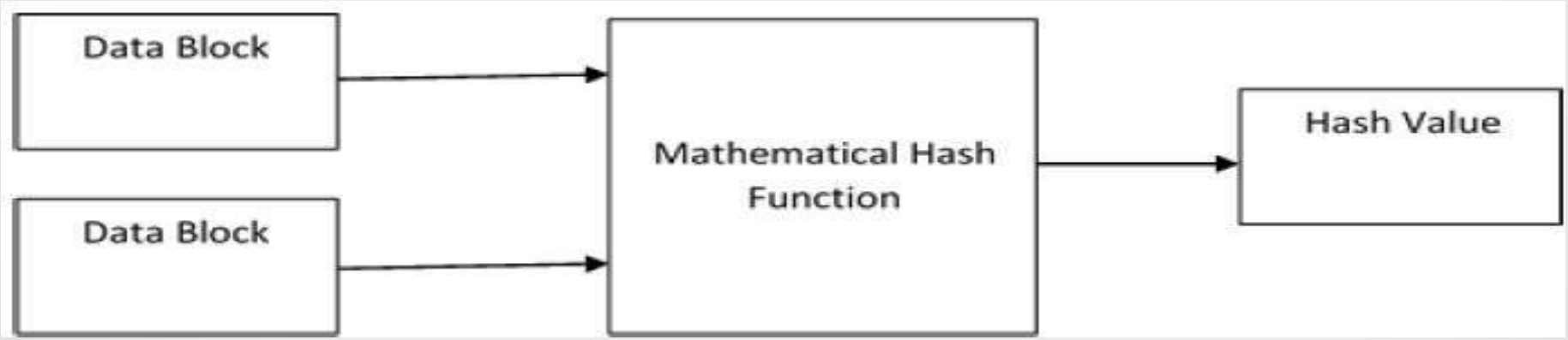


RSA SIGNATURE SCHEME

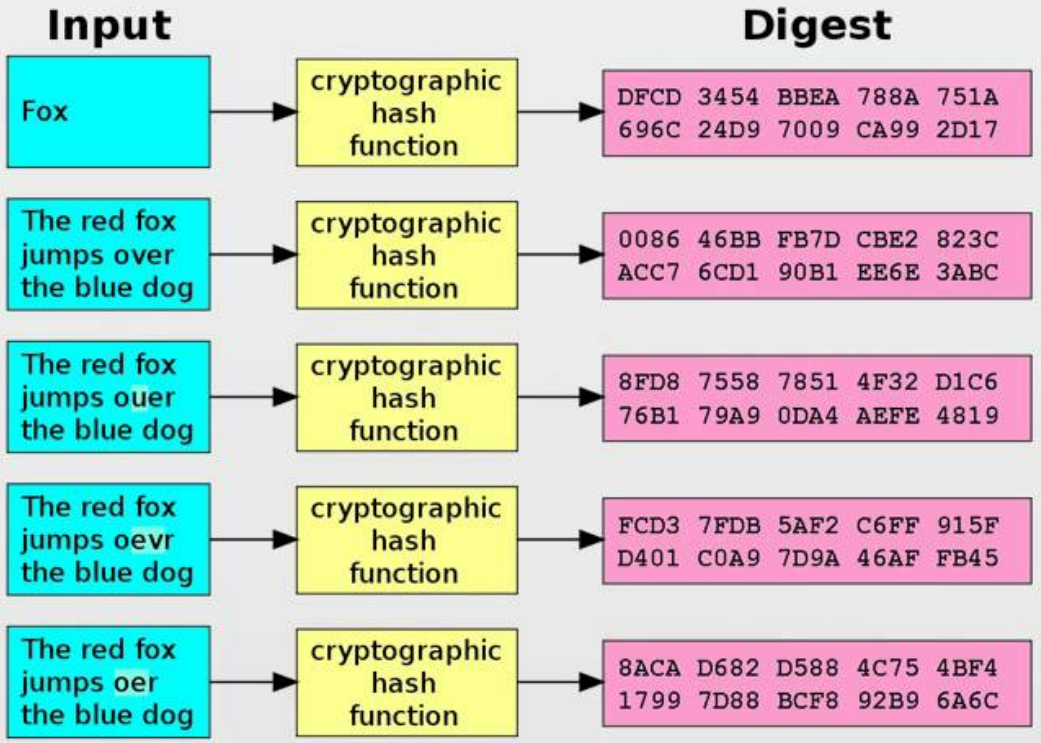


HASH FUNCTION

- Hash function is a mathematical function used to take numeric input to produce another numeric value.
- Input length is arbitrary but the output is of fixed length.
- Hash value is called message digest.
- https://www.fileformat.info/tool/hash.htm - play with hash function.



Cryptographic hash function



https://en.wikipedia.org/wiki/File:Cryptographic_Hash_Function.svg

Online Cryptography tools

- https://cryptii.com/pipes/caesar-cipher
- http://rumkin.com/tools/cipher/
- https://online-toolz.com/tools/text-encryption-decryption.php
- http://practicalcryptography.com/

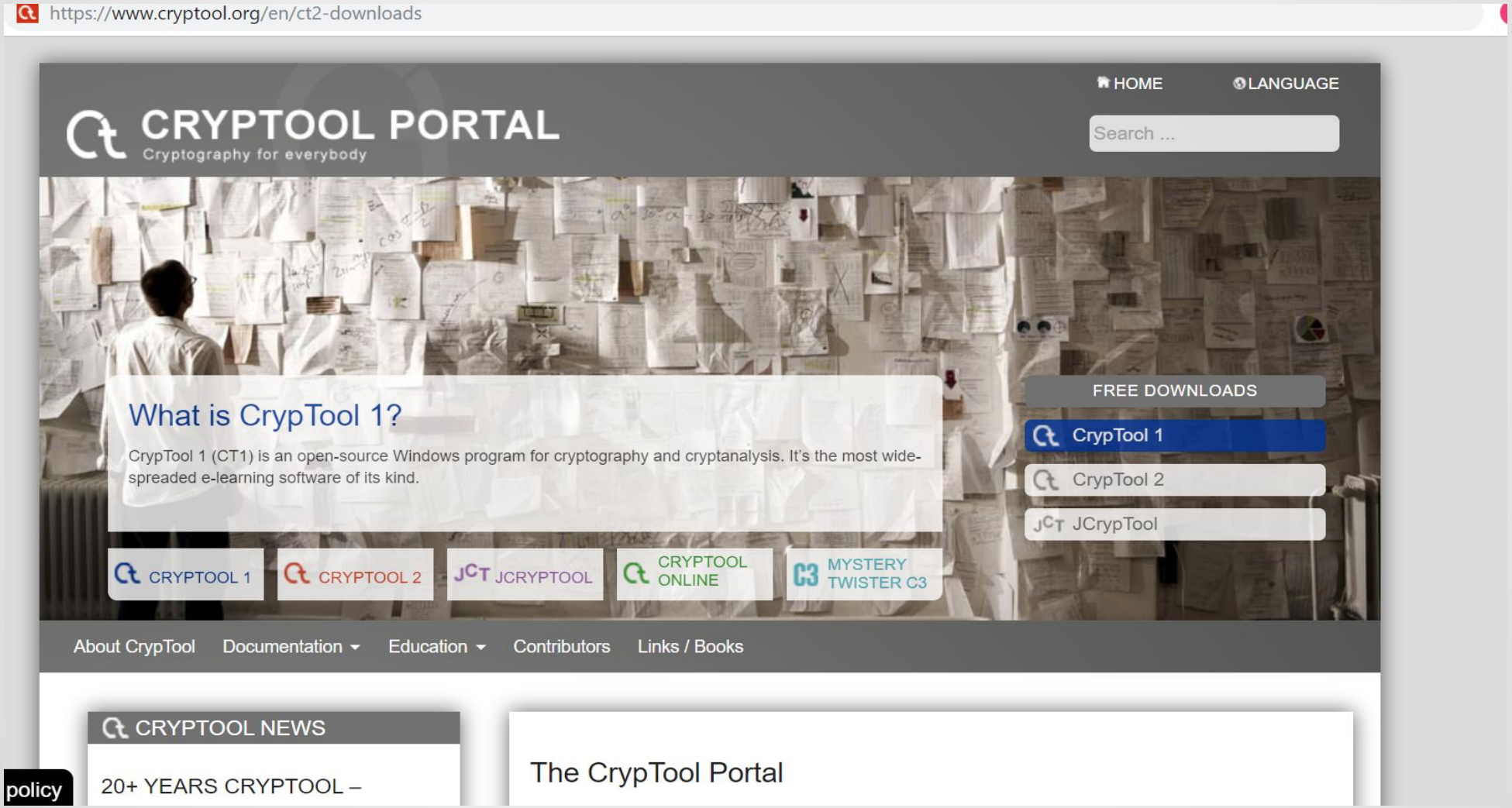
cryptools

Introduction

- It is an open source free software project started by German universities and few companies in 1998. It became open source in 2001.
- Its main aim is to define and understand the concept of cryptography and cryptanalysis .
- It not only supports traditional cryptography it also supports modern cryptography. Near about 400 cryptography algorithm is being supported by this tools.
- In addition it also contains didactical games like number shark and tutorial like primes, elementary cryptography and lattice cryptography.

Working of Cryptool

- Its official site is https://www.cryptool.org/en/.

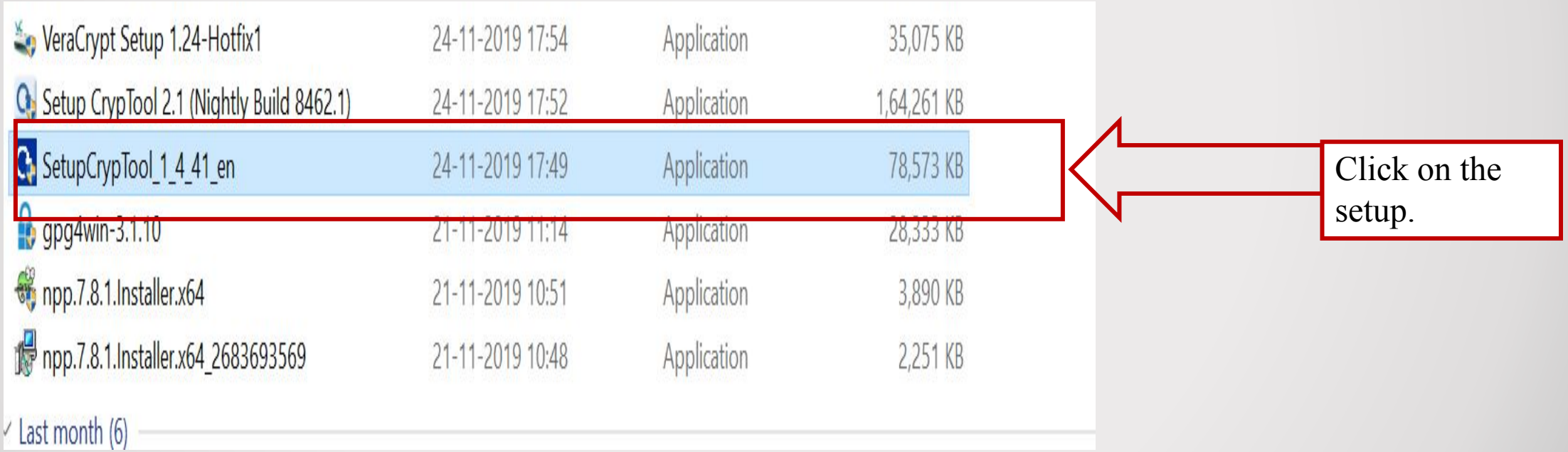


Cryptool1

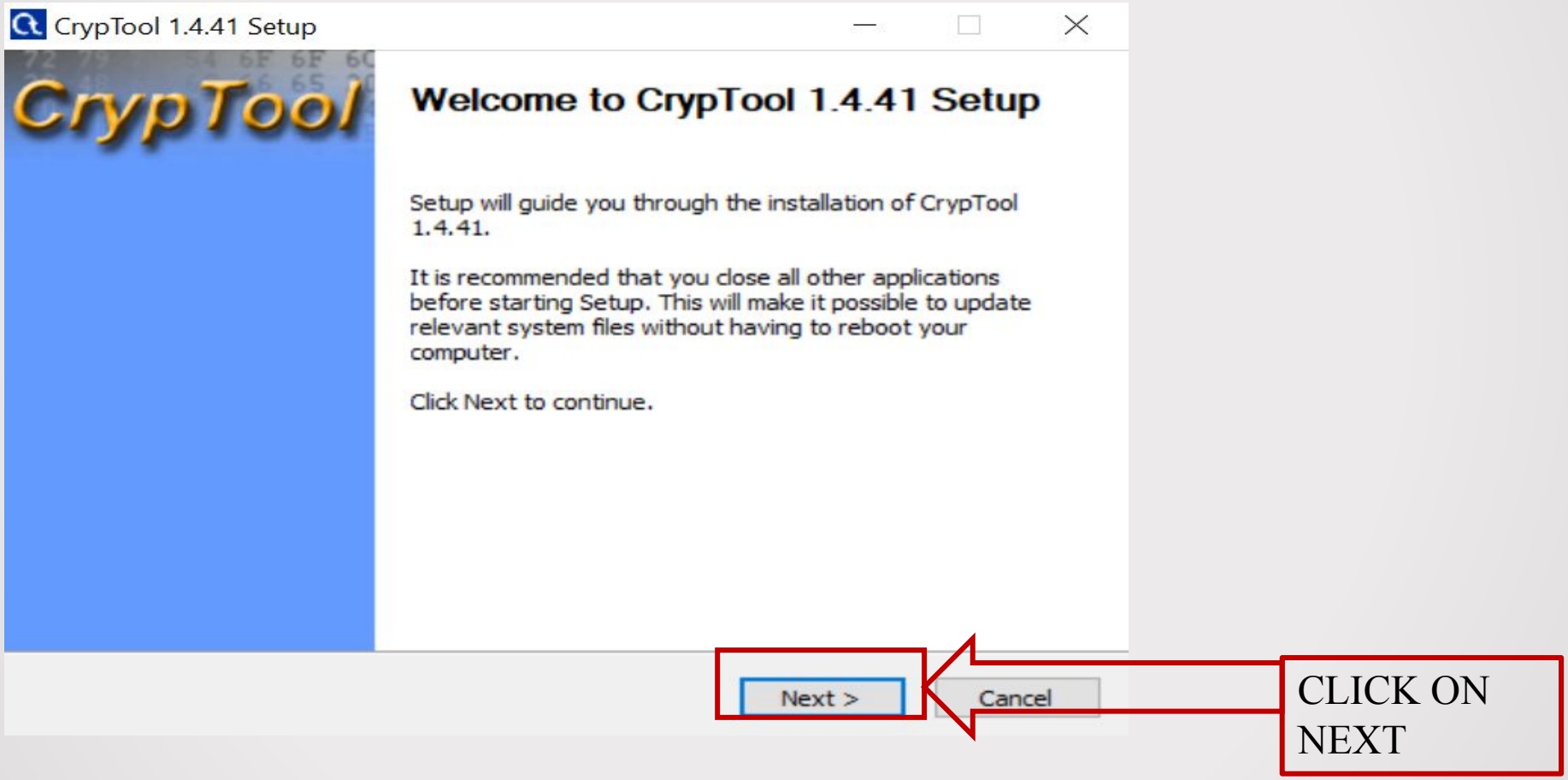
- **Cryptool 1 (CT1)** is a free Windows program for cryptography and cryptanalysis.
- CT1 supports both contemporary teaching methods at schools and universities as well as awareness training for employees and civil servants.
- The current version of Cryptool 1 offers among other things: Numerous classic and modern cryptographic algorithms (encryption and decryption, key generation, secure passwords, authentication, secure protocols, etc.)
- Visualization of several algorithms (Caesar, Enigma, RSA, Diffie-Hellman, digital signatures, AES, etc.)
- Cryptanalysis of several algorithms (Vigenère, RSA, AES, etc.)
- Crypt analytical measurement methods (entropy, n-grams, autocorrelation, etc.)
- Related auxiliary methods (primality tests, factorization, base64 encoding, etc.)

- To get detail documentation and idea :https://www.cryptool.org/en/ct1-screenshots/screenshots
- Lets see how it works

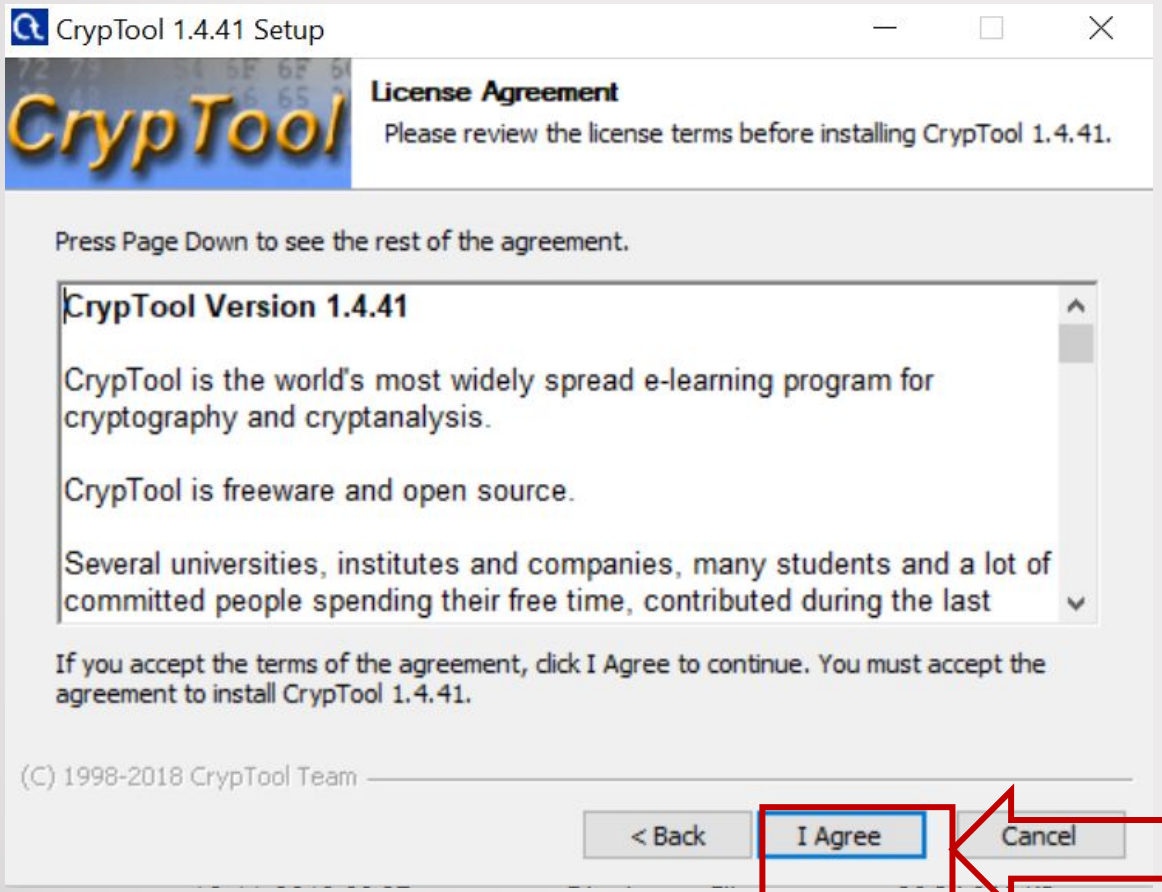
Step 1:-To download the cryptool1:- https://www.cryptool.org/en/ct1-downloads



STEP 2:- :- Follow the step of installation by clicking next



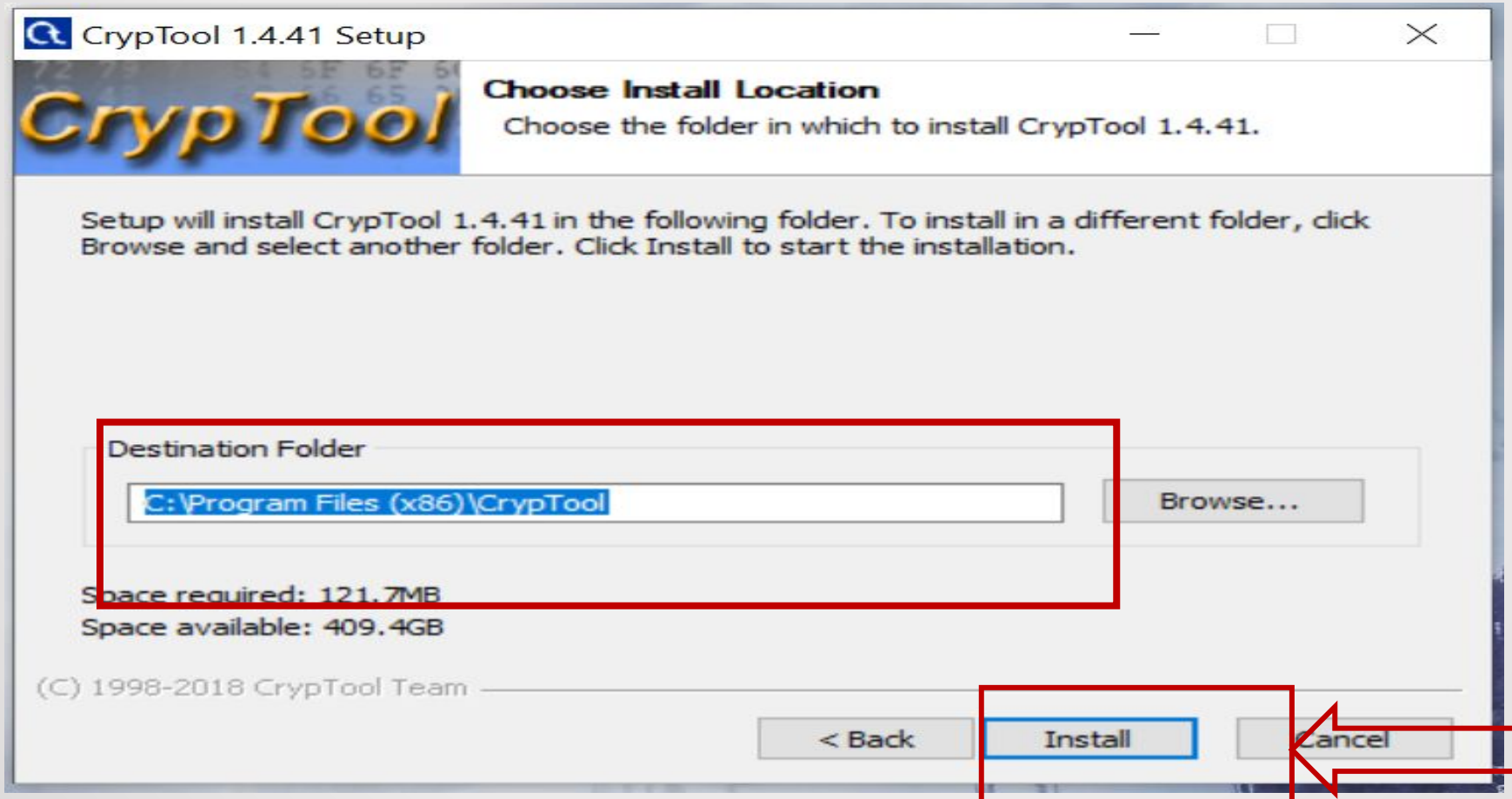
Step 3:- Agreement of license



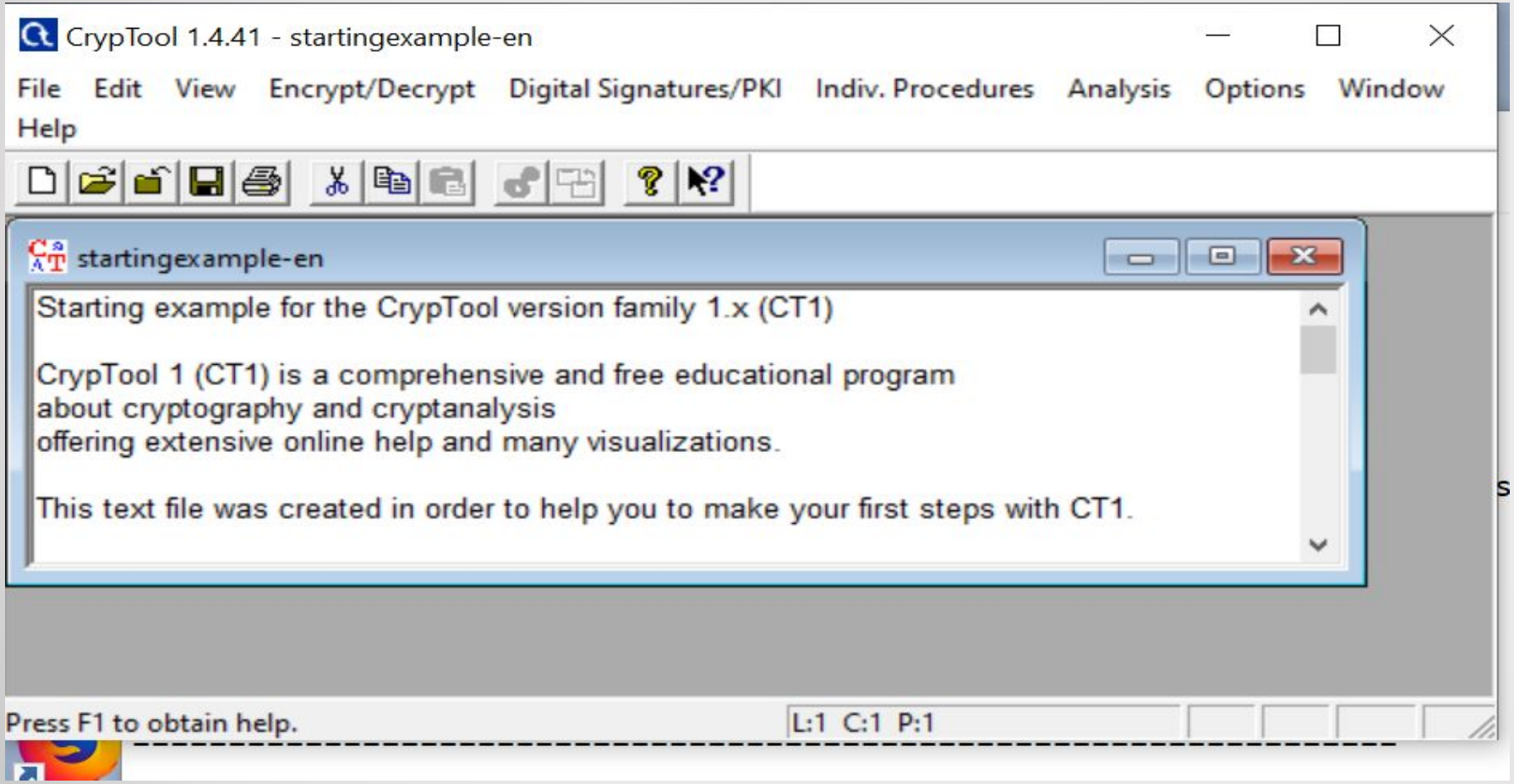
Click on “I Agree”

Step 4:- What type of installation you need?

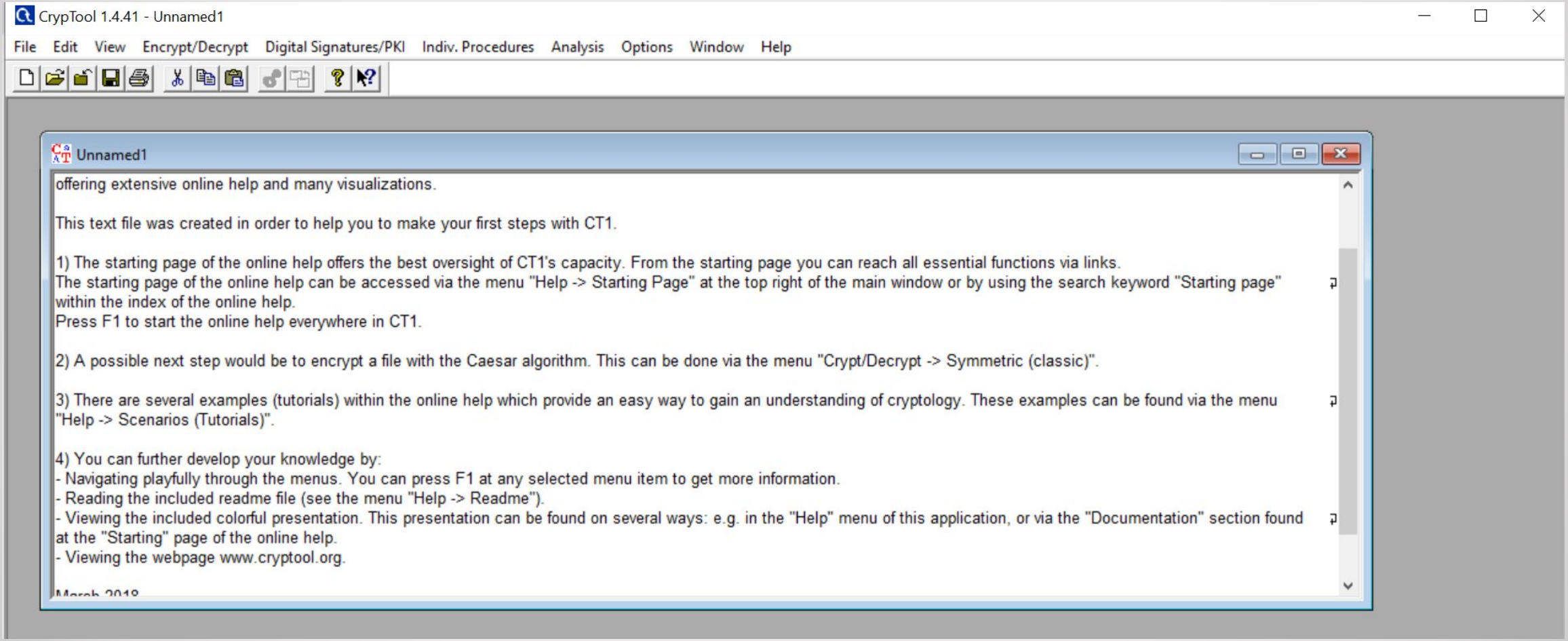
Step 5:- Set up the path:-



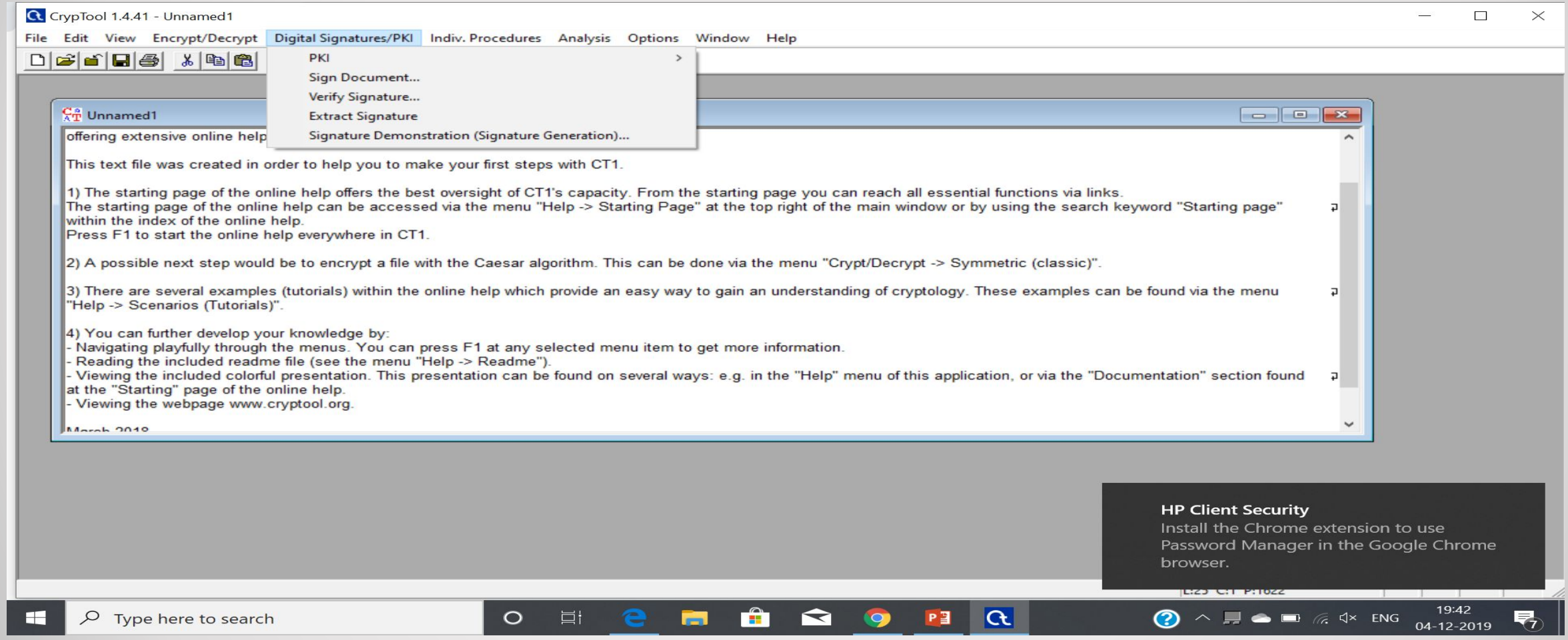
Step 6 :- We get the wizard page



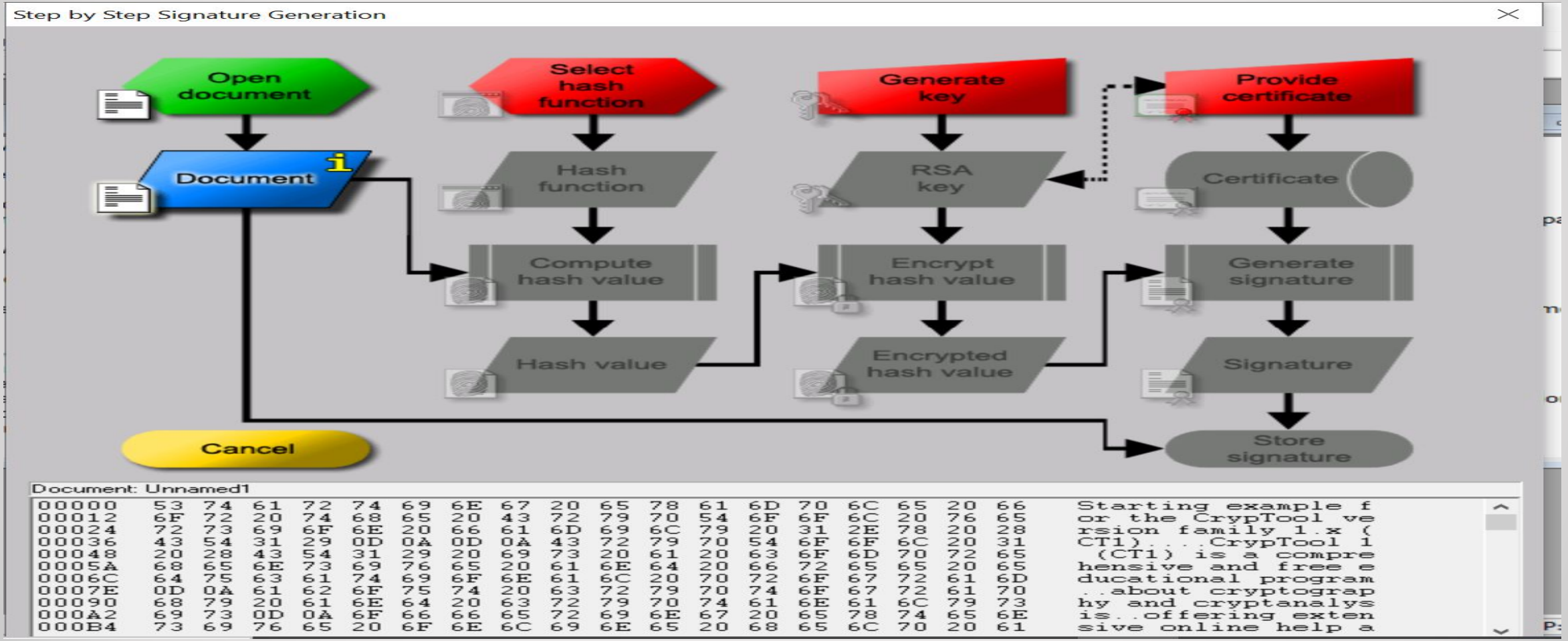
STEP 7:- CLICK ON NEW TO CREATE A WORKSPACE



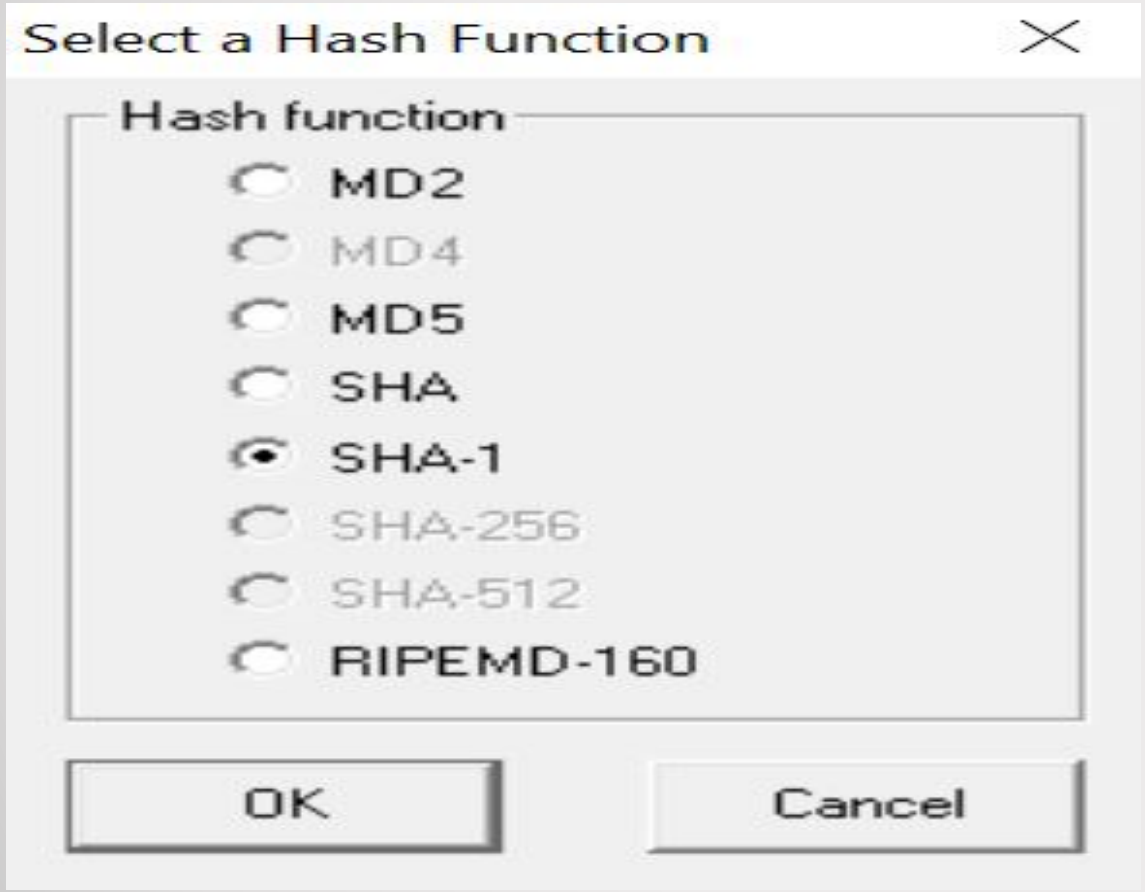
STEP8:- AFTER CREATING THE WORKSPACE COPY OR WRITE A TEXT MESSAGE

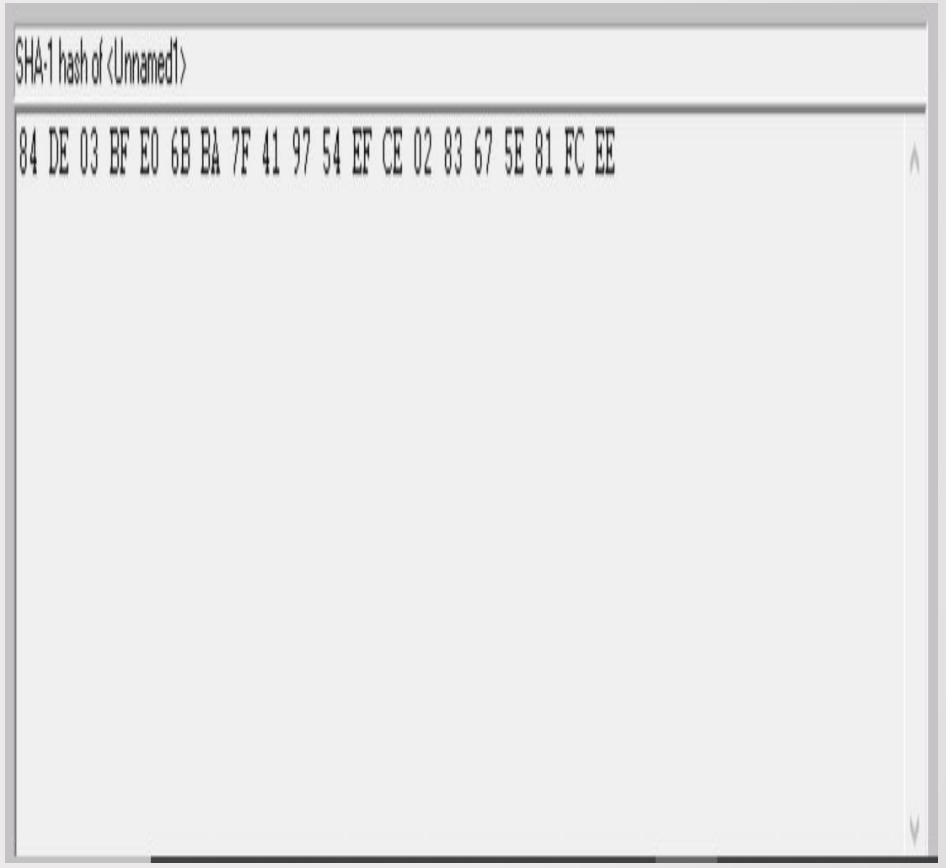


EXAMPLE OF DIGITAL SIGNATURE

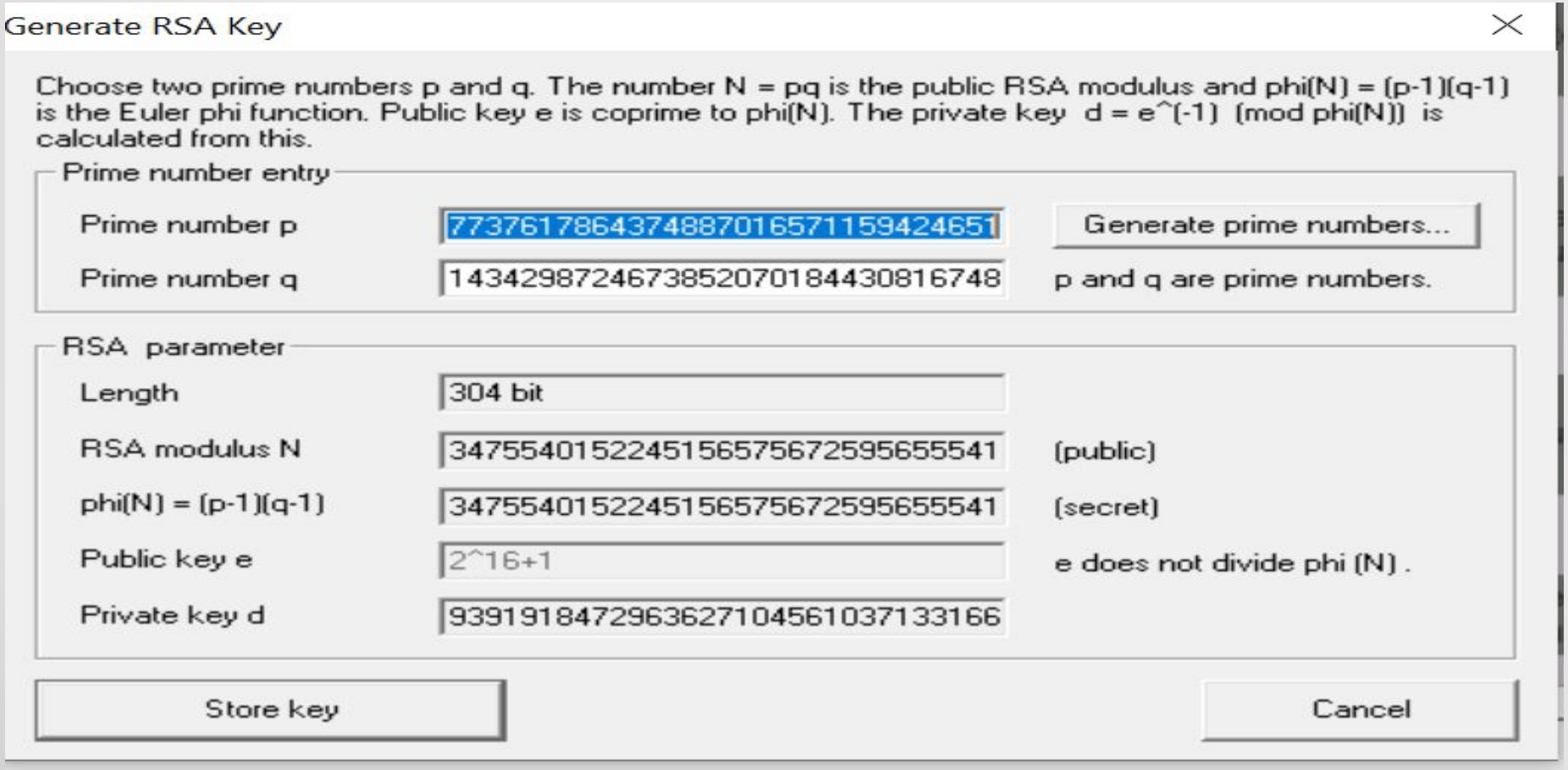


HASH FUCTION USED AND ITS VALUE

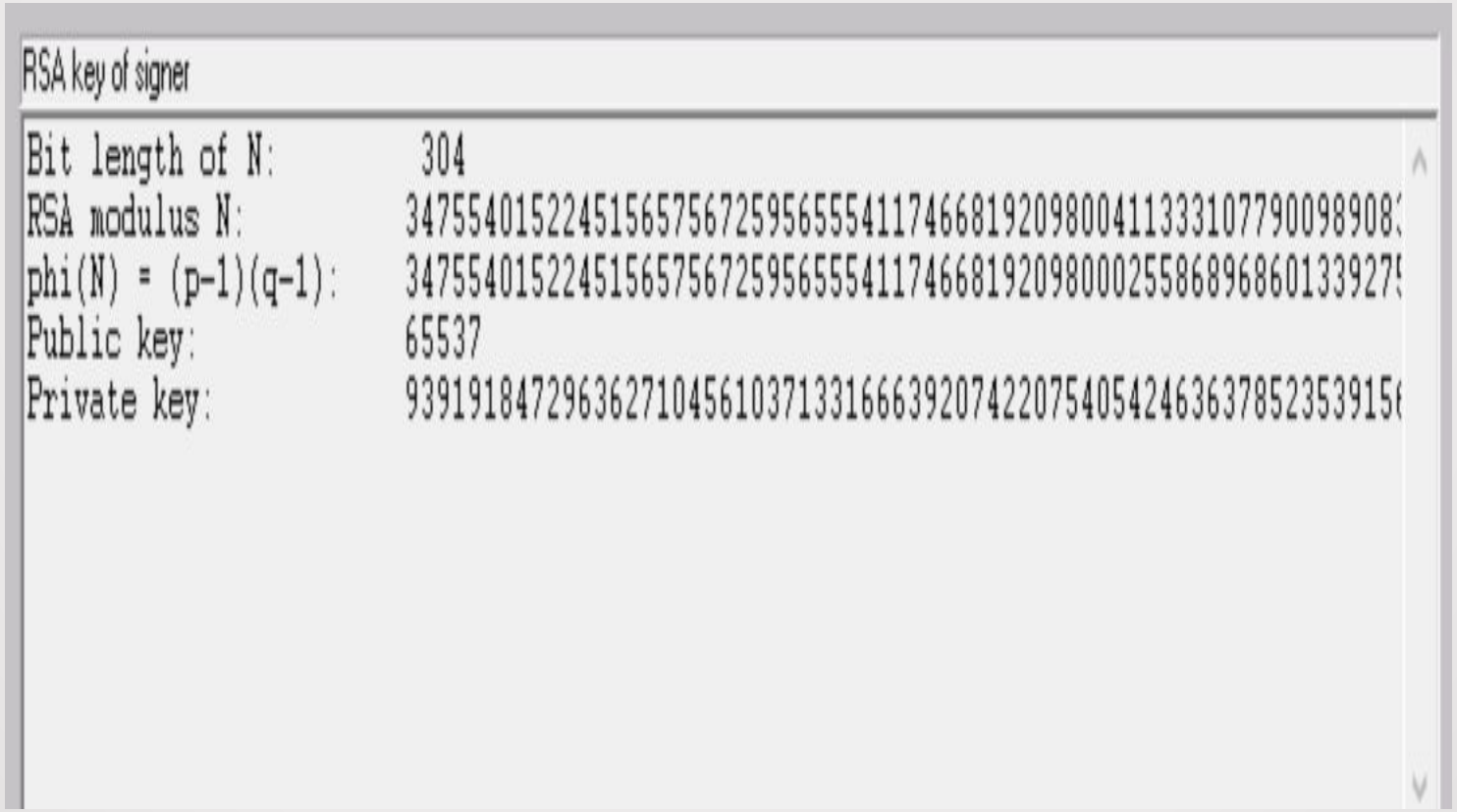




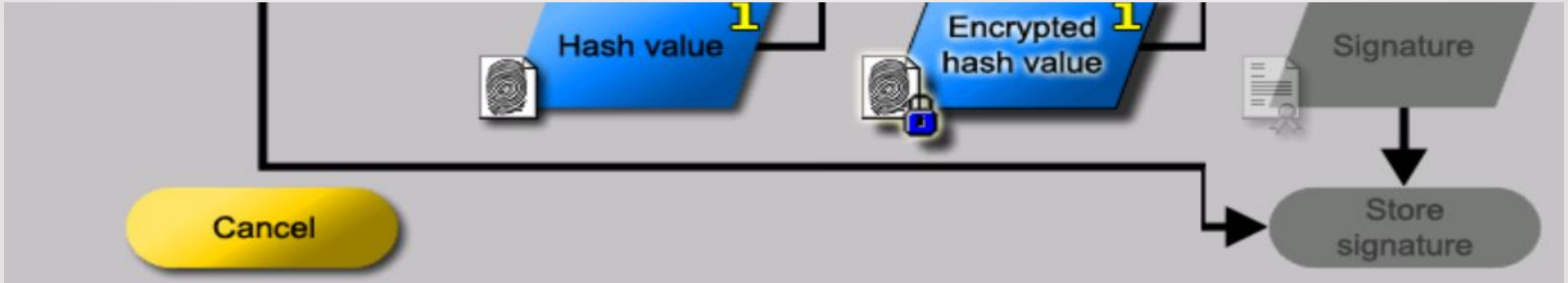
SIGNING ALGORITHIM(RSA)



RSA KEY OF SIGNER



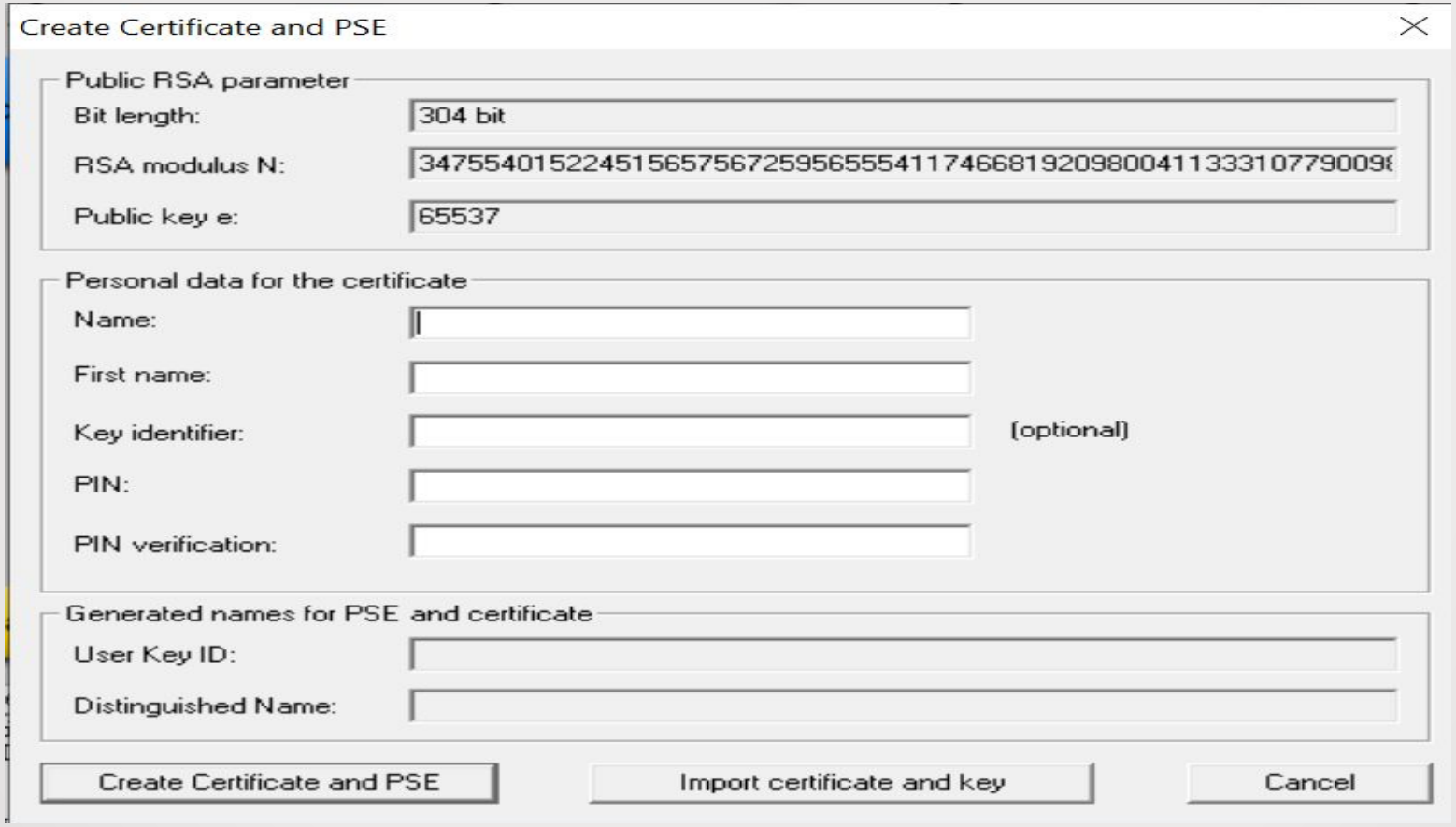
HASH VALUE ENCRYPTED WITH SIGNER PRIVATE KEY



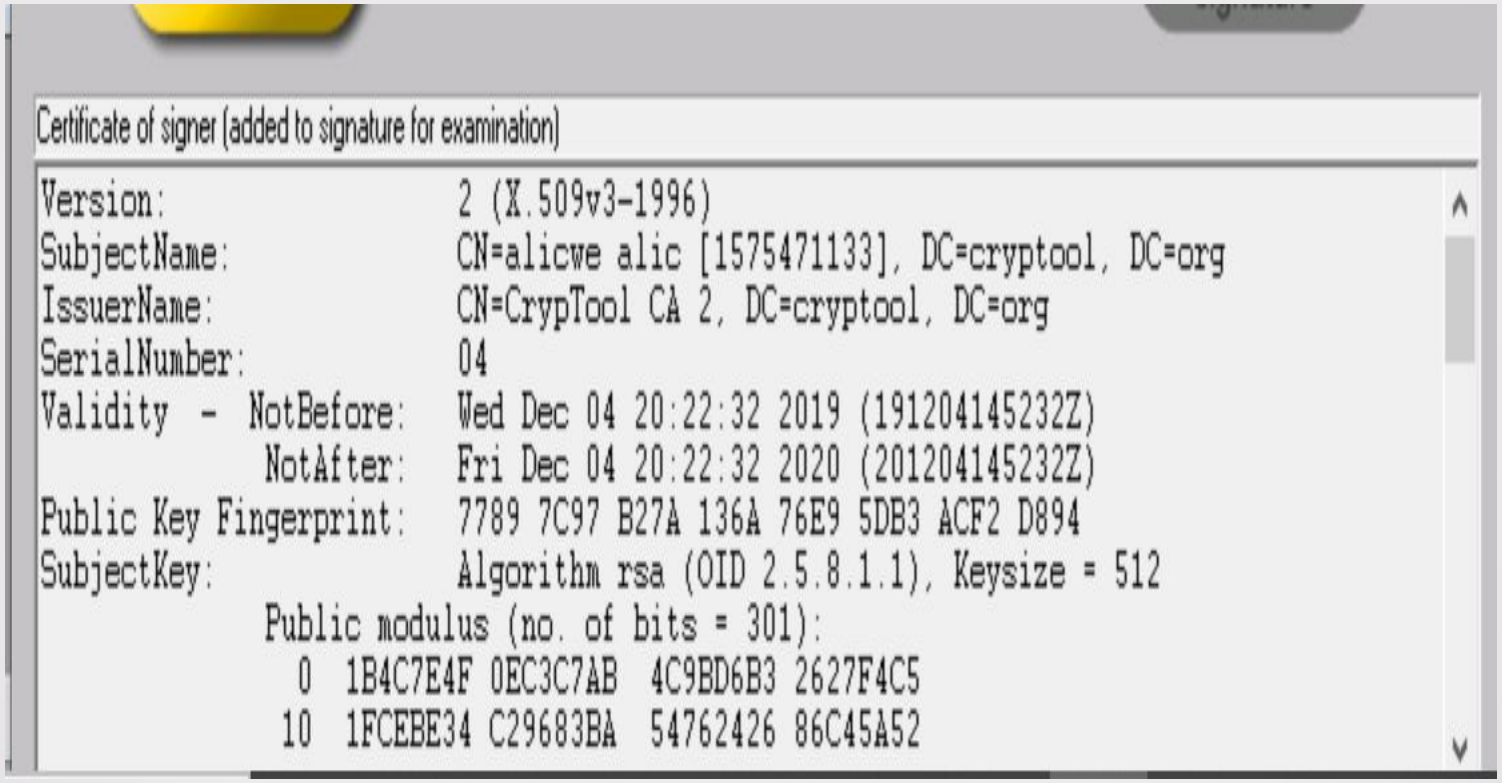
Hash value encrypted with the private key of the signer

```
Padding string:          01 00
Algorithm ID:            30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14
Hash value:              84 DE 03 BF E0 6B BA 7F 41 97 54 EF CE 02 83 67 5E 81 FC EE

ASN-1 hash value:        01 00 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 84 DE 03 E
Length in bits:          296

Encrypted hash value:    17 65 D0 0E B0 E7 26 9D 3C A8 A0 5E CF 1A 6B E4 42 65 FF 5D 8
Length in bits:          304
```

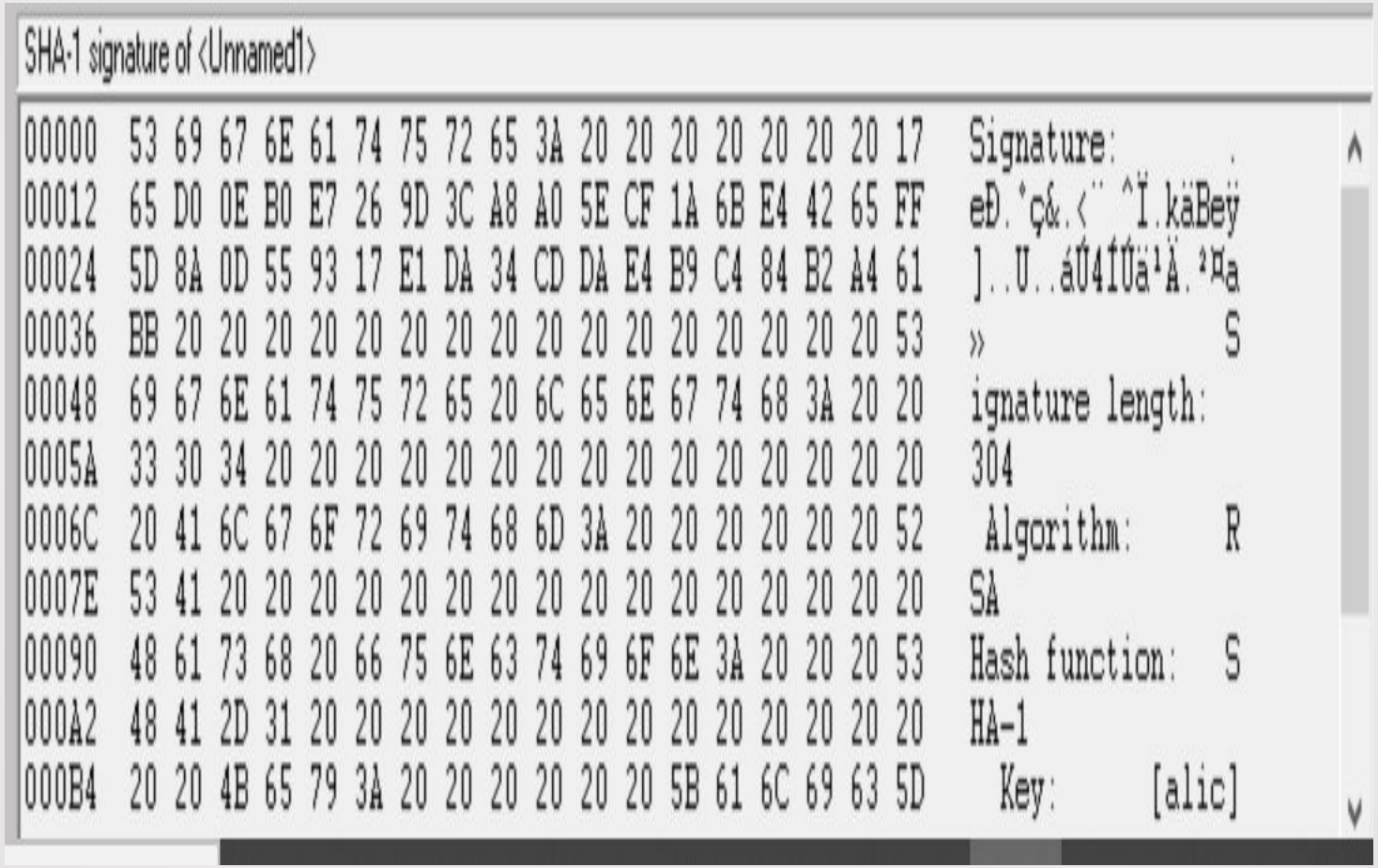
CREATION OF CERTIFICATE



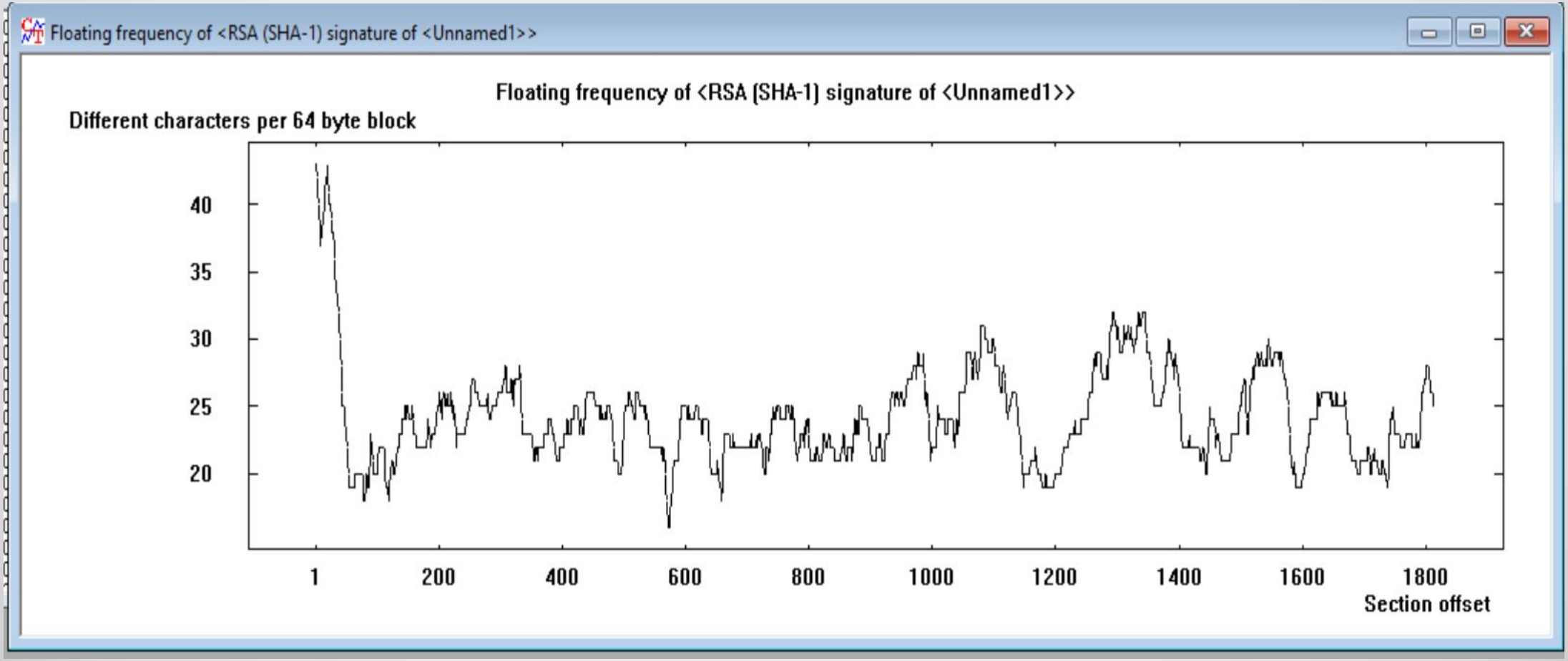
SIGNATURE VERIFICATION



GENRATED SIGNATURE

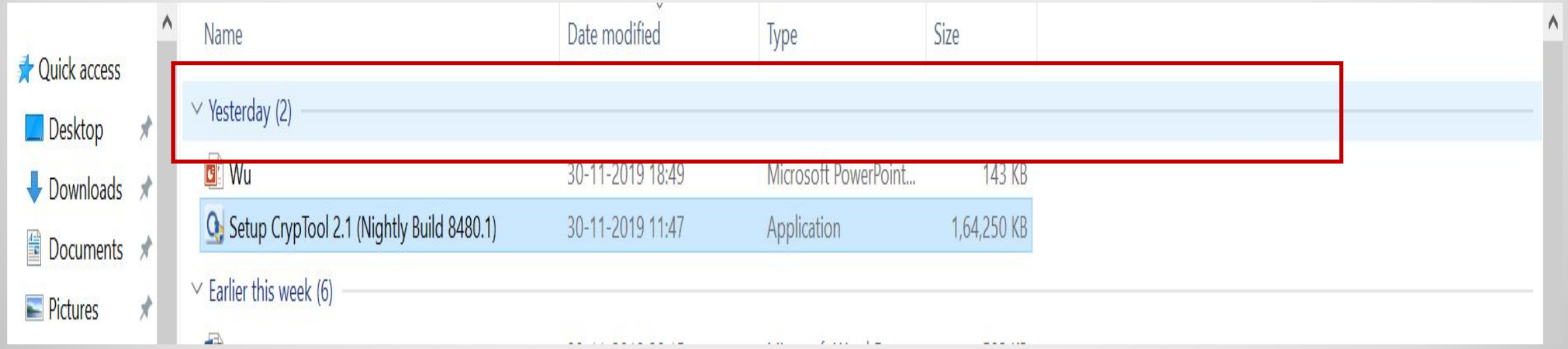


FREQUENCY ANALYSIS

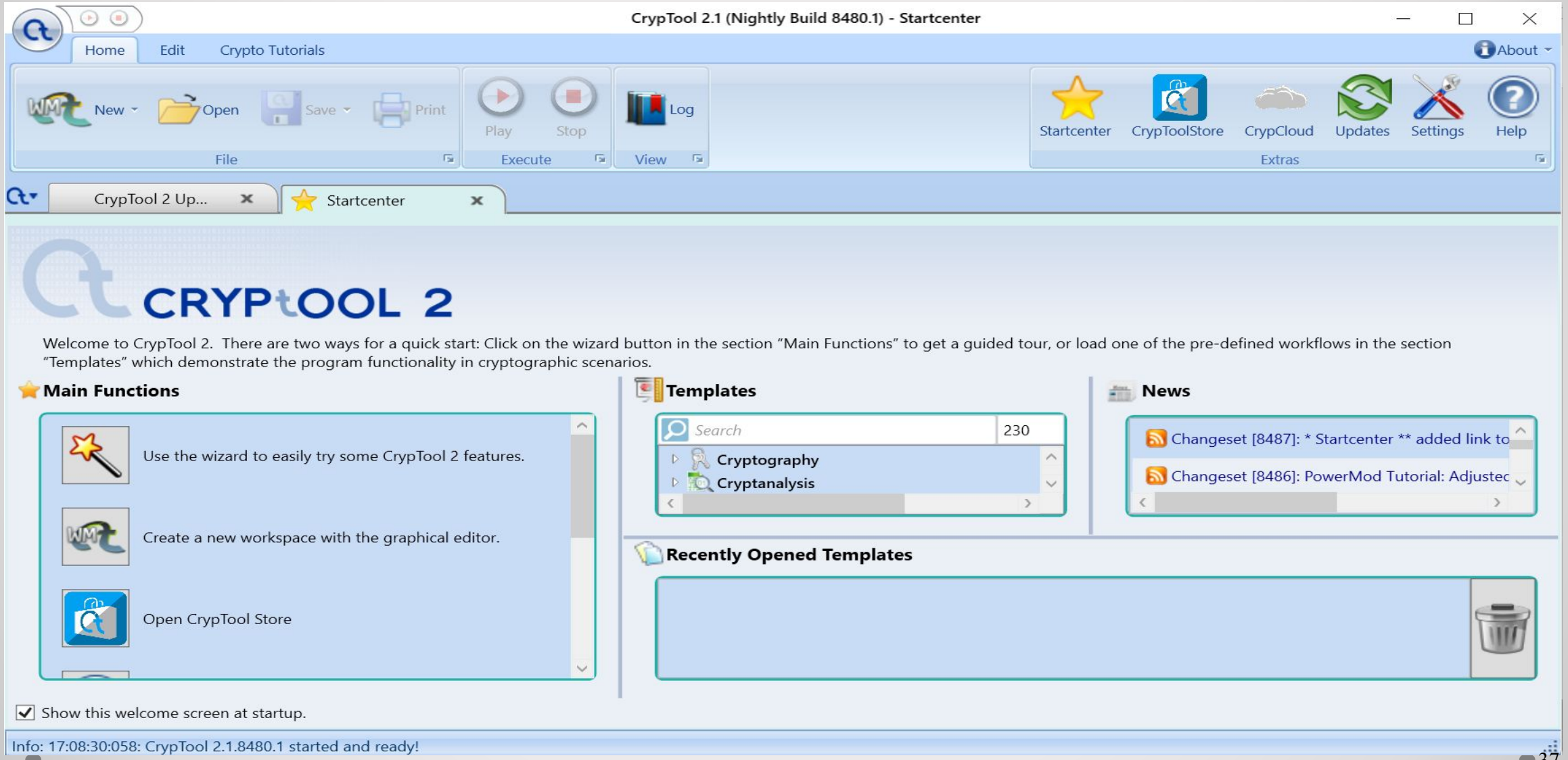


Cryptool 2

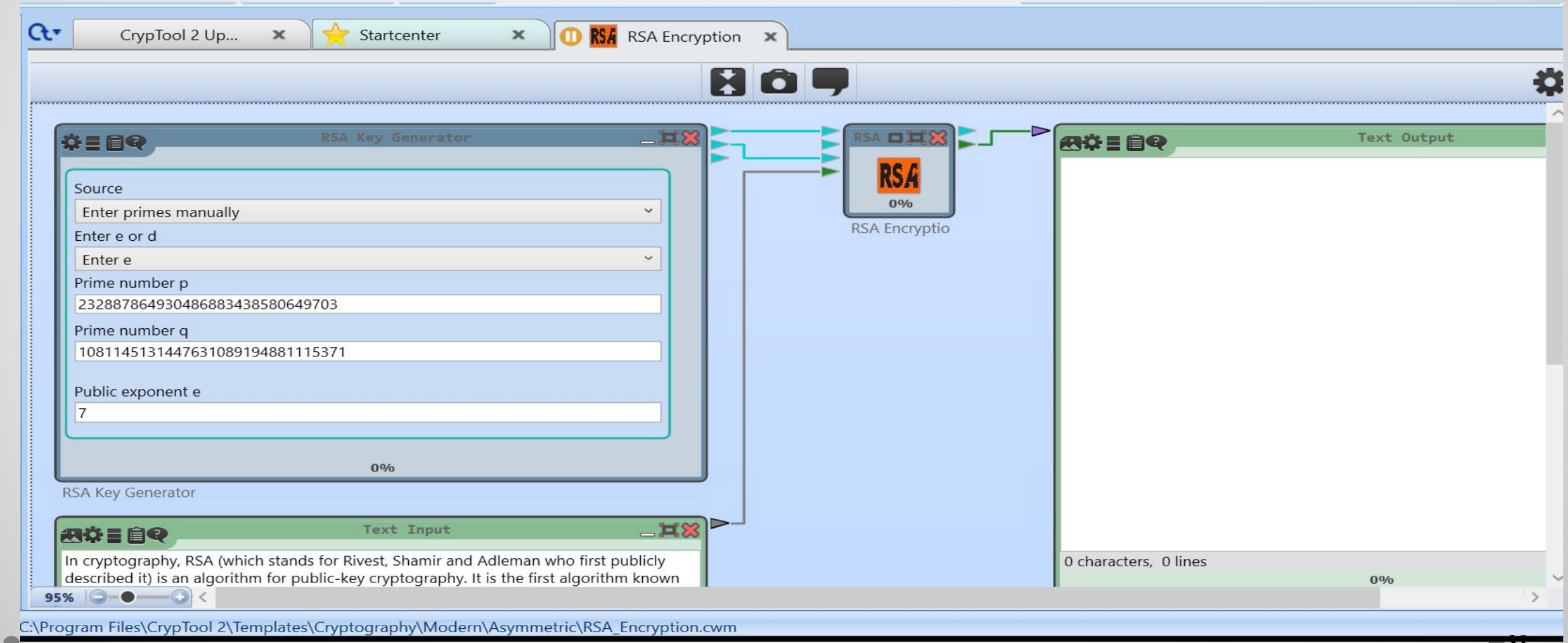
- It uses the concept of visual programming to clarify cryptographic processes. Currently, CT2 contains more than 150 crypto functions.
- To download it:-https://www.cryptool.org/en/ct2-downloads
- After download we get:-



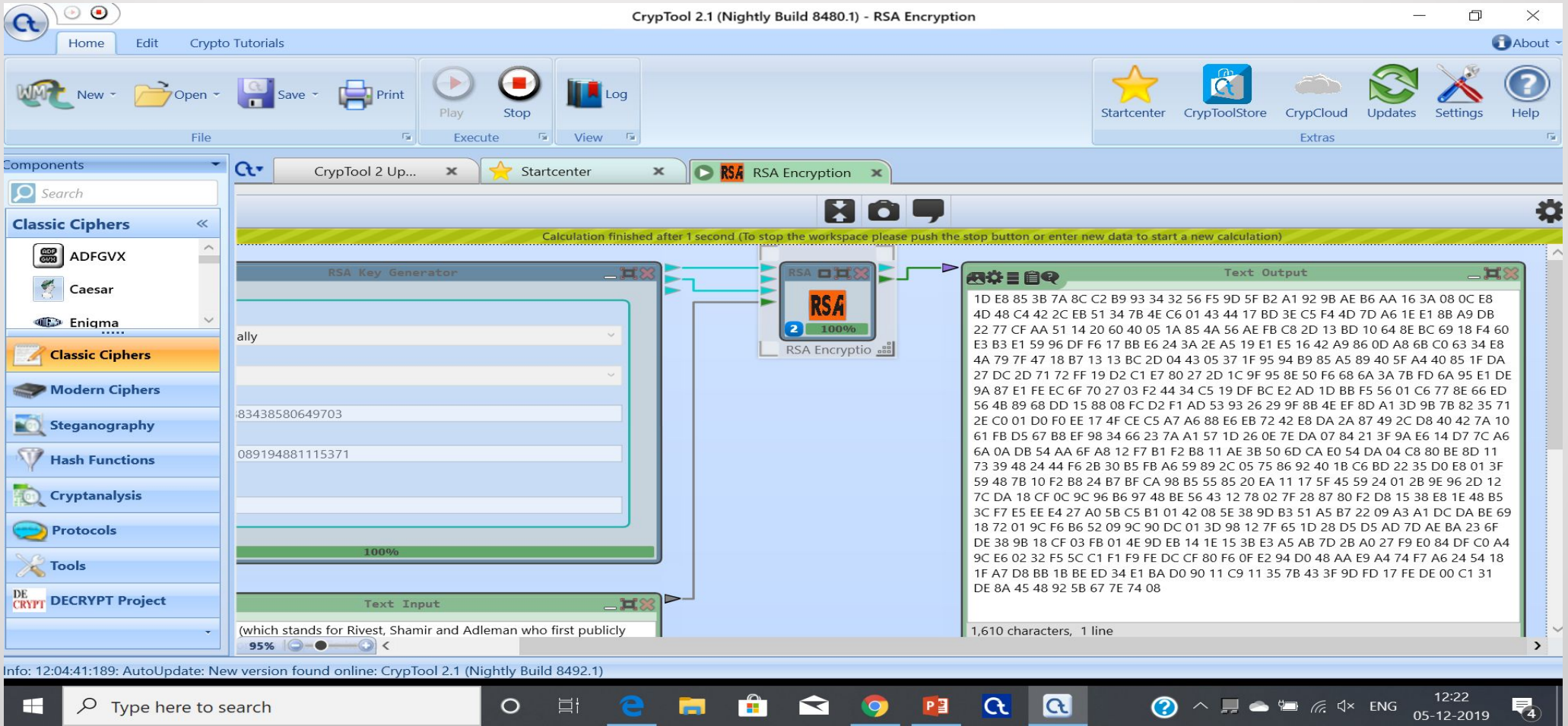
- For installation I will proceed in the same manner as cryptool-1.



WORKING WITH CRYPTOOL USING RSA



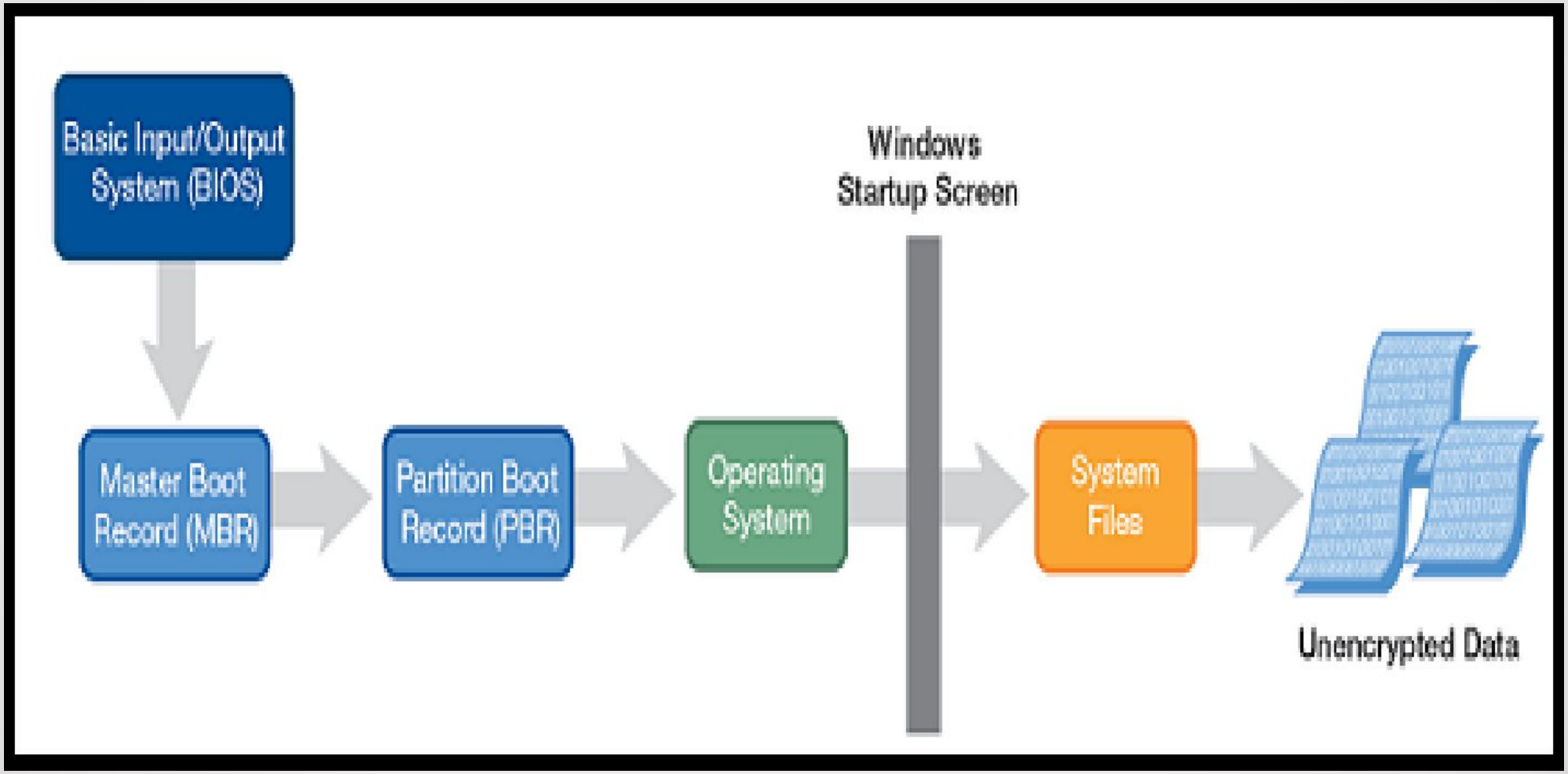
RESULT AFTER CLICKING PLAY



Disk and File Encryption

- **Disk encryption** is a technology which protects information by converting it into unreadable code .
- Disk encryption usually includes all aspects of the disk, including directories, so that an adversary cannot determine content, name or size of any file.
- It is well suited to portable devices such as laptop computers and thumb drives which are particularly susceptible to being lost or stolen.
- If used properly, someone finding a lost device cannot penetrate actual data, or even know what files might be present.

System startup



FILE ENCRYPTION

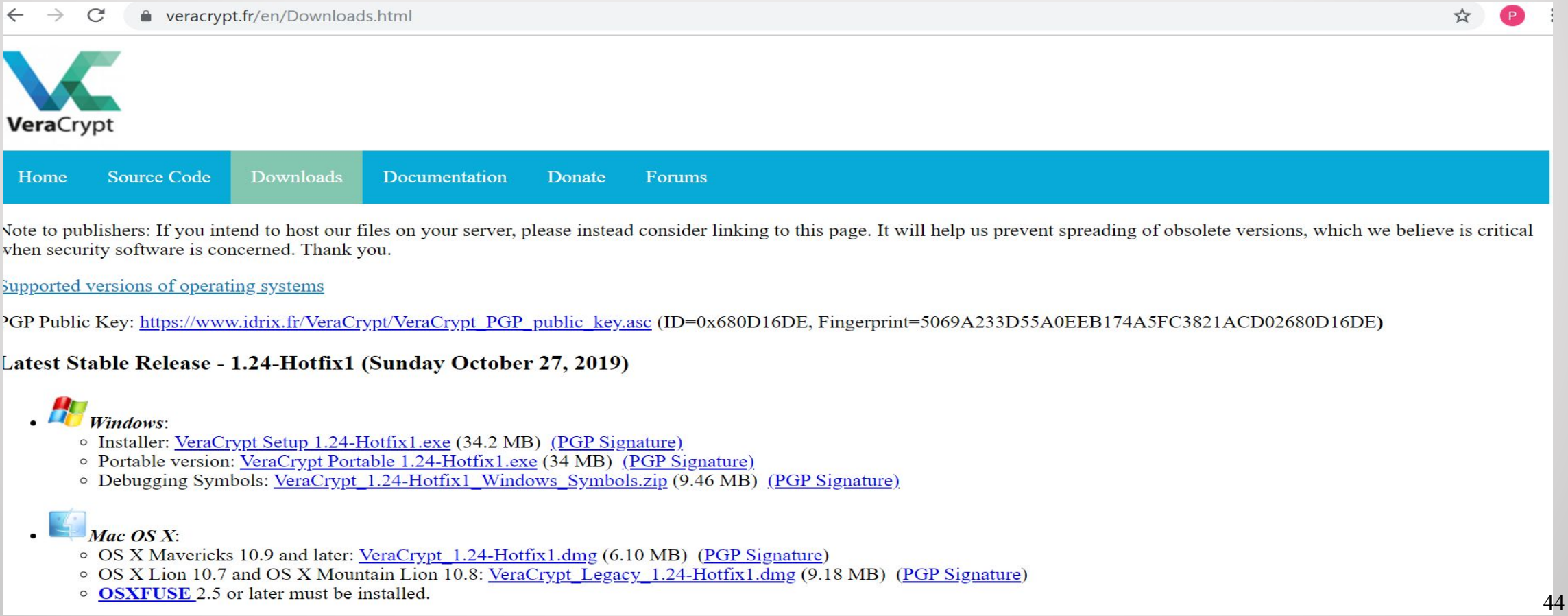
- The **Encrypting File System** (**EFS**) on Microsoft Windows is a feature introduced in version 3.0 of NTFS.
- The technology enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer.

Veracrypt

- VeraCrypt is a full disk and partition encryption system that gives you flexibility and enables you to choose what to encrypt. It uses 256-bit AES encryption.
- Creates a **virtual encrypted disk** within a file and mounts it as a real disk.
- Encryption is **automatic, real-time**(on-the-fly) and **transparent**.
- This software enables you to create two vaults, each with a different password.
- Like True Crypt, VeraCrypt is a free and open source software, so anyone can use it

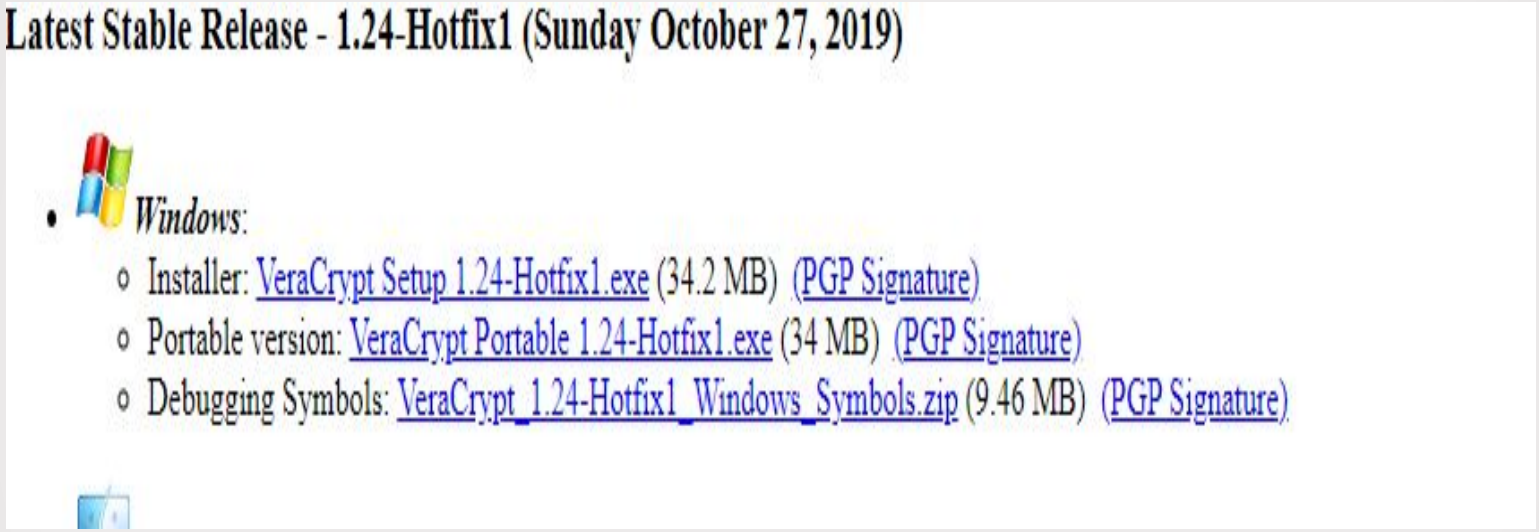
Working with Veracrypt

- To download the software:- https://www.veracrypt.fr/en/Downloads.html



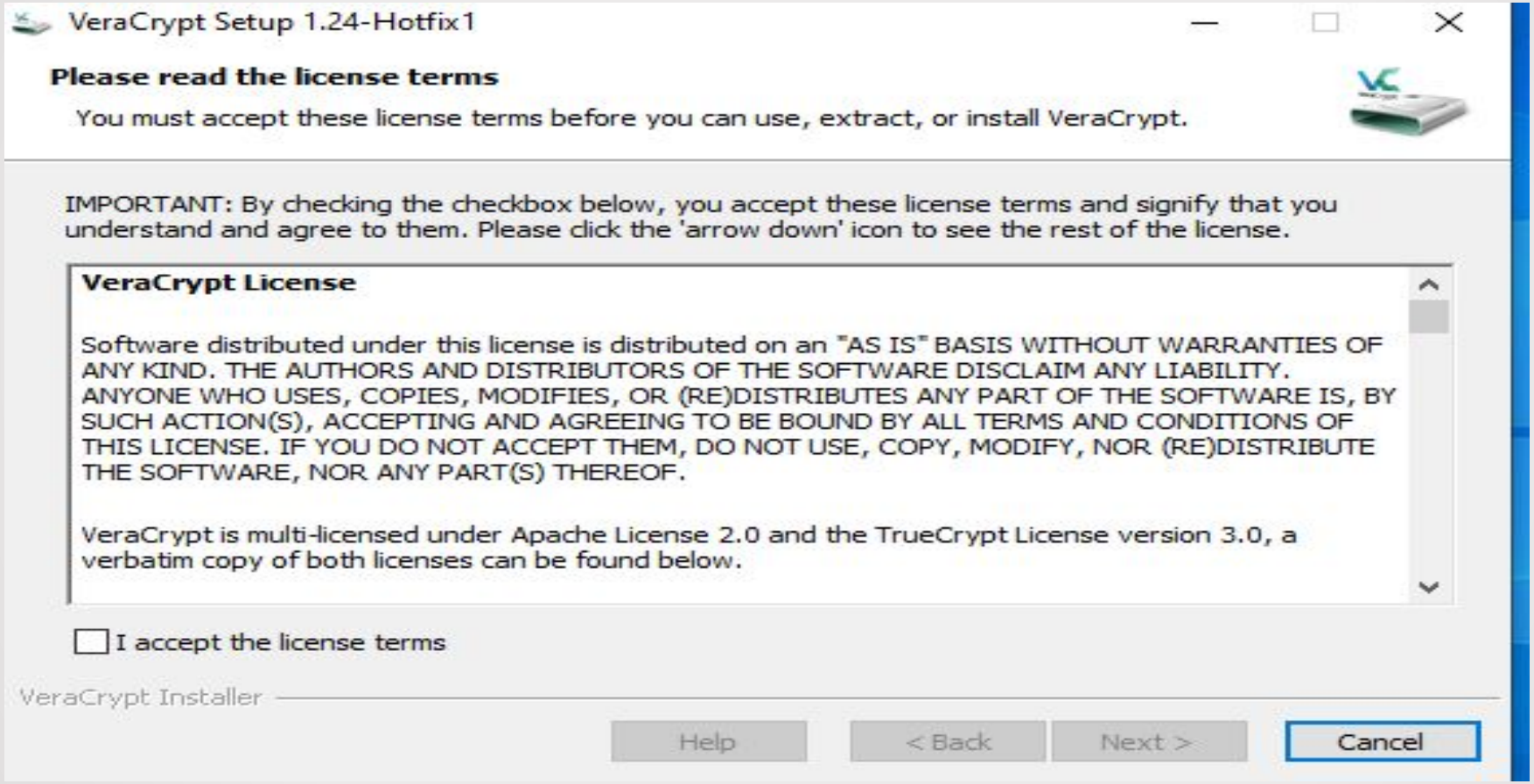
Installation for windows

- Step1:-

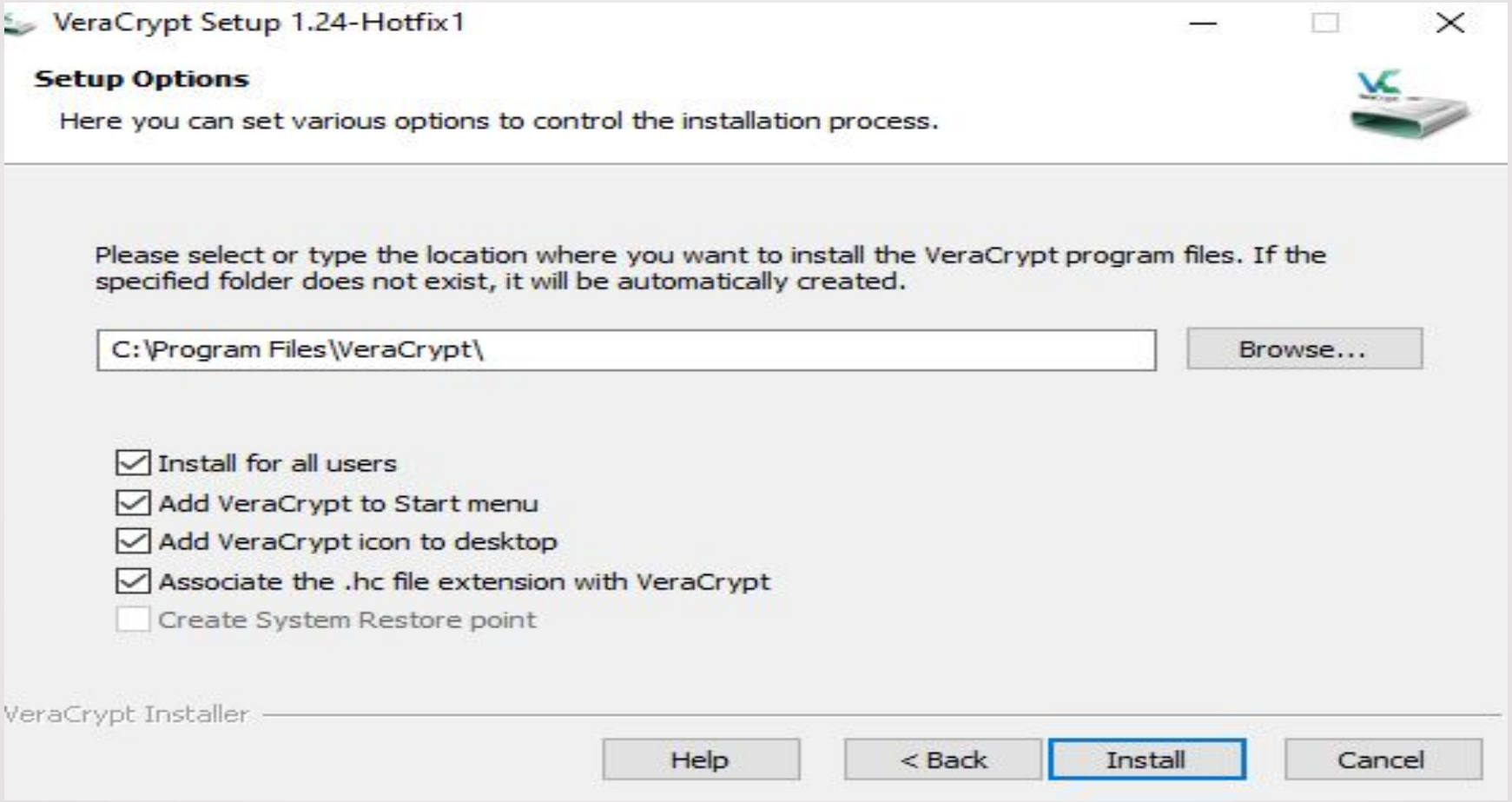


- As soon as it got downloaded and we click on the set up we get the following

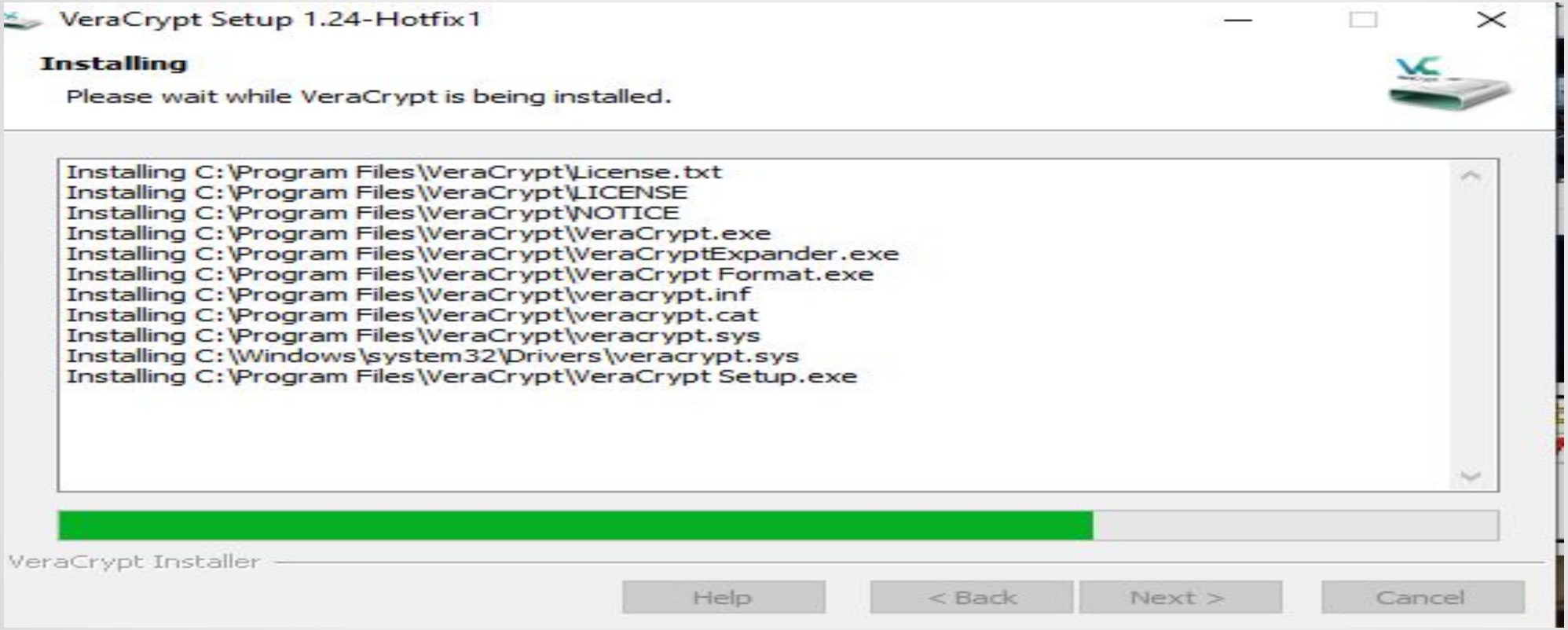
- Step2:- This page is the license agreement:-



- Step 3:- Path setup:-

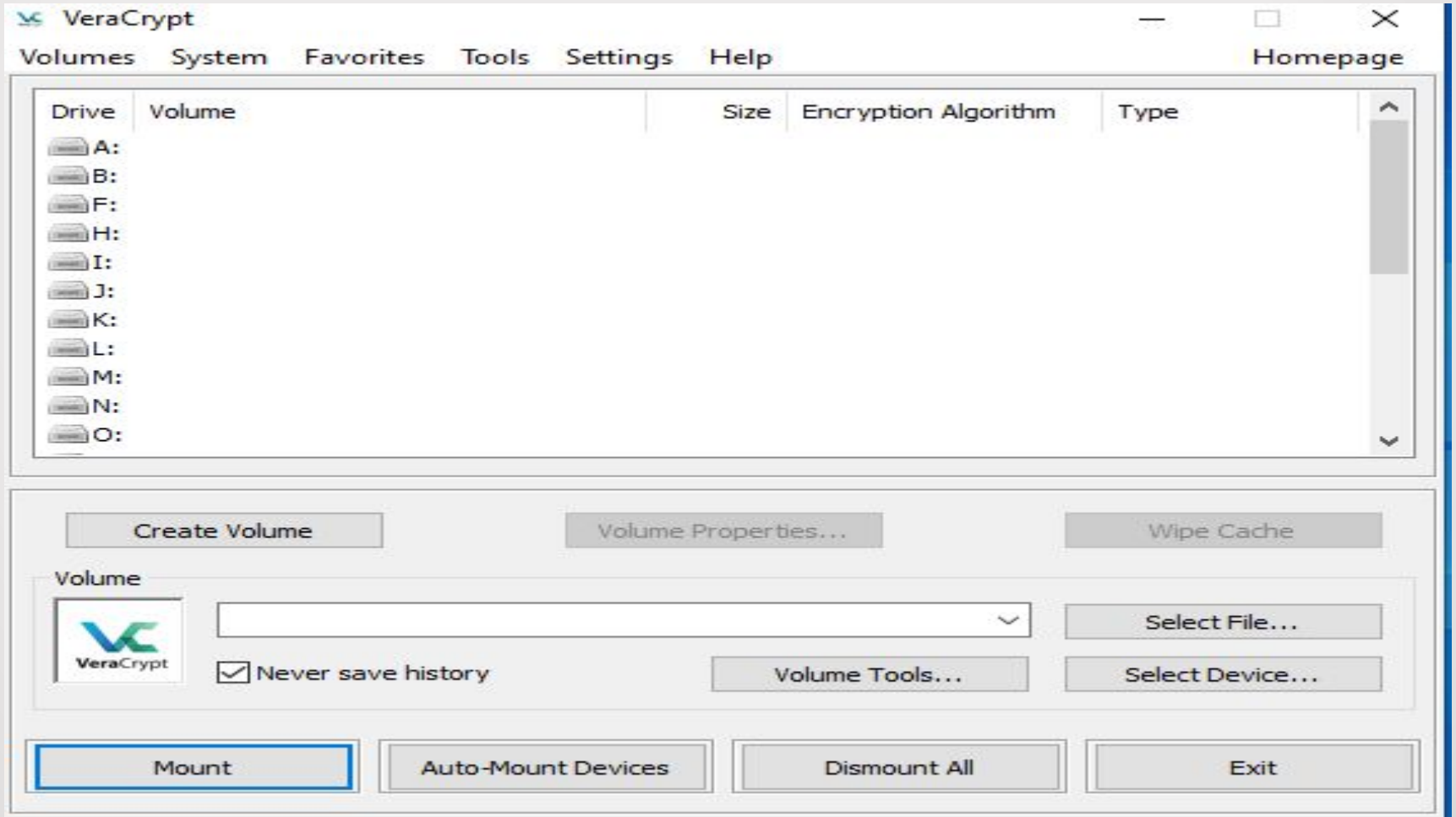


- Now the installation process :-

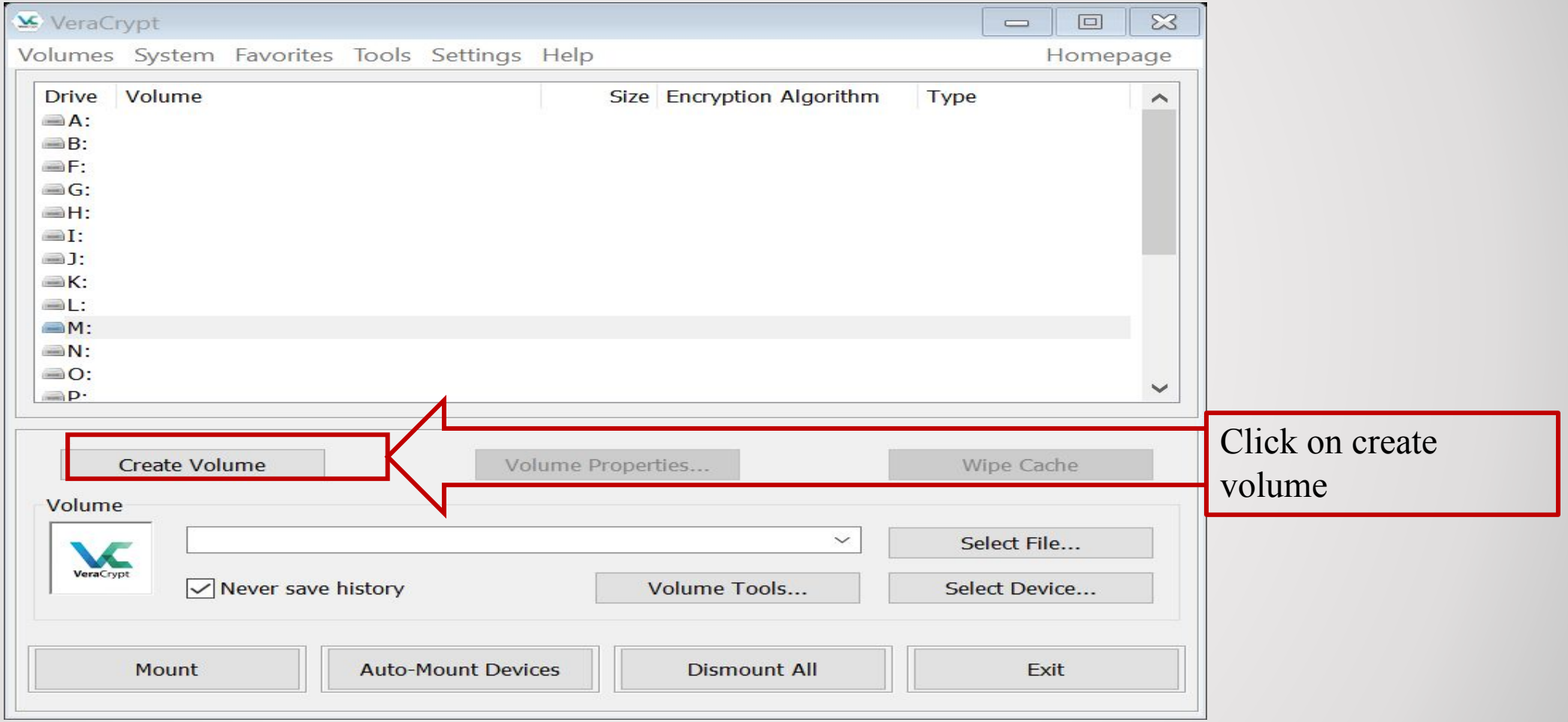


How it works?

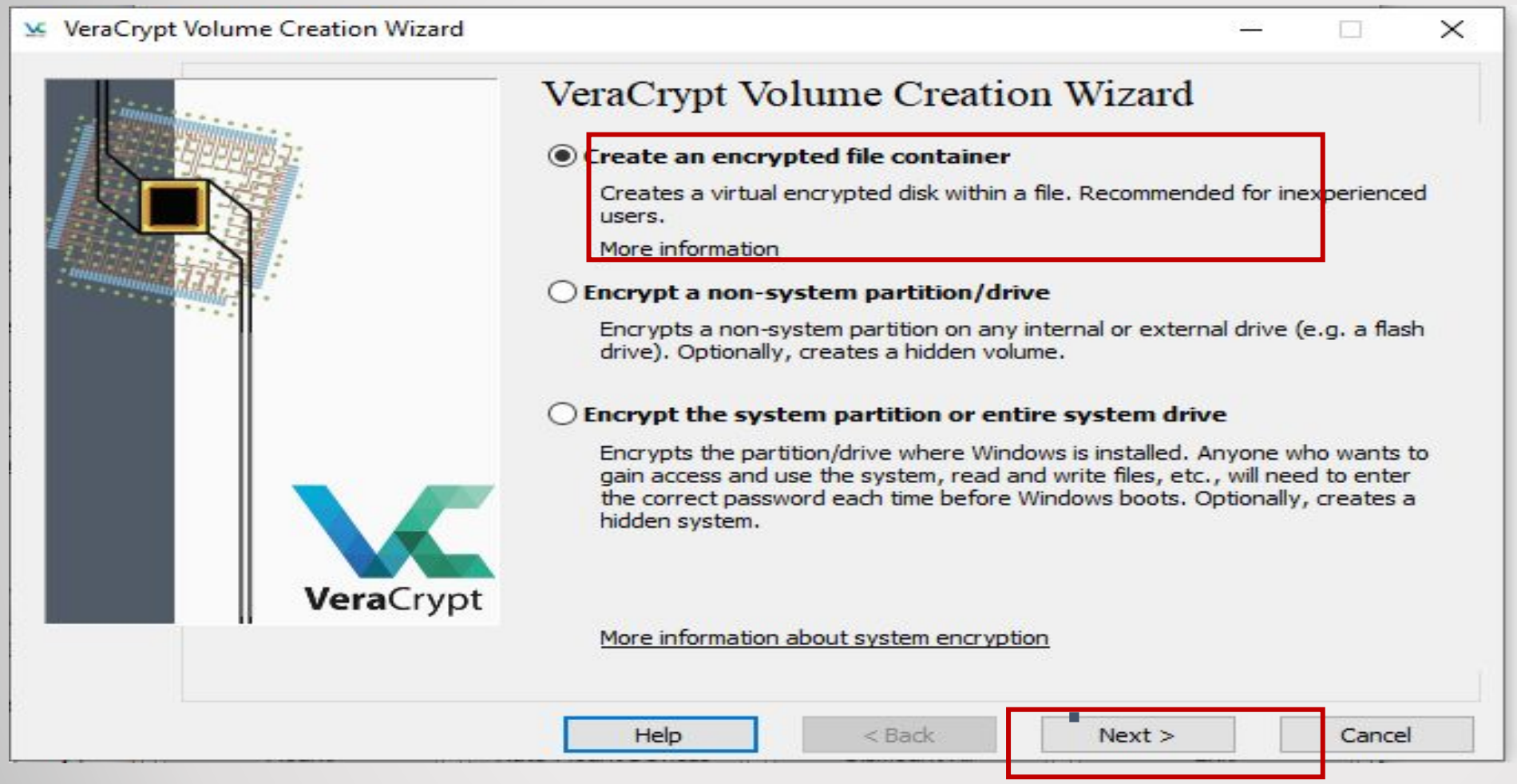
- As soon as we click on veracrypt option



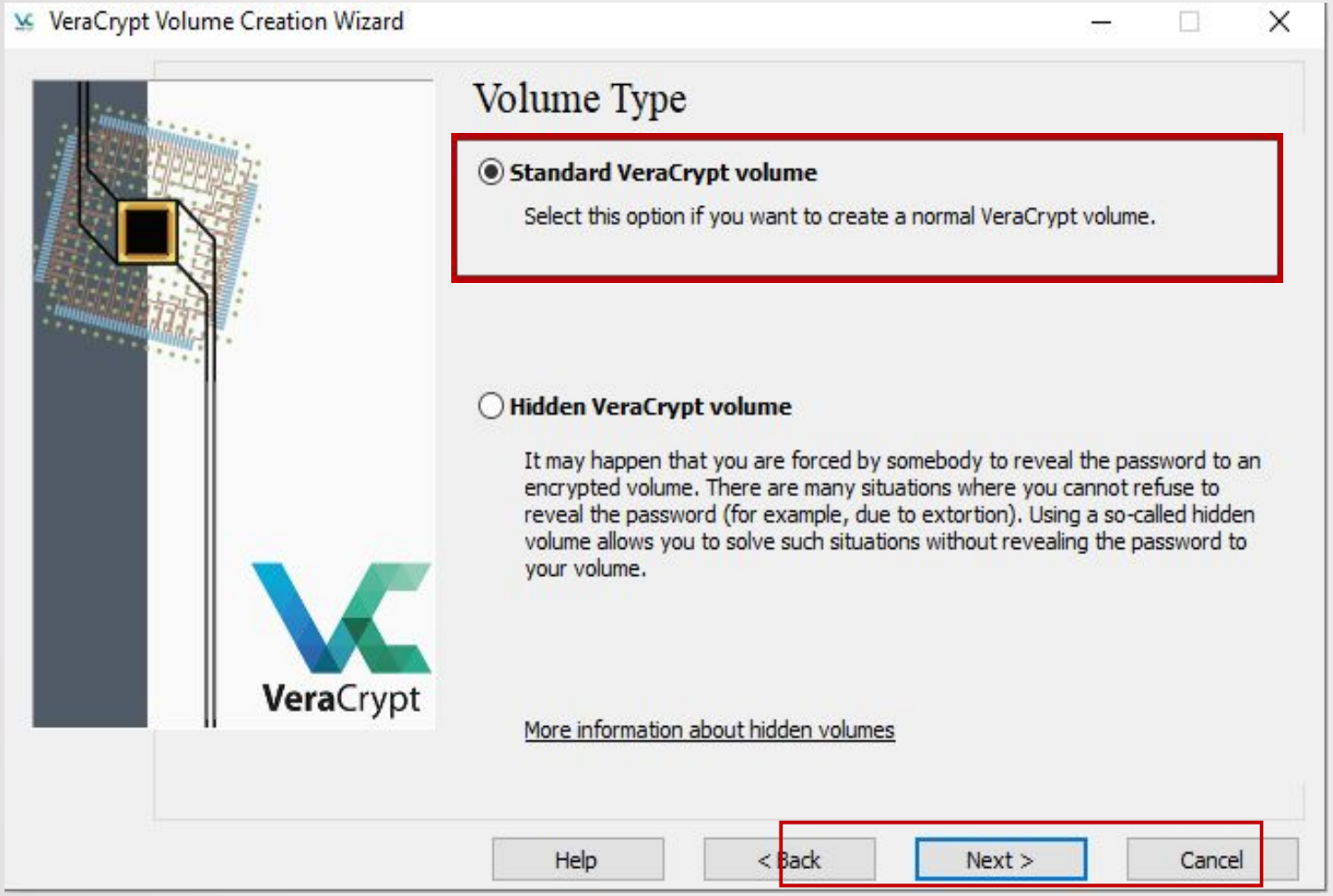
- Step1:- we will create a volume:-



- Step2 :- for the encrypted file container:-



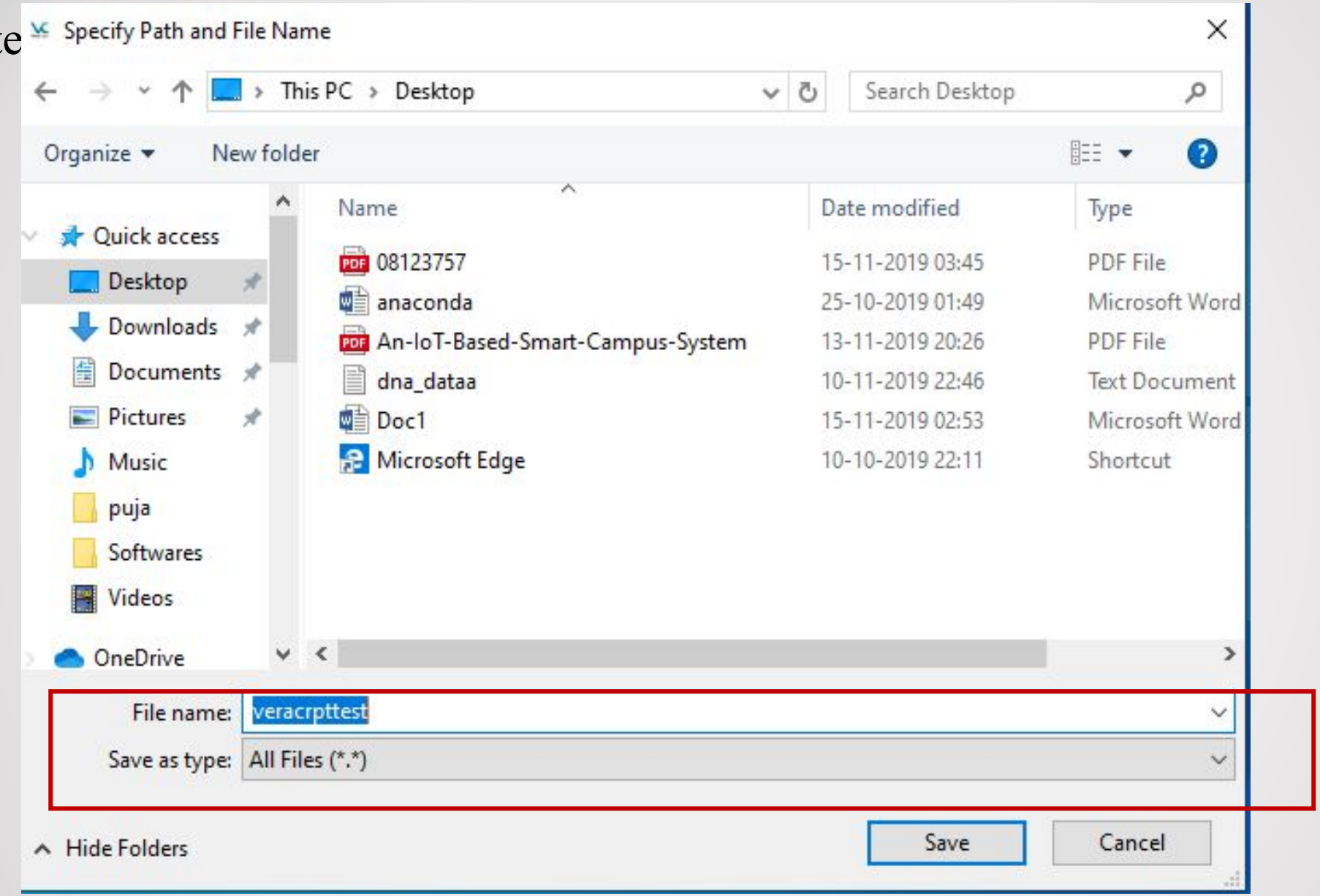
- Step 3:- we will create standard volume file:-



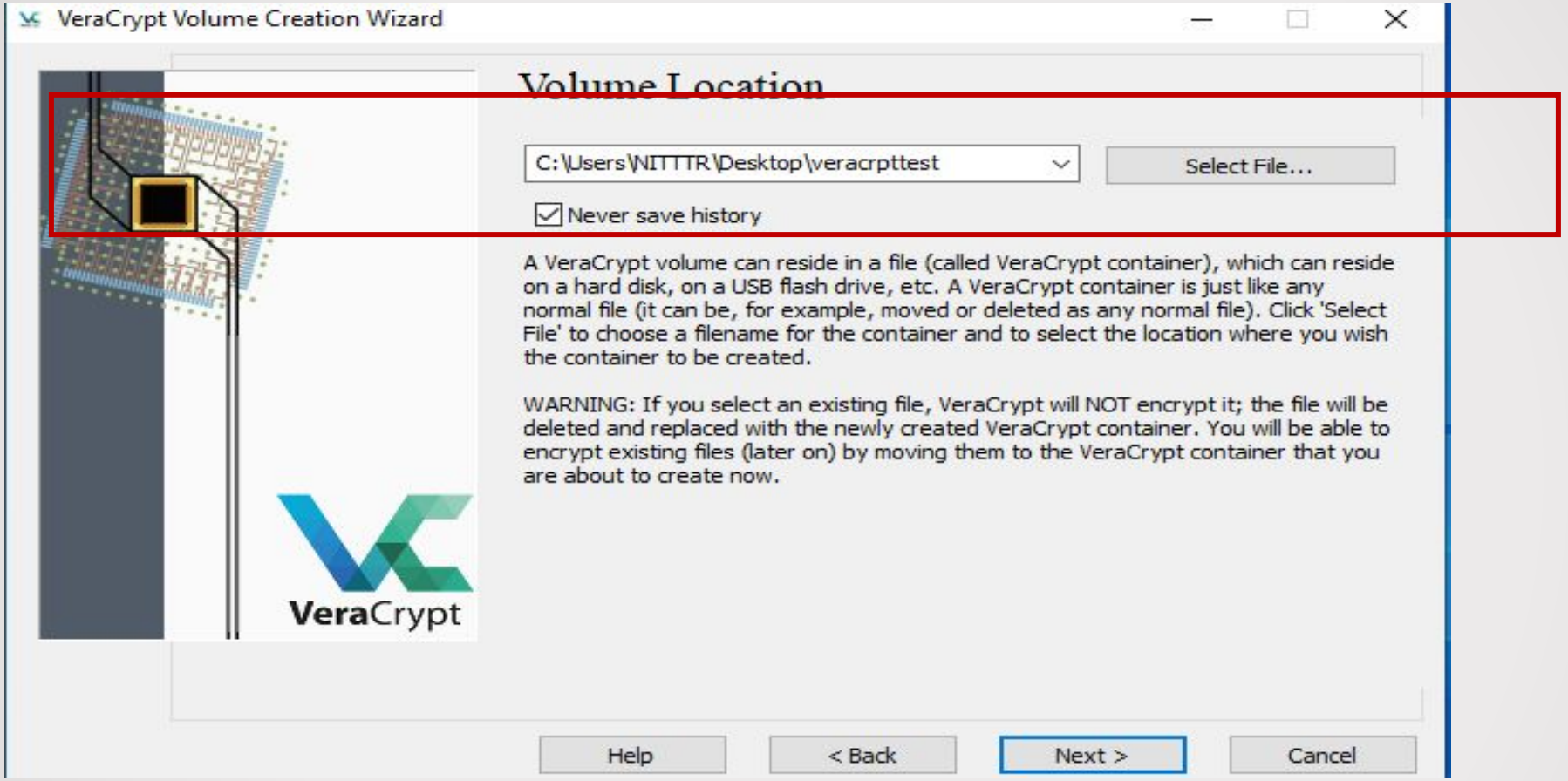
- Step4:-


VeraCrypt Volume Creation Wizard
Volume Location
Select File...
Never save history
A VeraCrypt volume can reside in a file (called VeraCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A VeraCrypt container is just like any normal file (it can be, for example, moved or deleted as any normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created.
WARNING: If you select an existing file, VeraCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created VeraCrypt container. You will be able to encrypt existing files (later on) by moving them to the VeraCrypt container that you are about to create now.
VeraCrypt
Help
< Back
Next >
Cancel

- Ste

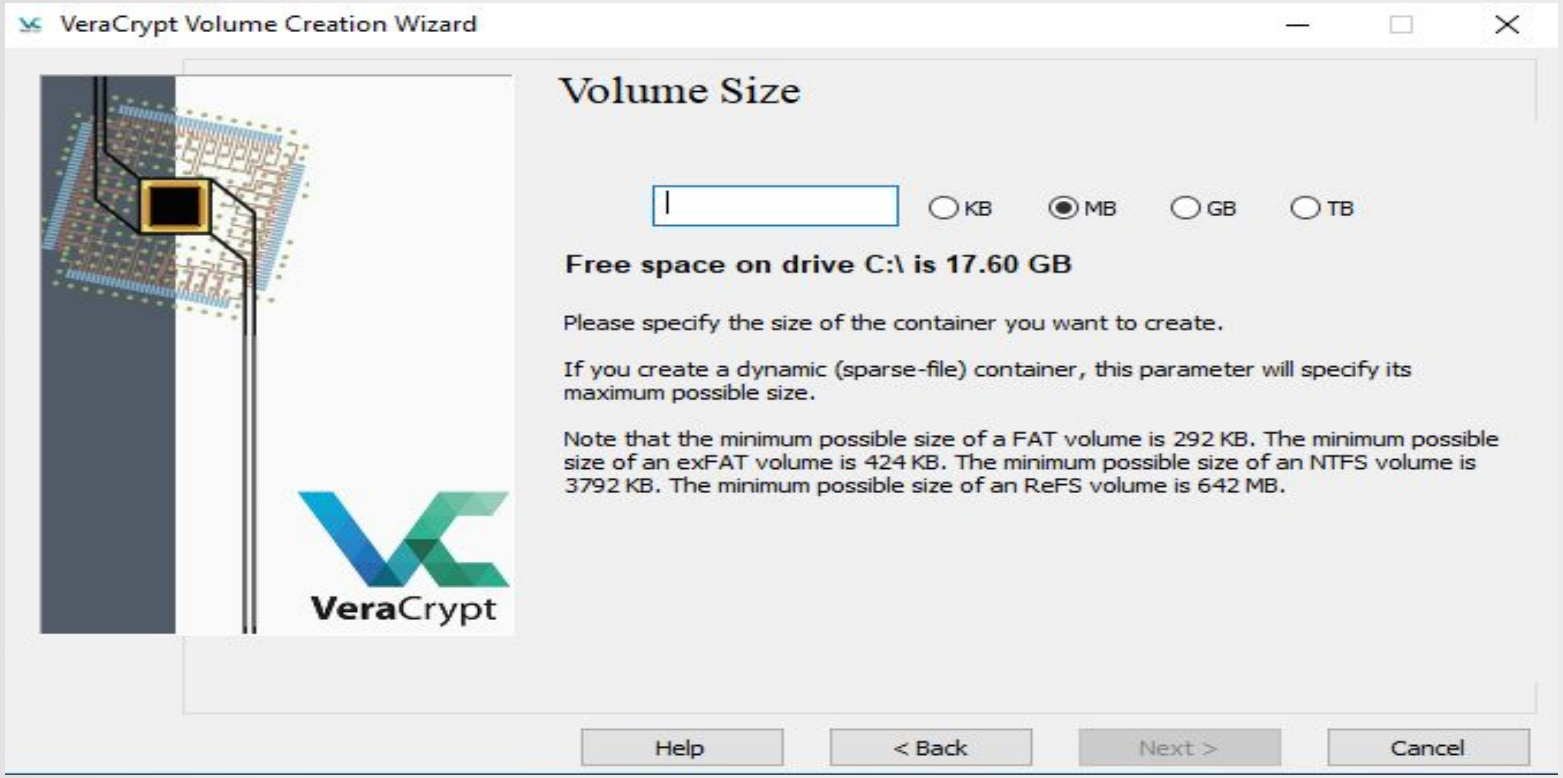

Specify Path and File Name
This PC › Desktop
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Music
puja
Softwares
Videos
OneDrive
Name
Date modified
Type
08123757
15-11-2019 03:45
PDF File
anaconda
25-10-2019 01:49
Microsoft Word
An-IoT-Based-Smart-Campus-System
13-11-2019 20:26
PDF File
dna_dataa
10-11-2019 22:46
Text Document
Doc1
15-11-2019 02:53
Microsoft Word
Microsoft Edge
10-10-2019 22:11
Shortcut
File name:
veracrpttest
Save as type:
All Files (*.*)
Hide Folders
Save
Cancel

- Step 5:- path has been setup:-

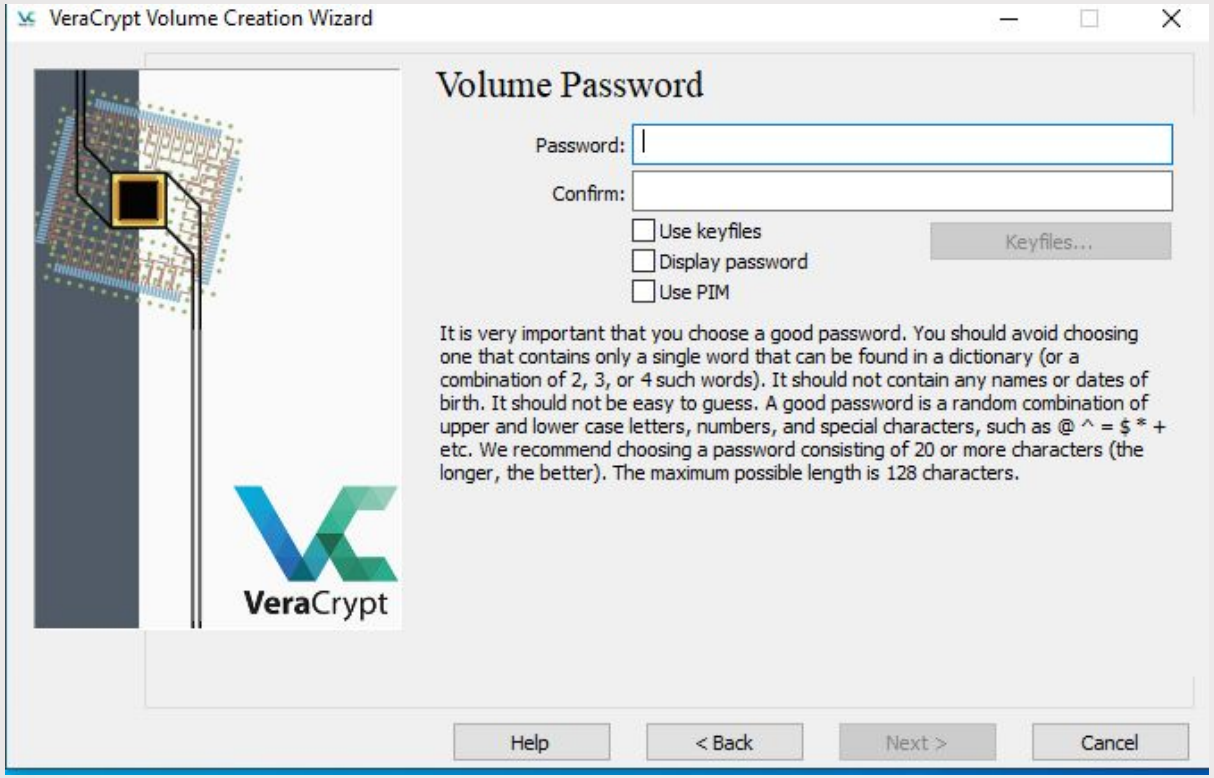


- Type of encryption we want:-

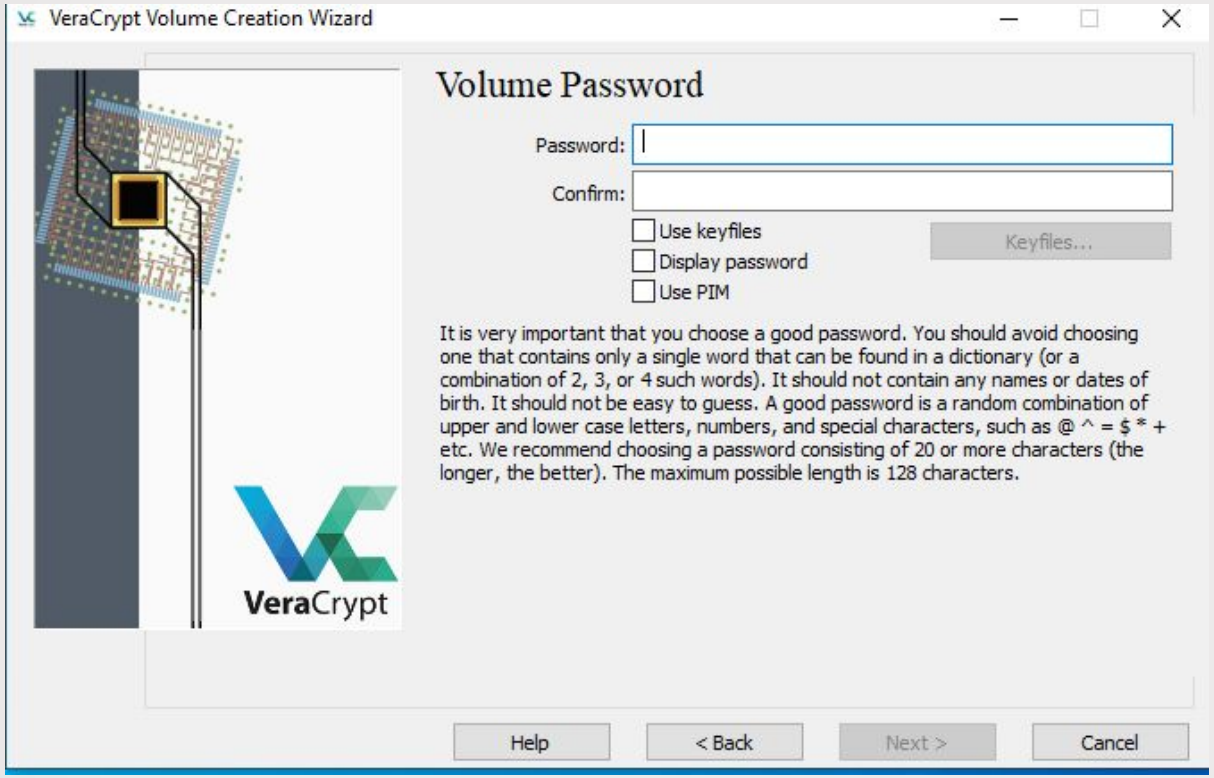
- File size:-


VeraCrypt Volume Creation Wizard
Volume Size
KB
MB
GB
TB
Free space on drive C:\ is 17.60 GB
Please specify the size of the container you want to create.
If you create a dynamic (sparse-file) container, this parameter will specify its maximum possible size.
Note that the minimum possible size of a FAT volume is 292 KB. The minimum possible size of an exFAT volume is 424 KB. The minimum possible size of an NTFS volume is 3792 KB. The minimum possible size of an ReFS volume is 642 MB.
VeraCrypt
Help
< Back
Next >
Cancel

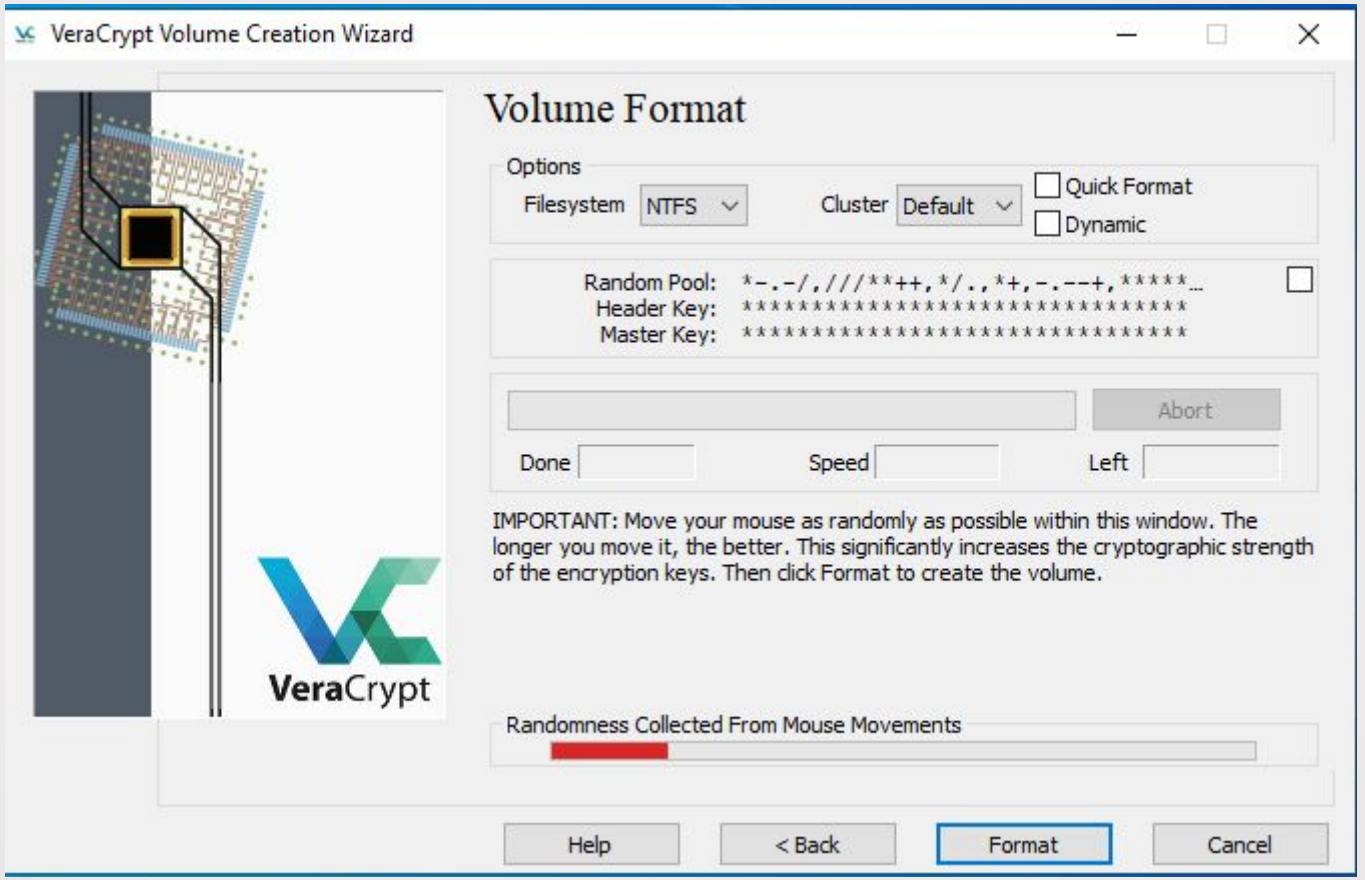
Password setup:-



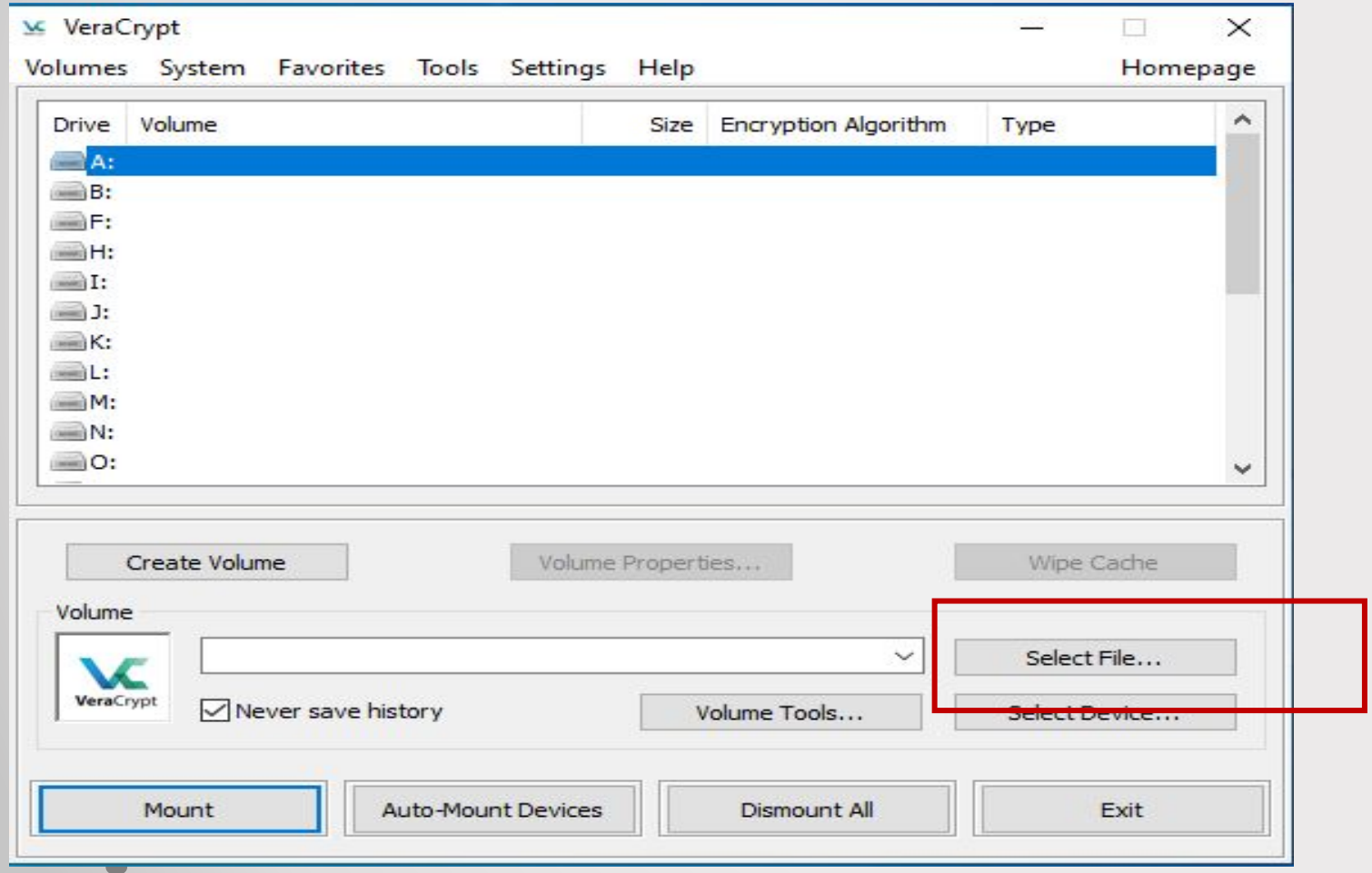
Password setup:-



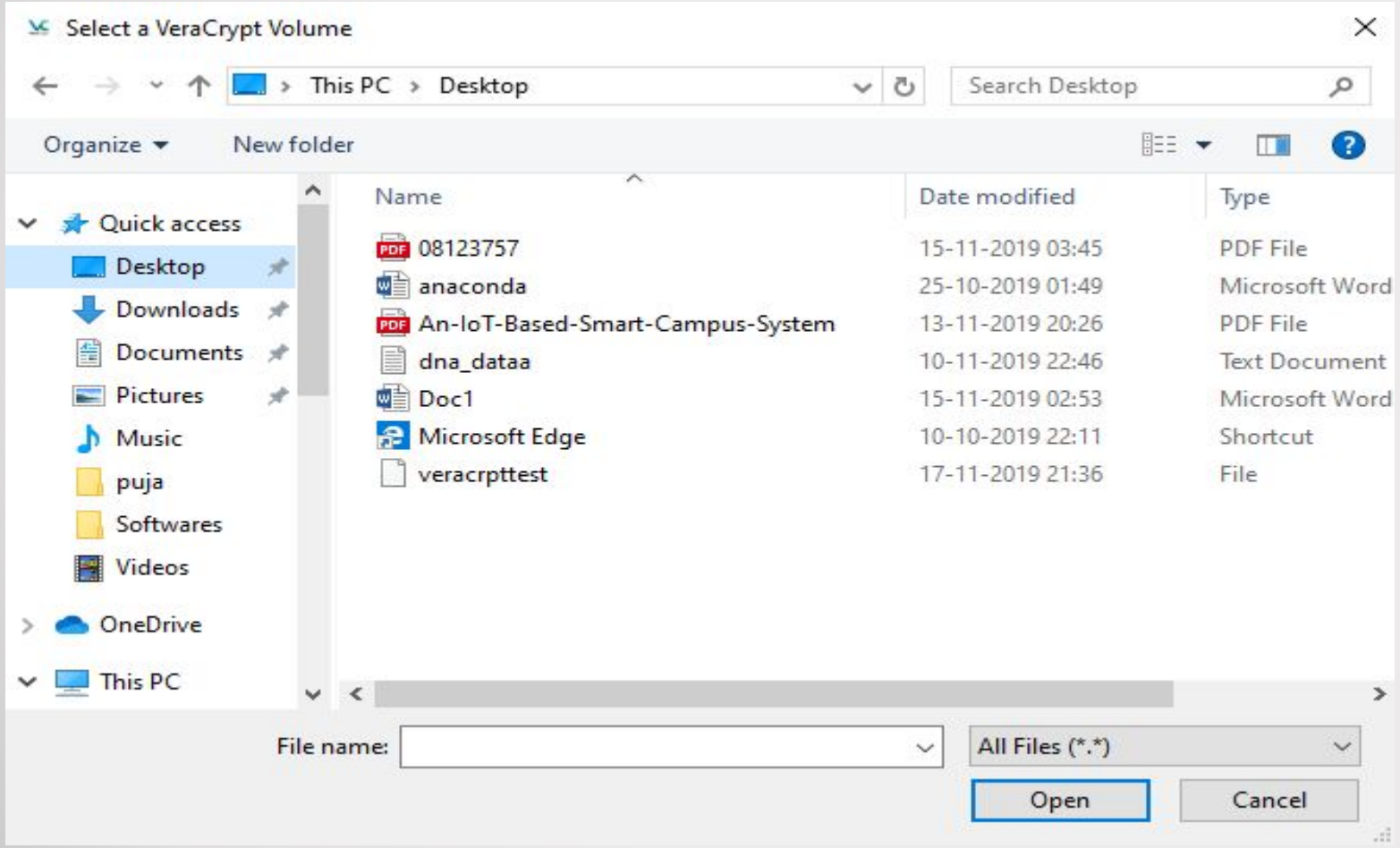
After creation we will click exit



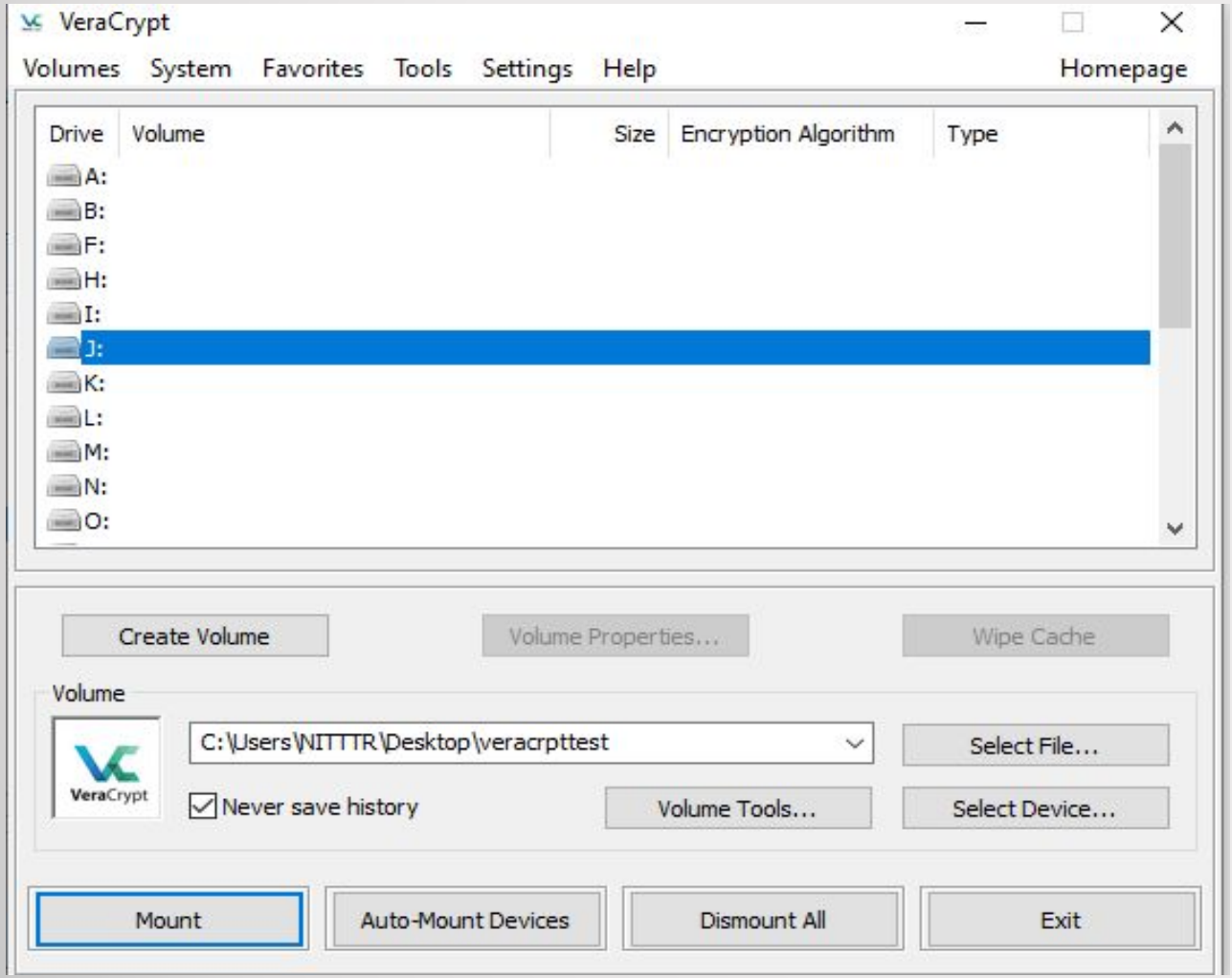
NOW ON CLICK ON THE VERCRYPT WIZARD AND SELECT FILE



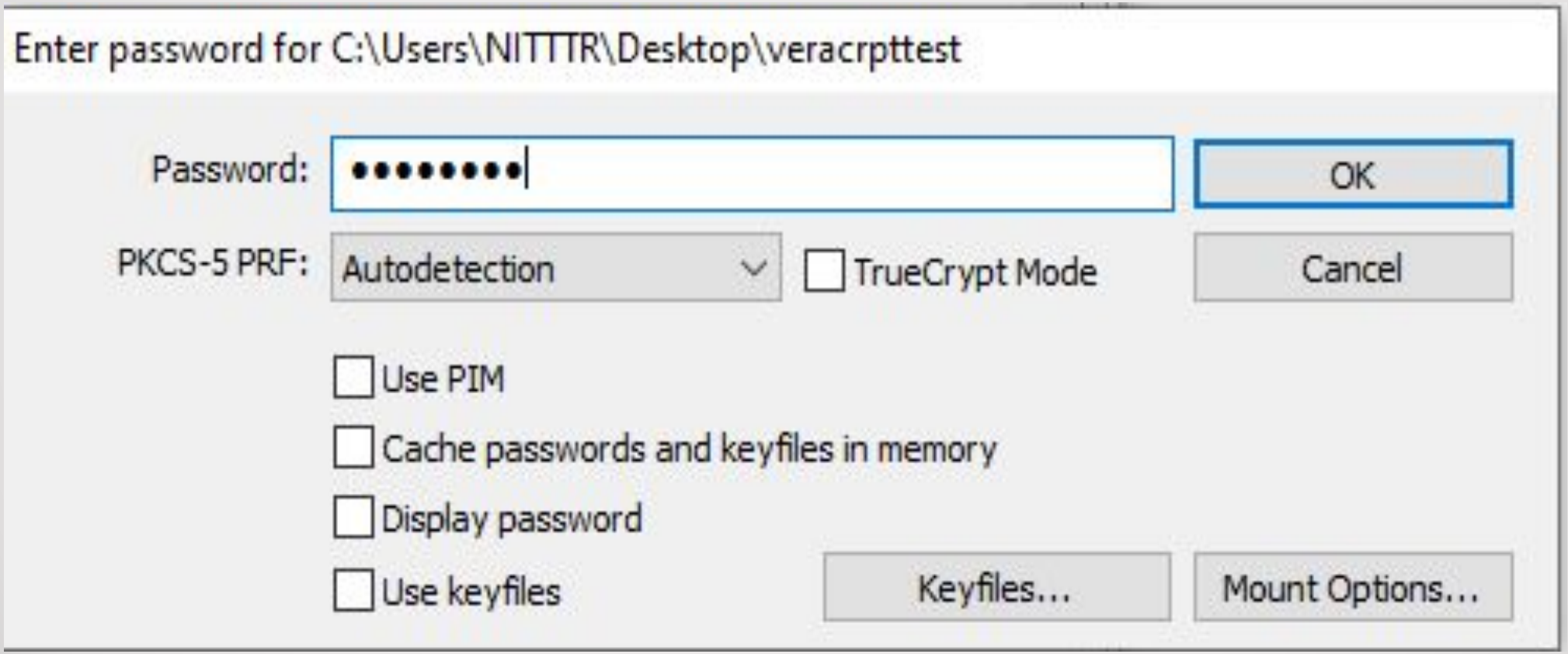
SETTING OF PATH



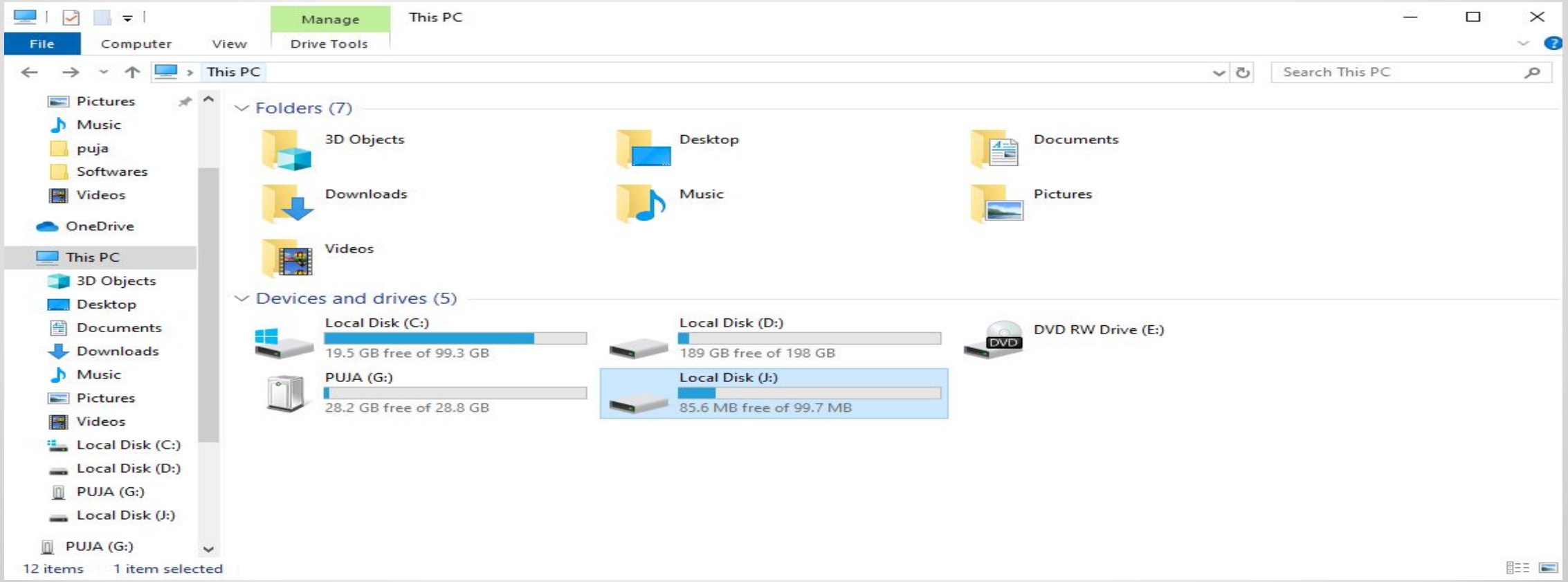
SELECT DRIVE LETTER SHOW IN THE LIST, SELECT MOUNT WHICH WILL ACT AS VERACRYPT CONTAINER



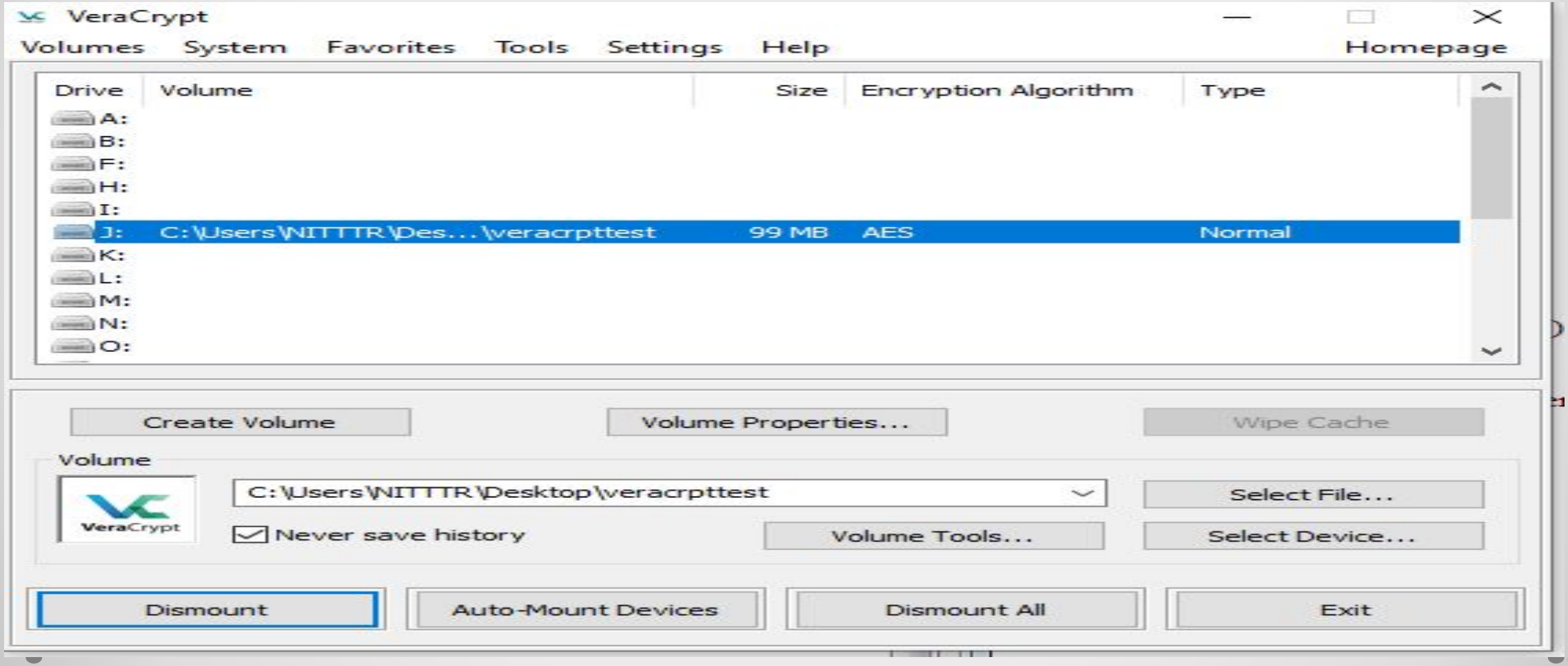
NOW GIVE THE PASSWORD USED PREVIOUSLY AND CLICK OK



NOW WE CAN SEE THE ENCRYPTED DRIVE



TO DISMOUNT SIMPLY CLICK DISMOUNT



GPG4WIN

- Gpg4win enables users to securely transport emails and files with the help of encryption and digital signatures.
- Encryption protects the contents against an unwanted party reading it.
- Digital signatures make sure that it was not modified and comes from a specific sender.
- Gpg4win supports both relevant cryptography standards, **OpenPGP** and **S/MIME (X.509)**, and is the official GnuPG distribution for Windows.
- Gpg4win and the software included with Gpg4win are Free Software (Open Source; among other things free of charge for all commercial and non-commercial purposes).

ITS REQUIREMENTS

- Gpg4win runs on Windows versions 7 or newer (up to Windows 10). Both 32 and 64bit systems are supported.
- If you have at least Windows XP, some parts of Gpg4win can be used, but are not officially supported.
- The Outlook plugin GpgOL is compatible with Microsoft Outlook 2010, 2013, 2016 and 2019 (both 32 and 64bit) and supports transporting emails via SMTP/IMAP and MS Exchange Server (version 2010 or newer).
- For elder Outlook versions 2003 and 2007 less functionality is offered.

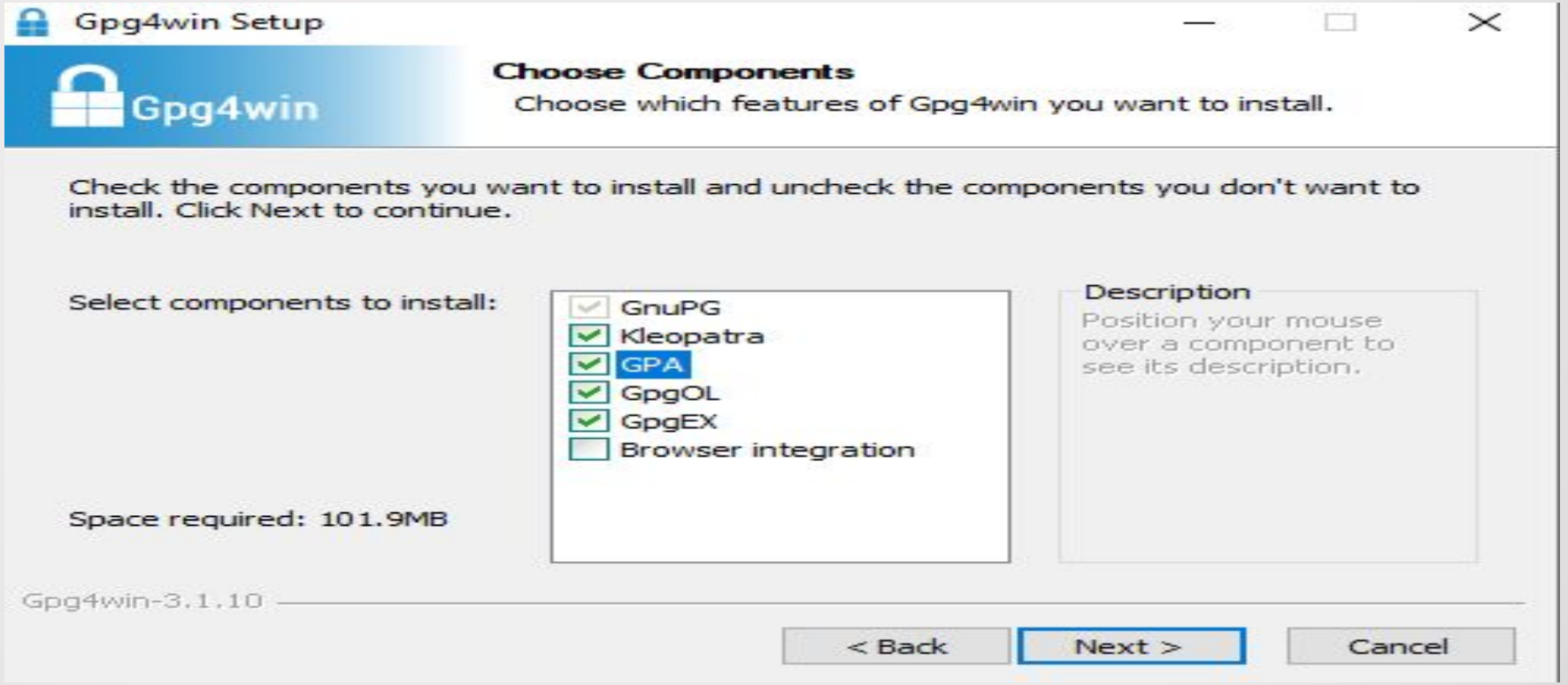
WOIKING WITH GPP4WIN

- Step1:- Installation:-https://www.gpg4win.org/get-gpg4win.html

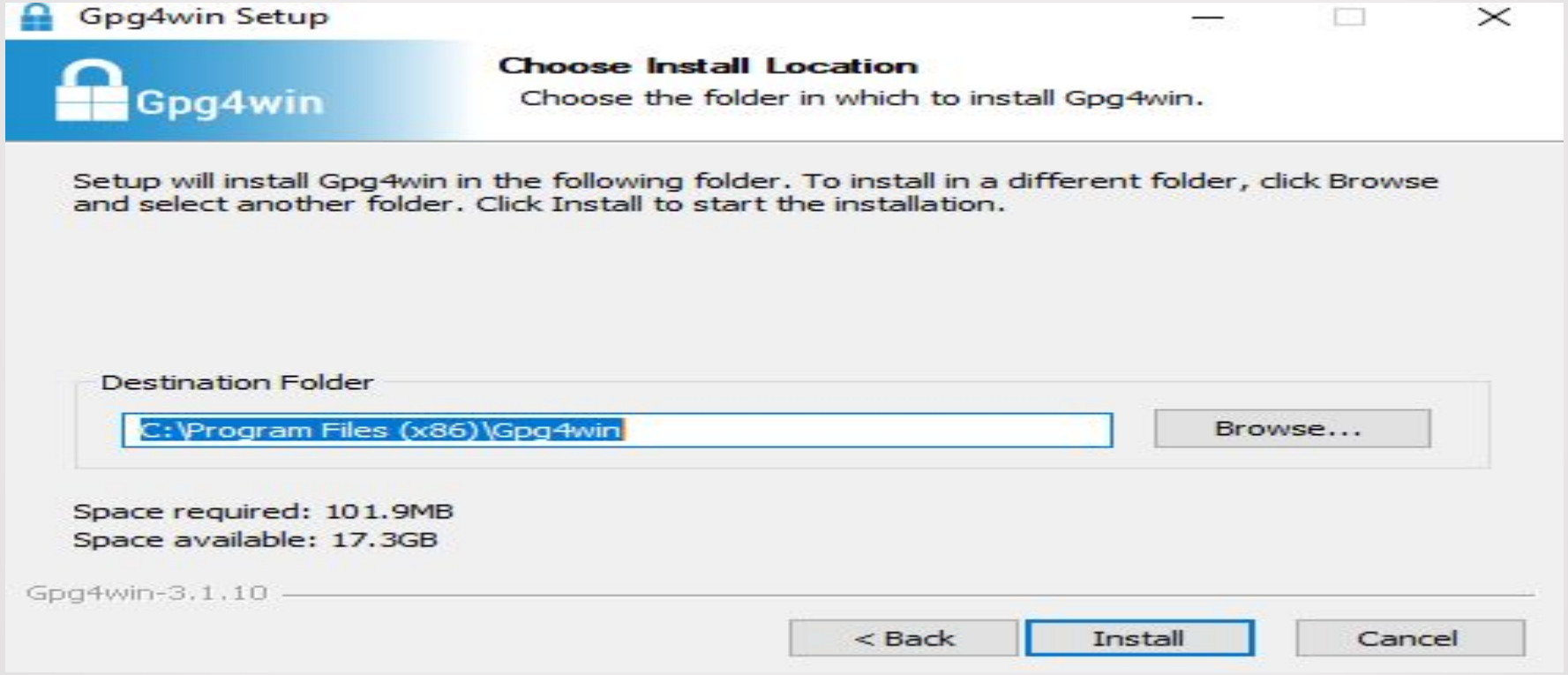
Wizard page


Gpg4win Setup
Gpg4win
GnuPG for Windows
Welcome to the installation of Gpg4win
Gpg4win is an installer package for Windows for EMail and file encryption using the core component GnuPG for Windows. Both relevant cryptography standards are supported, OpenPGP and S/MIME. Gpg4win and the software included with Gpg4win is Free Software.
Click Next to continue.
This is Gpg4win version 3.1.10
Release date 2019-07-14
Next >
Cancel

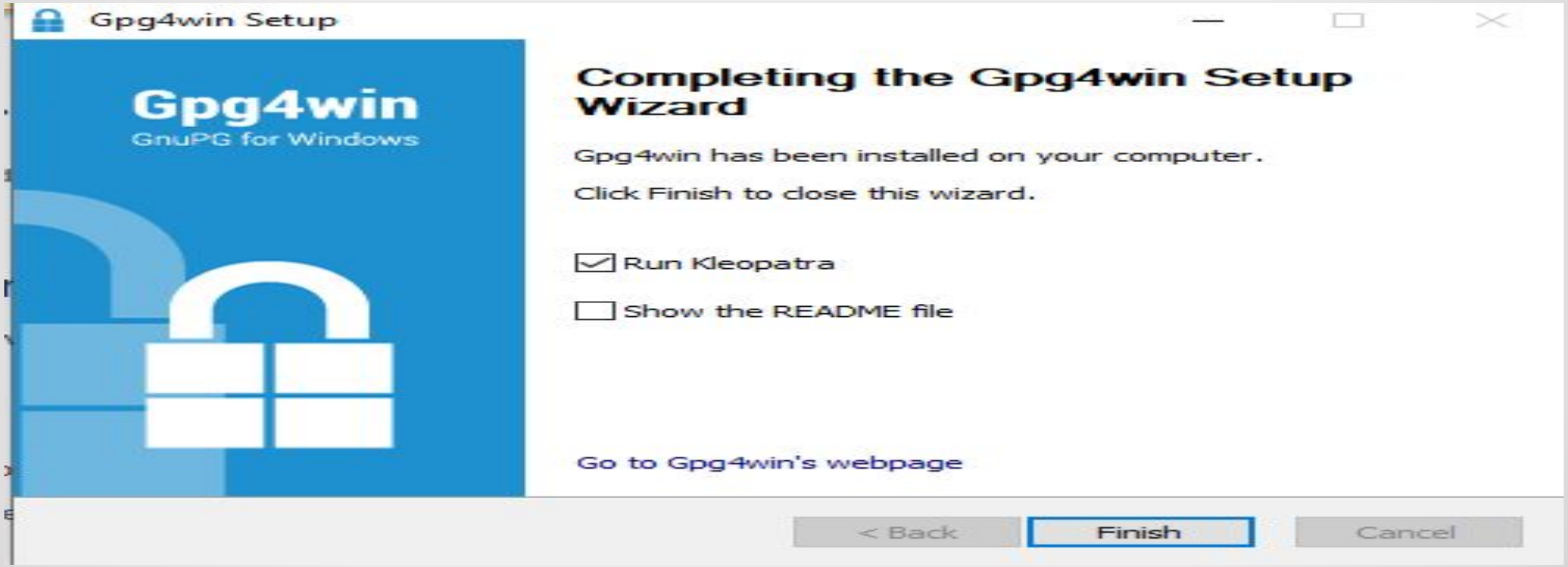
Choosing of components



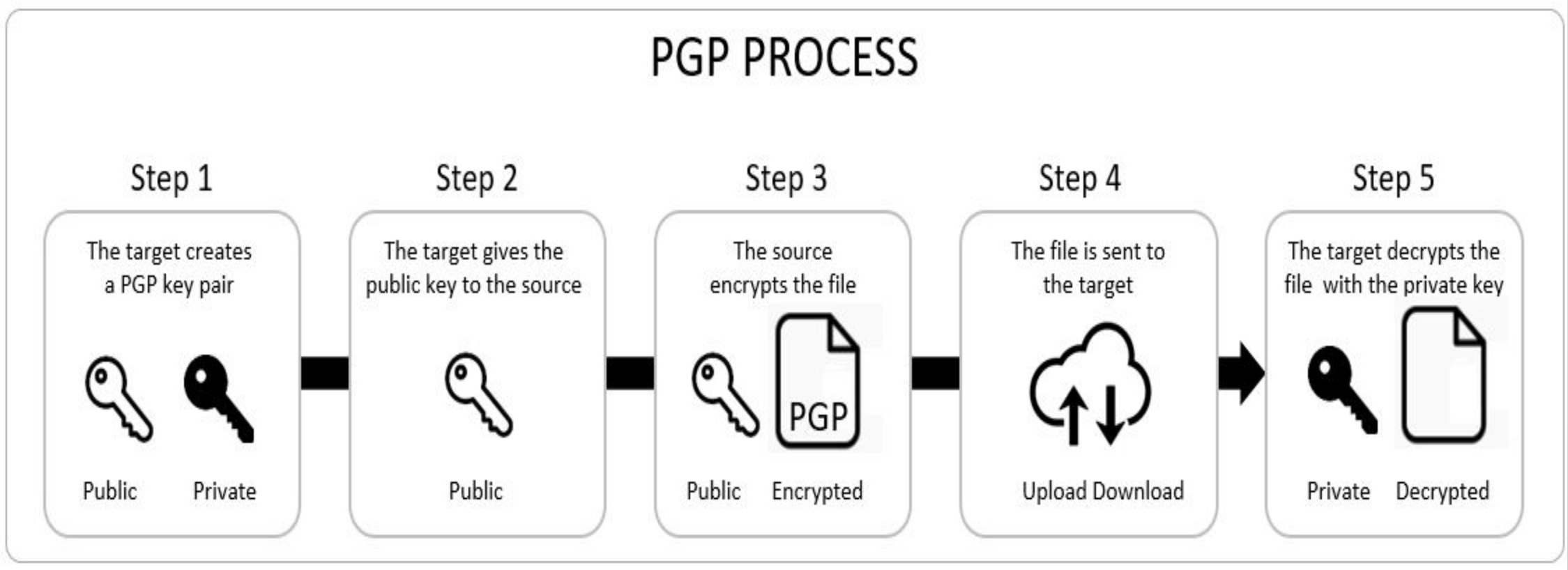
Path setup


Gpg4win Setup
Gpg4win
Choose Install Location
Choose the folder in which to install Gpg4win.
Setup will install Gpg4win in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files (x86)\Gpg4win
Browse...
Space required: 101.9MB
Space available: 17.3GB
Gpg4win-3.1.10
< Back
Install
Cancel

Show that installation has been completed

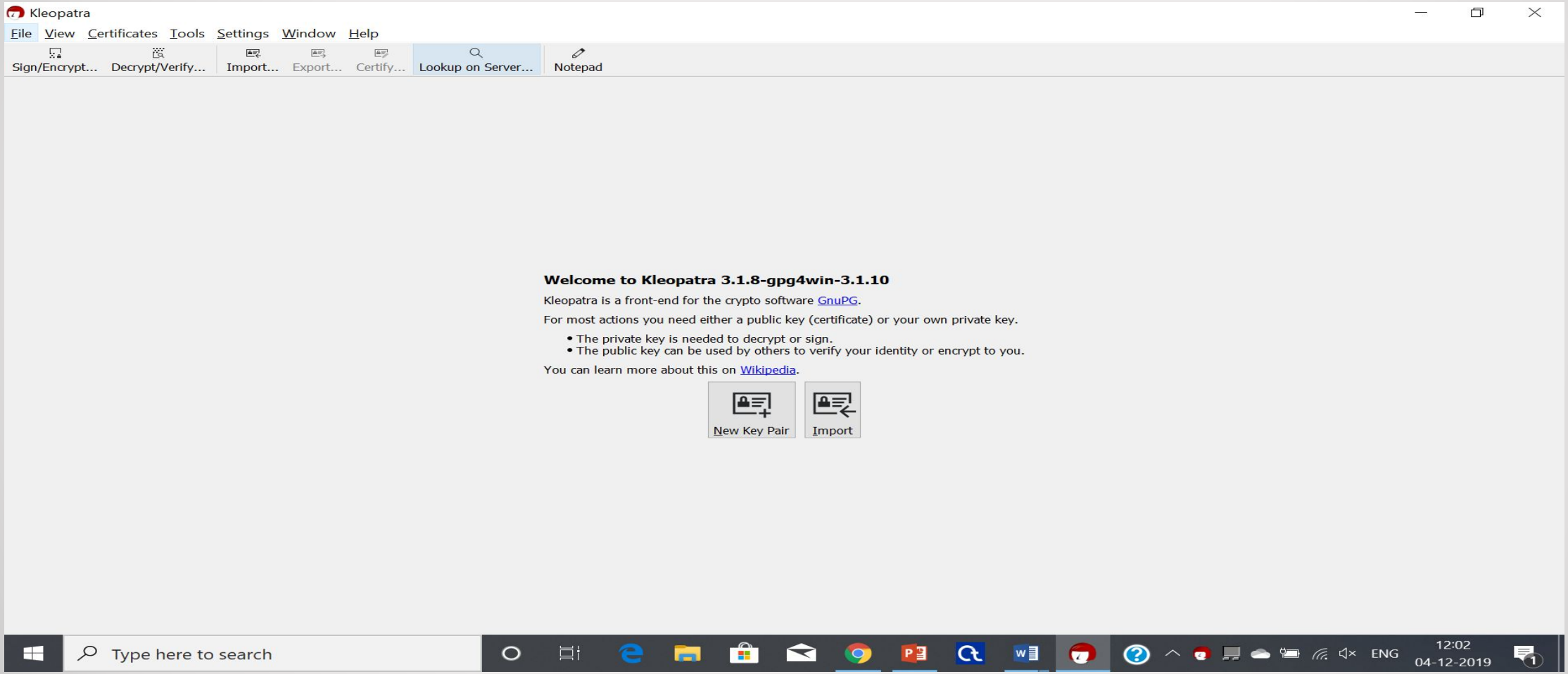


WORKFLOW DIAGRAM

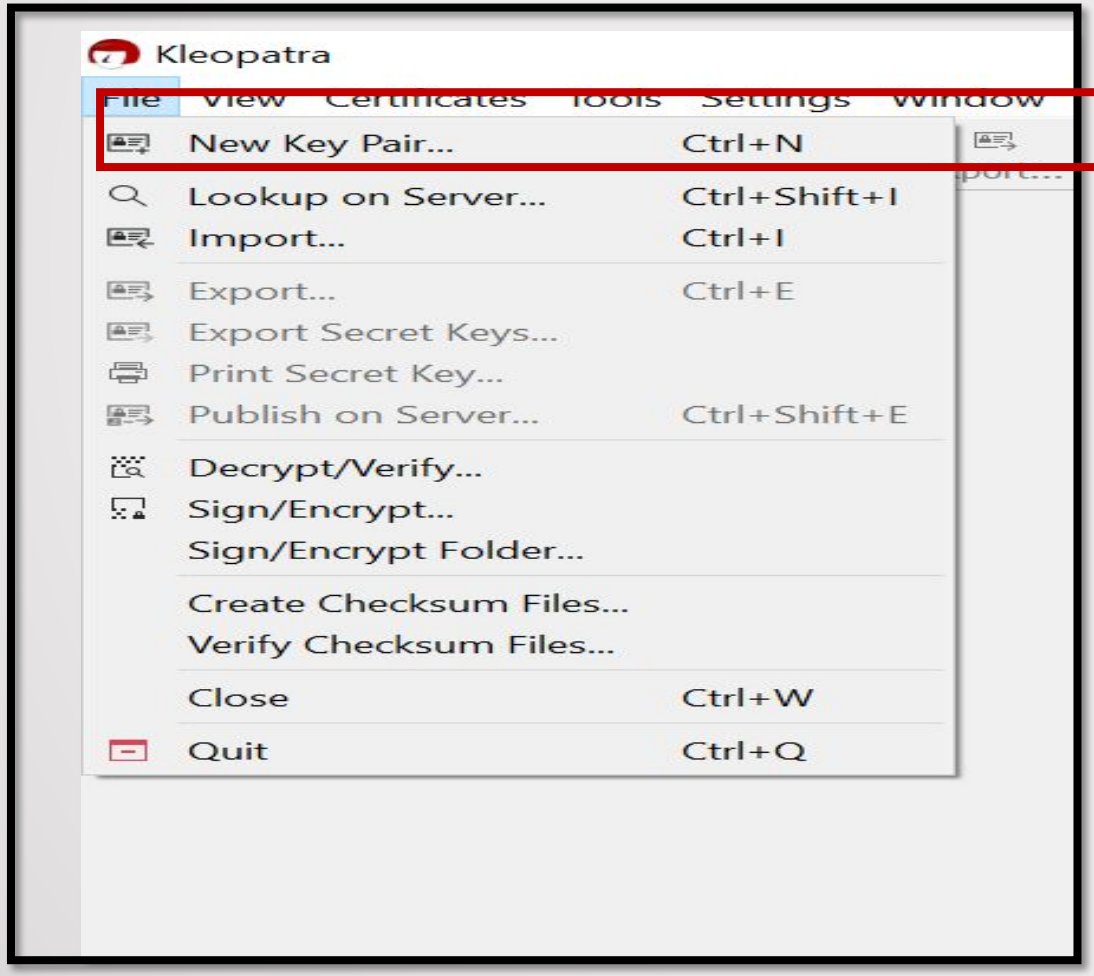


Now lets see ITS WORKING

STEP 1:- ON CLICKING THE ICON IT OPENS THE WORKING PAGE

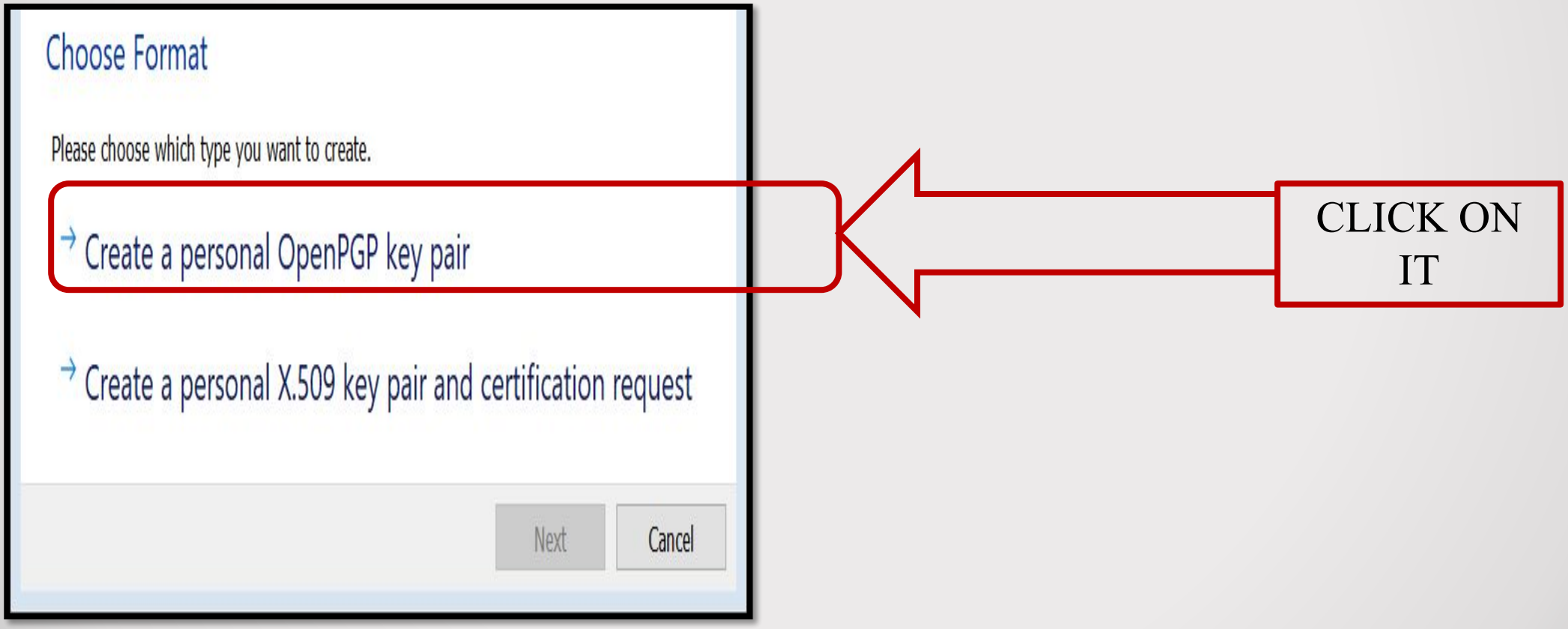


STEP 2:- TO CREATE KEY PAIRS

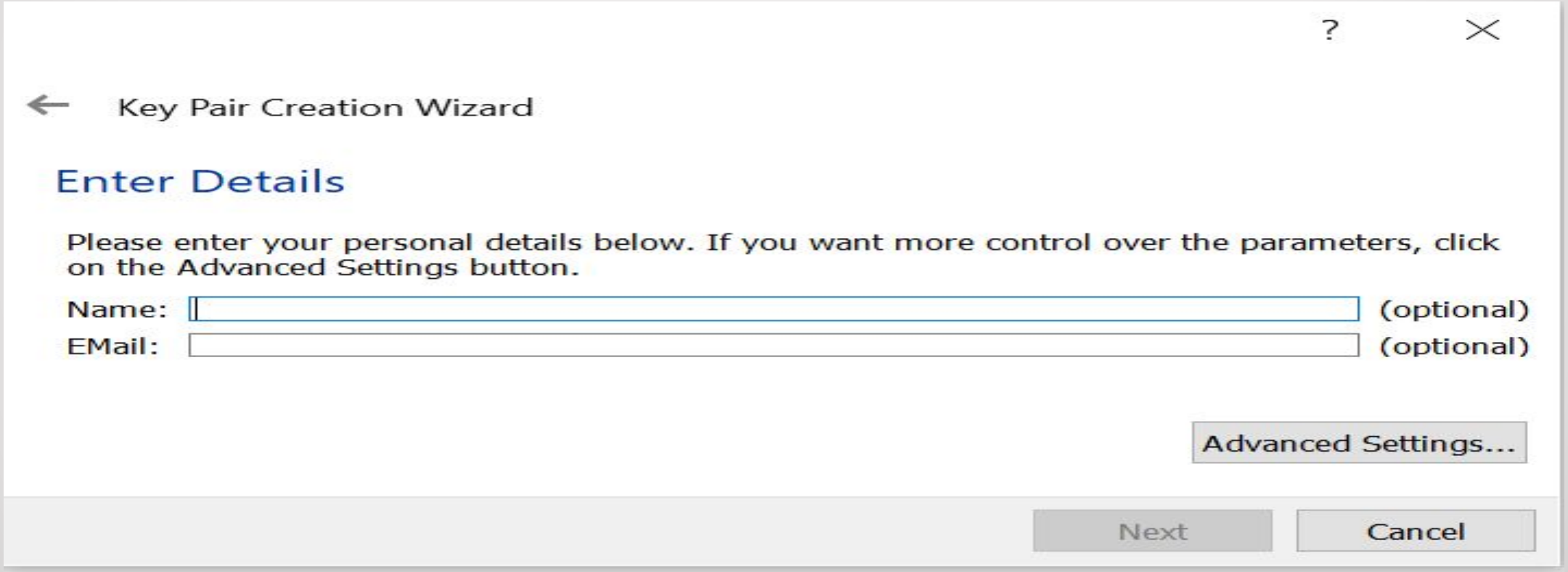


CLICK ON NEW KEY PAIR

STEP 3:-TO CONFIRMING THE FINGERPRINT OF PUBLIC KEY

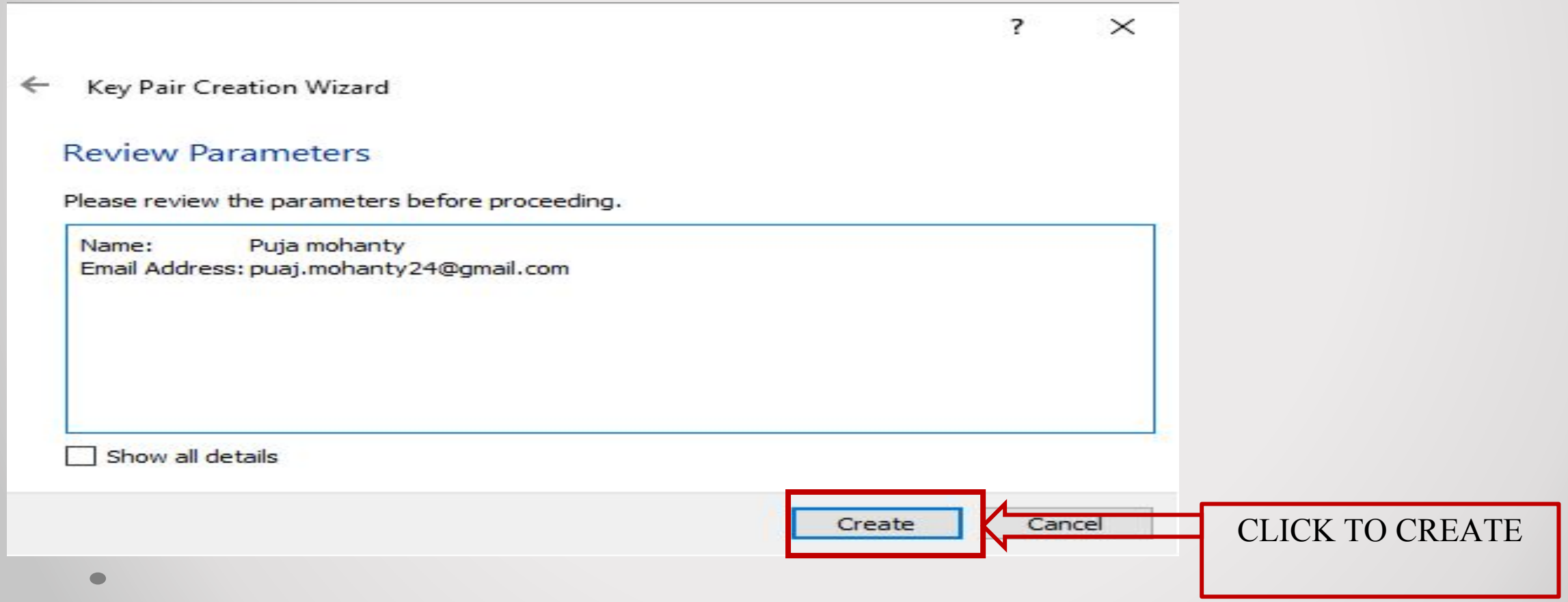


STEP 4 :- CREATION OF IDENTITY

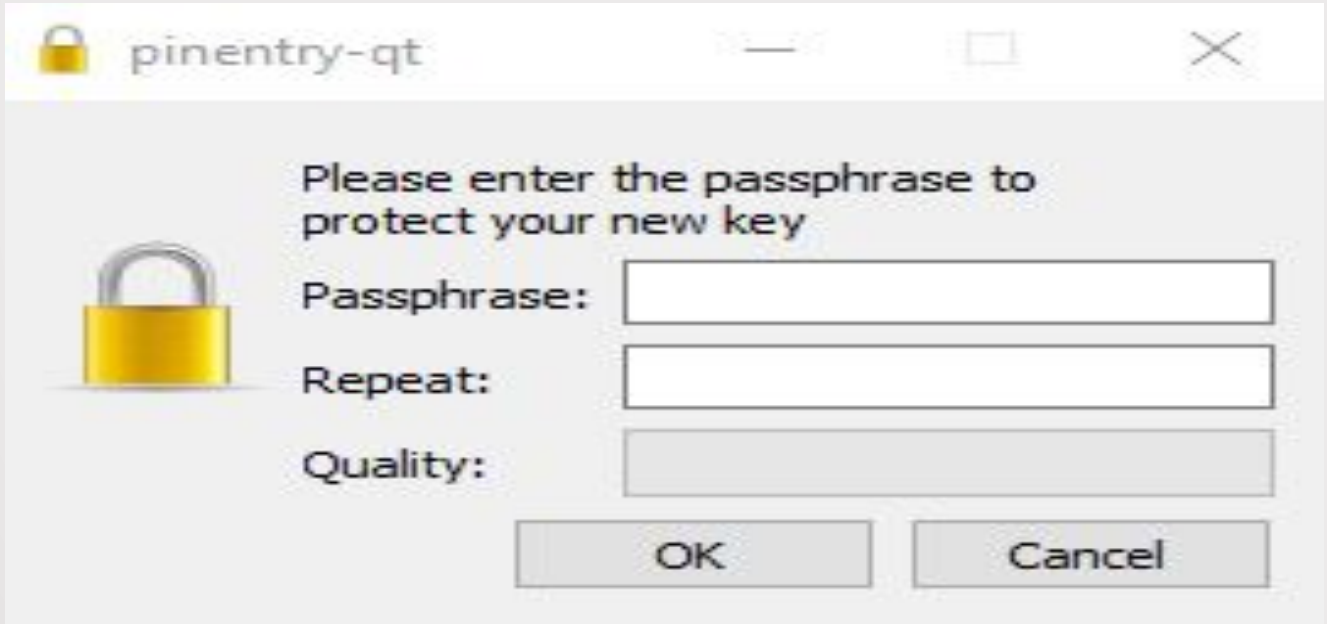


Step 5 GIVING REVIEW OF PARAMETERS

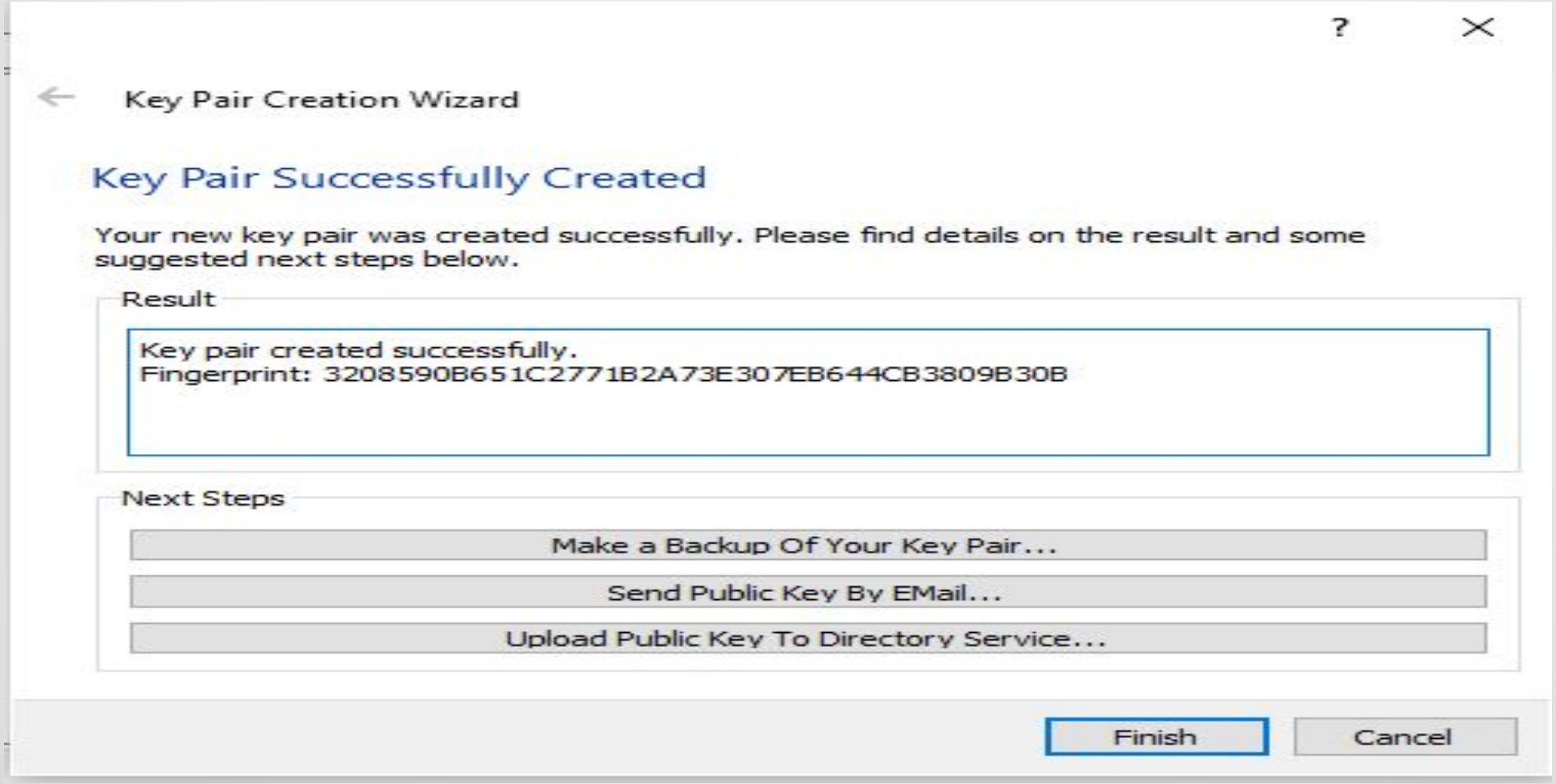
- Now we will create the fingerprint by clicking “ok”.



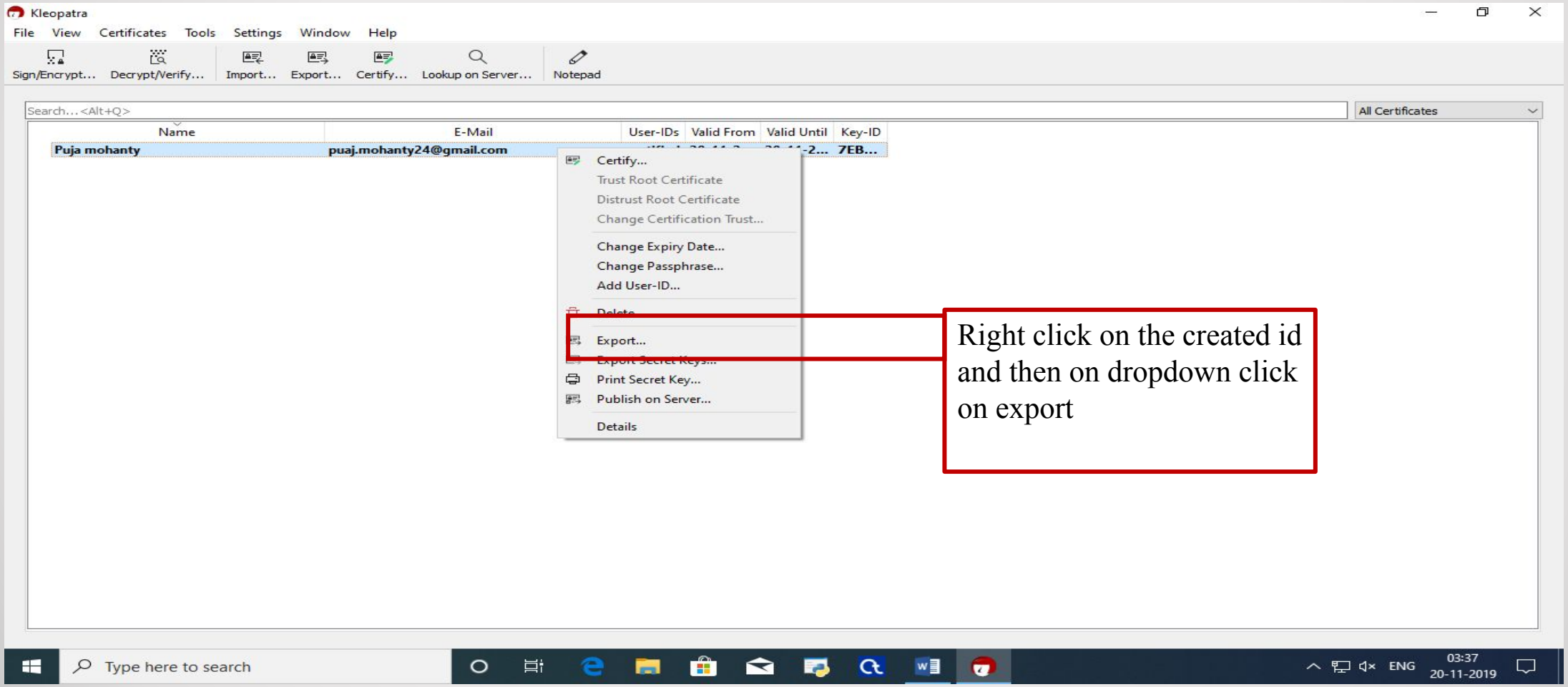
STEP6:- TO PROTECT THE KEY WE CREATE A PARAPHRASE



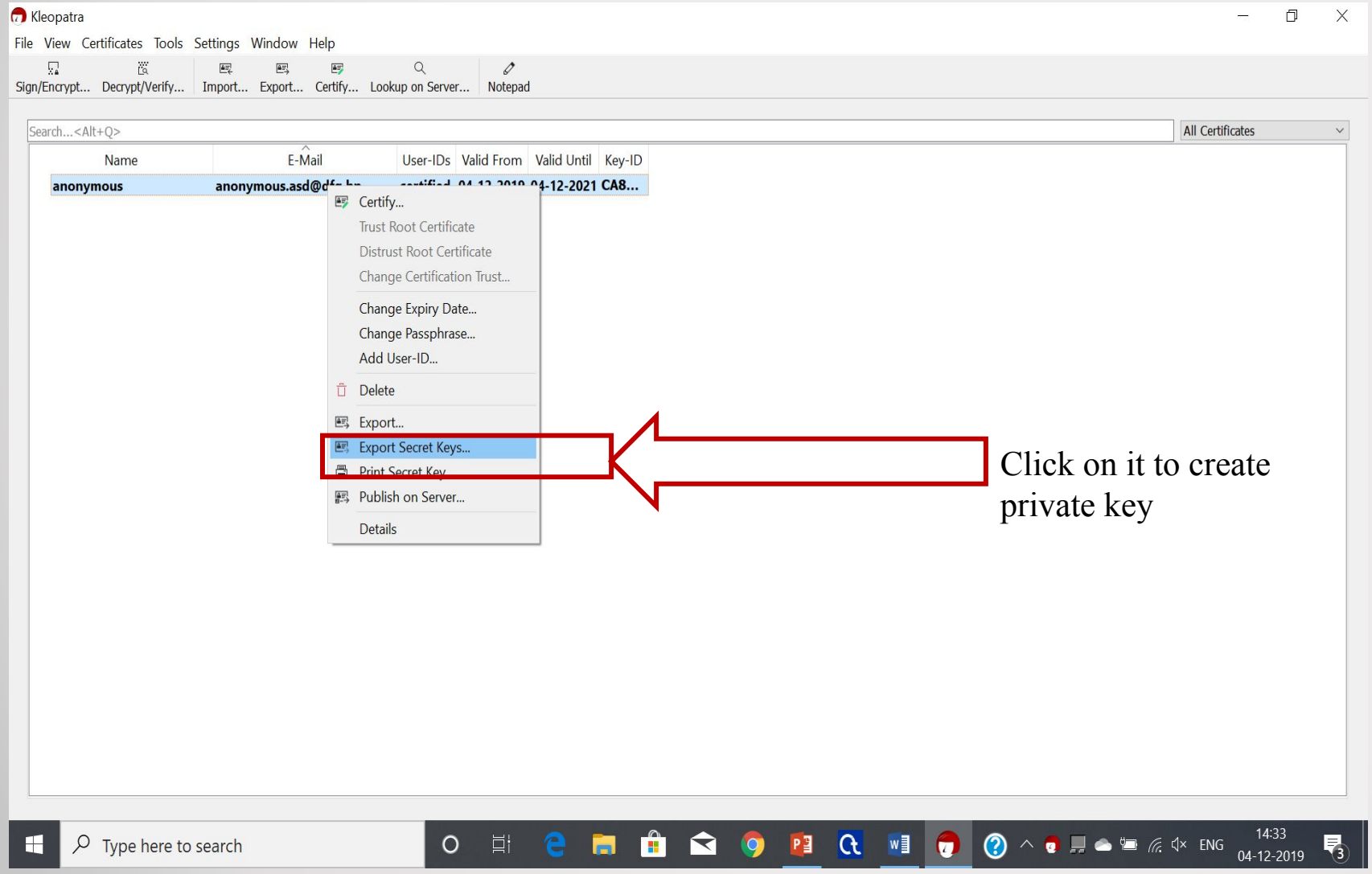
KEY PAIR IS CREATED SUCESSFULY



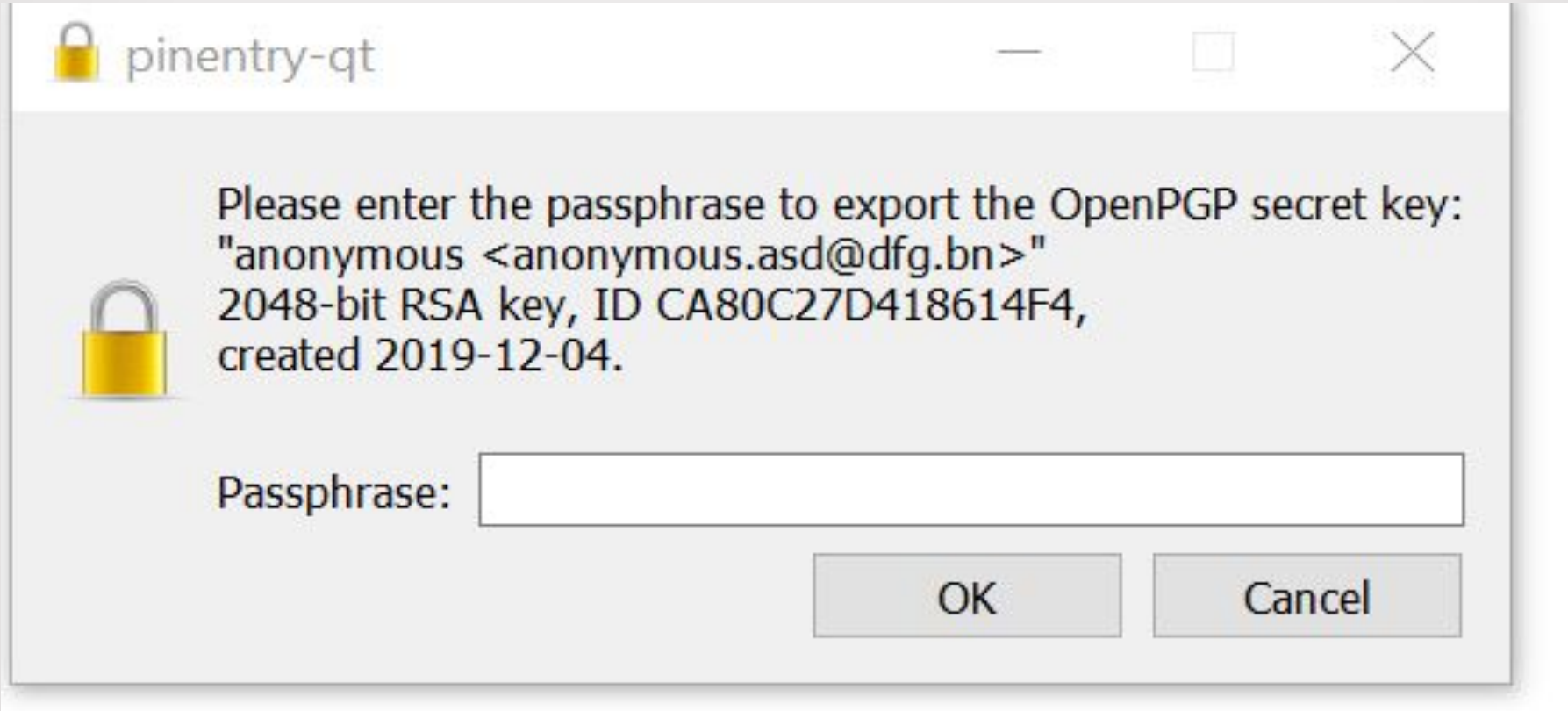
STEP 7 TO CREATE THE PUBLIC KEY AND EXPORT IT



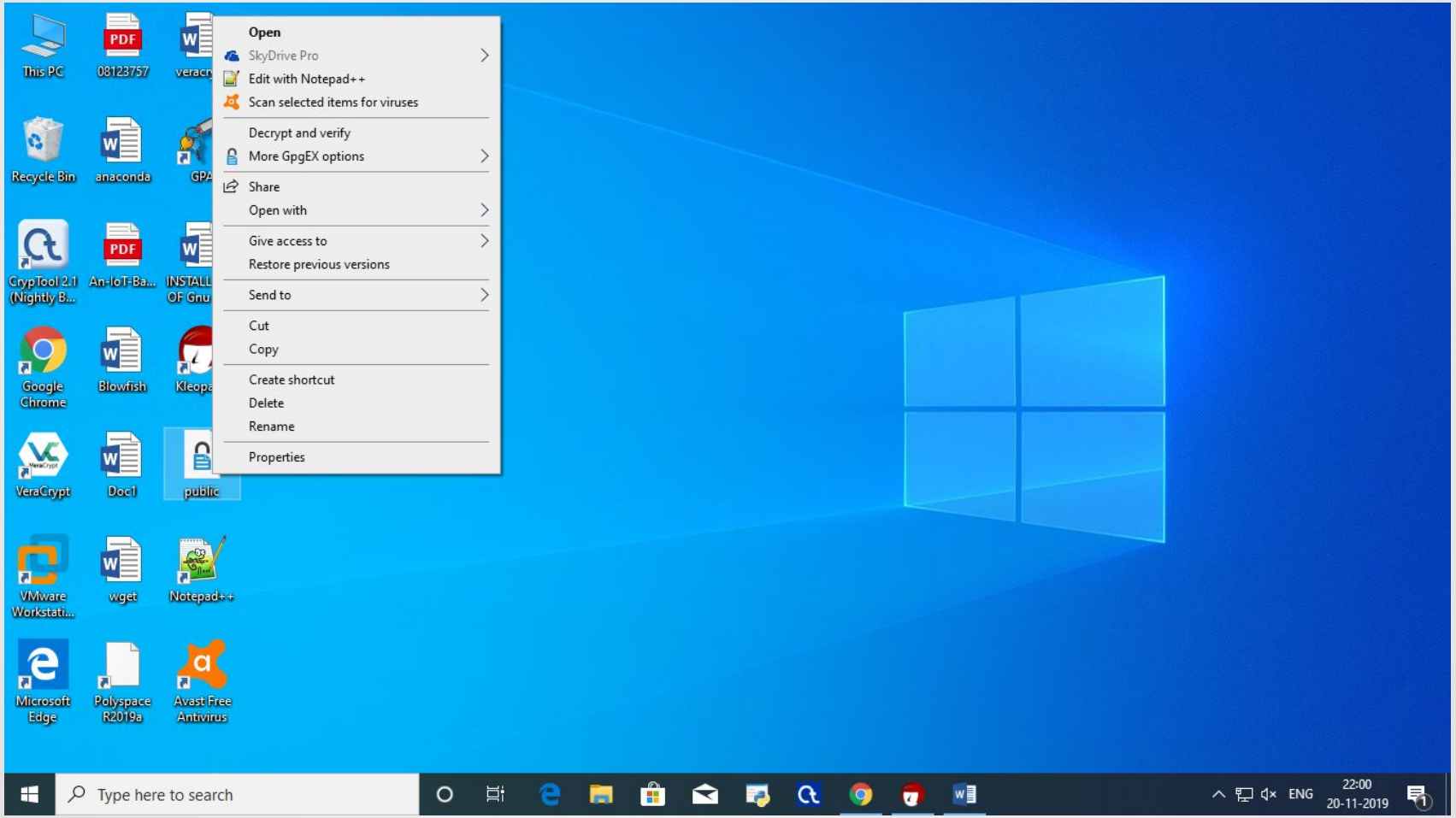
STEP 8:- Creation of private key and export it



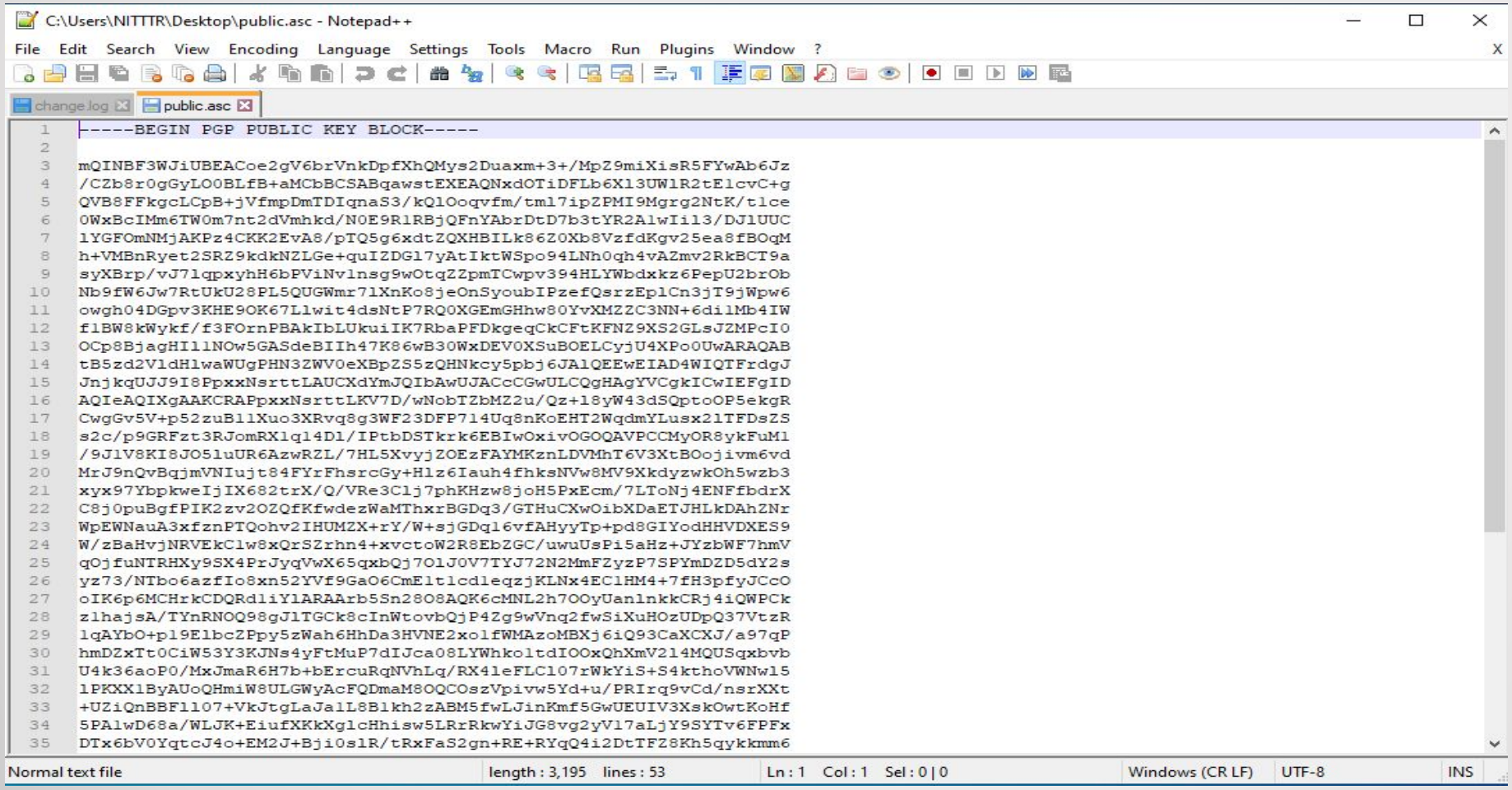
STEP 9 :-GIVE THE PARAPHRASE CREATED DURING KEY PAIR GENRATION



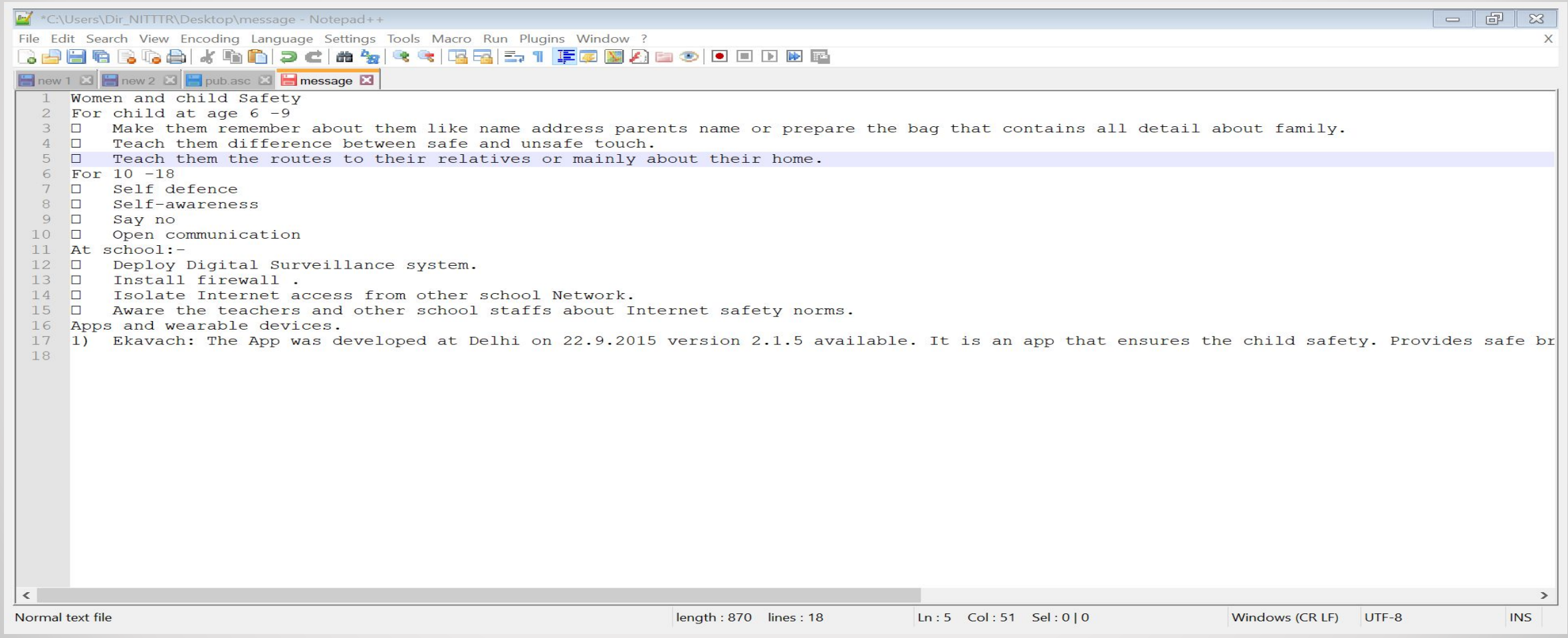
STEP 10:- OPEN THE PUBLIC WITH TEXT EDITOR



PUBLIC KEY VIEW



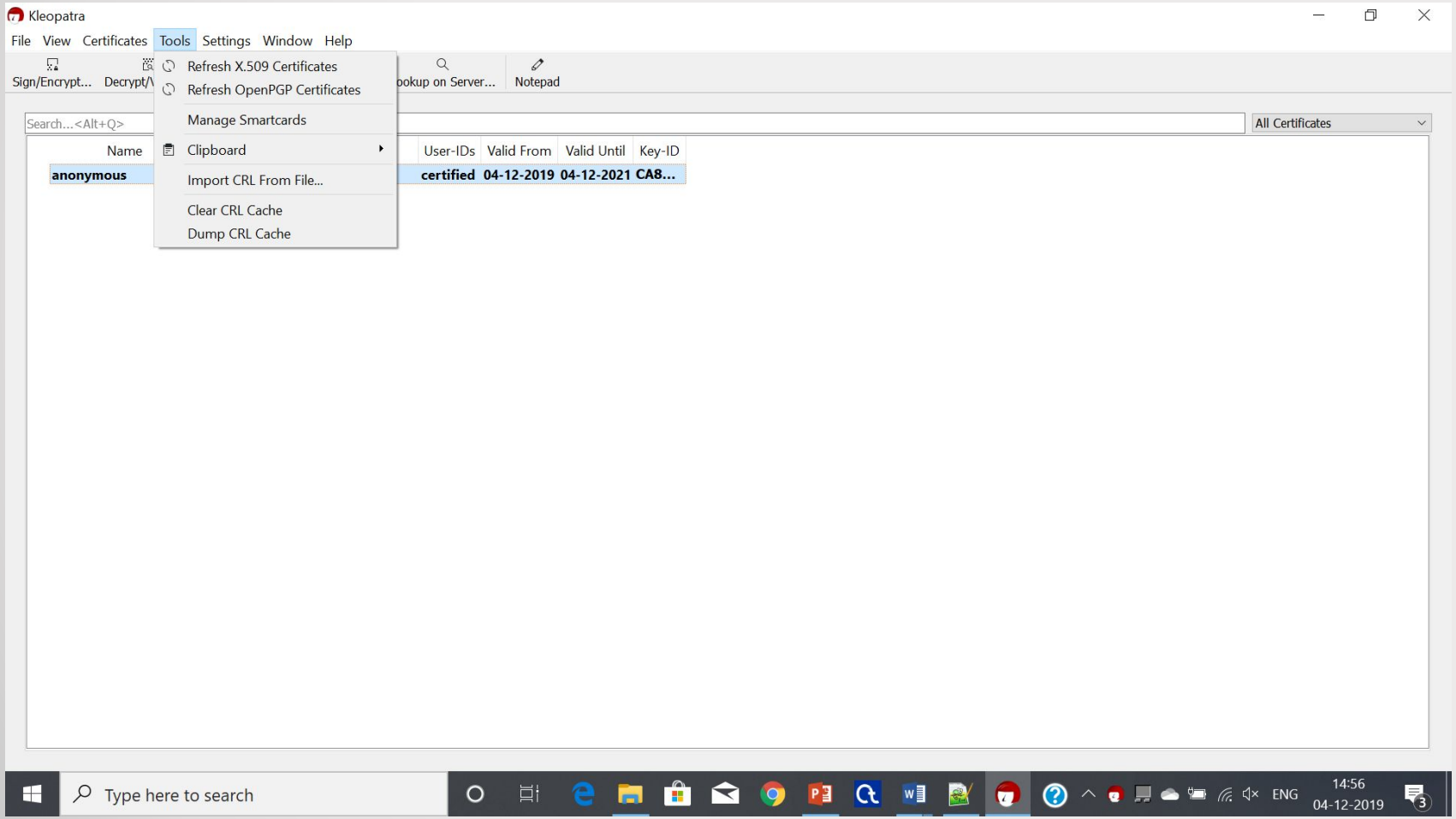
STEP 11:- CREATE A NEW TEXT EDITOR A WRITE THE MESSASGE



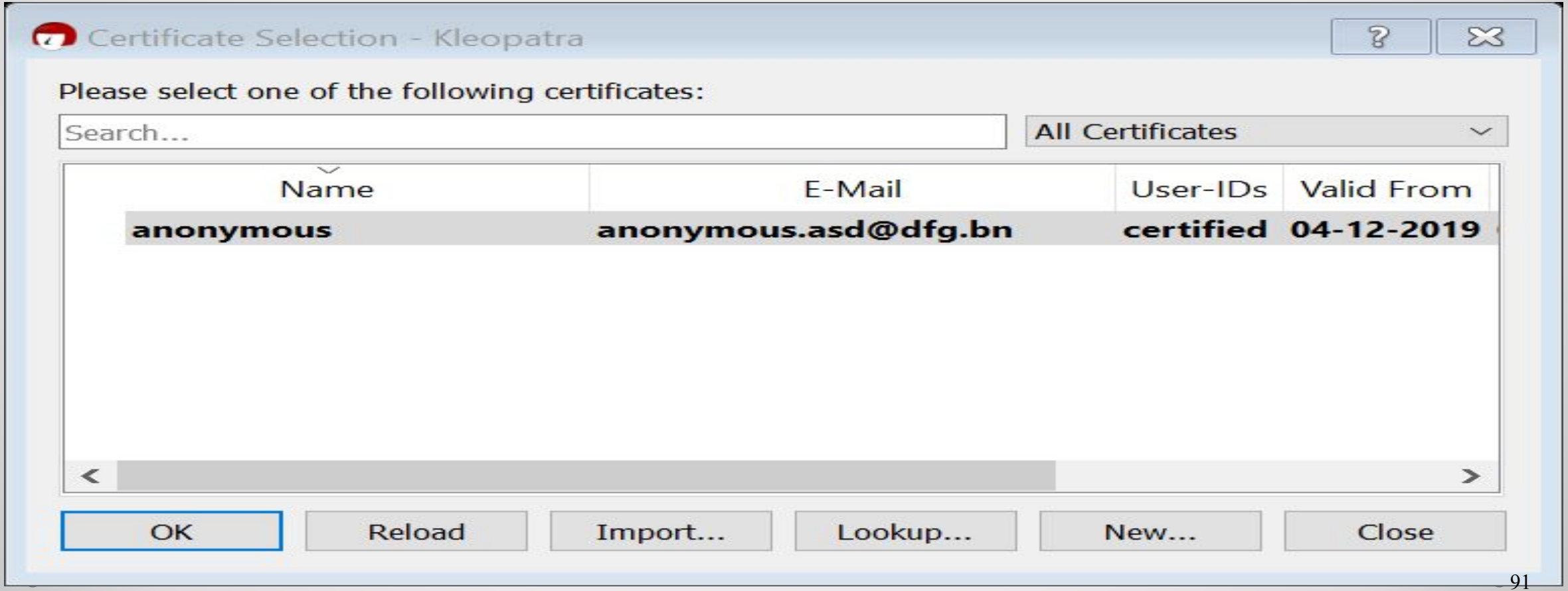
TO ENCRYPT THE MESSAGE

- 1 COPY THE PUBLIC KEY .
- 2 THEN COPY THE MESSAGE.

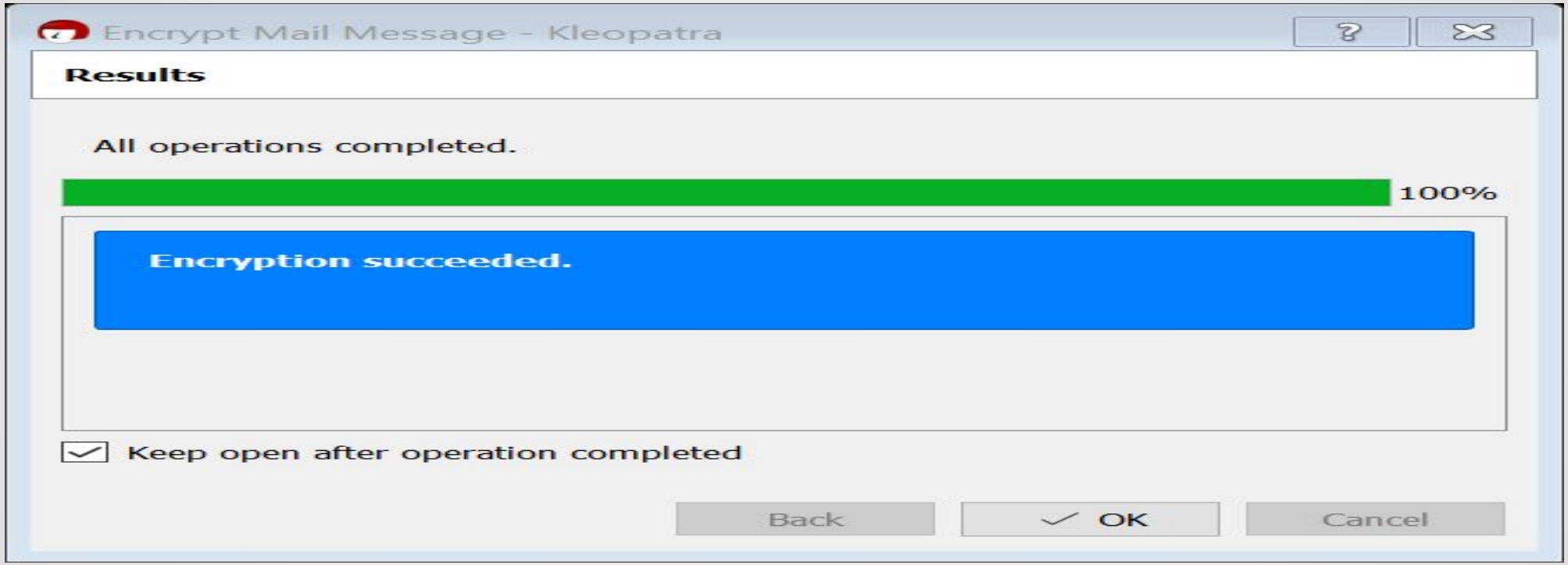
STEP 12:- CLICK ON THE TOOLS OF THE WIZARD AND CLICK ENCRYPT



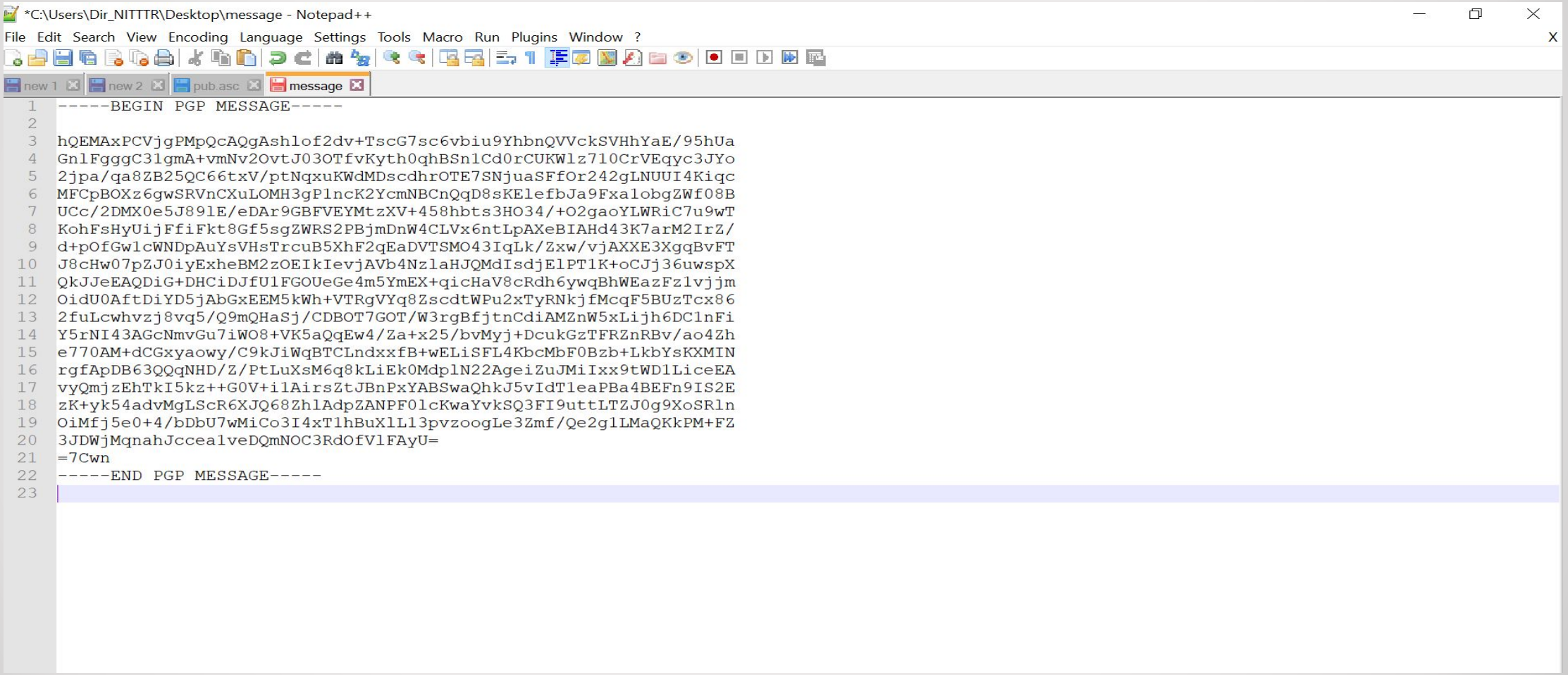
STEP13:- THEN ADD THE RECIPIENT



THEN THE MESSAGE IS SUCCESSFULLY ENCRYPTED



STEP 14:- TO GET THE RESULT CREATE NEW EDITOR AND PASTE THE MESSGE



THANK YOU