



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

BASIC
ON
CRYPTOGRAPHY

ONLINE
SITES FOR
BASIC

CRYPTOOLS

FILE AND
DISK
ENCRYPTION
TOOL

GNU PRIVACY
GUARD

CONCLUSION

introduction

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

1-A

20-T

20-T

1-A

3-C

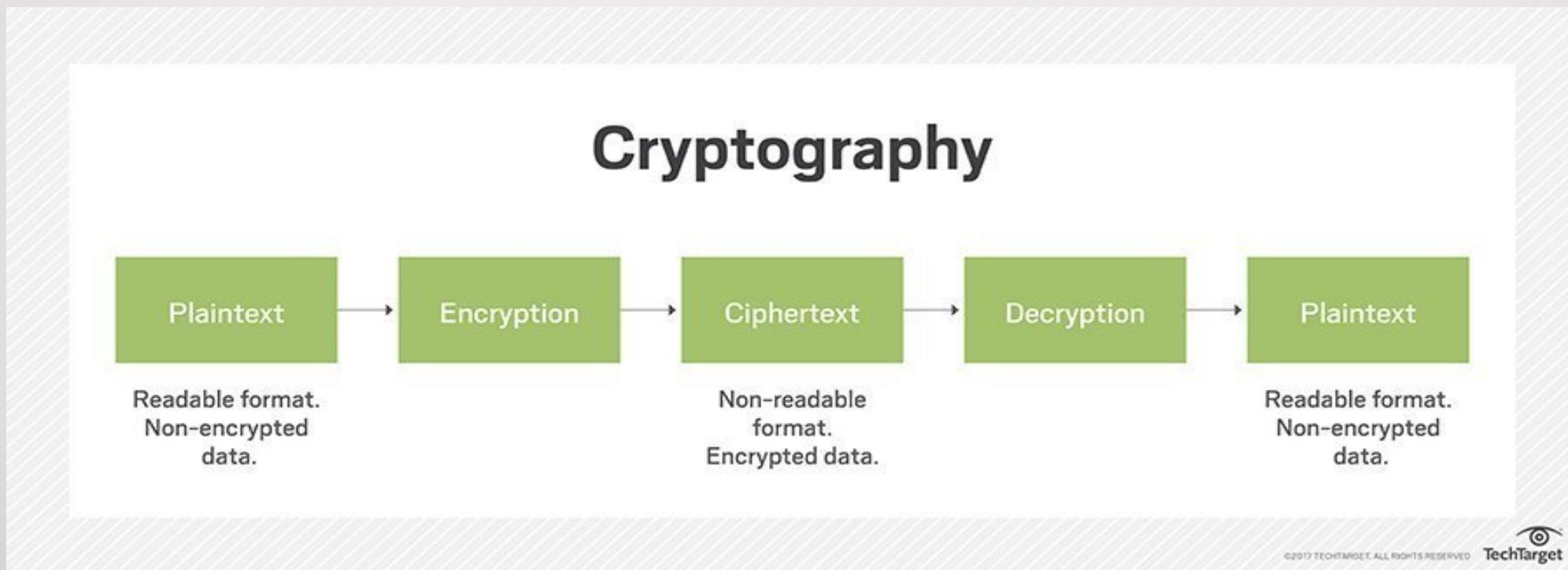
11-K

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

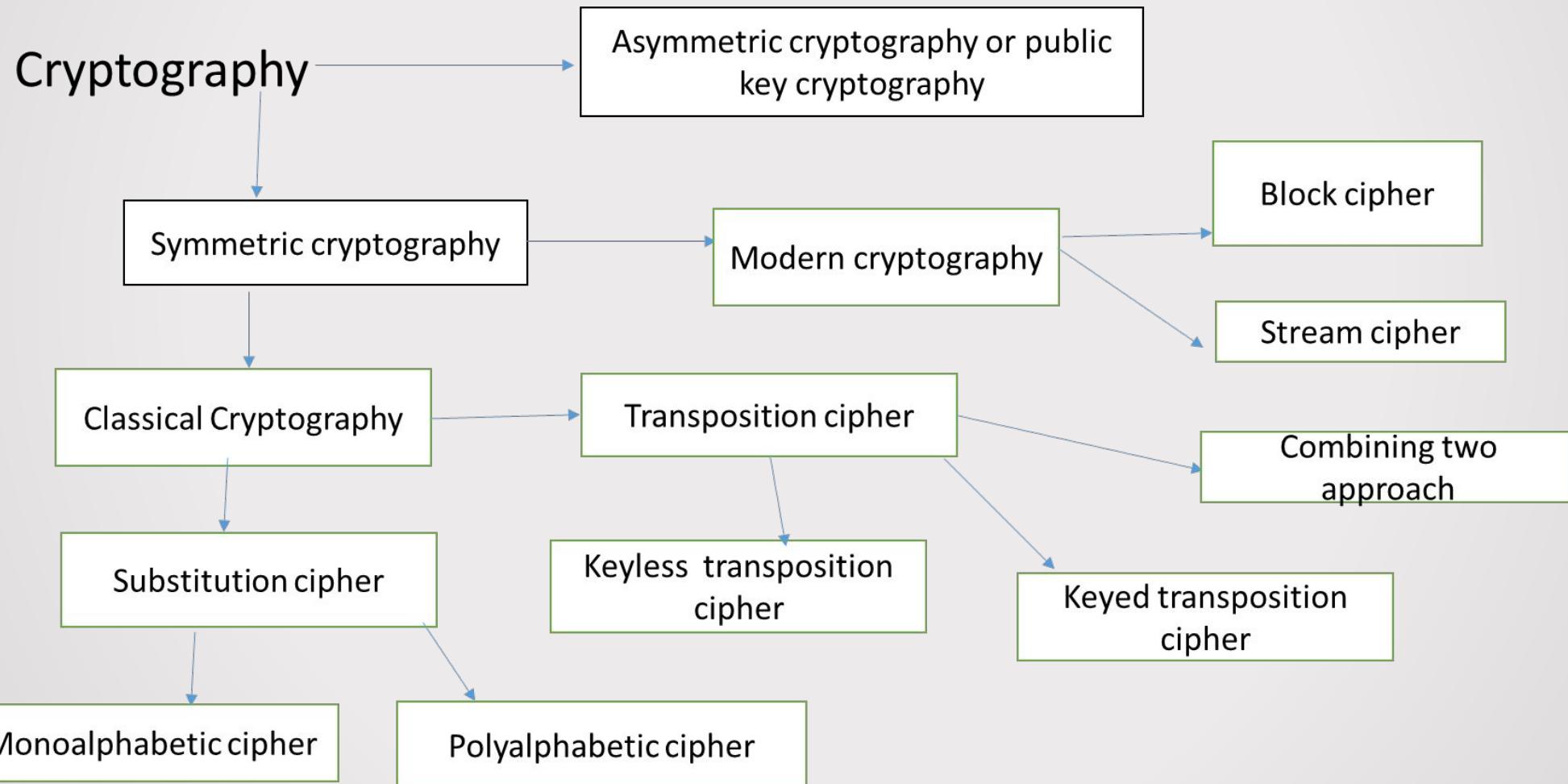
- The history of cryptography starts from the ancient era when it was practiced by secret societies or by troops in battlefields.
- The roots of cryptography are found in Roman and Egyptian civilizations.
- Back to 1900 B.C the Egyptians used to communicate by messages written in hieroglyph.
- During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

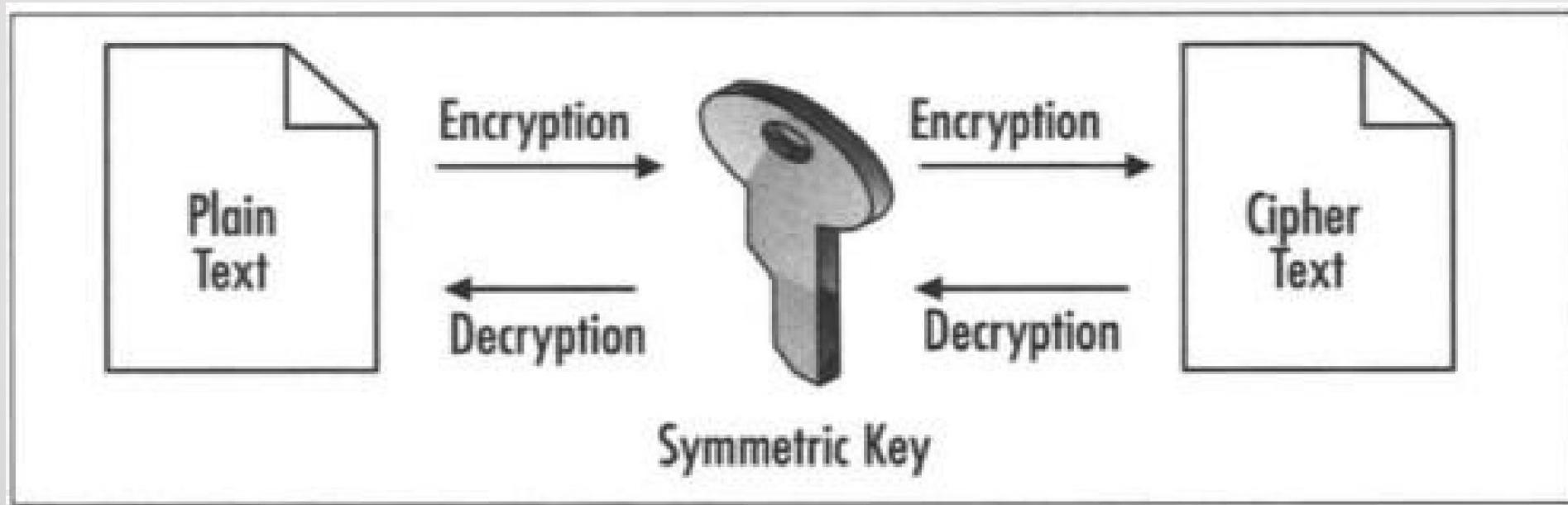
Types of cryptography

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.

MONO-ALPHABETIC
CIPHER

- ✓ Caesar cipher
- ✓ Affine Cipher
- ✓ Additive And Multiplicative Cipher

POLY-ALPHABETIC
CIPHER

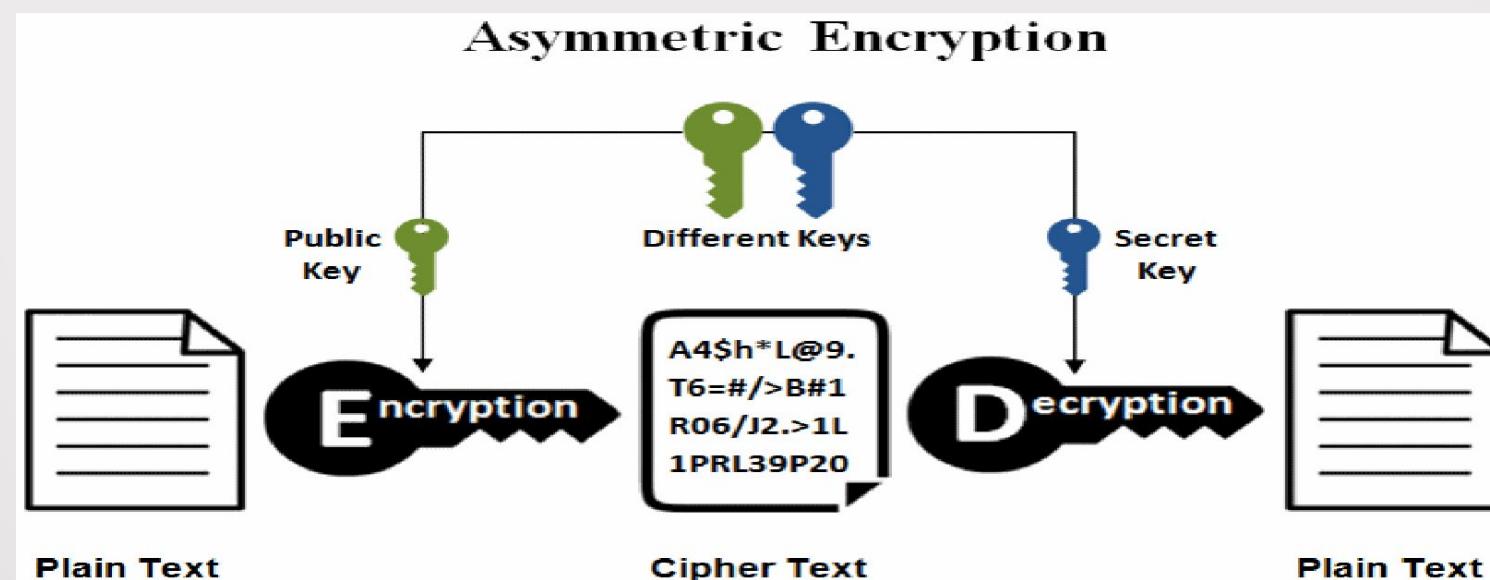
- ✓ Playfair cipher
- ✓ Vigenere Cipher
- ✓ One Time Pad

- Transposition cipher:-

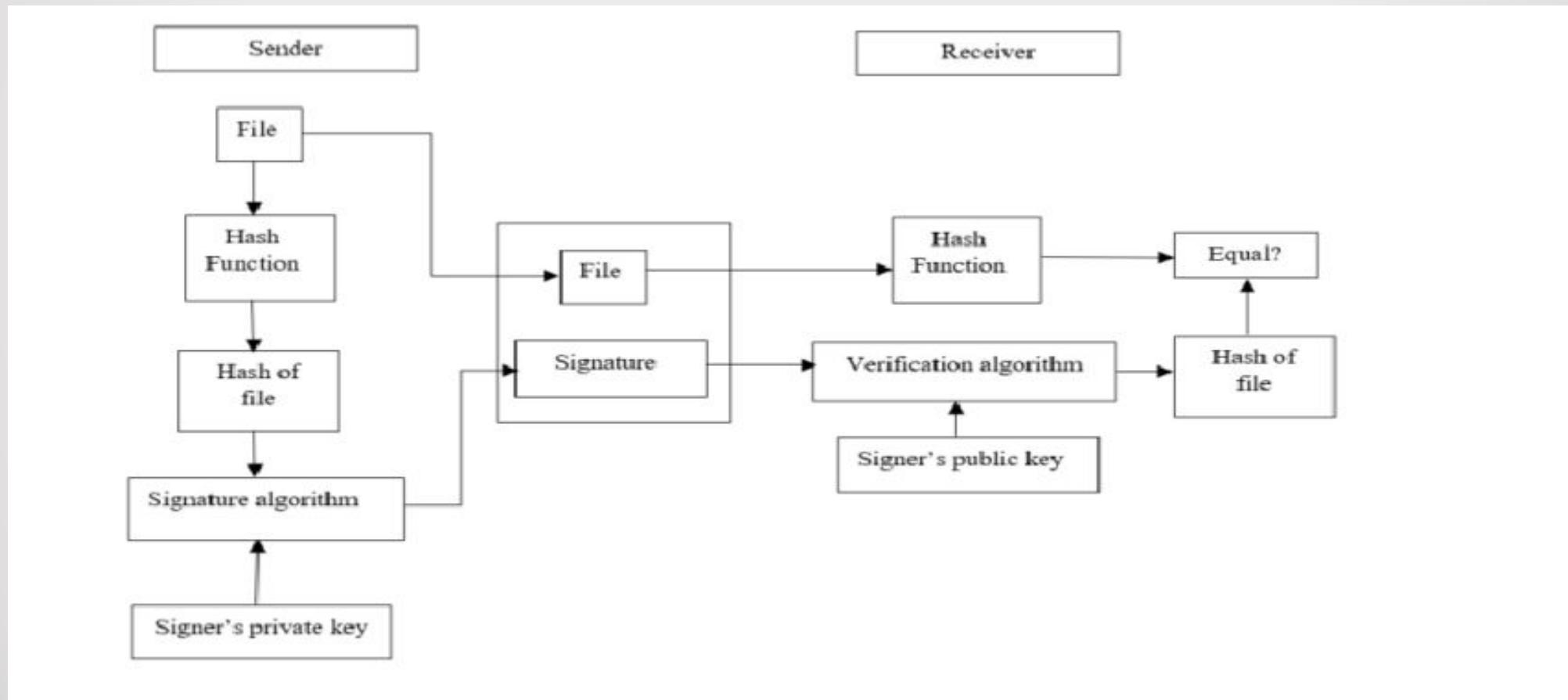
- ✓ Rail fence Cipher
- ✓ Columnar cipher
- ✓ Double columnar Cipher
- ✓ Route Cipher

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

RSA Algorithm

Key Generation

Select p, q

Calculate $n = p \times q$

Calculate $\phi(n) = (p-1)(q-1)$

Select integer e

Calculate d

Public key

Private key

p and q , both prime; $p \neq q$

$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$

$de \bmod \phi(n) = 1$

KU = { e, n }

KR = { d, n }

Encryption

Plaintext:

Ciphertext:

$M < n$

$C = M^e \pmod{n}$

Decryption

Plaintext:

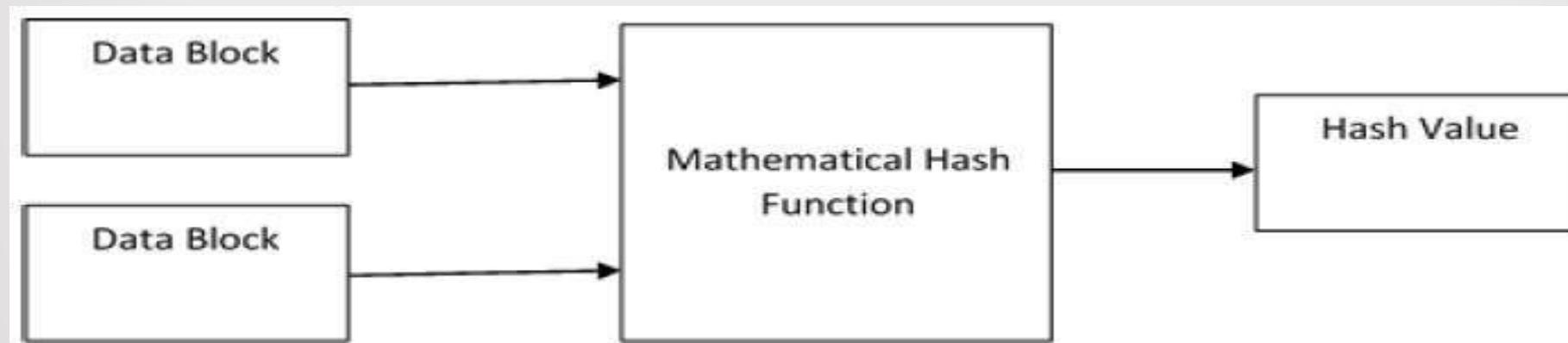
Ciphertext:

C

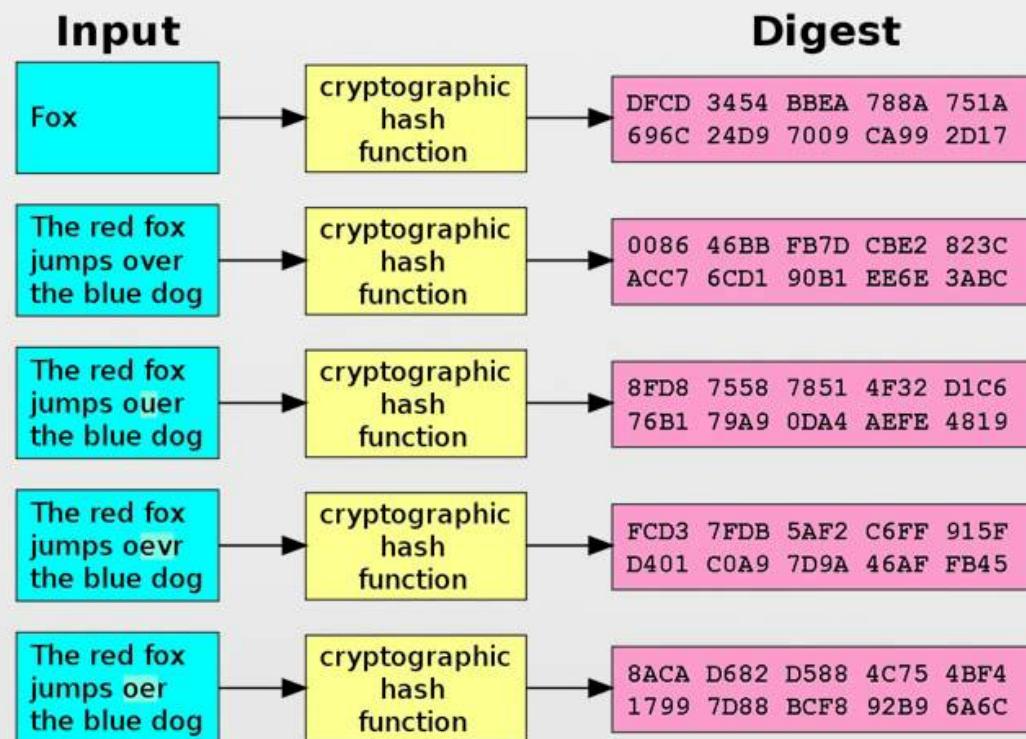
$M = C^d \pmod{n}$

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/>.

The screenshot shows the homepage of the Cryptool Portal. At the top, there is a navigation bar with a magnifying glass icon and the URL "https://www.cryptool.org/en/ct2-downloads". On the right side of the navigation bar are links for "HOME" and "LANGUAGE". Below the navigation bar is a search bar with the placeholder "Search ...". The main header features the "CRYPTOOL PORTAL" logo with the tagline "Cryptography for everybody". A large background image shows a person standing in front of a wall covered in many pieces of paper, possibly representing a cryptanalyst working on a complex problem. In the center, a white callout box contains the text "What is CrypTool 1?". Below this, a paragraph describes CrypTool 1 as an open-source Windows program for cryptography and cryptanalysis, noting it's the most widespread e-learning software of its kind. To the right of this box is a "FREE DOWNLOADS" section with four buttons: "CrypTool 1" (highlighted in blue), "CrypTool 2", "JCrypTool", and "JCT". At the bottom of the page, there is a footer menu with links: "About CrypTool", "Documentation", "Education", "Contributors", and "Links / Books". The footer also includes a "CRYPTOOL NEWS" section with a "policy" link and a "The CrypTool Portal" section.

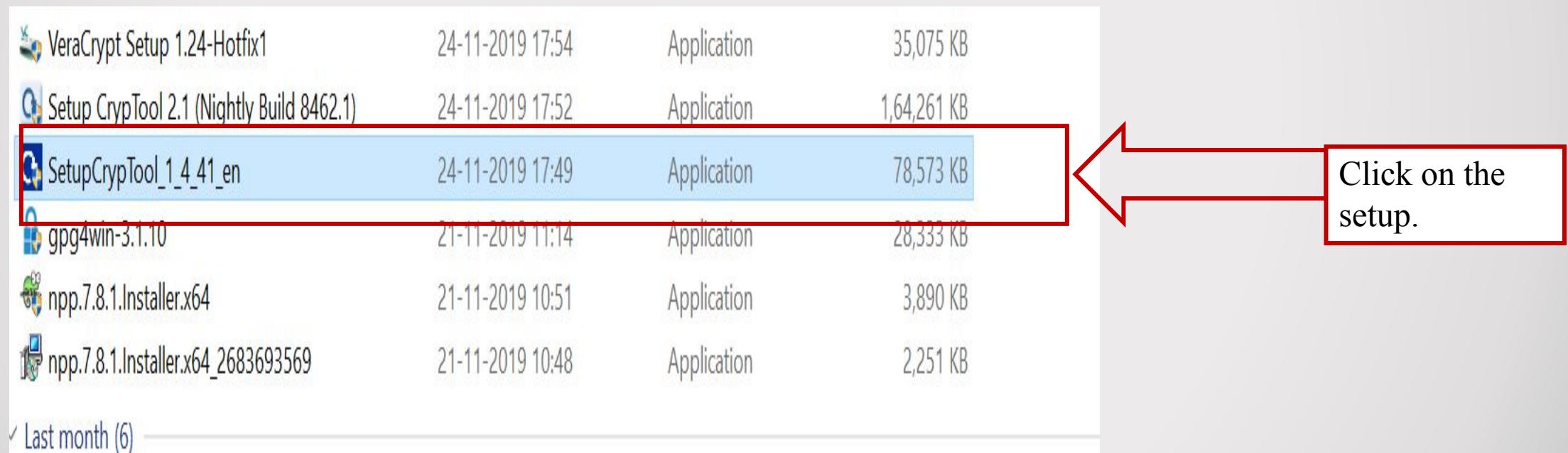
Cryptool1

- **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

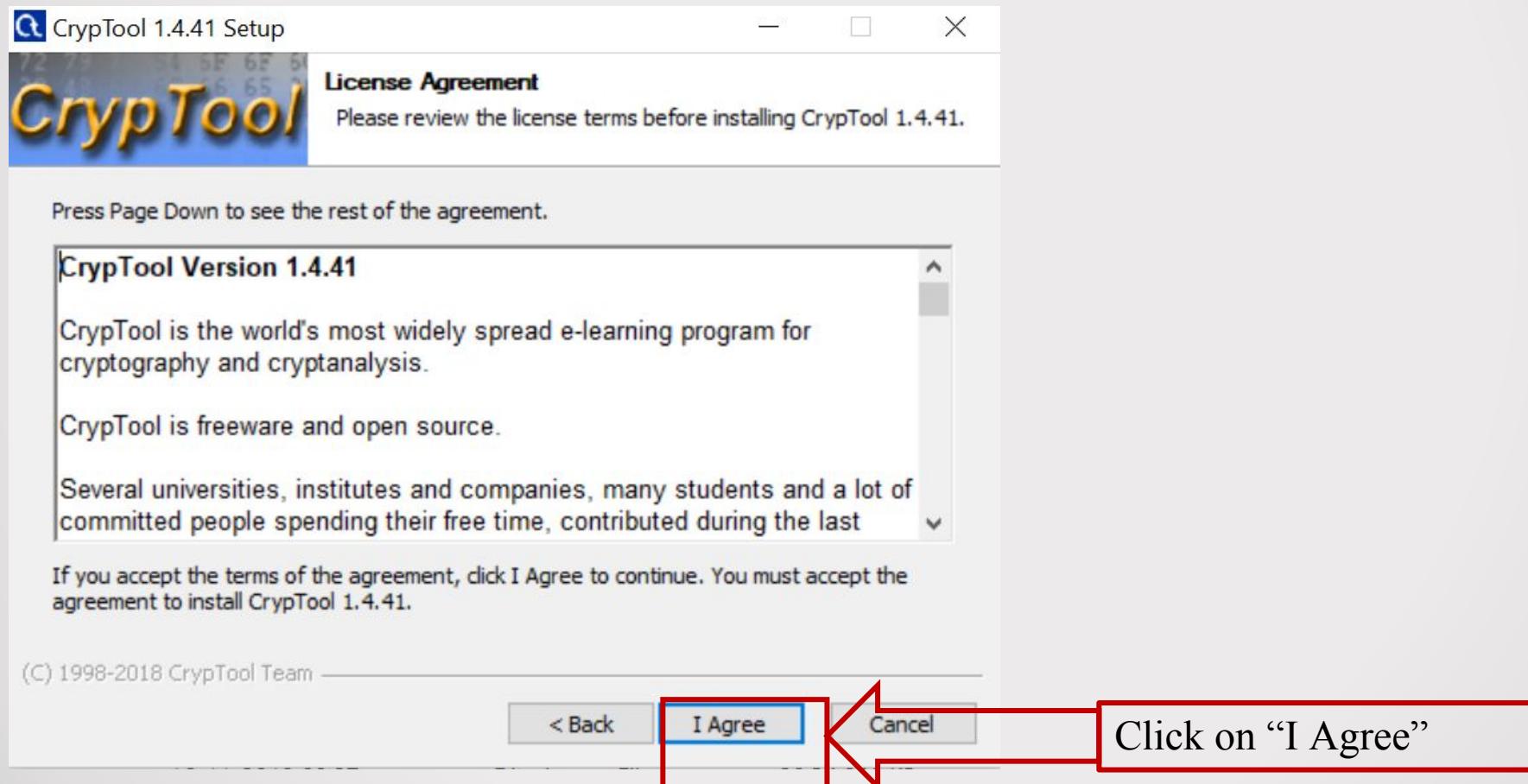
Step 1:-To download the cryptool11:- <https://www.cryptool.org/en/ct1-downloads>



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



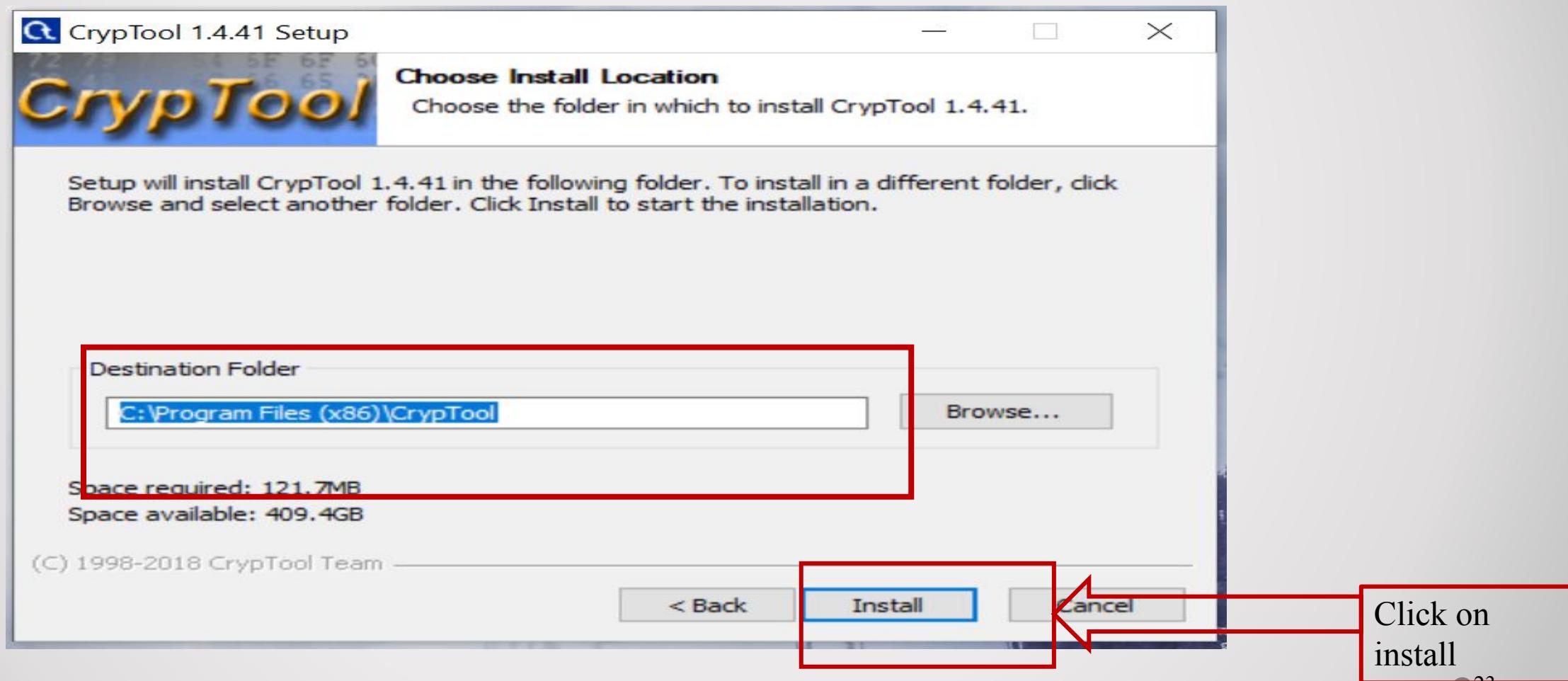
Step 3:- Agreement of license



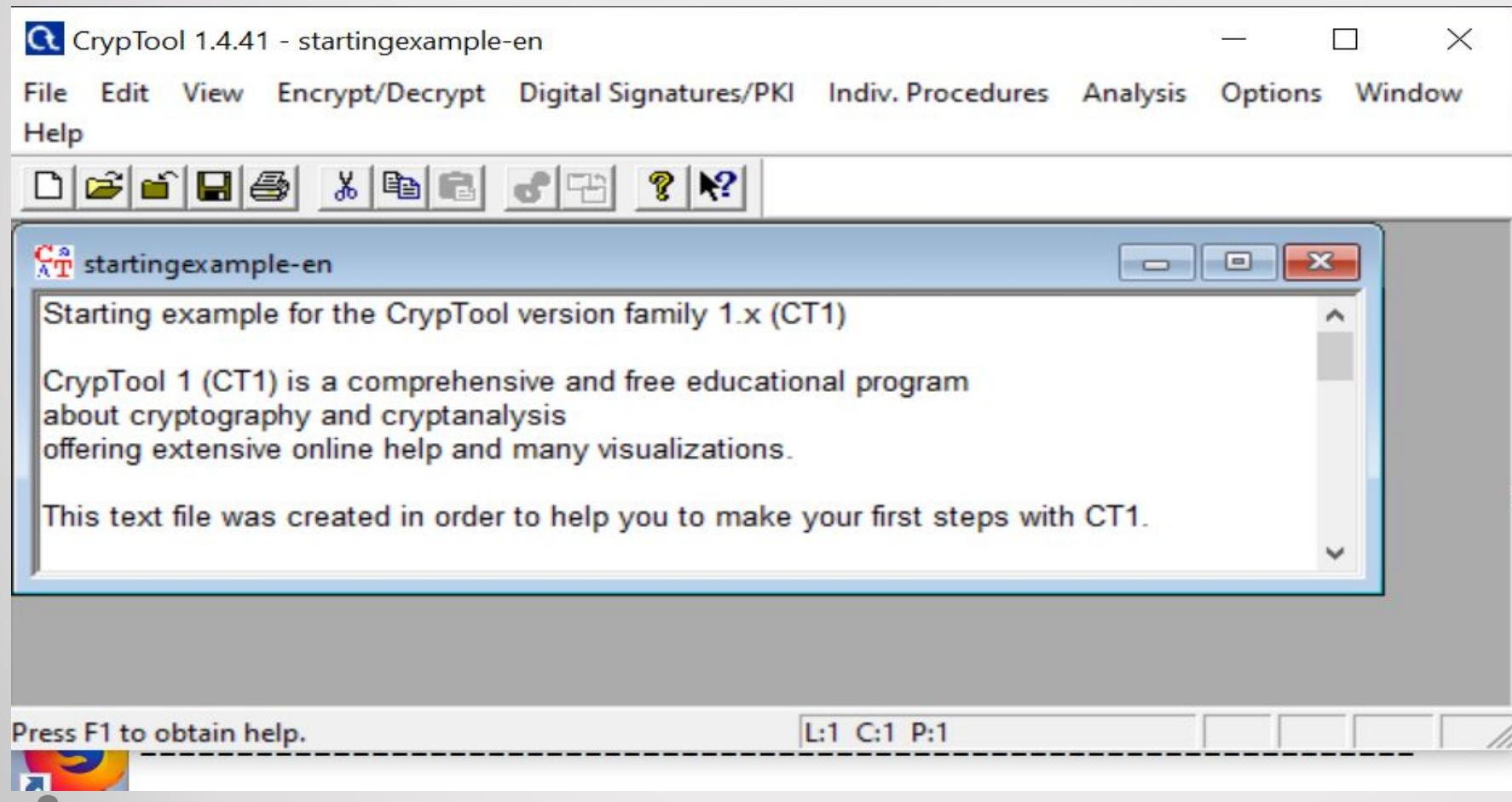
Step 4:- What type of installation you need?



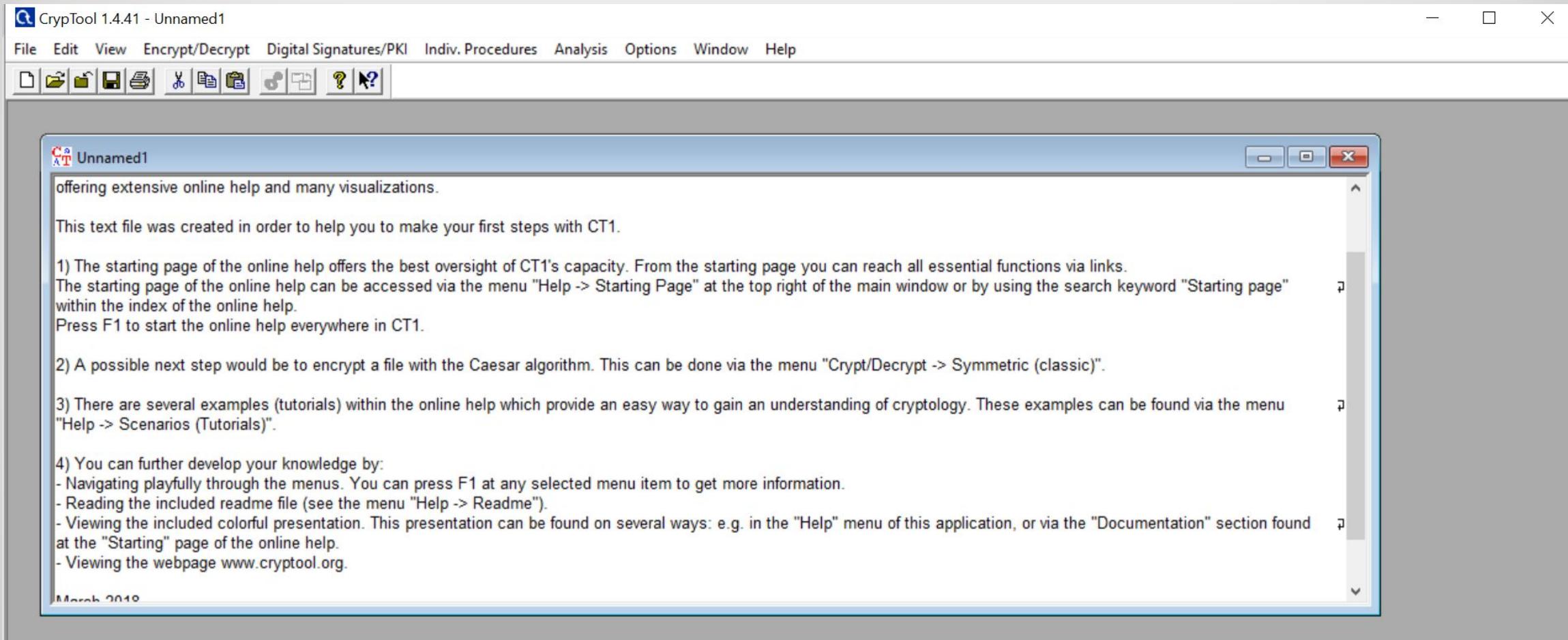
Step 5:- Set up the path:-



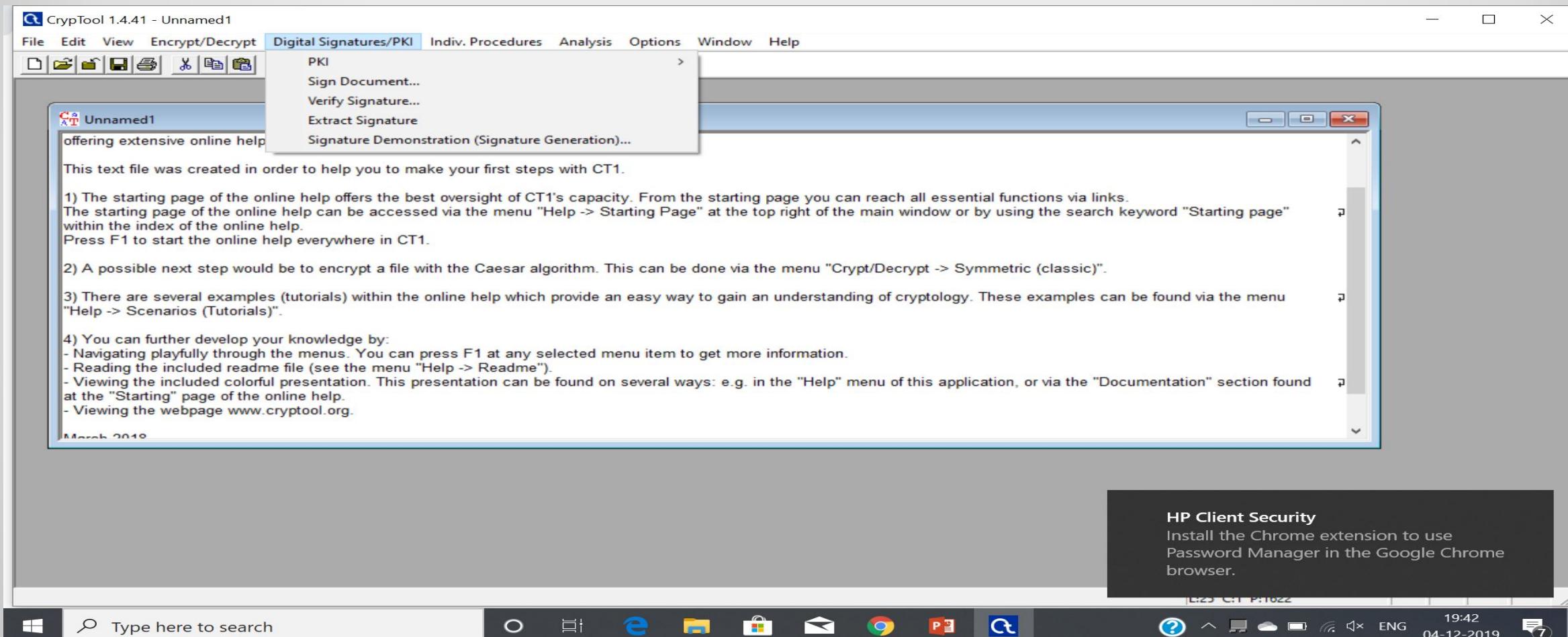
Step 6 :- We get the wizard page



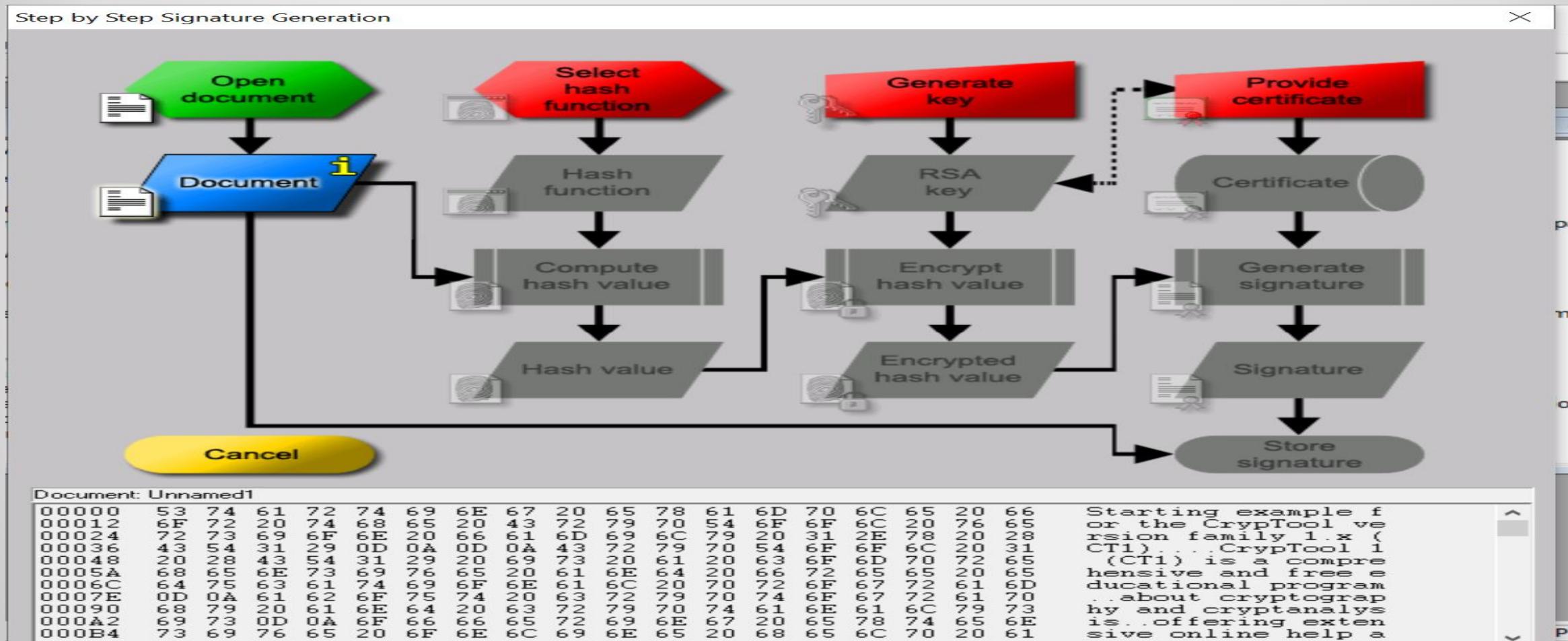
STEP 7:- CLICK ON NEW TO CREATE A WORKSPACE



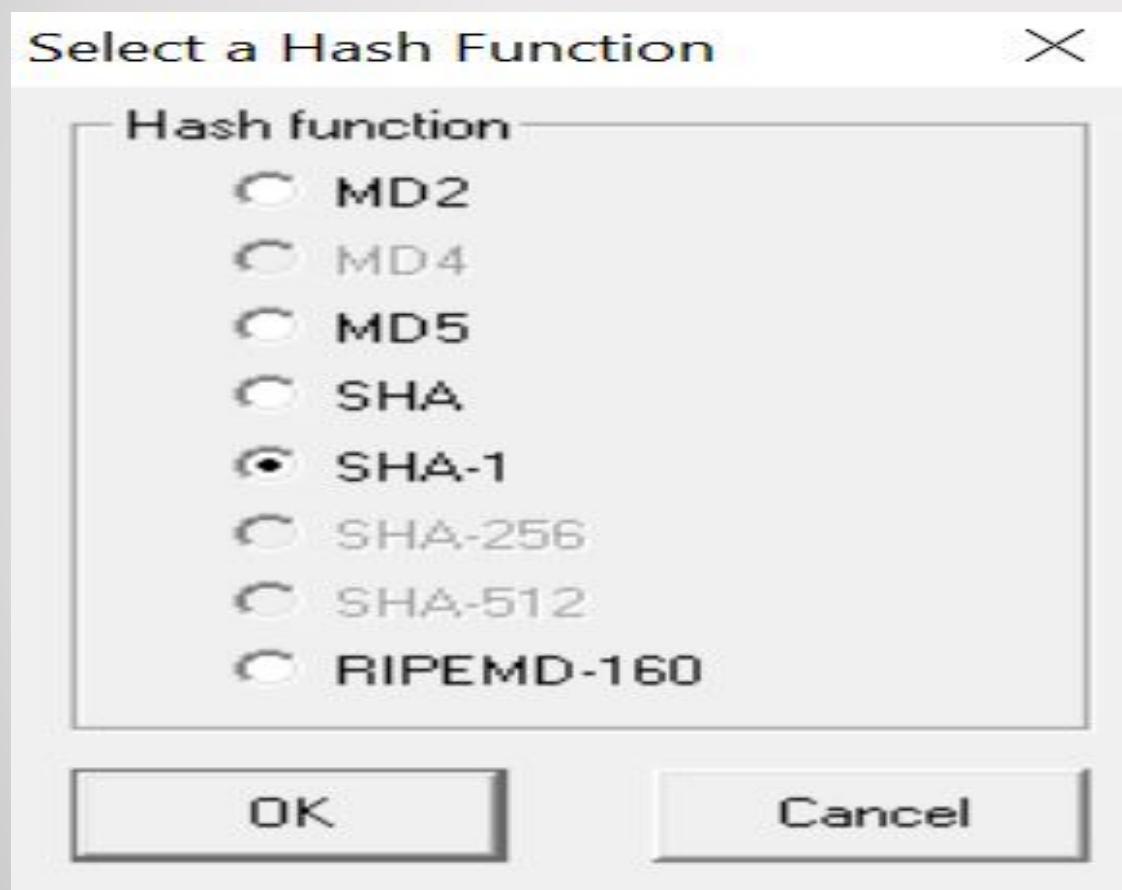
STEP8:- AFTER CREATING THE WORKSPACE COPY OR WRITE A TEXT MESSAGE



EXAMPLE OF DIGITAL SIGNATURE



HASH FUNCTION USED AND ITS VALUE



SIGNING ALGORITHM(RSA)

Generate RSA Key X

Choose two prime numbers p and q. The number $N = pq$ is the public RSA modulus and $\phi(N) = (p-1)(q-1)$ is the Euler phi function. Public key e is coprime to $\phi(N)$. The private key $d = e^{-1} \pmod{\phi(N)}$ is calculated from this.

Prime number entry

Prime number p	<input type="text" value="7737617864374887016571159424651"/>	<input type="button" value="Generate prime numbers..."/>
Prime number q	<input type="text" value="1434298724673852070184430816748"/>	p and q are prime numbers.

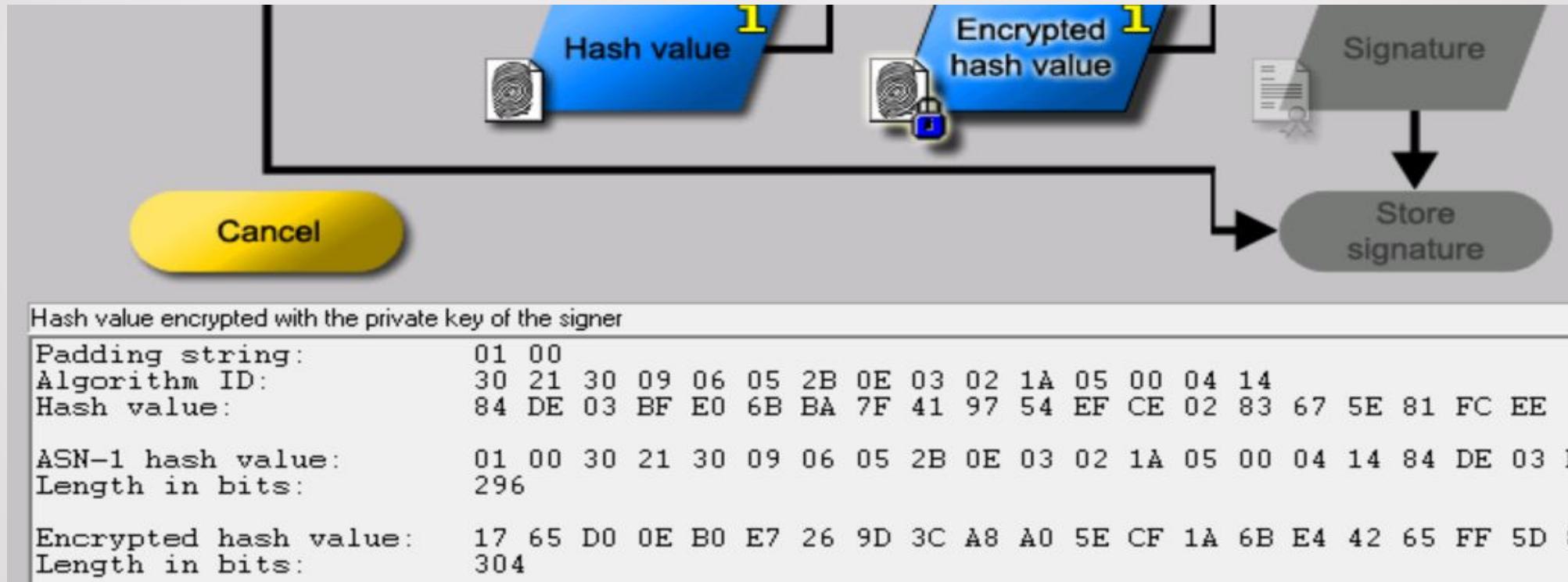
RSA parameter

Length	<input type="text" value="304 bit"/>
RSA modulus N	<input type="text" value="3475540152245156575672595655541"/> (public)
$\phi(N) = (p-1)(q-1)$	<input type="text" value="3475540152245156575672595655541"/> (secret)
Public key e	<input type="text" value="2^16+1"/> e does not divide $\phi(N)$.
Private key d	<input type="text" value="9391918472963627104561037133166"/>

RSA KEY OF SIGNER

RSA key of signer	
Bit length of N:	304
RSA modulus N:	3475540152245156575672595655541174668192098004113331077900989081
phi(N) = (p-1)(q-1):	3475540152245156575672595655541174668192098000255868968601339271
Public key:	65537
Private key:	9391918472963627104561037133166639207422075405424636378523539156

HASH VALUE ENCRYPTED WITH SIGNER PRIVATE KEY



CREATION OF CERTIFICATE

Create Certificate and PSE ×

Public RSA parameter

Bit length:

RSA modulus N:

Public key e:

Personal data for the certificate

Name:

First name:

Key identifier: (optional)

PIN:

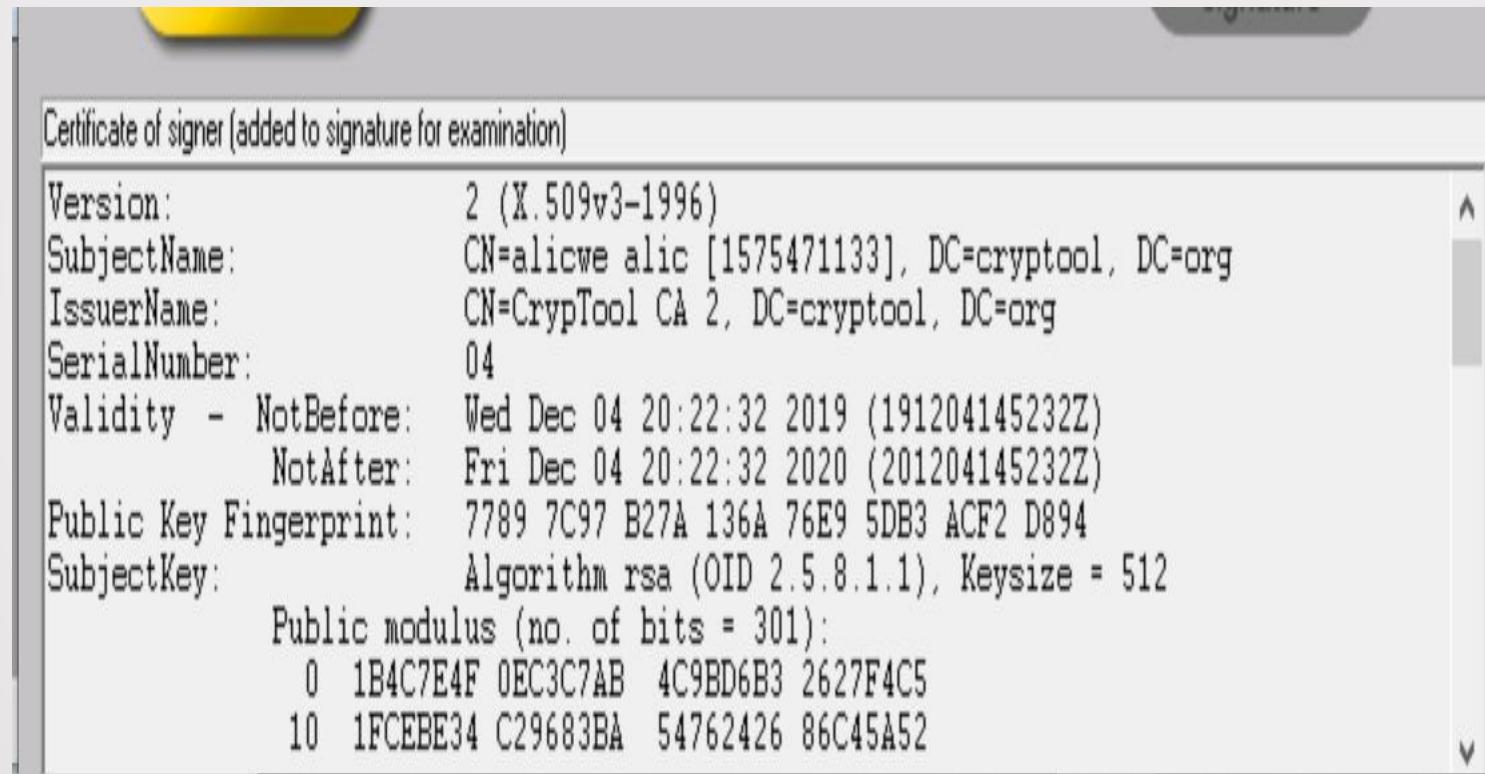
PIN verification:

Generated names for PSE and certificate

User Key ID:

Distinguished Name:

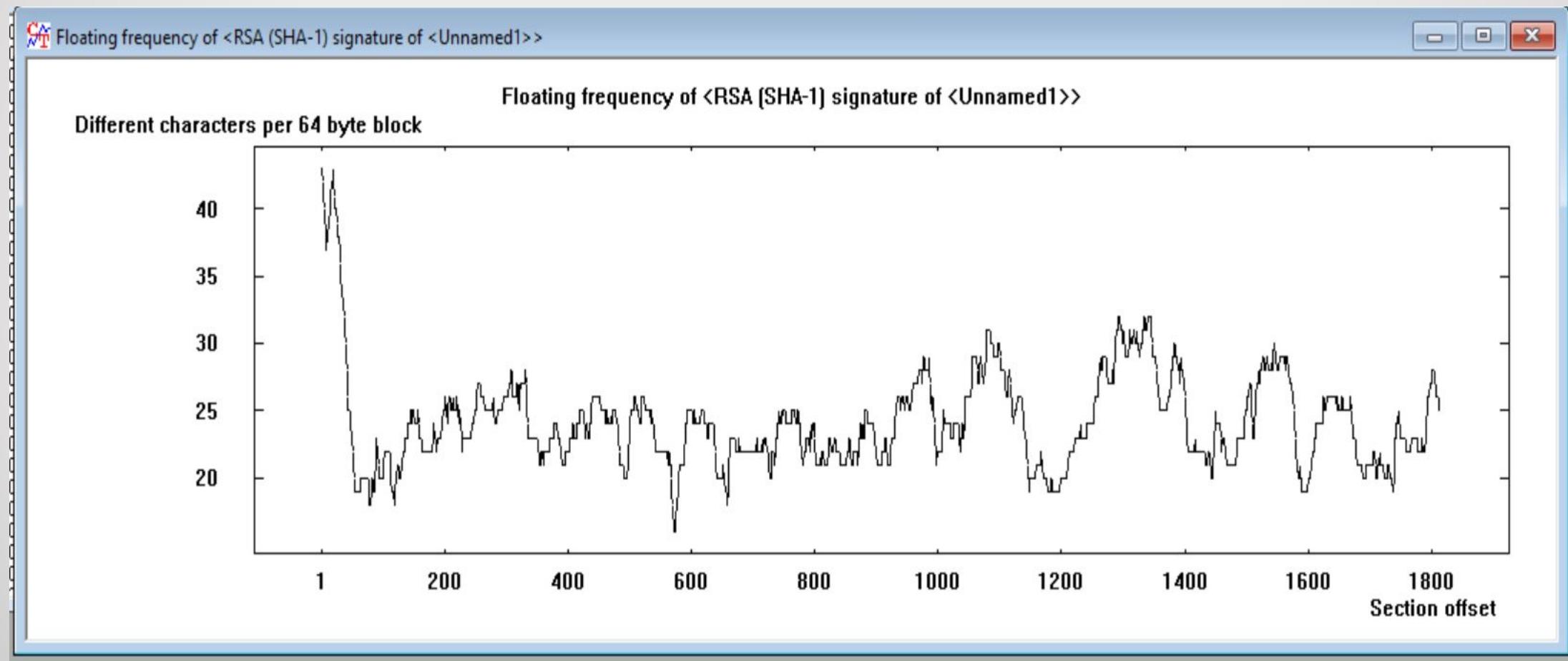
SIGNATURE VERIFICATION



GENERATED SIGNATURE

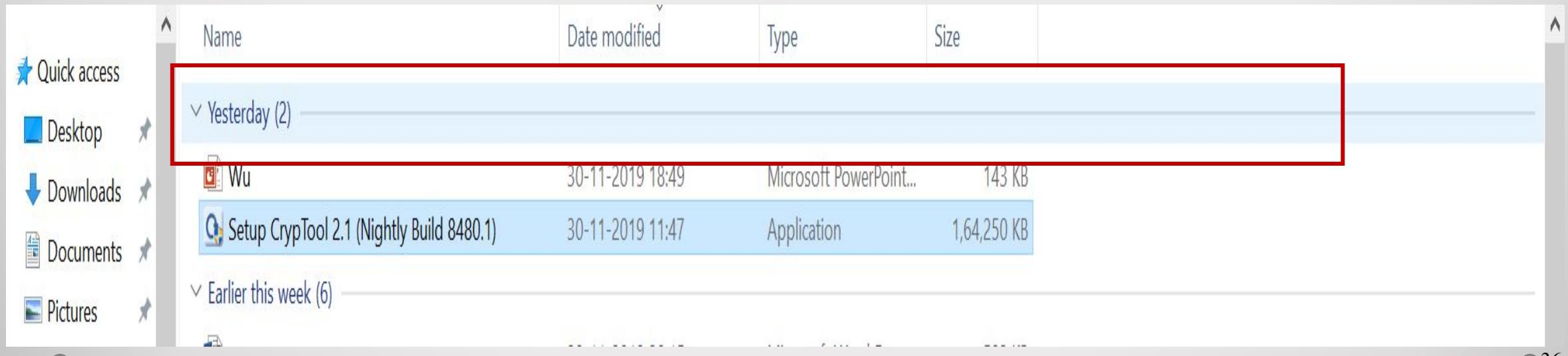
SHA-1 signature of <Unnamed1>	
00000	53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 20 17
00012	65 D0 0E B0 E7 26 9D 3C A8 A0 5E CF 1A 6B E4 42 65 FF
00024	eD .ç&. < ^İ .käBey
00036	5D 8A 0D 55 93 17 E1 DA 34 CD DA E4 B9 C4 84 B2 A4 61
00048] ..áU4fÜä¹Ä .²¤a
0005A	BB 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53 » S
0006C	69 67 6E 61 74 75 72 65 20 6C 65 6E 67 74 68 3A 20 20
0007E	signature length:
00090	33 30 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 304
000A2	20 41 6C 67 6F 72 69 74 68 6D 3A 20 20 20 20 20 20 52
000B4	Algorithm: R
000C4	53 41 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000D6	SA
000E8	48 61 73 68 20 66 75 6E 63 74 69 6F 6E 3A 20 20 20 53
000FA	Hash function: S
000G2	48 41 2D 31 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000H4	HA-1
000I6	20 20 4B 65 79 3A 20 20 20 20 20 5B 61 6C 69 63 5D
000J8	Key: [alic]

FREQUENCY ANALYSIS

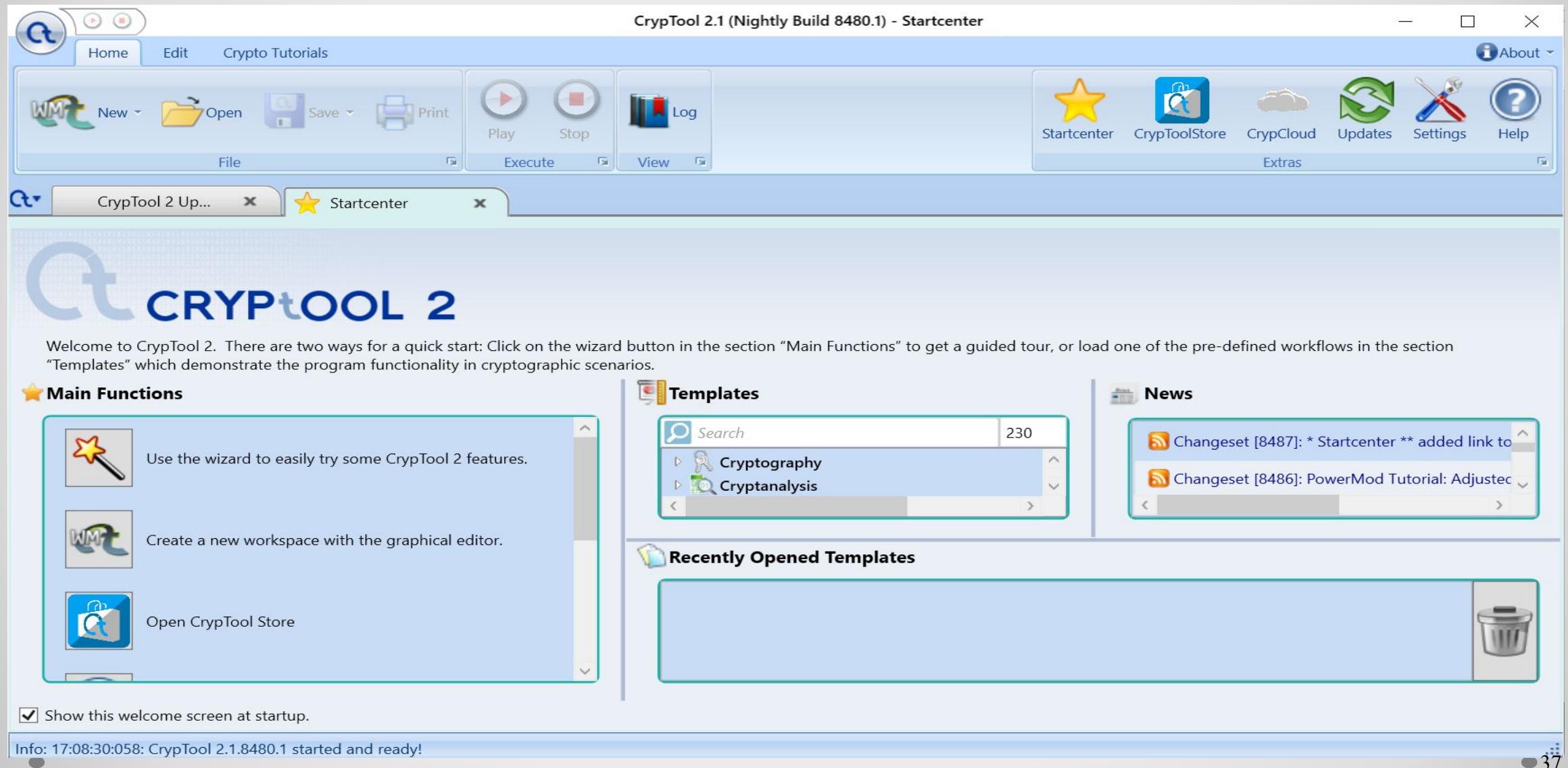


Cryptool 2

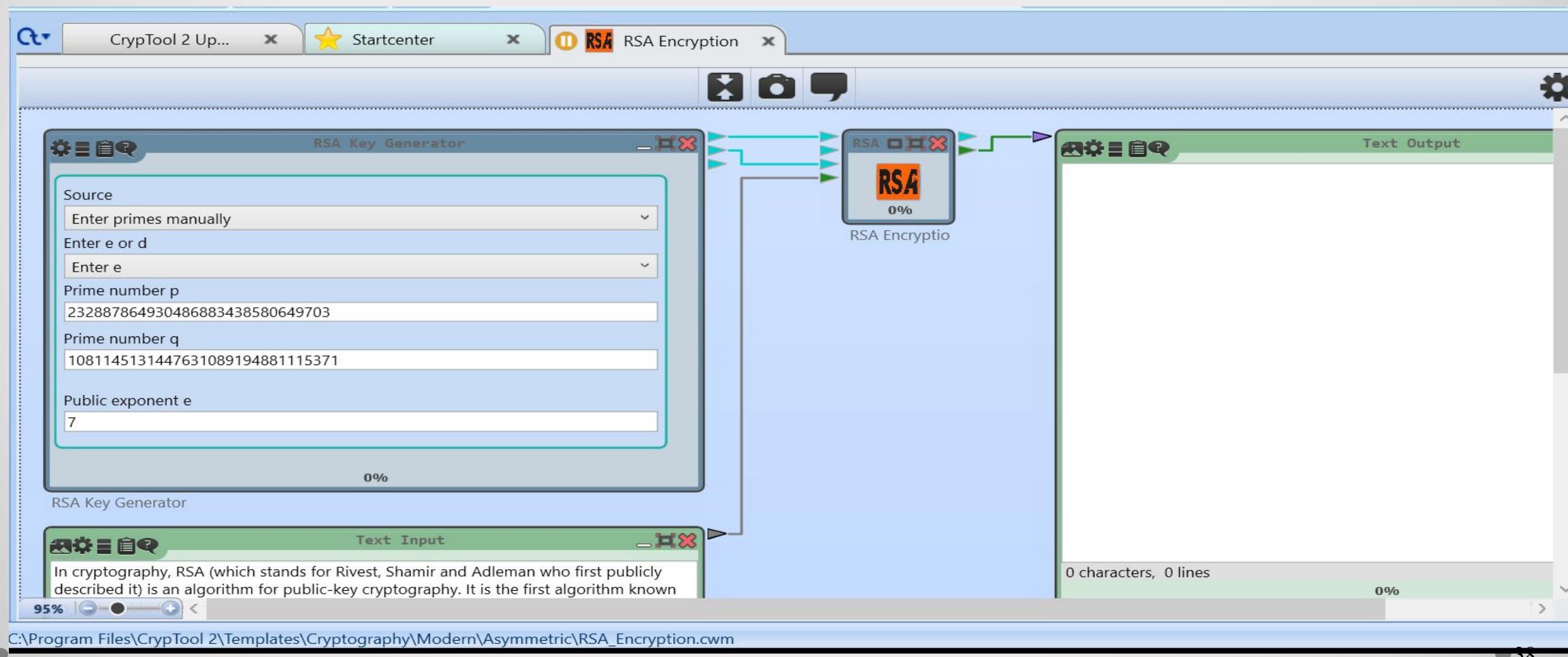
- It uses the concept of visual programming to clarify cryptographic processes.
Currently, CT2 contains more than 150 crypto functions.
- To download it:-<https://www.cryptool.org/en/ct2-downloads>
- After download we get:-



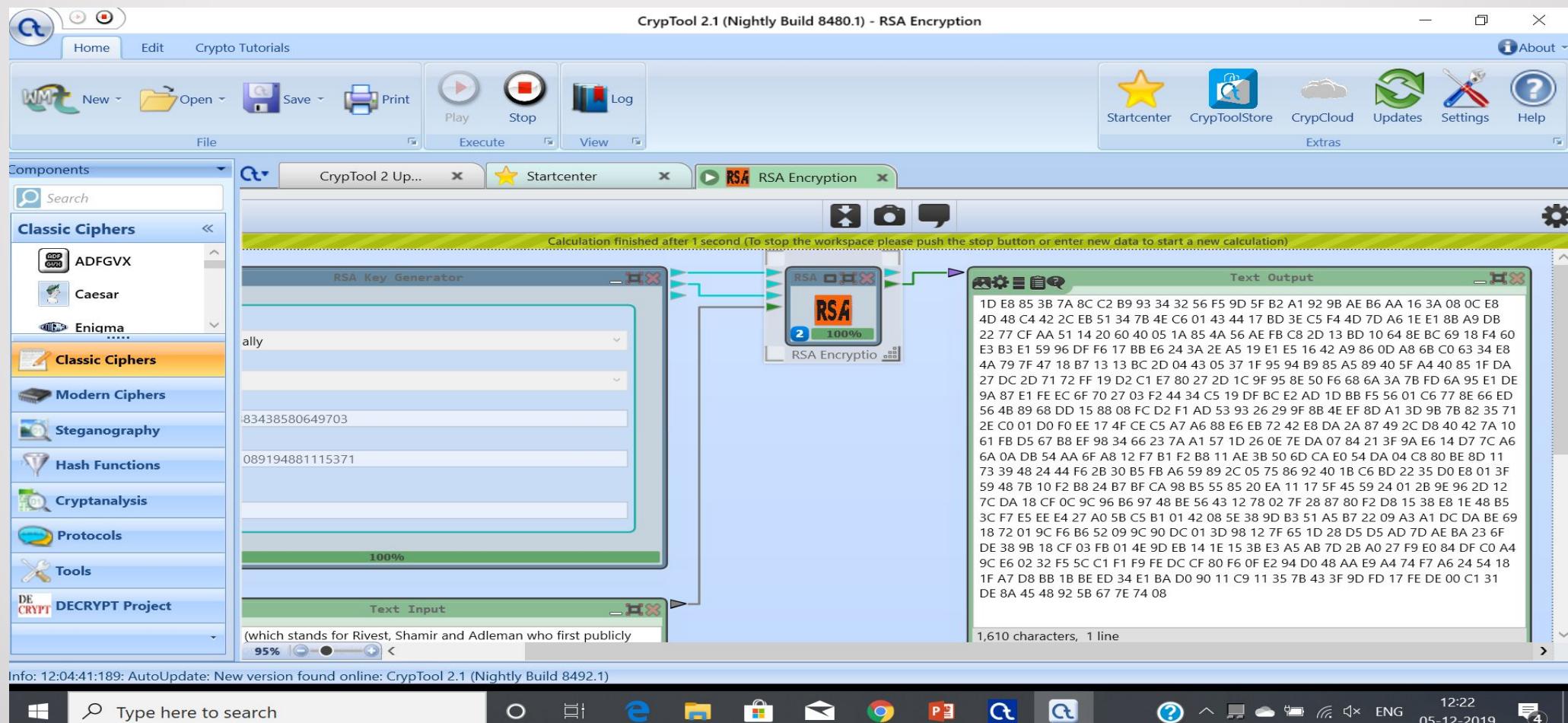
- For installation I will proceed in the same manner as cryptool-1.



WORKING WITH CRYPTOTOOL USING RSA



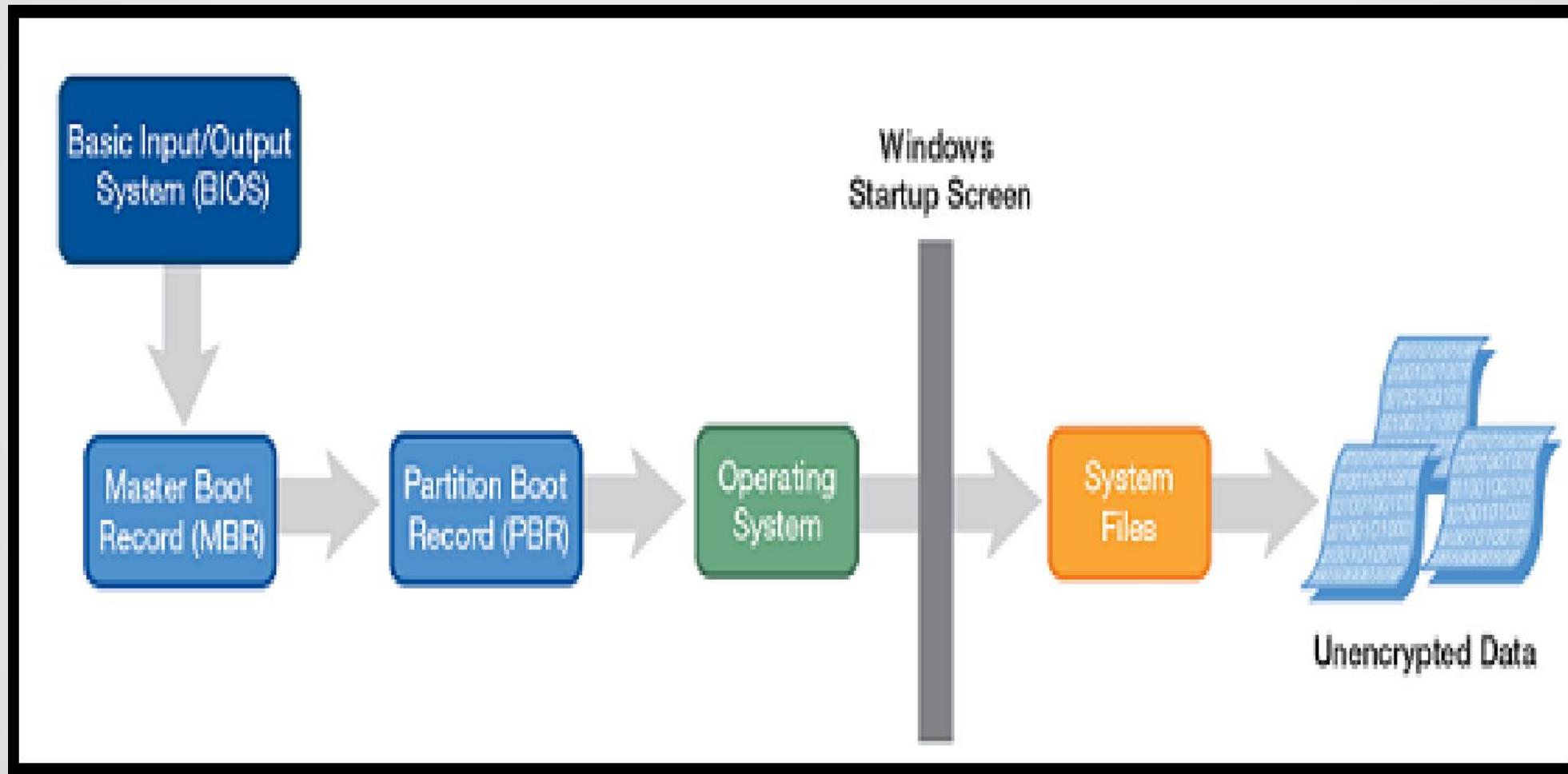
RESULT AFTER CLICKING PLAY



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

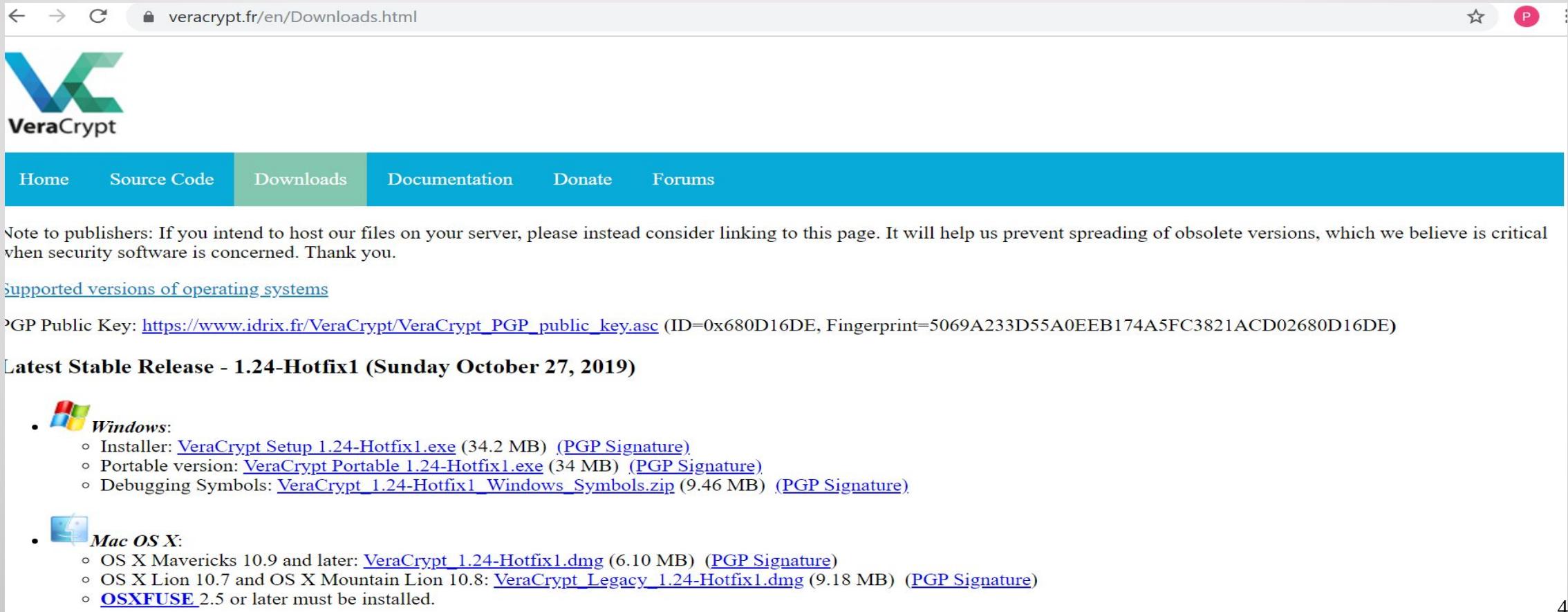
- The **Encrypting File System (EFS)** on [Microsoft Windows](#) is a feature introduced in version 3.0 of [NTFS](#).
- The technology enables files to be [transparently encrypted](#) to protect confidential data from attackers with physical access to the computer.

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>



The screenshot shows a web browser displaying the VeraCrypt Downloads page at <https://www.veracrypt.fr/en/Downloads.html>. The page features a large VeraCrypt logo and navigation links for Home, Source Code, Downloads, Documentation, Donate, and Forums. A note to publishers about linking to the page is present. Below, it lists the latest stable release (1.24-Hotfix1) from October 27, 2019, and provides download links for Windows and Mac OS X, including PGP signatures.

Note to publishers: If you intend to host our files on your server, please instead consider linking to this page. It will help us prevent spreading of obsolete versions, which we believe is critical when security software is concerned. Thank you.

[Supported versions of operating systems](#)

PGP Public Key: https://www.idrix.fr/VeraCrypt/VeraCrypt_PGP_public_key.asc (ID=0x680D16DE, Fingerprint=5069A233D55A0EEB174A5FC3821ACD02680D16DE)

Latest Stable Release - 1.24-Hotfix1 (Sunday October 27, 2019)

-  **Windows:**
 - Installer: [VeraCrypt Setup 1.24-Hotfix1.exe](#) (34.2 MB) ([PGP Signature](#))
 - Portable version: [VeraCrypt Portable 1.24-Hotfix1.exe](#) (34 MB) ([PGP Signature](#))
 - Debugging Symbols: [VeraCrypt 1.24-Hotfix1_Windows_Symbols.zip](#) (9.46 MB) ([PGP Signature](#))
-  **Mac OS X:**
 - OS X Mavericks 10.9 and later: [VeraCrypt 1.24-Hotfix1.dmg](#) (6.10 MB) ([PGP Signature](#))
 - OS X Lion 10.7 and OS X Mountain Lion 10.8: [VeraCrypt_Legacy_1.24-Hotfix1.dmg](#) (9.18 MB) ([PGP Signature](#))
 - [OSXFUSE](#) 2.5 or later must be installed.

Installation for windows

- Step1:-

Latest Stable Release - 1.24-Hotfix1 (Sunday October 27, 2019)



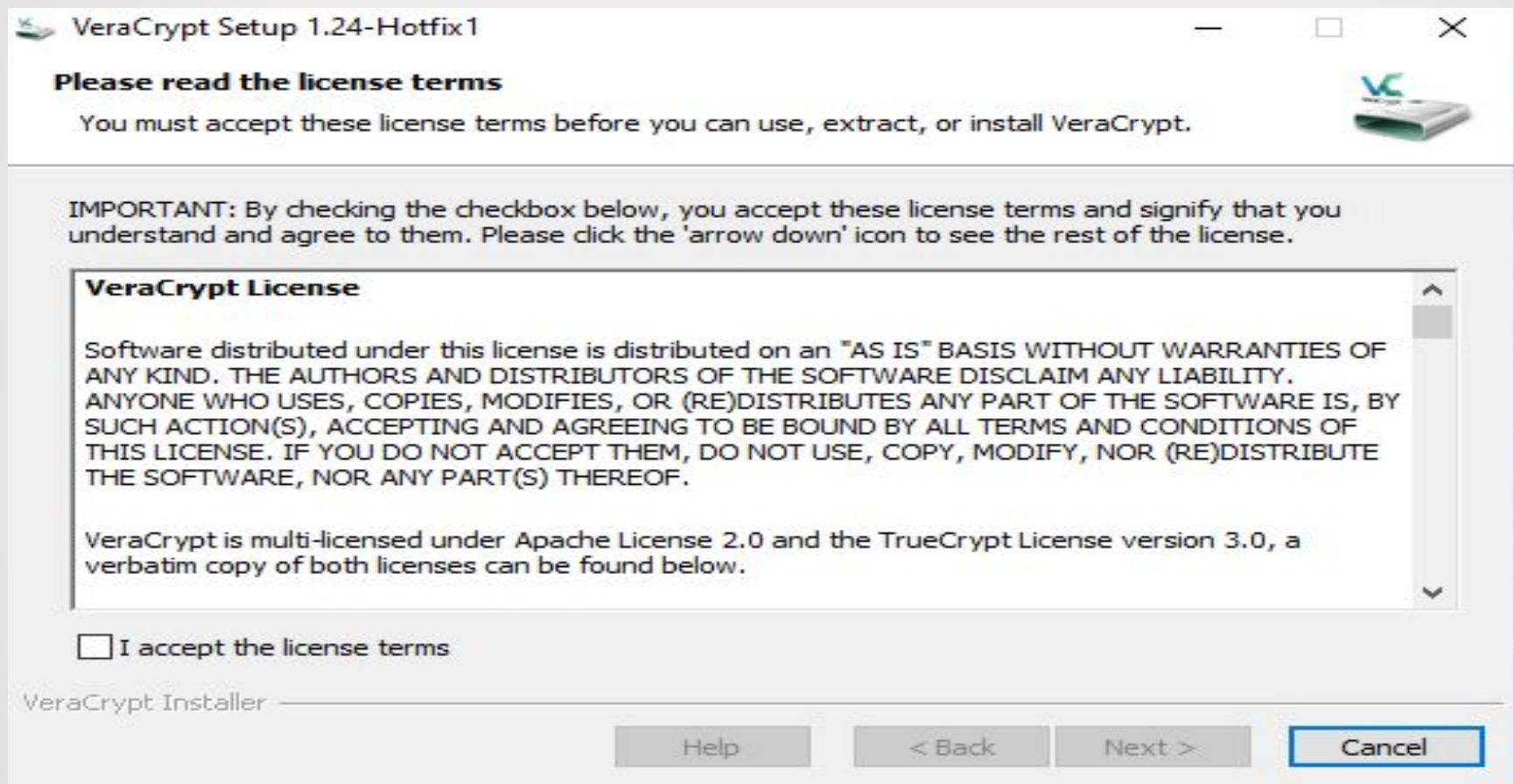
Windows:

- Installer: [VeraCrypt Setup 1.24-Hotfix1.exe](#) (34.2 MB) ([PGP Signature](#))
- Portable version: [VeraCrypt Portable 1.24-Hotfix1.exe](#) (34 MB) ([PGP Signature](#))
- Debugging Symbols: [VeraCrypt 1.24-Hotfix1 Windows Symbols.zip](#) (9.46 MB) ([PGP Signature](#))

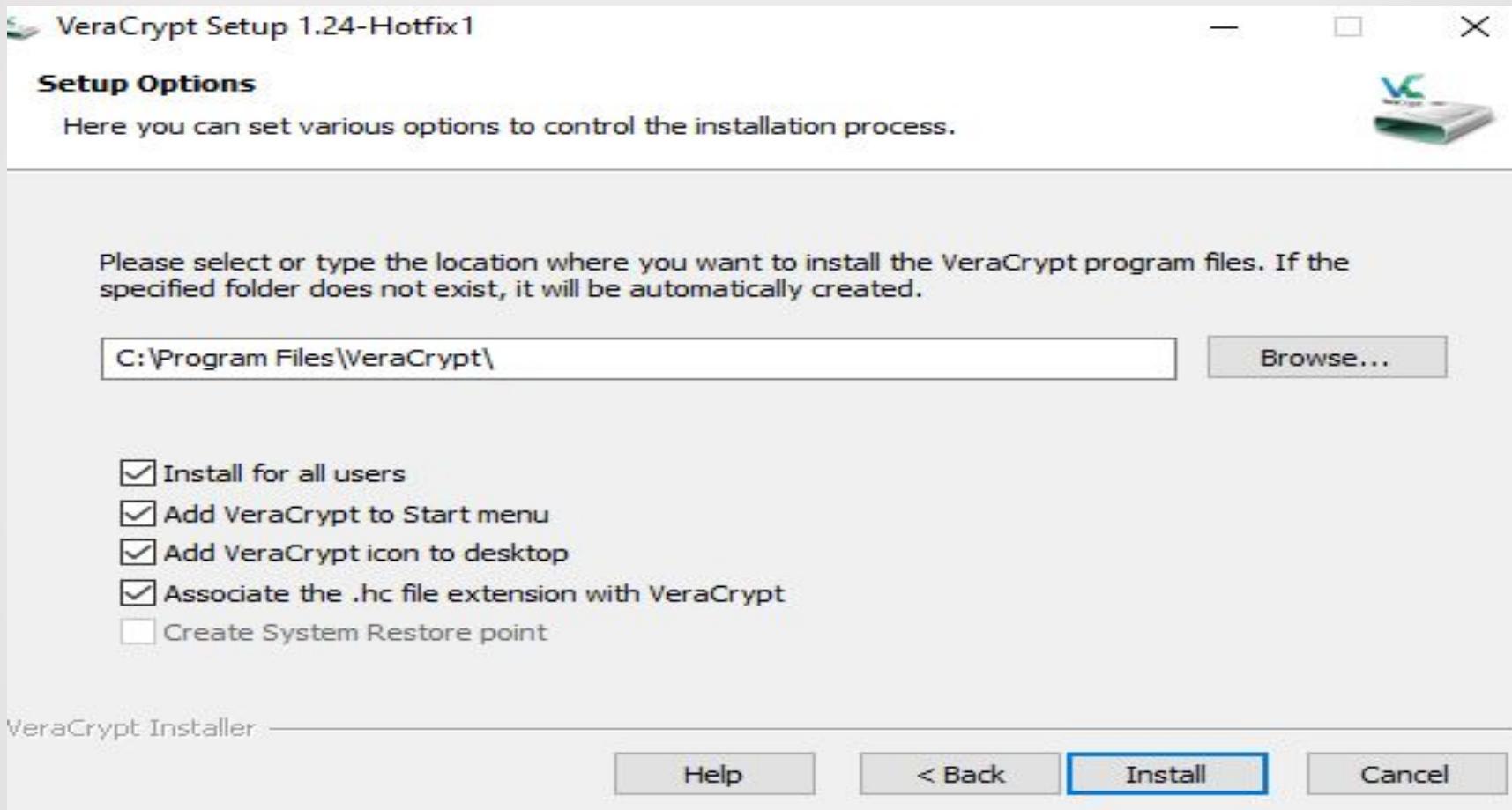


- As soon as it got downloaded and we click on the set up we get the following

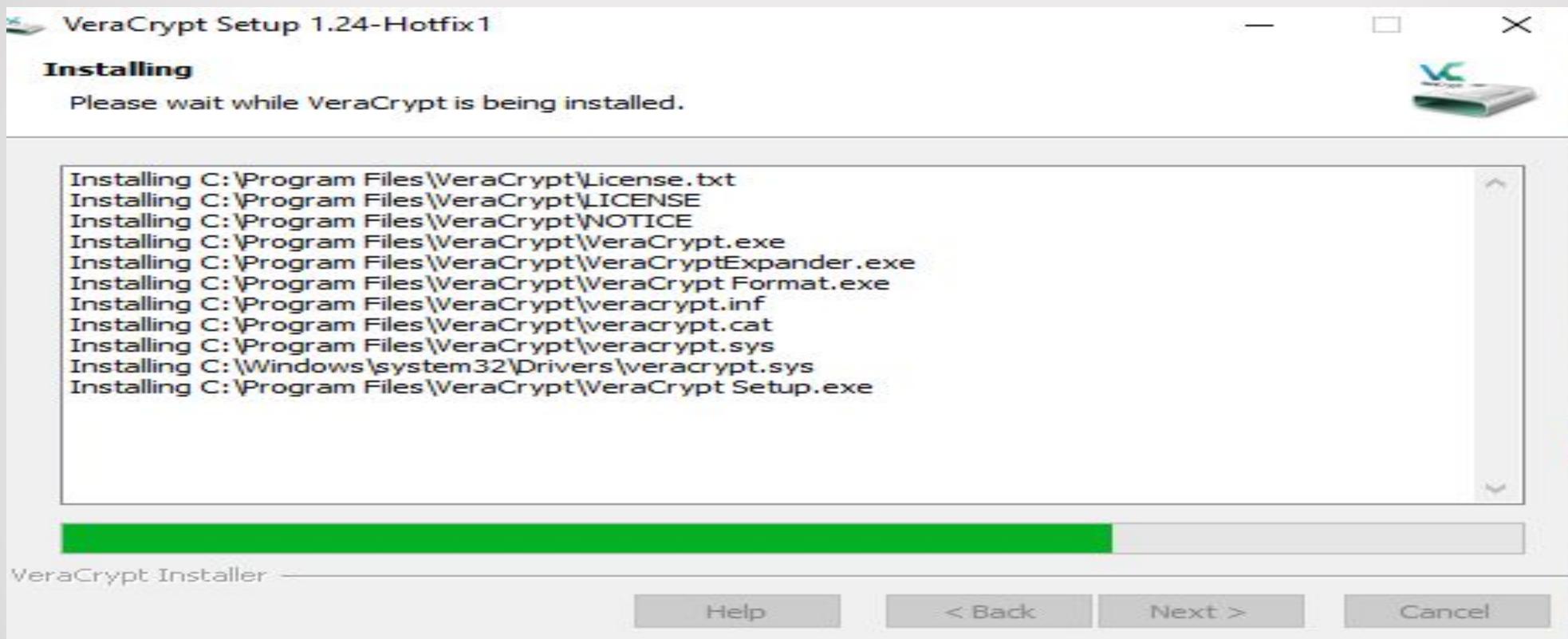
- Step2:- This page is the license agreement:-



- Step 3:- Path setup:-

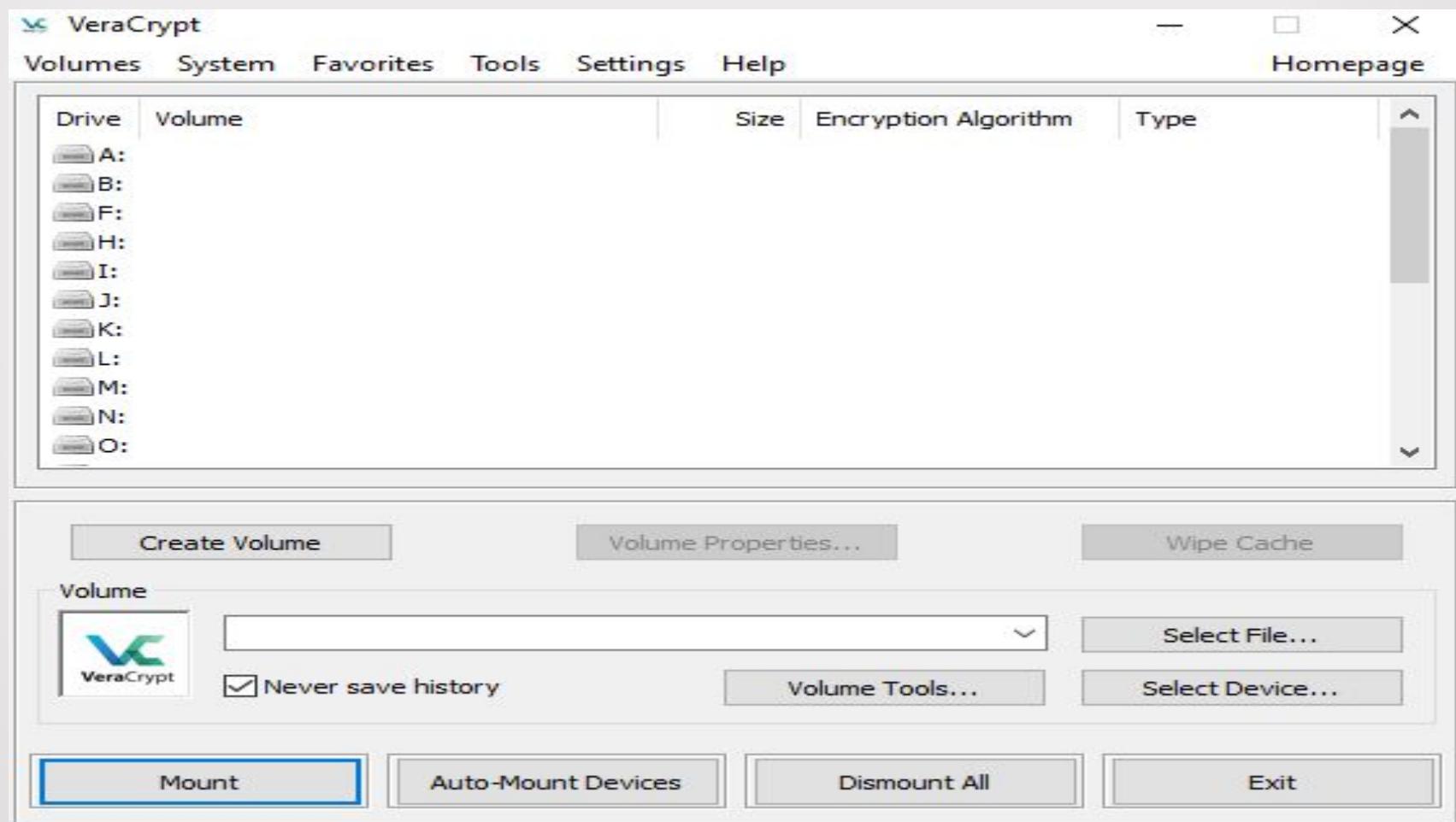


- Now the installation process :-

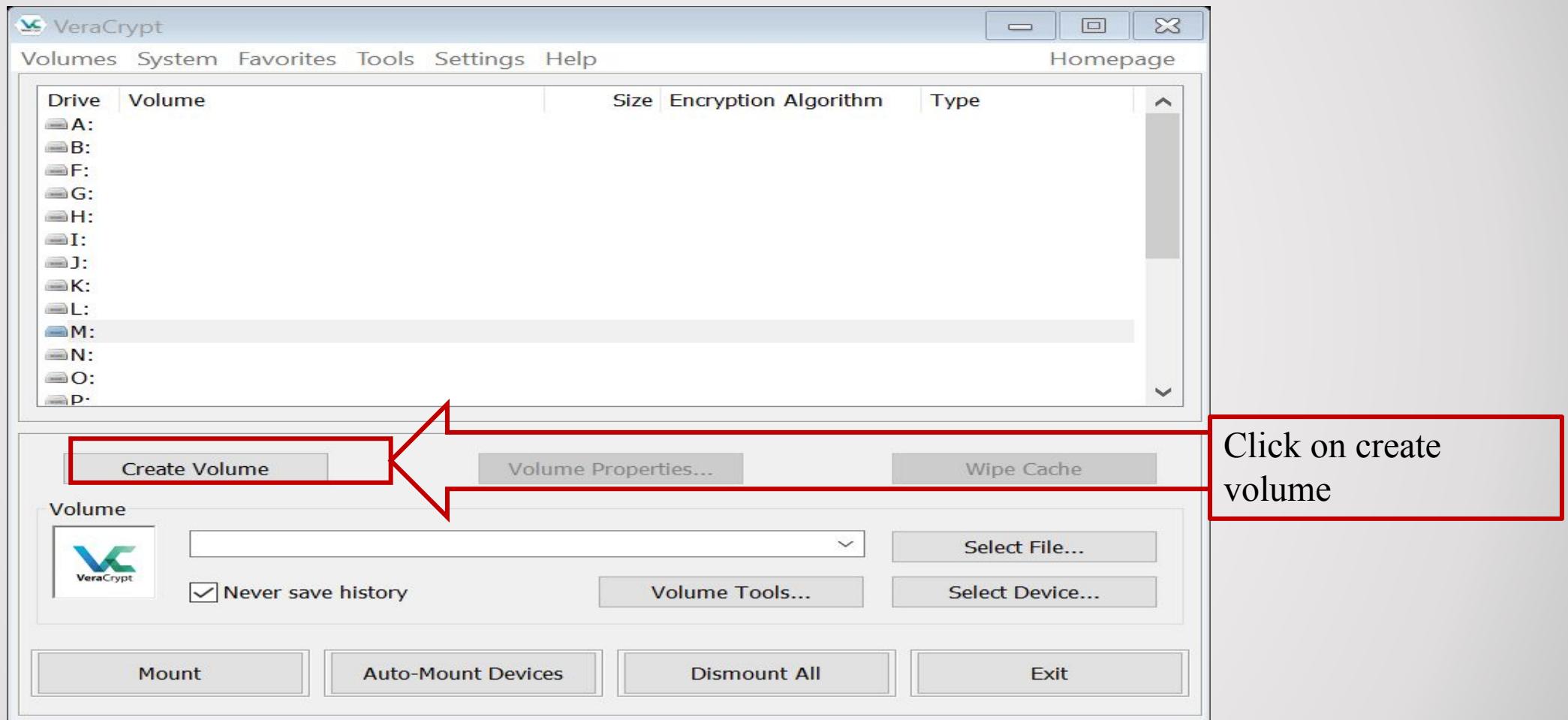


How it works?

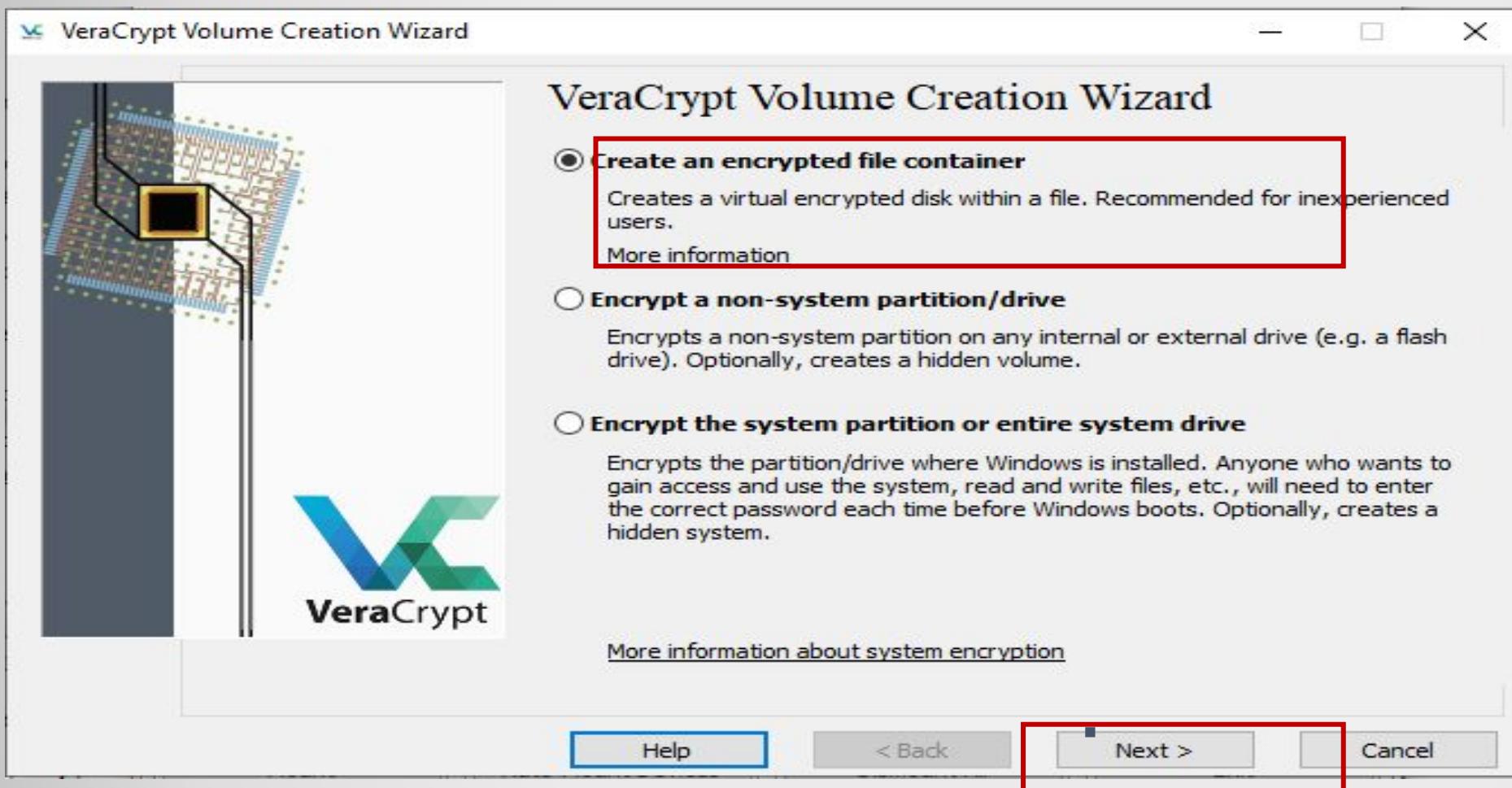
- As soon as we click on veracrypt option



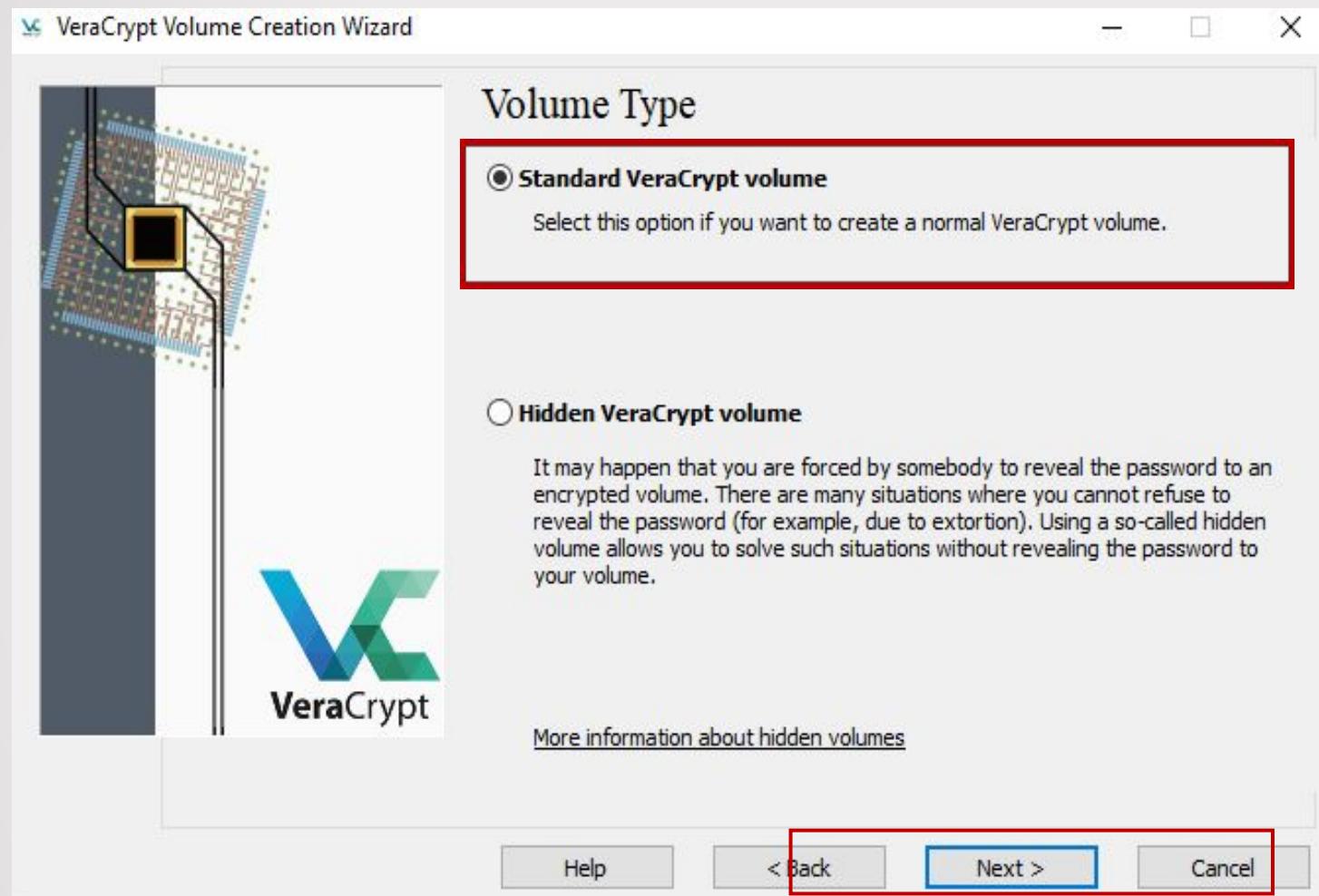
- Step1:- we will create a volume:-



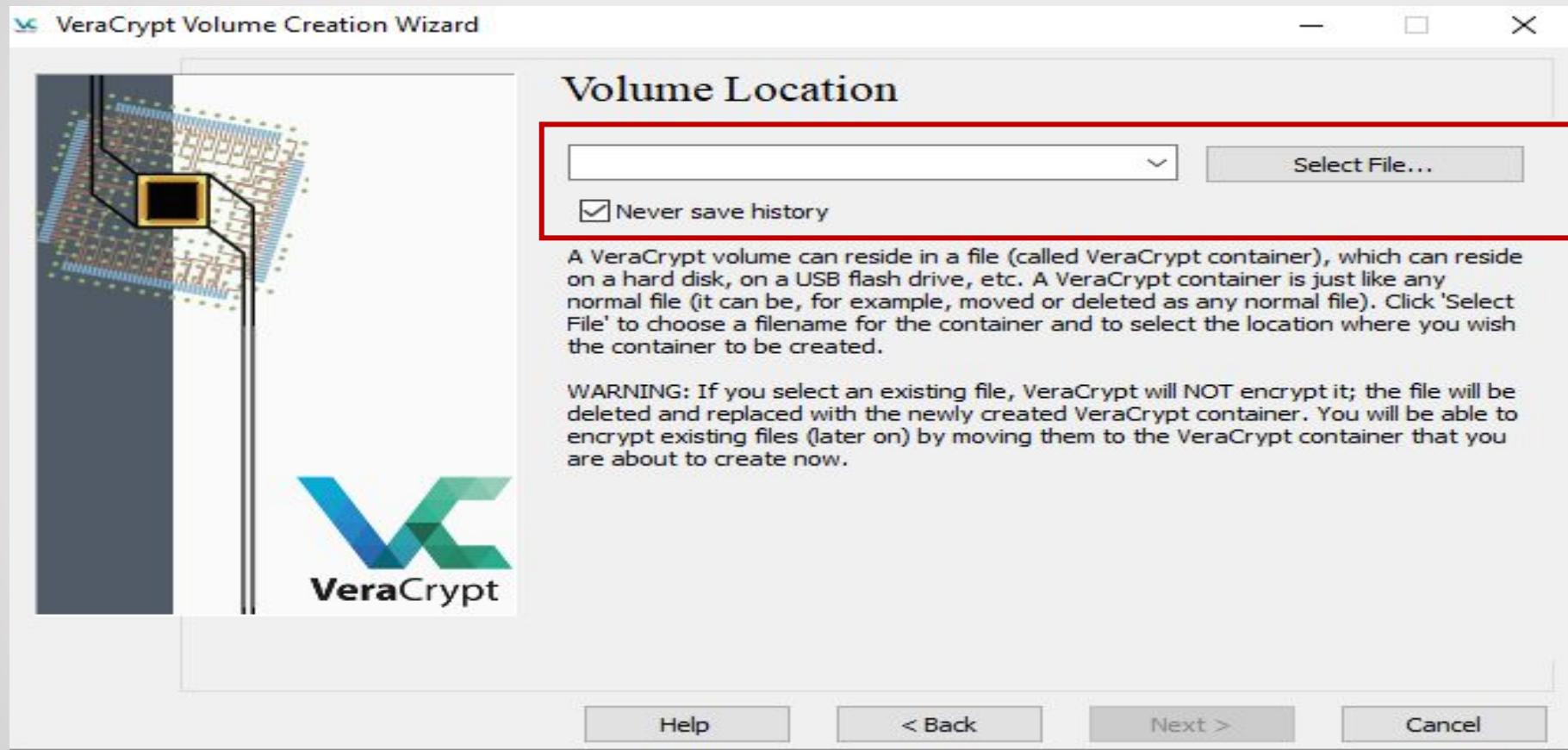
- Step2 :- for the encrypted file container:-



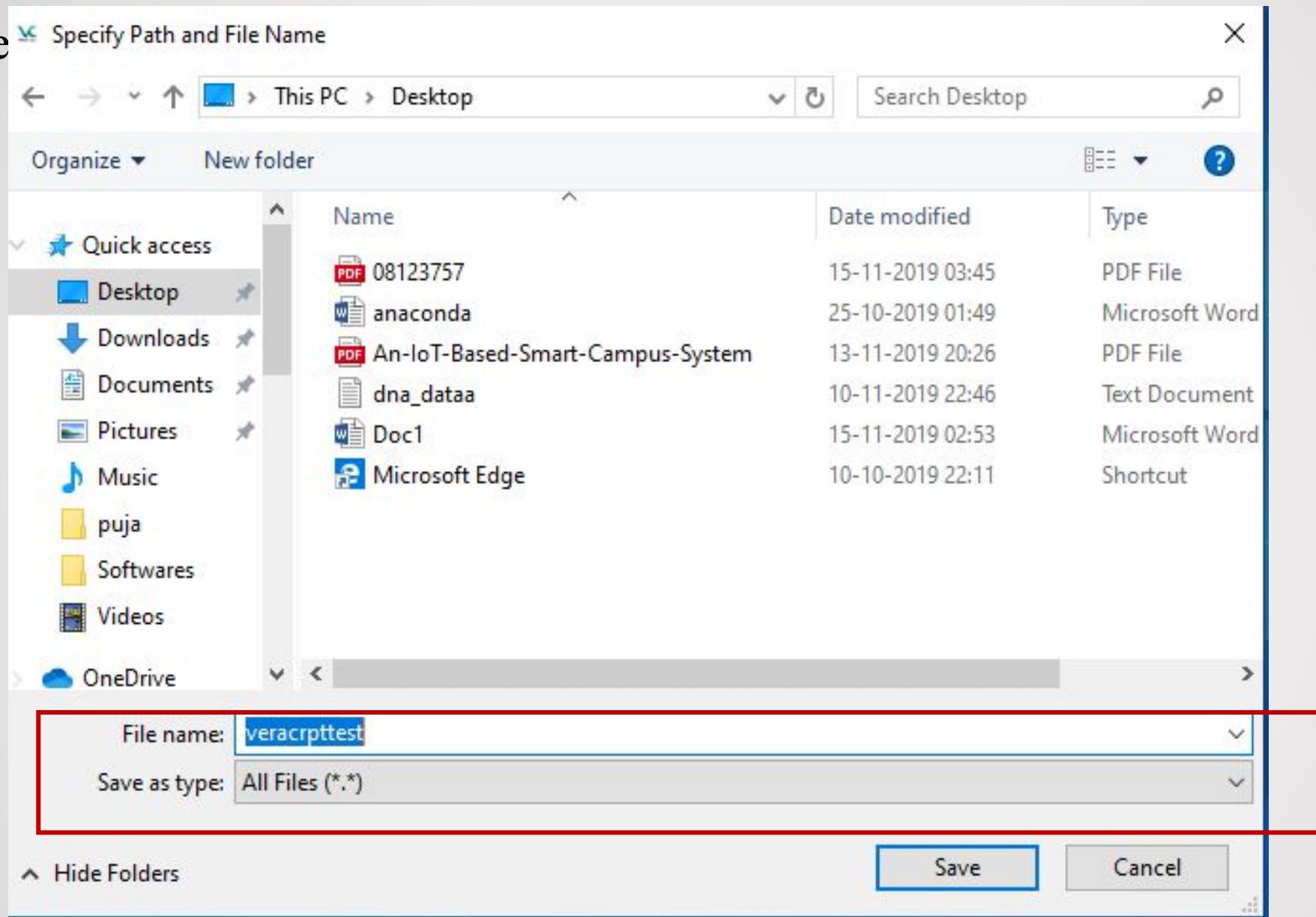
- Step 3:- we will create standard volume file:-



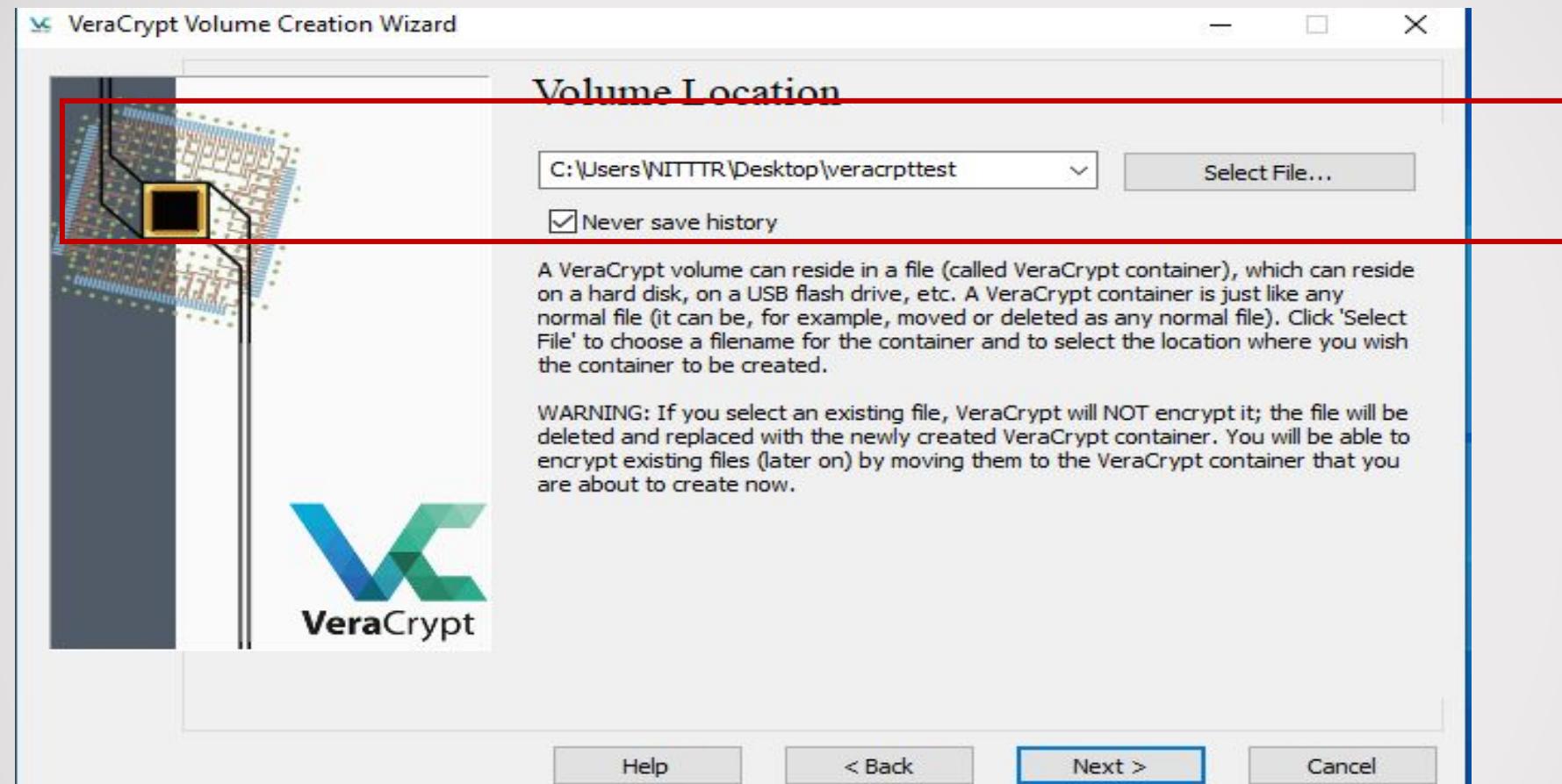
- Step4:-



- Step



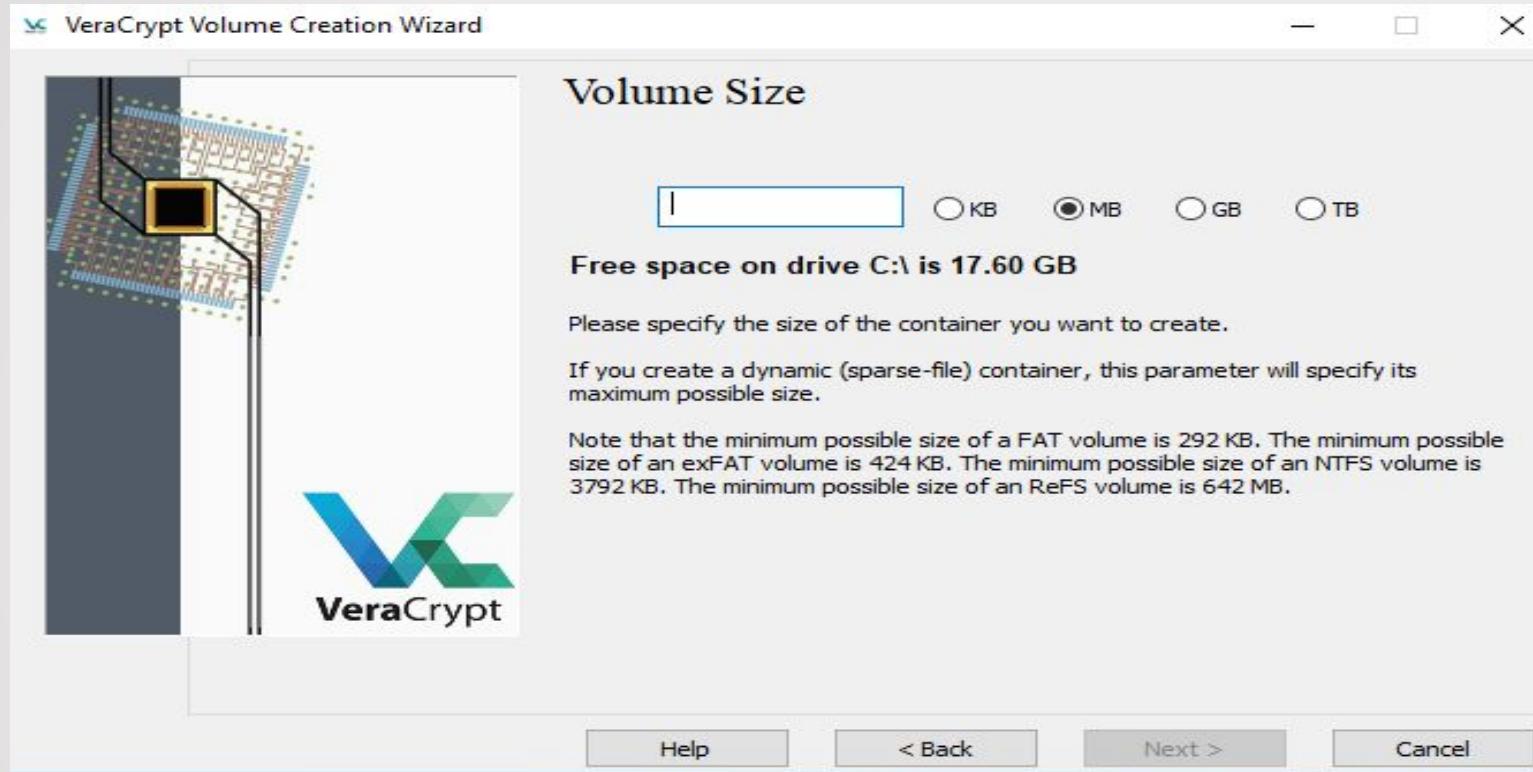
- Step 5:- path has been setup:-



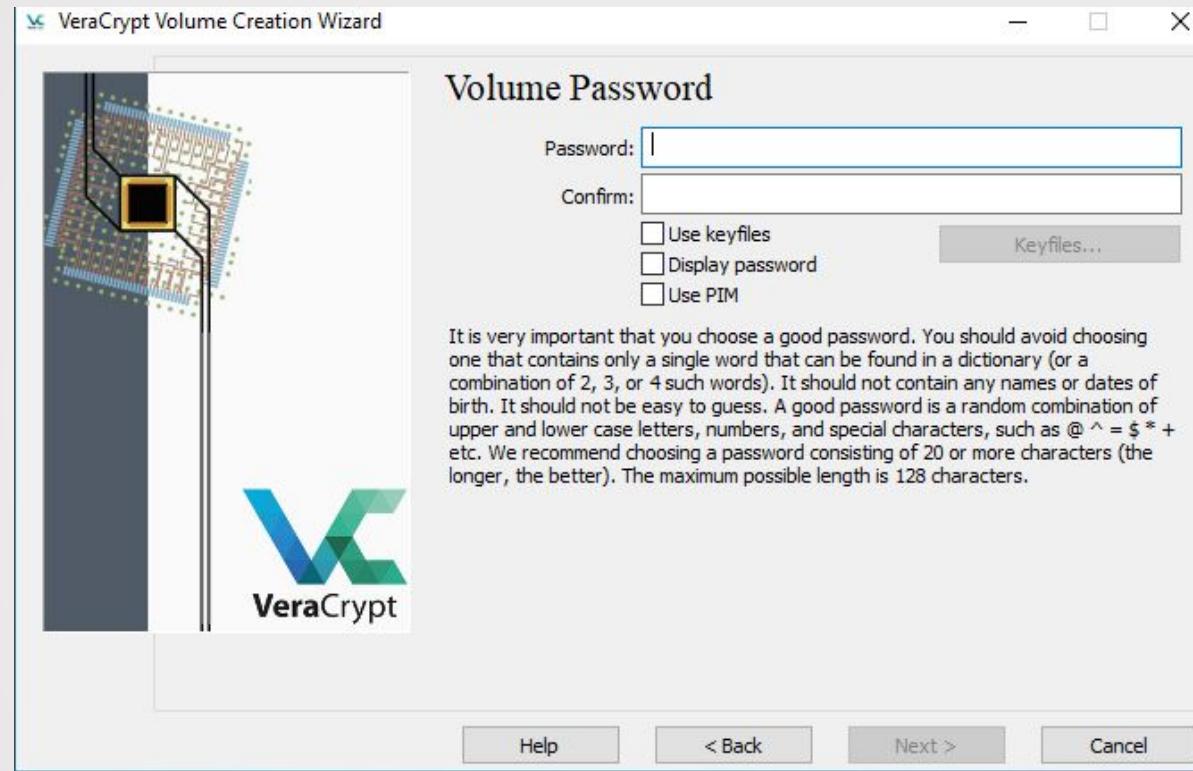
- Type of encryption we want:-



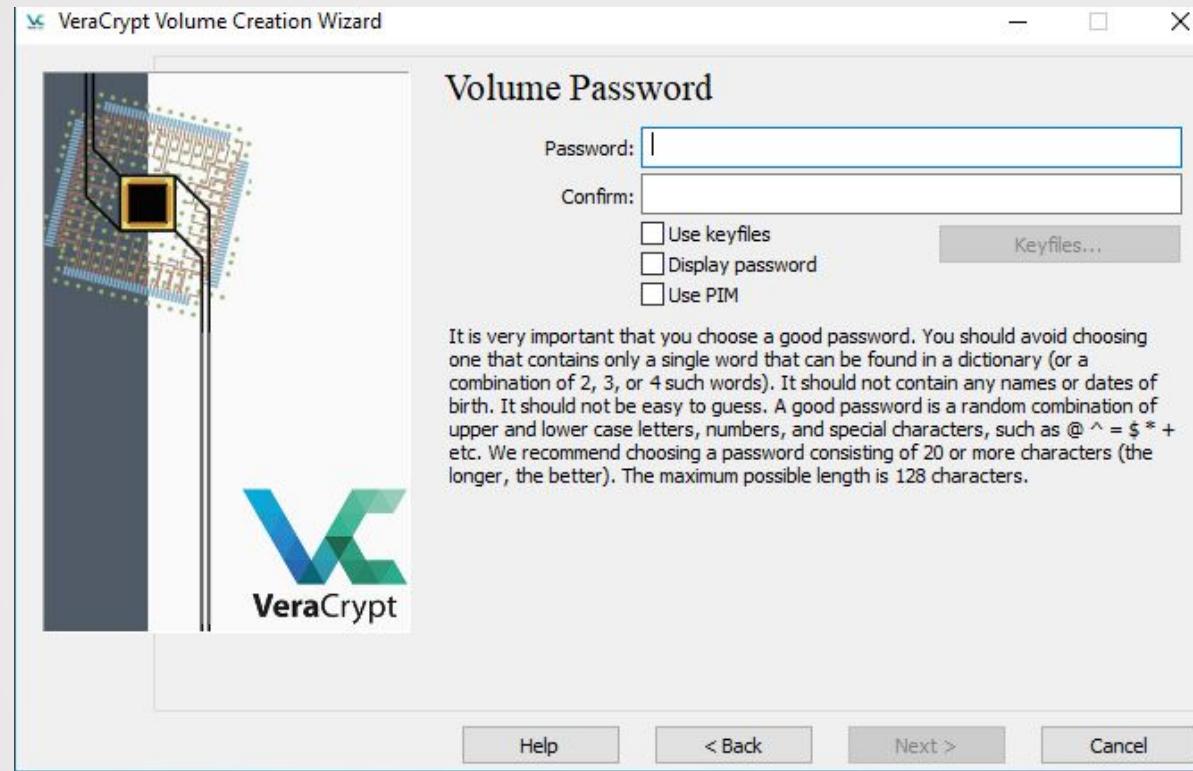
- File size:-



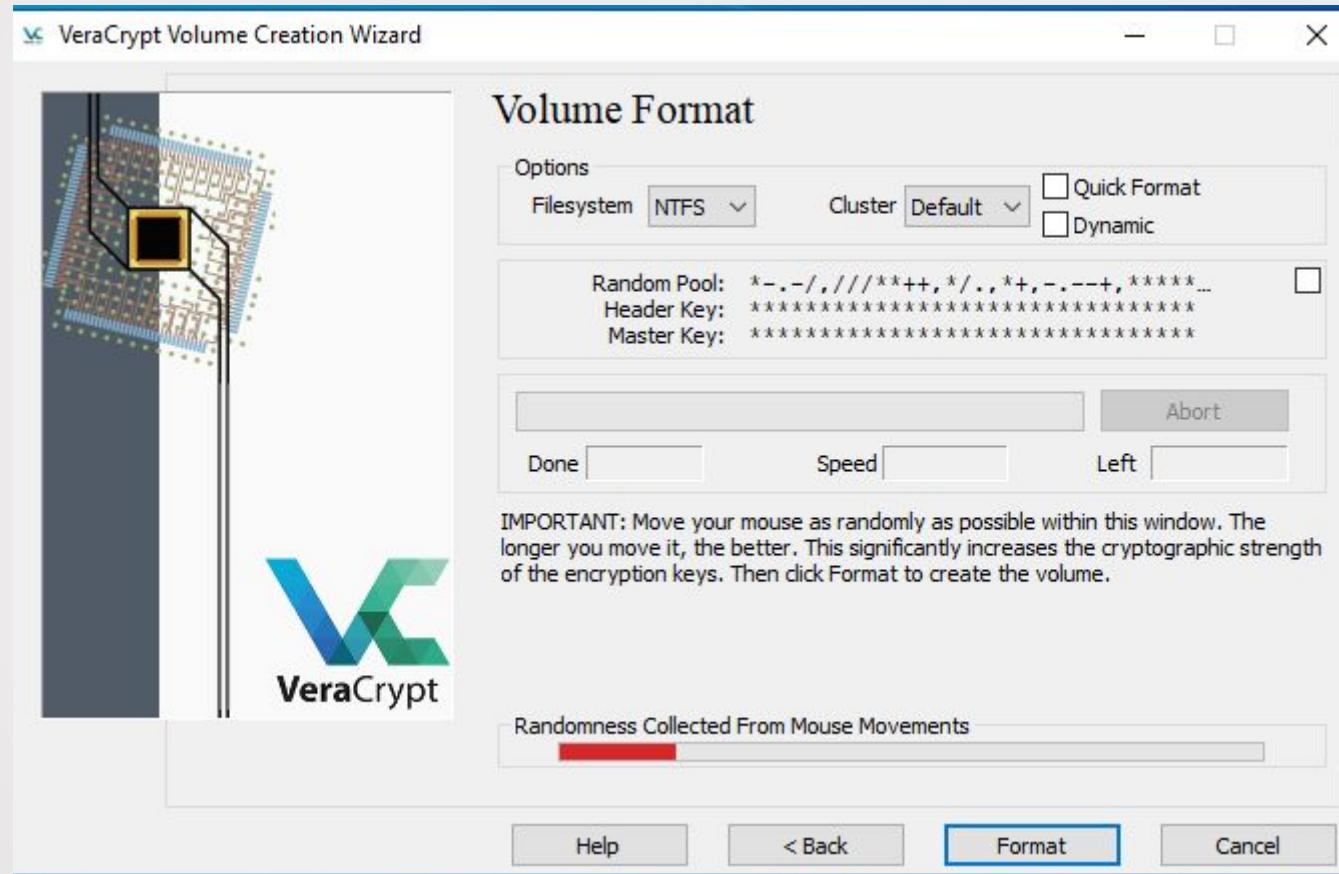
Password setup:-



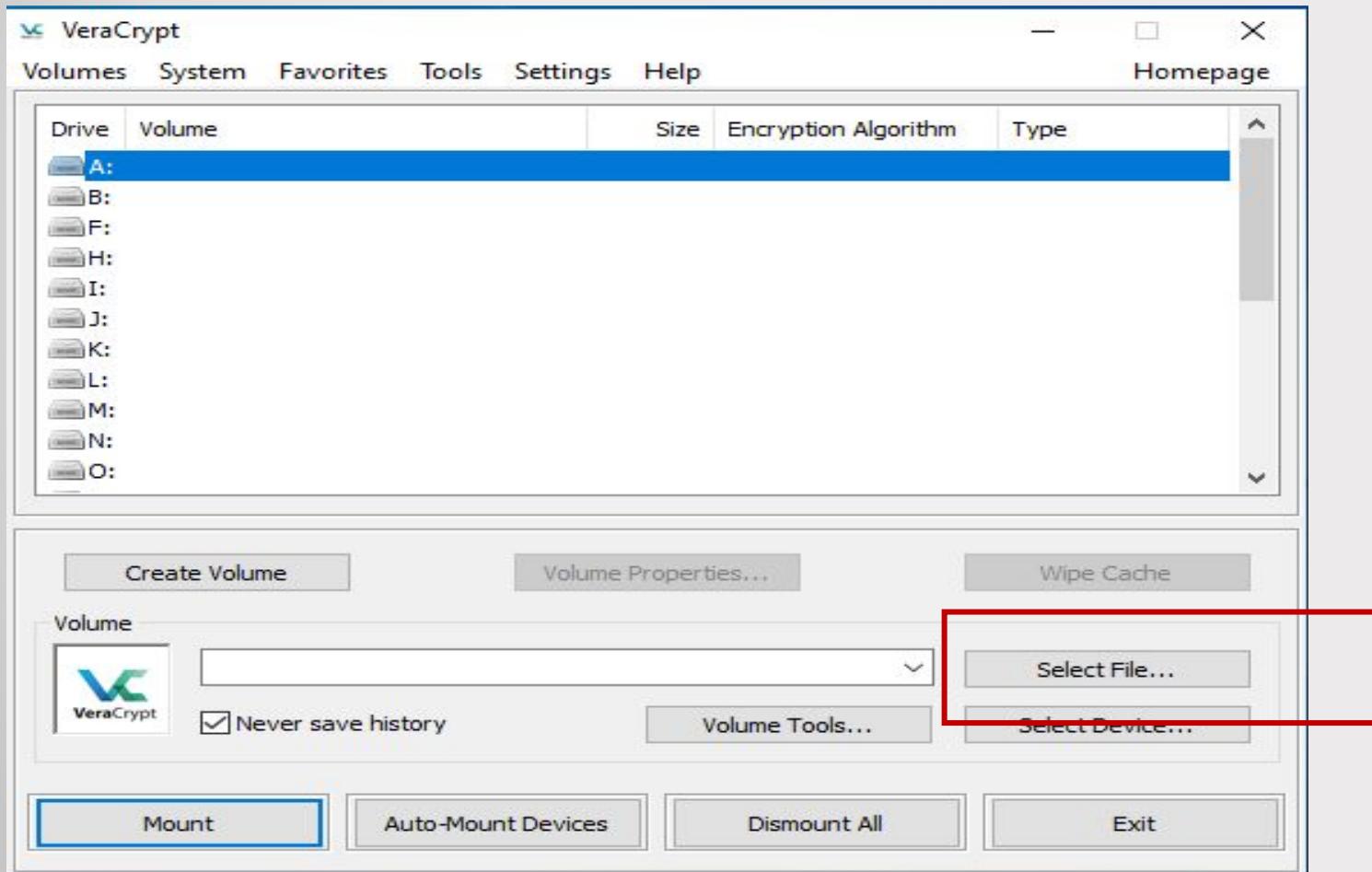
Password setup:-



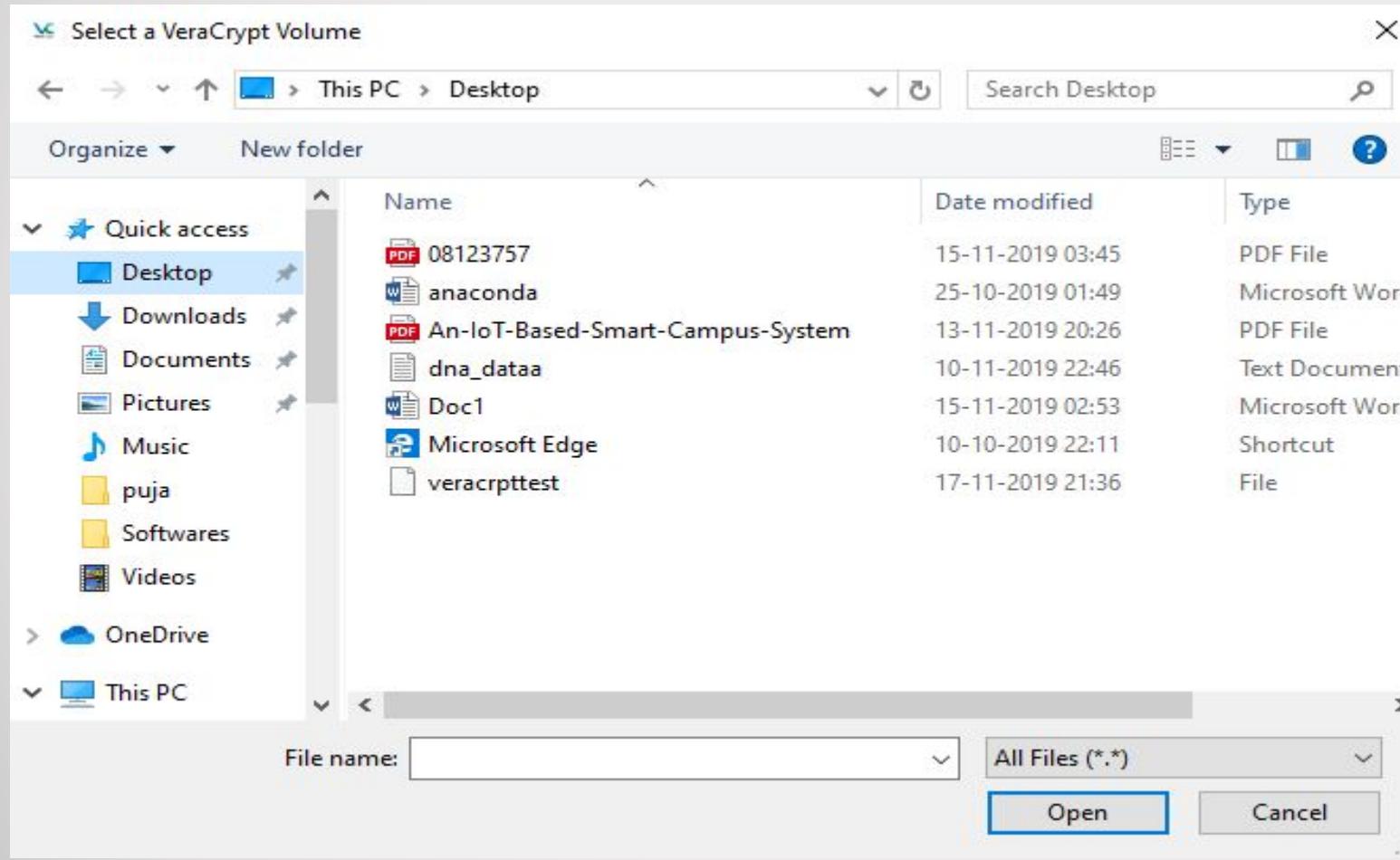
After creation we will click exit



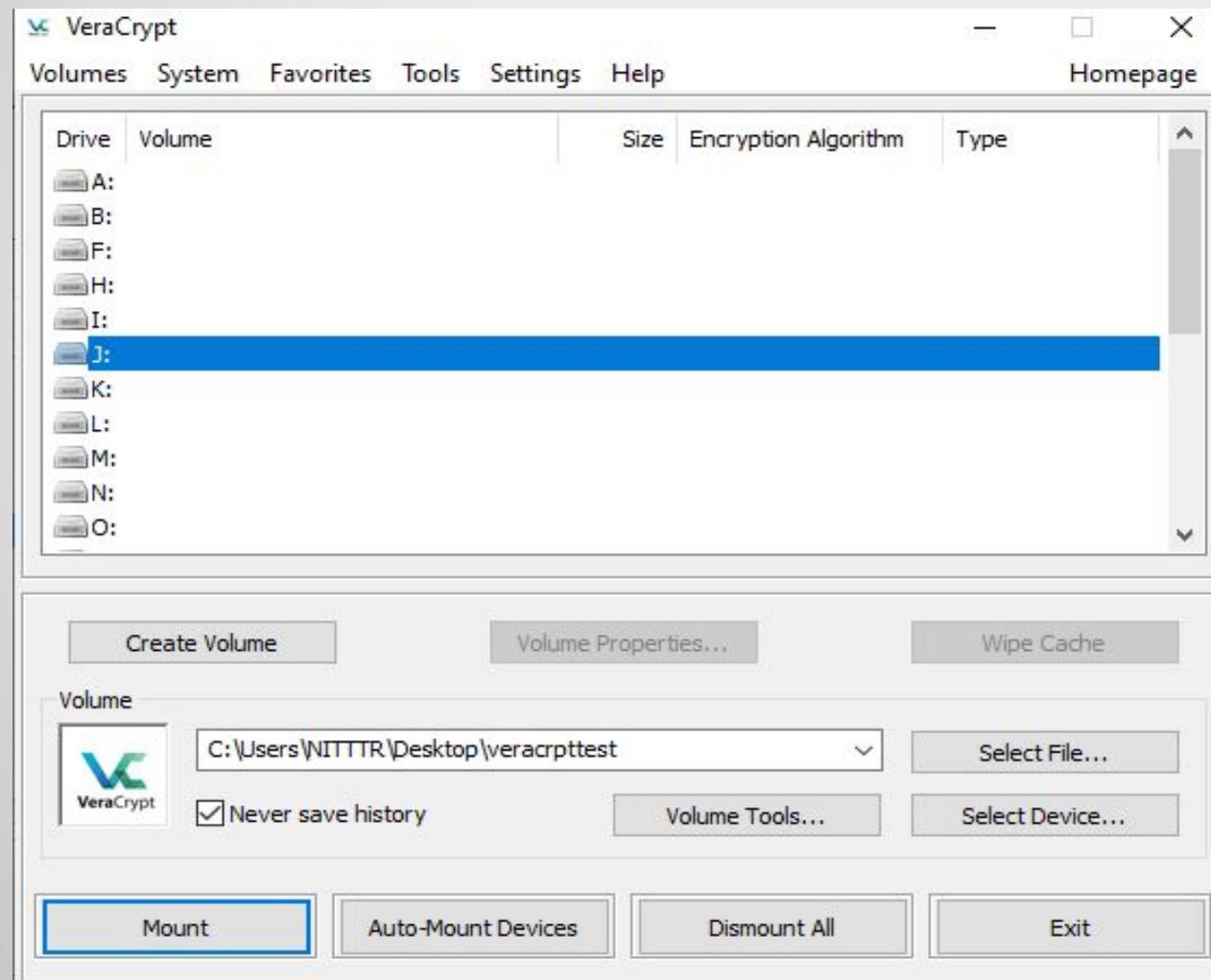
NOW ON CLICK ON THE VERCRYPT WIZARD AND SELECT FILE



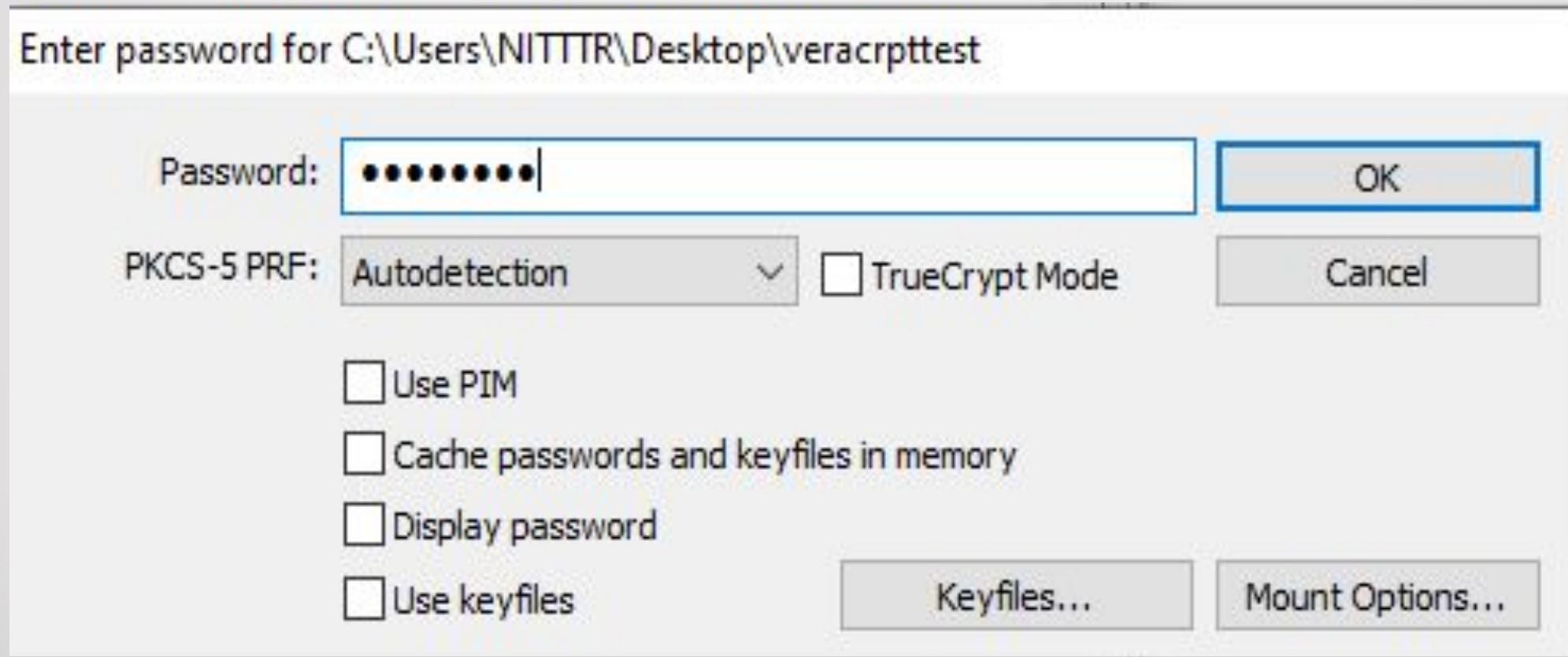
SETTING OF PATH



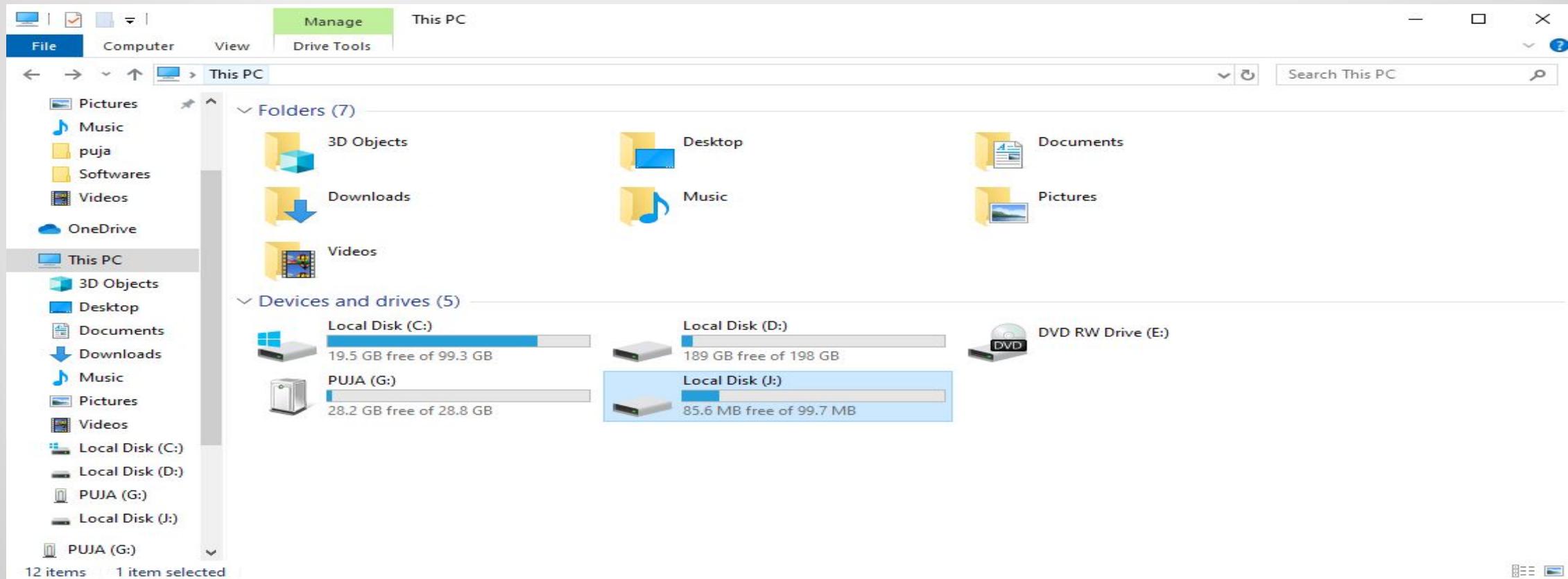
SELECT DRIVE LETTER SHOW IN THE LIST, SELECT MOUNT WHICH WILL ACT AS VERACRYPT CONTAINER



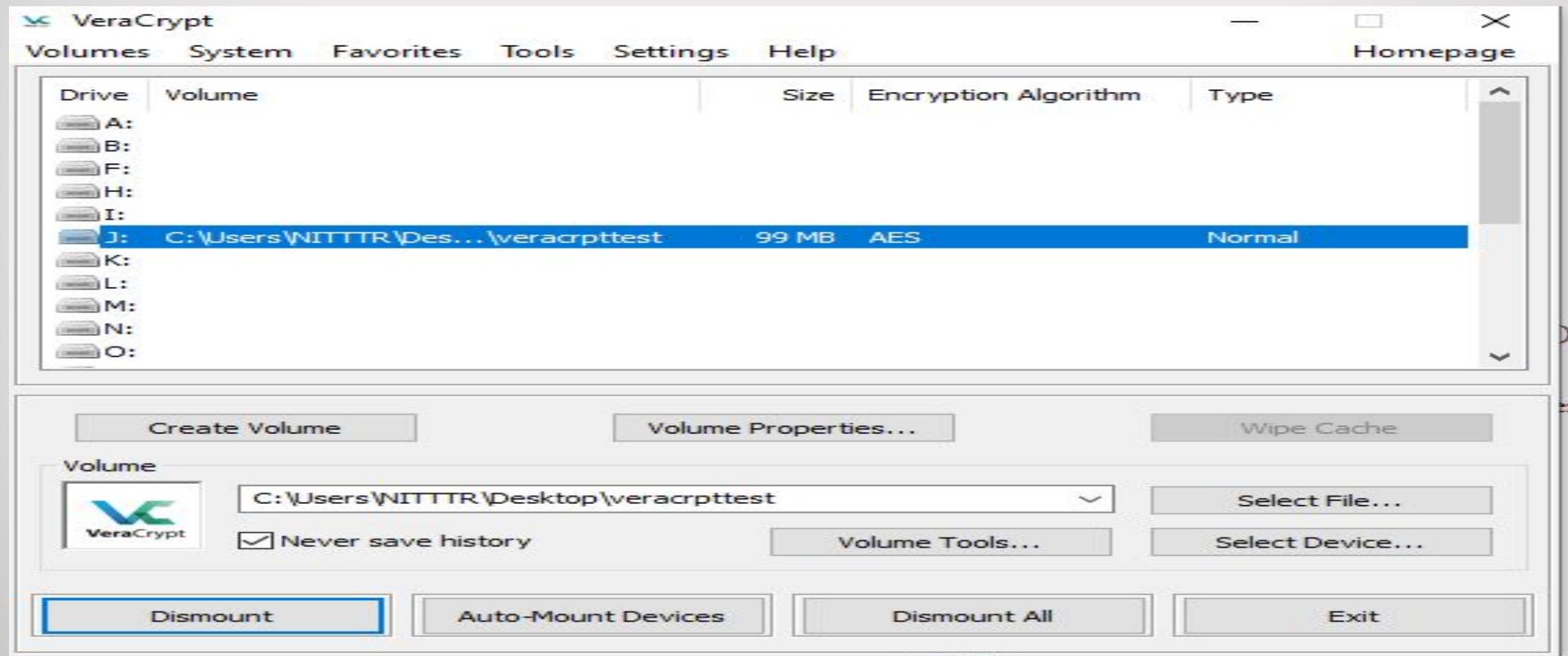
NOW GIVE THE PASSWORD USED PREVIOUSLY AND CLICK OK



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

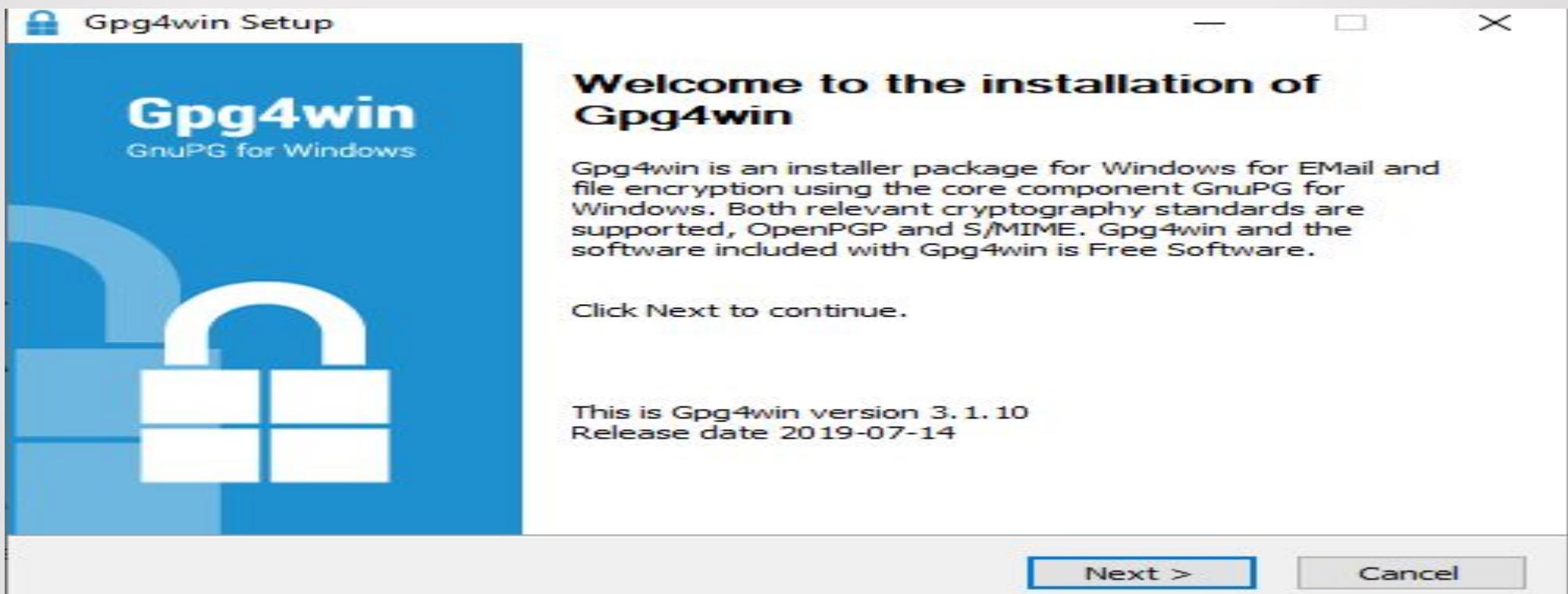
- Gpg4win runs on Windows versions 7 or newer (up to Windows 10). Both 32 and 64bit systems are supported.
- If you have at least Windows XP, some parts of Gpg4win can be used, but are not officially supported.
- The Outlook plugin GpgOL is compatible with Microsoft Outlook 2010, 2013, 2016 and 2019 (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.

WORKING WITH GPP4WIN

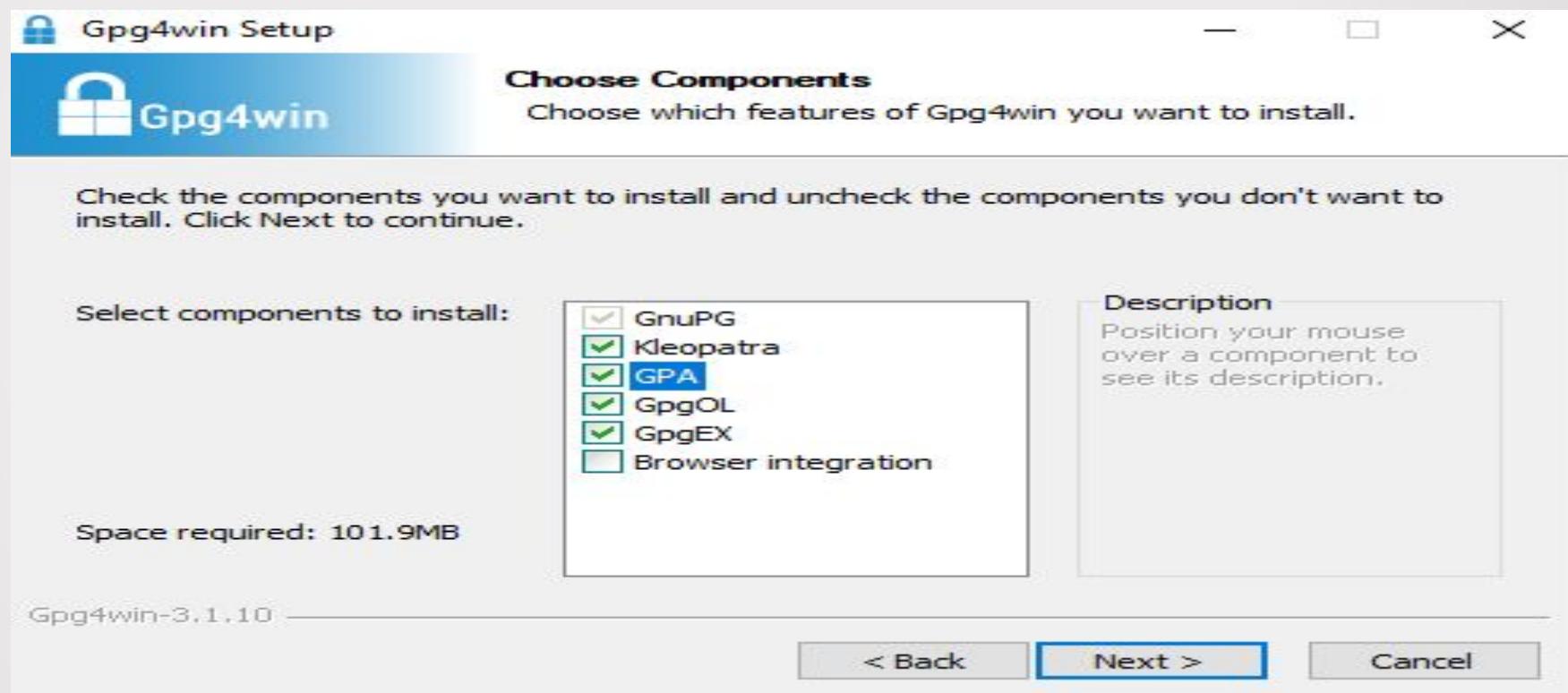
- Step1:- Installation:-<https://www.gpg4win.org/get-gpg4win.html>



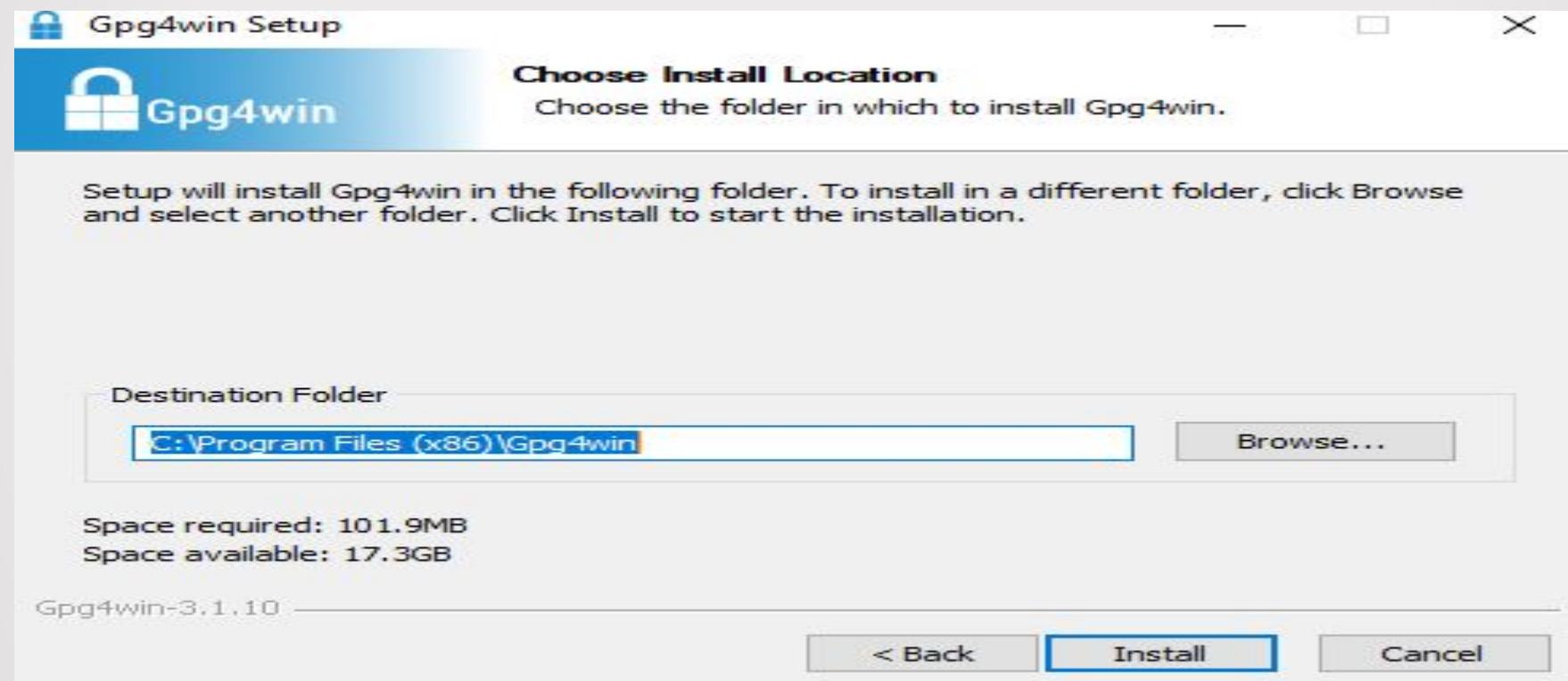
Wizard page



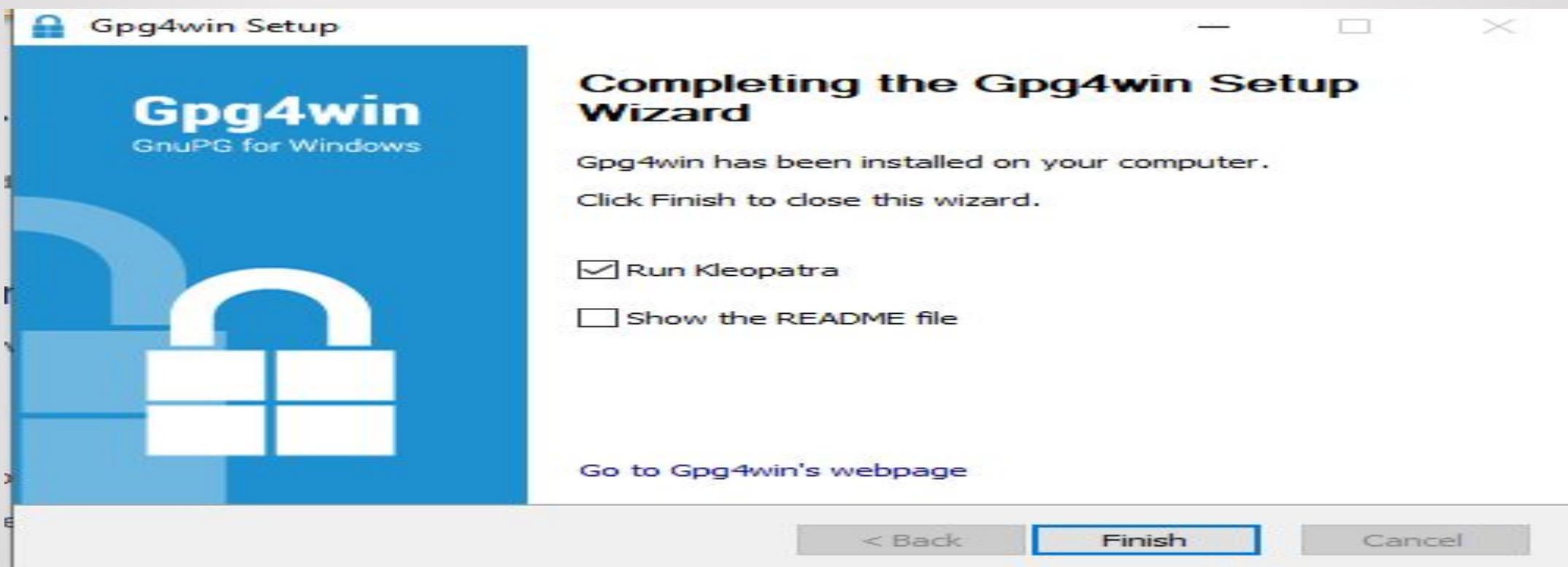
Choosing of components



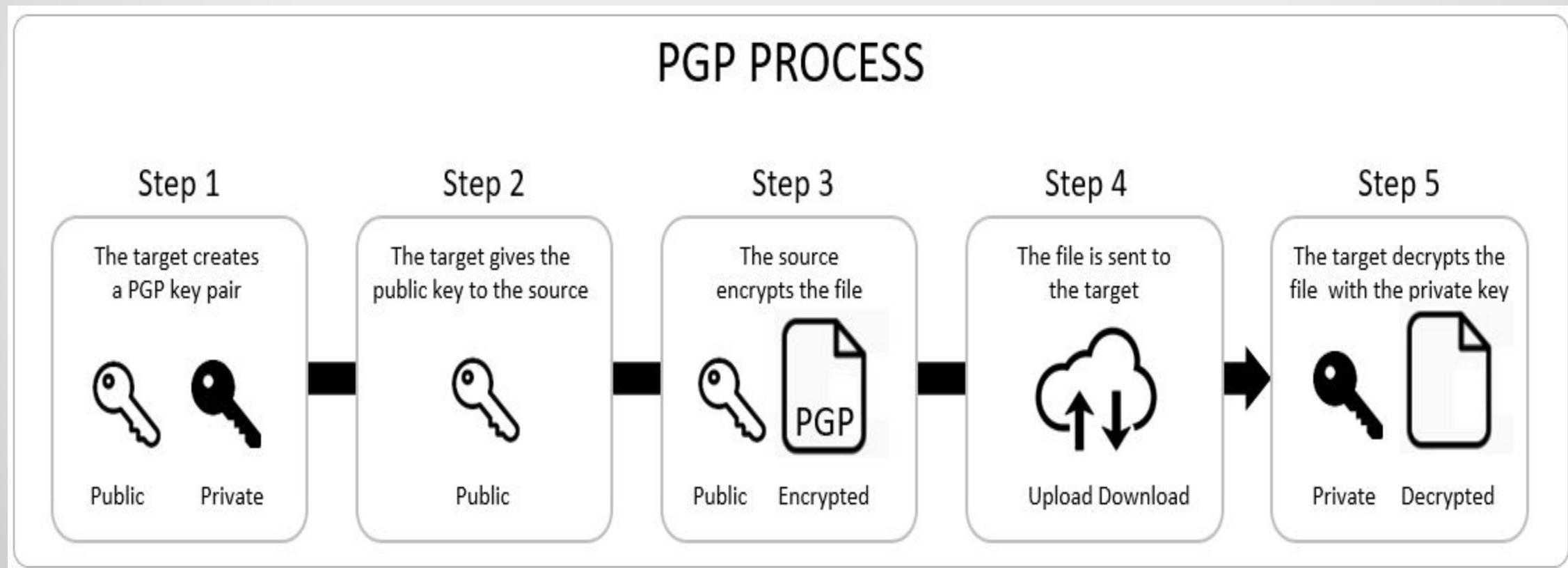
Path setup



Show that installation has been completed



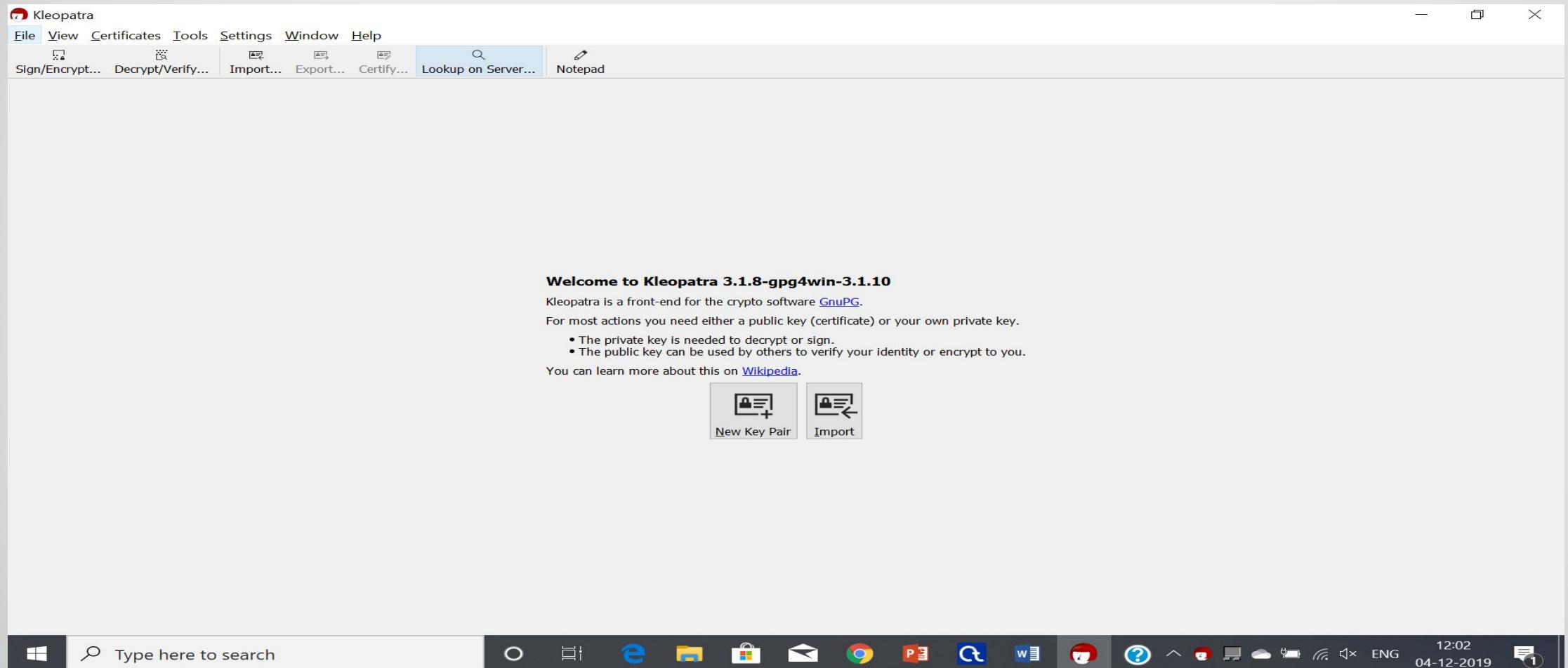
WORKFLOW DIAGRAM



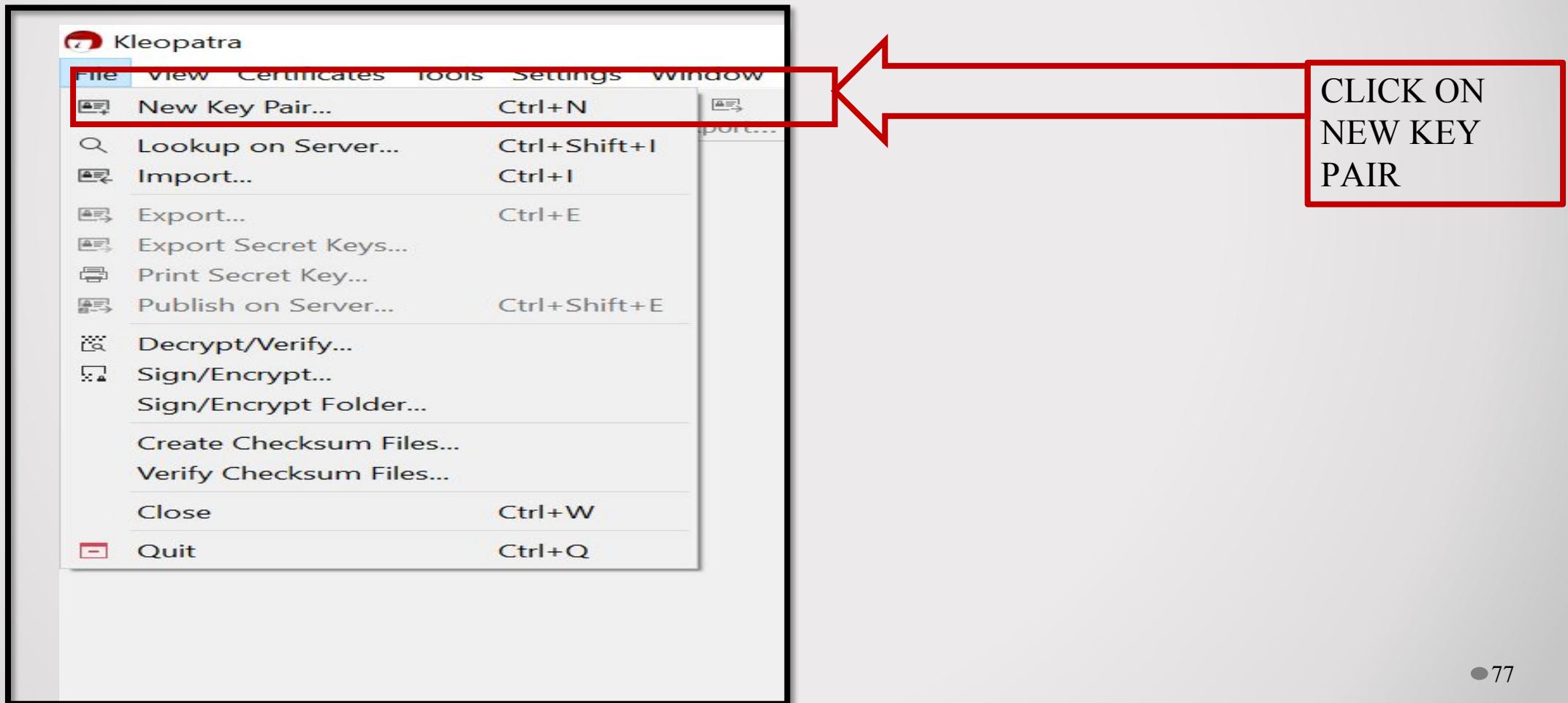
Now lets see ITS WORKING



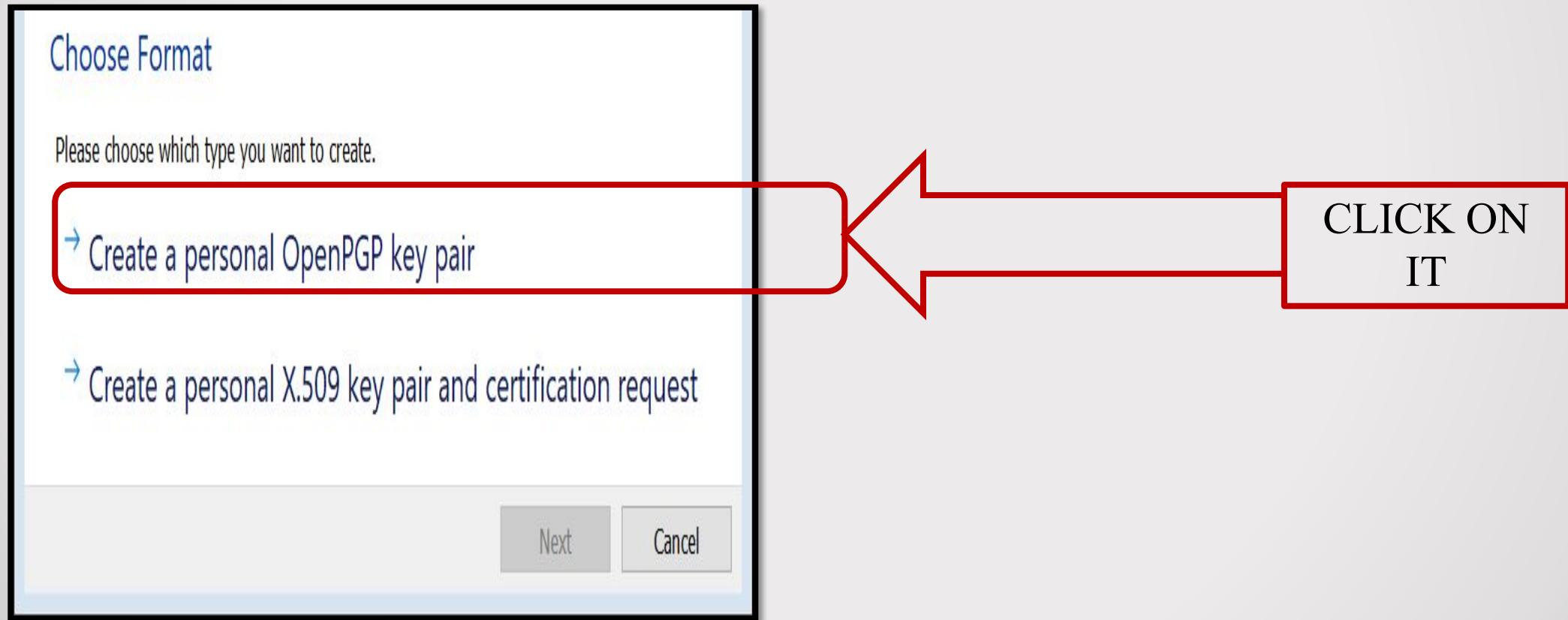
STEP 1:- ON CLICKING THE ICON IT OPENS THE WORKING PAGE



STEP 2:- TO CREATE KEY PAIRS



STEP 3:-TO CONFIRMING THE FINGERPRINT OF PUBLIC KEY



STEP 4 :- CREATION OF IDENTITY

The screenshot shows a window titled "Key Pair Creation Wizard" with the sub-step "Enter Details". The window has standard operating system controls at the top right: a question mark icon, a close (X) icon, and a back arrow labeled "Key Pair Creation Wizard".

Enter Details

Please enter your personal details below. If you want more control over the parameters, click on the Advanced Settings button.

Name: (optional)

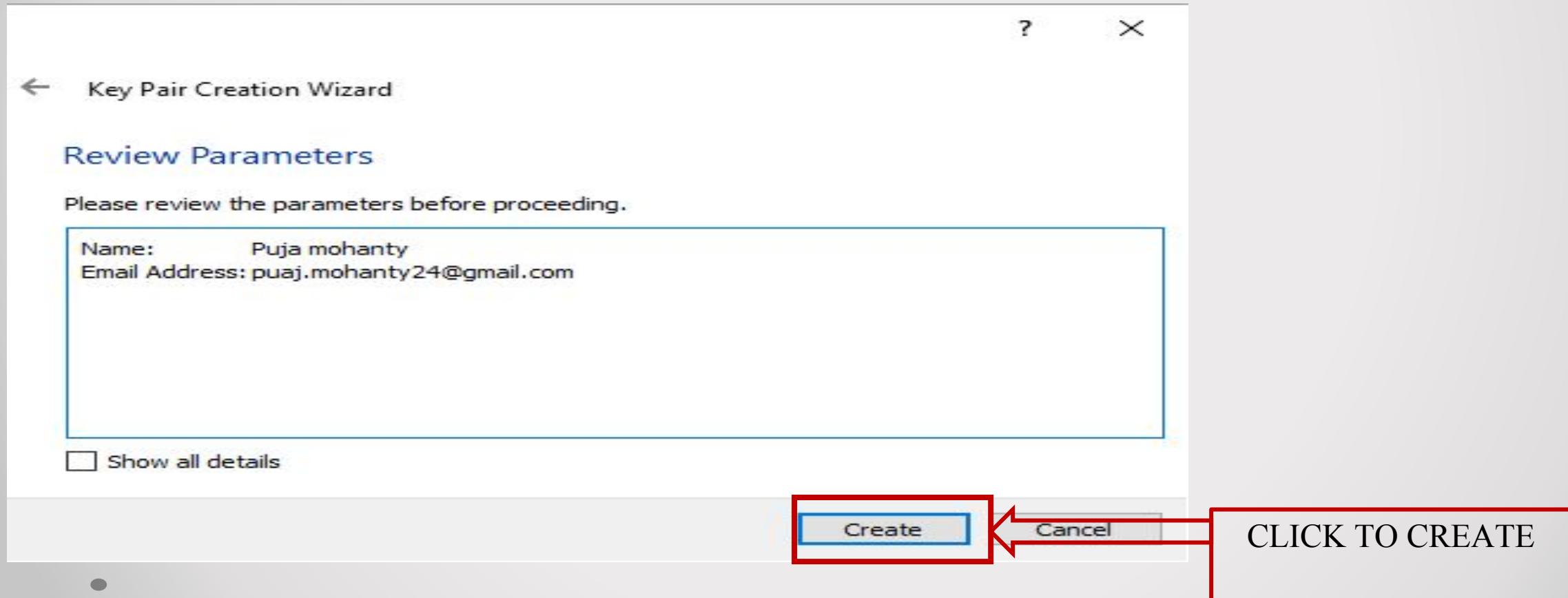
Email: (optional)

Advanced Settings...

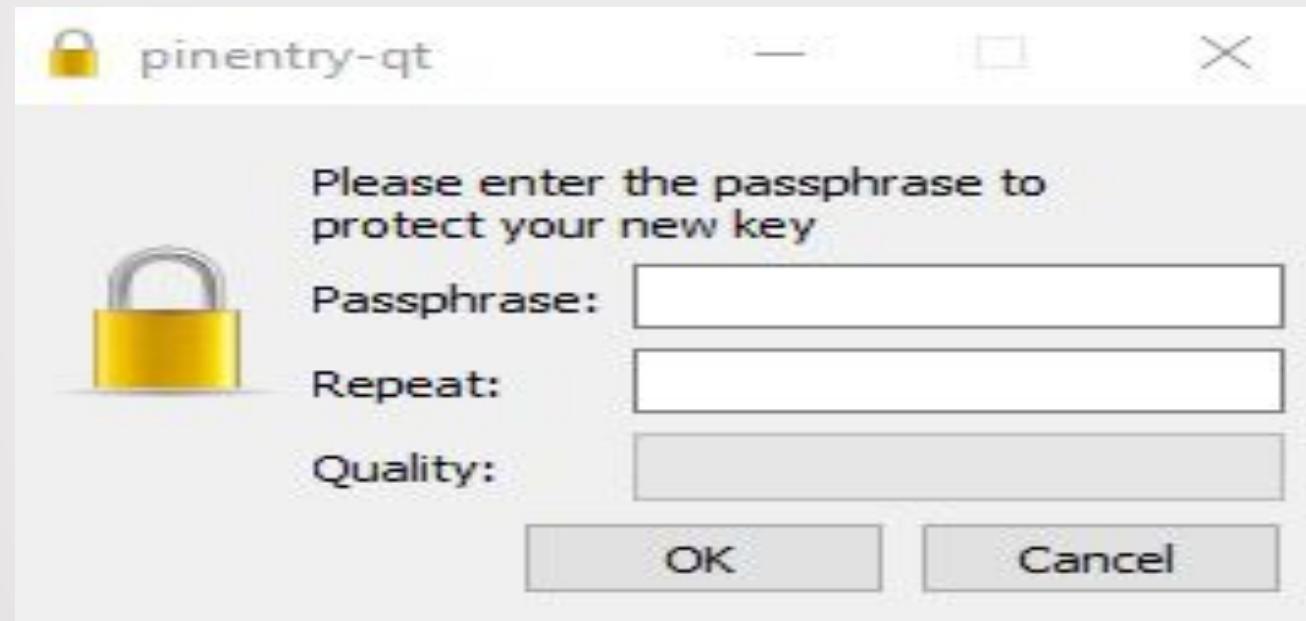
Next Cancel

Step 5 GIVING REVIEW OF PARAMETERS

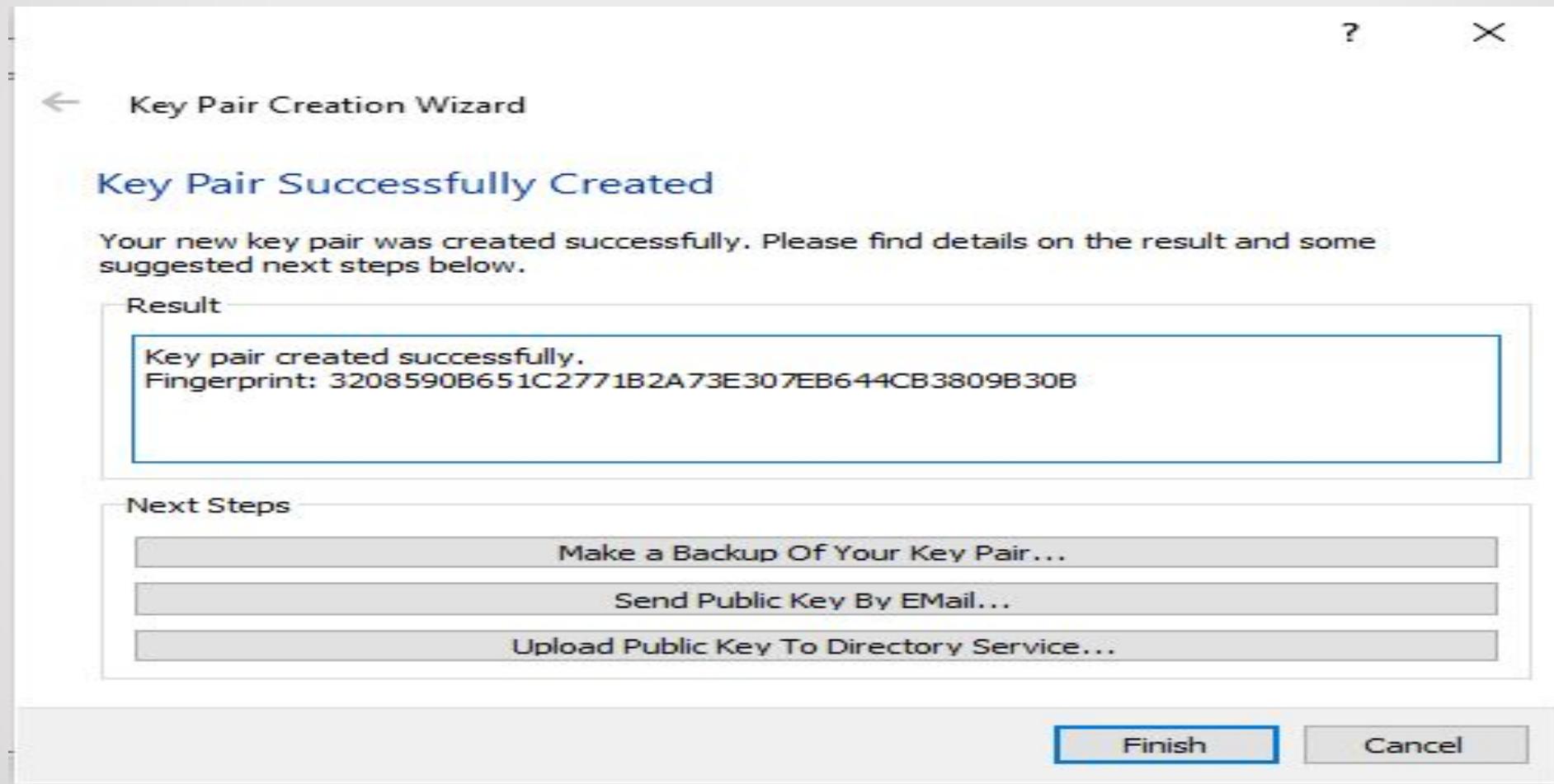
- Now we will create the fingerprint by clicking “ok”.



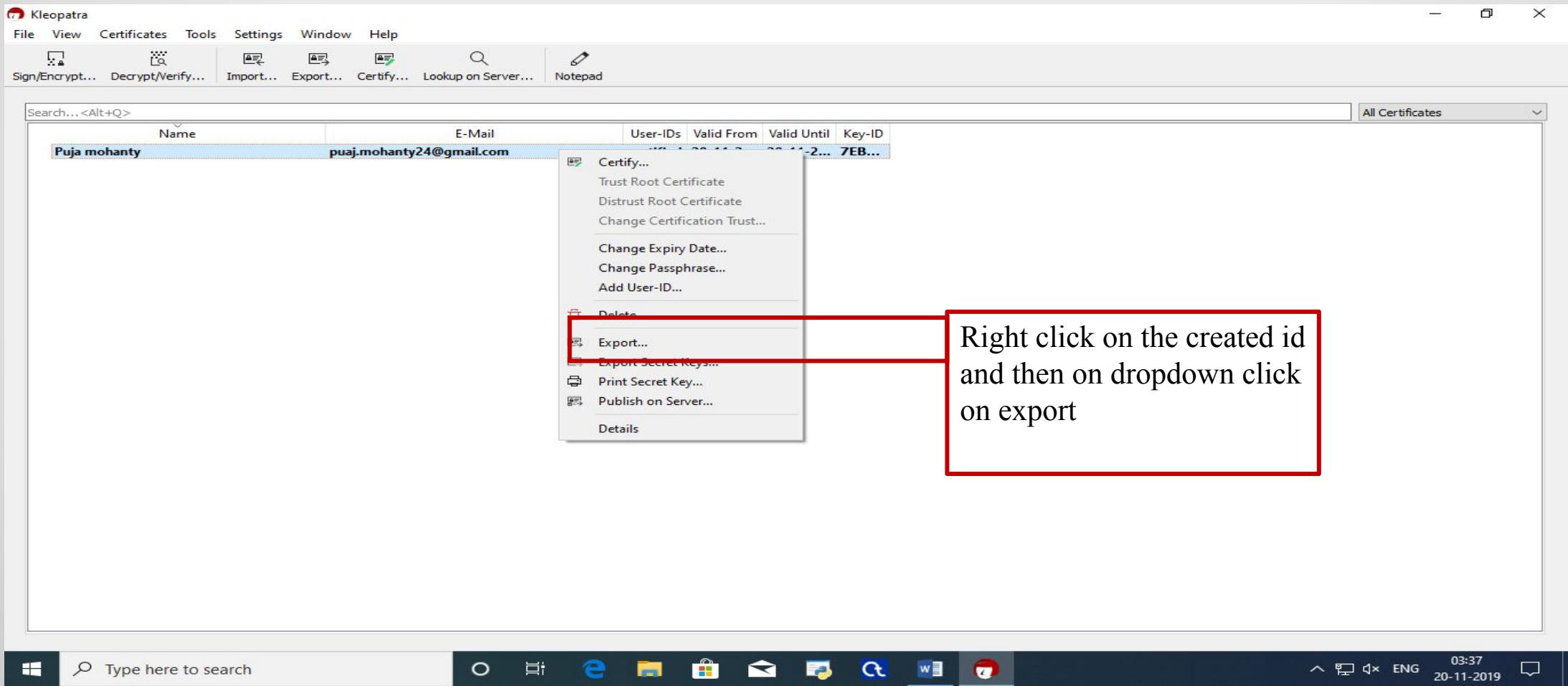
STEP6:- TO PROTECT THE KEY WE CREATE A PARAPHRASE



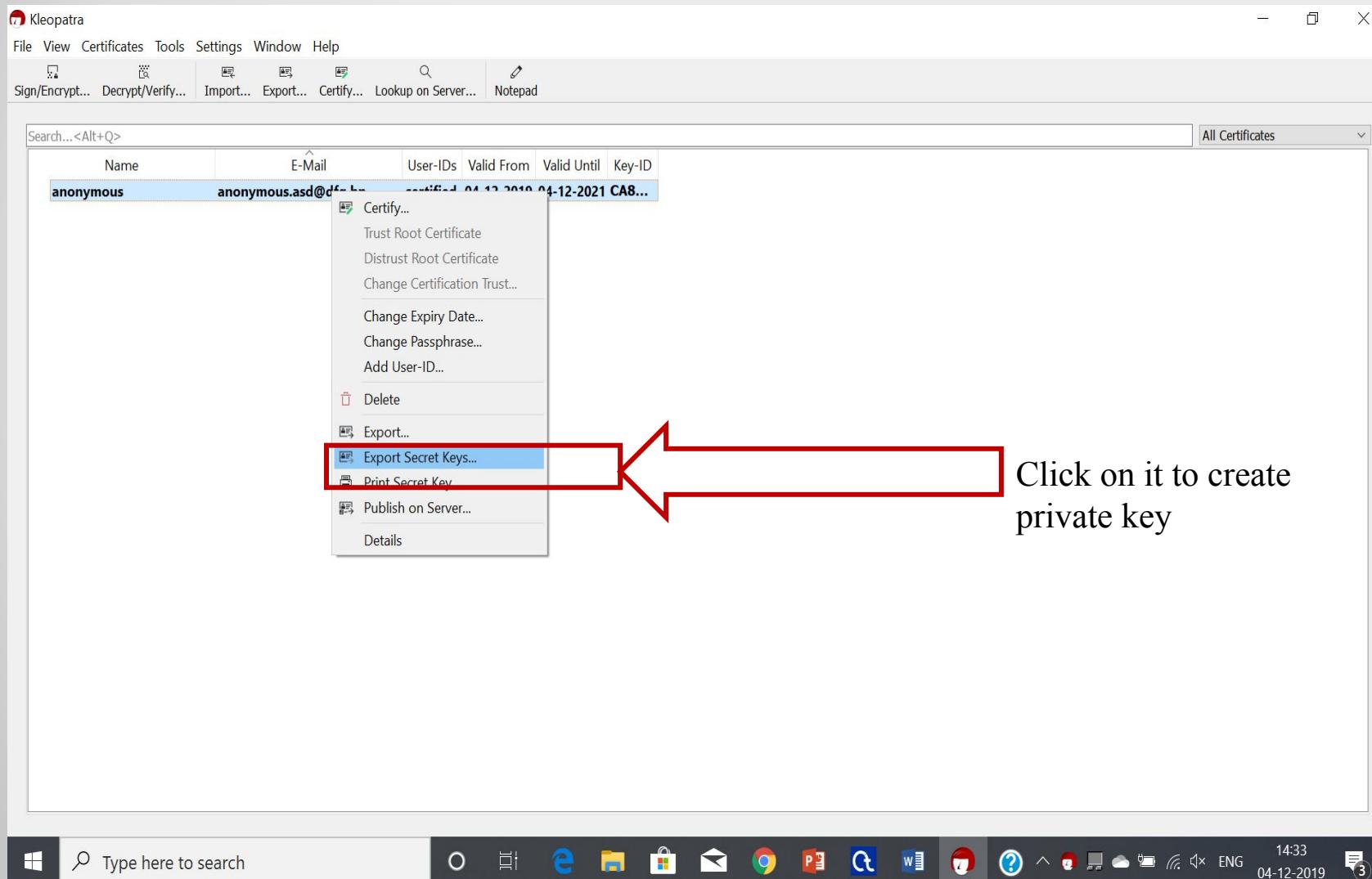
KEY PAIR IS CREATED SUCESSFULLY



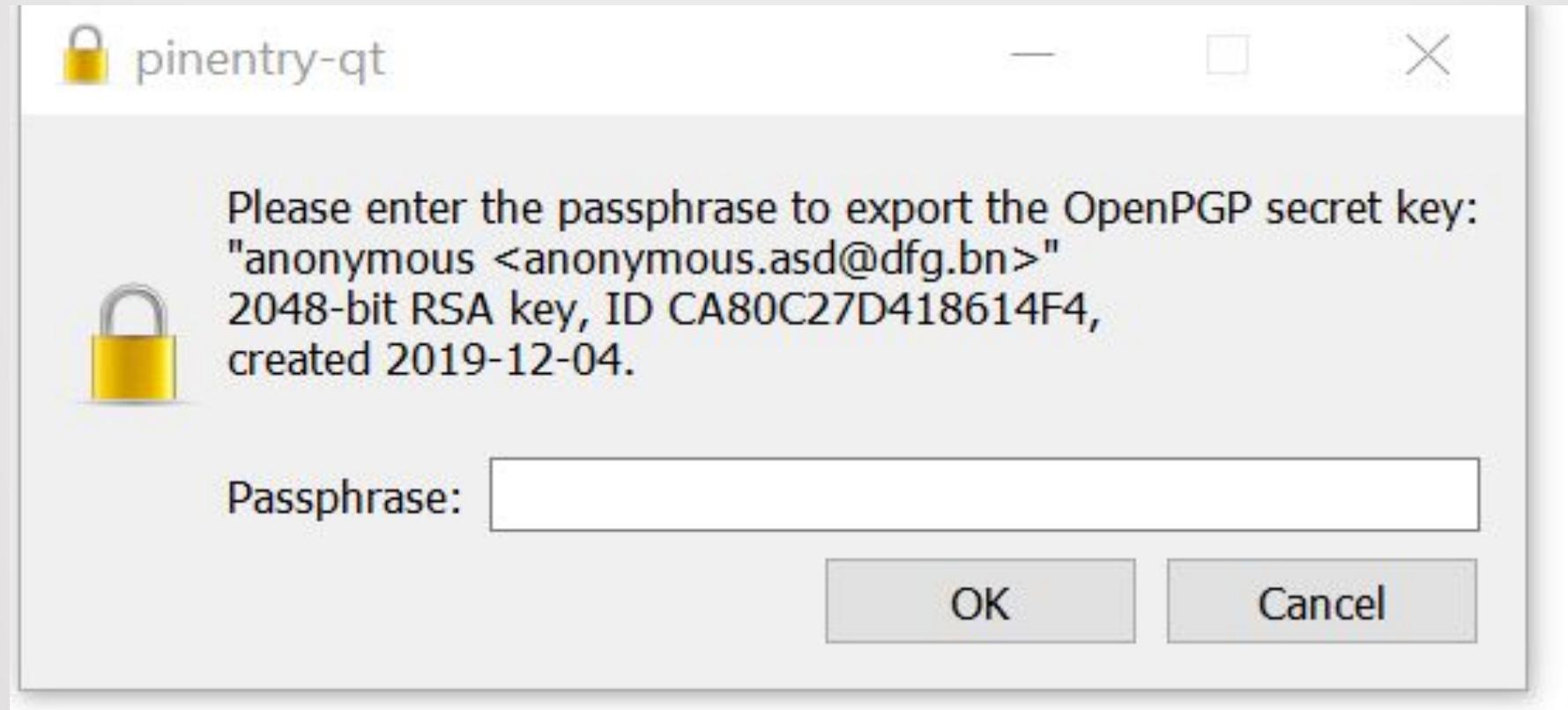
STEP 7 TO CREATE THE PUBLIC KEY AND EXPORT IT



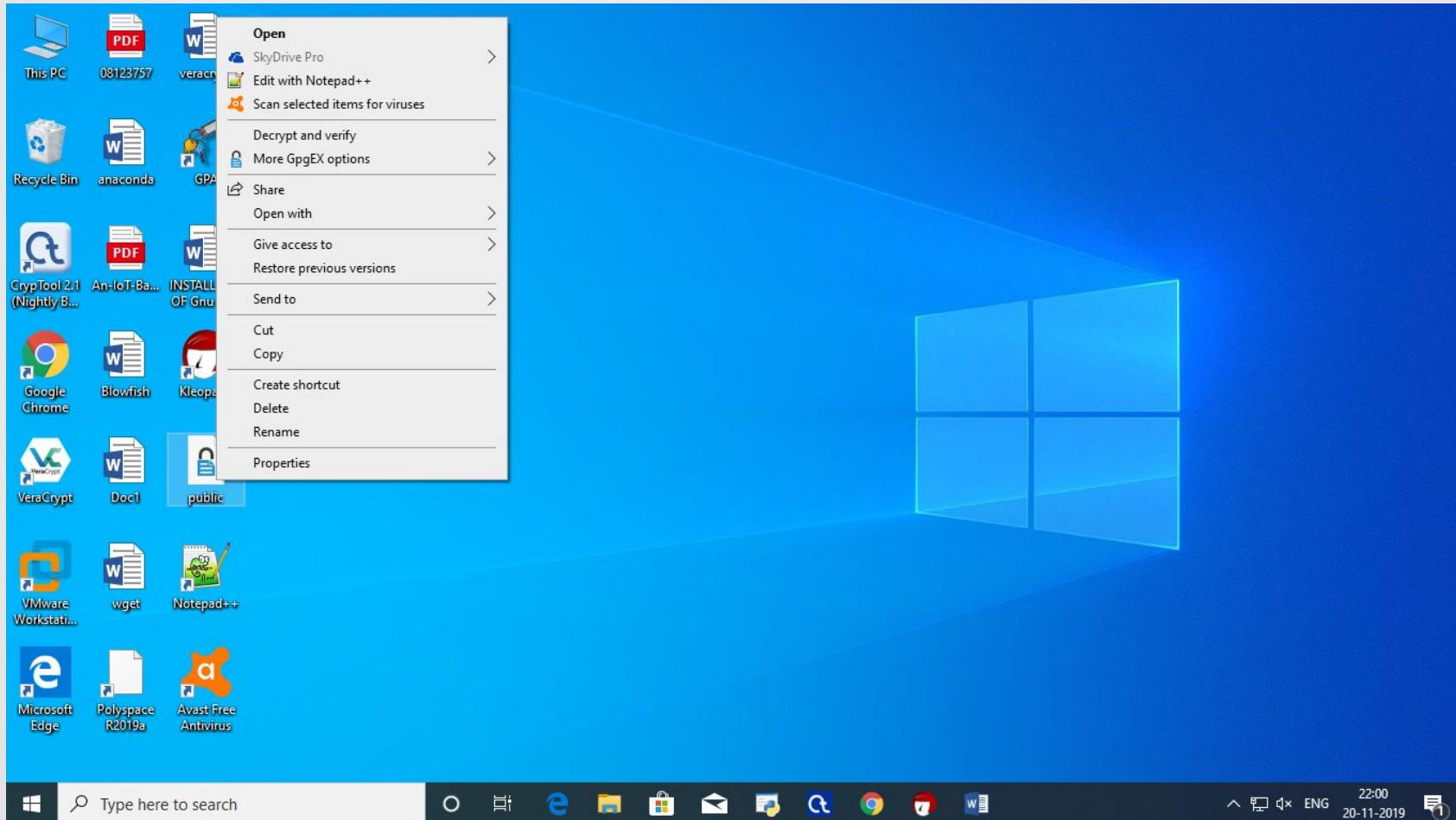
STEP 8:- Creation of private key and export it



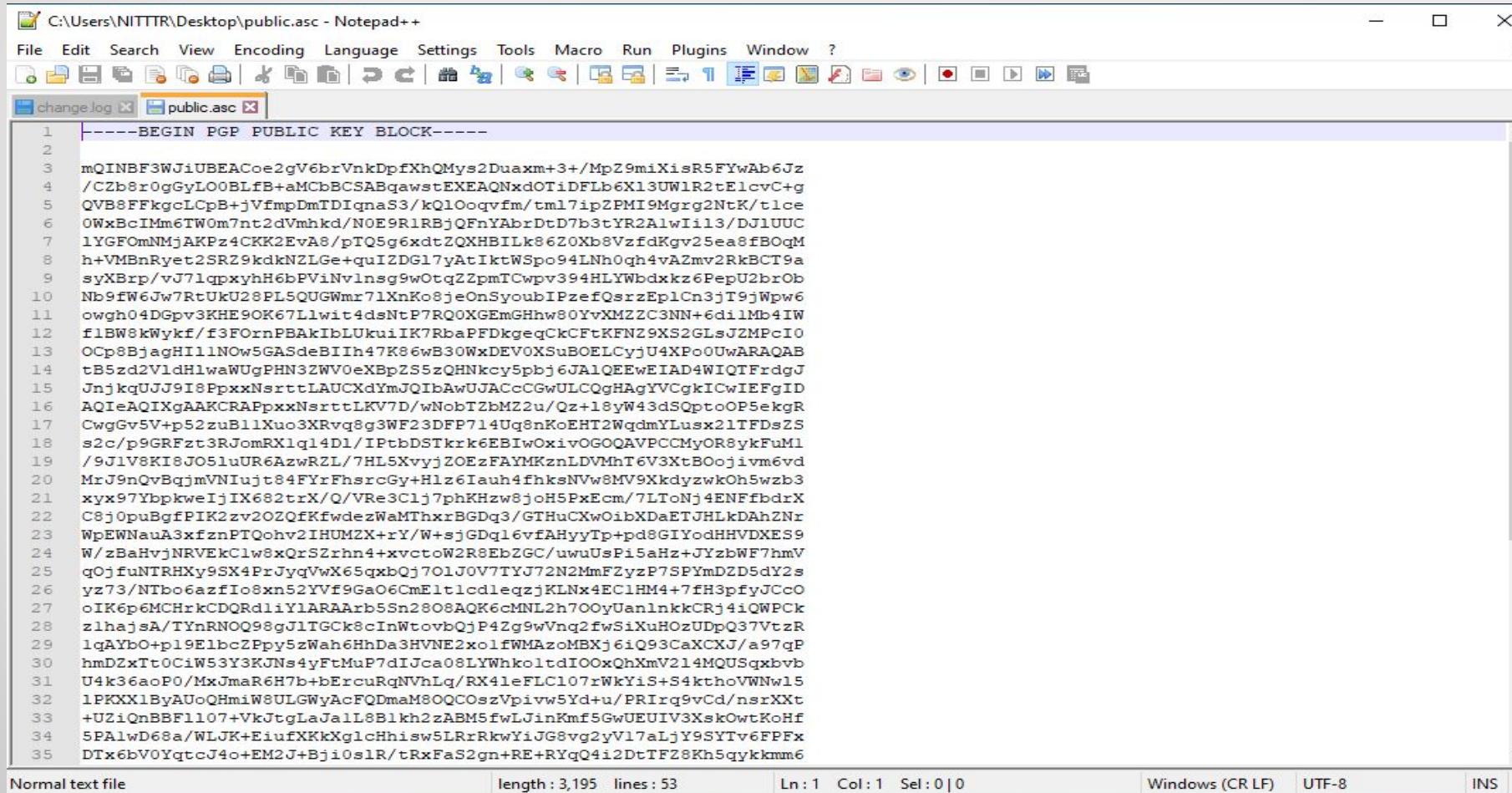
STEP 9 :-GIVE THE PARAPHRASE CREATED DURING KEY PAIR GENRATION



STEP 10:- OPEN THE PUBLIC WITH TEXT EDITOR



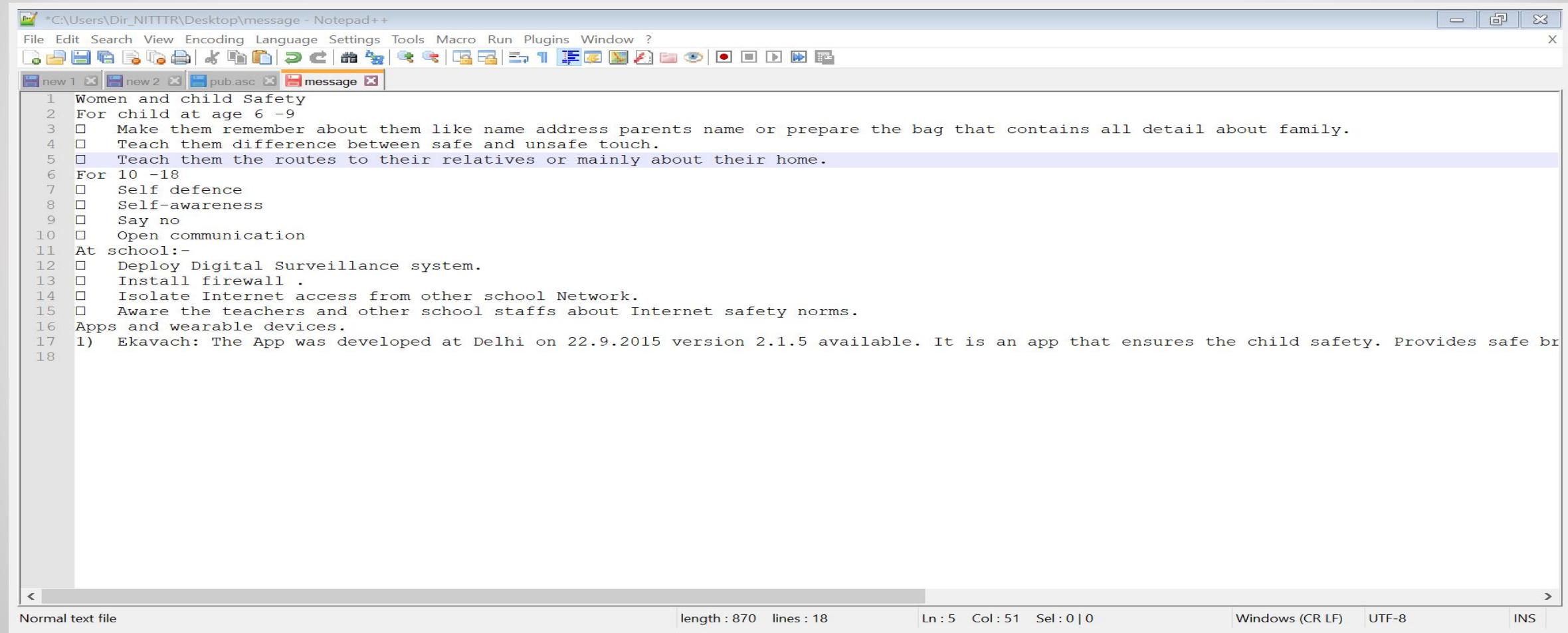
PUBLIC KEY VIEW



The screenshot shows a Notepad++ window with the title bar "C:\Users\NITTTR\Desktop\public.asc - Notepad++". The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Tools, Macro, Run, Plugins, Window, and ?. The toolbar below has icons for file operations like Open, Save, Find, and Print. Below the toolbar, two tabs are visible: "change.log" and "public.asc", with "public.asc" being the active tab. The main text area contains a long string of characters representing a PGP public key block, starting with "-----BEGIN PGP PUBLIC KEY BLOCK-----". The text is wrapped in a monospaced font. At the bottom of the window, there is a status bar with the text "Normal text file", "length : 3,195 lines : 53", "Ln : 1 Col : 1 Sel : 0 | 0", "Windows (CR LF)", "UTF-8", and "INS". A scroll bar is on the right side of the text area.

```
1 -----BEGIN PGP PUBLIC KEY BLOCK-----
2 
3 mQINBF3WJiUBEACoe2gV6brVnkDpfXhQMys2Duaxm+3+/MpZ9miXisR5FYwAb6Jz
4 /Czb8r0gGyLOOBLfB+aMCbBCSAQwastEXEAQNxdOTiDfLb6X13UW1R2tElcvC+g
5 QVB8FFkgcLCpB+jVfmpDmTDIqnaS3/kQlOoqvfm/tm17ip2PMI9Mgrg2NtK/t1ce
6 0WxBcIMm6TW0m7nt2dVmhd/NOE9R1RBjQFnYAbtD7b3tYR2Alwi13/DJ1UUC
7 1YGF0mNmjAKPz4CKK2EvA8/pTQ5g6xdtZQXBILk86Z0Xb8VzfdKgv25ea8fBOqM
8 h+VMBnRyet2SRz9kdLGe+quI2d7AtIktWSpo94LNh0qh4vA2mv2RkBCT9a
9 syXBp/vJ7lqpxyh6bPVivNvnsg9w0tq2ZpmTCwpv394HLYWbdxkz6PepU2brOb
10 Nb9fw6Jw7RtUkU28FL5QUGWmr71XnKo8jeOnSyoubIPzefQsrzEplCn3jT9jWp6
11 owgh04DGpv3KHE9OK67L1wt4dsNtP7RQ0XGEmGHhw80YvXMZC3NN+6dilMb4IW
12 f1BW8kWykf/f3FOrnPBAkIbLUkuiIK7RbaPFDkgeqCkCFTkFNZ9XS2GLsJZMPcI0
13 OCp8BjagHI11NOw5GASdeBIIh47K86wB30WxDEVOXSuBOELCyjU4XPo0UwARAQAB
14 tB5zd2V1dH1waWUgPHN3ZWV0eXBpZS5zQHNkcy5pbj6JTA1QEEwEIAD4WIQTFrJ
15 JnjkqUJJ9IS8PpxNsrttLAUCXdYmQJIBAwUJACcCGwULCQgHAgYVCgkICwIEFgID
16 AQIeAQIXgAAKCRAPpxxNsrttLKv7D/wNobT2bMZ2u/Qz+18yW43dSQptoOP5ekgR
17 CwgGv5V+p52ub1lXuc3XRvg8g3WPf23DFP714Uq8nKoEHT2WqdmYLusx21TfDsZS
18 s2c/p9GRFzt3RJomRXlql4D1/IPtbDStkrk6EBIwOxivOGOQAVPCCMyOR8ykFuM1
19 /9J1V8KI8JO5luUR6AzwRZL/7HL5XvyjZOEZFAYMKznLDVMfhT6V3XtB0ojivm6vd
20 MrJ9nQvBqjmVNlIujt84FYrFhsrGy+Hlz6Iauh4fhksNvW8MV9XkdyzwkOh5wzb3
21 xyx97YbpkweIjIX682trX/Q/VRe3Clj7phKHzw8j0H5PxEcM/7LT0nJ4ENFFbdrx
22 C8j0puBgfPIK2zv2OZQfKfwdezWaMThxrBGDq3/GTHuCXwOibXDaETJHLkDAhZNr
23 WpEWNauA3xfznPTQohv2IHUM2X+rY/W+sjGDq16vFAHyyTp+pd8GIYodHHVDXES9
24 W/zBaHvjNRVEkC1w8xQrSzrhns4+xvctoW2R8EbZGC/uwuUsPi5aHz+JYzbWF7hmV
25 qOjfufNTRHxy9SX4PrJyqVwX65qxbQj701J0V7TYJ72N2MmFZyzP7SPYmDZD5dY2s
26 yz73/NTbo6azflc8xn52Yv9GaO6CmEl1cdleqzjKLNx4EC1HM4+7fH3pfyJCCO
27 oIK6p6MChrkCDQRd1y1ARAAb5Sn2808AQK6cMNL2h7OoyUanlnkkCRj4iQWPCK
28 zlhajsA/TyNROQ98gJ1TGck8cInWtovbQjP4Zg9wVnq2fwSiXuHOzUDpQ37VtzR
29 1qAYbO+p19E1bcZPpy5zWah6HhDa3HVNE2x0lfWMAMoBXj6iQ93CaXCXJ/a97qP
30 hmDzxTt0CiW53Y3KJNs4yFtMuP7dIJca08LYWhk0tdIOOxQhXmV214MQUSqxbvb
31 U4k36aoP0/MxJmaR6H7b+bErcuRqhvLq/RX41eFLC107rWkYiS+S4kthoVWNw15
32 1PKXX1ByAUoQHniW8ULGwyAcFQDMA8OQCOSzVpiw5Ydu/u/PRIrq9vCd/nsrXXt
33 +UZiQnBBFl107+VkJtgLaJall8B1kh2zABM5fwLJinKmf5GwUEUIV3XskOwtKoHf
34 5PA1wD68a/WLJK+EiufXKkXg1cHhiSw5LRrRkwYiJG8vg2yV17aLjY9SYTv6FPFx
35 DTx6bV0YqtcJ4o+EM2J+BjiOs1R/tRxFaS2gn+RE+RYqQ4i2DtTFZ8Kh5qykkmm6
```

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



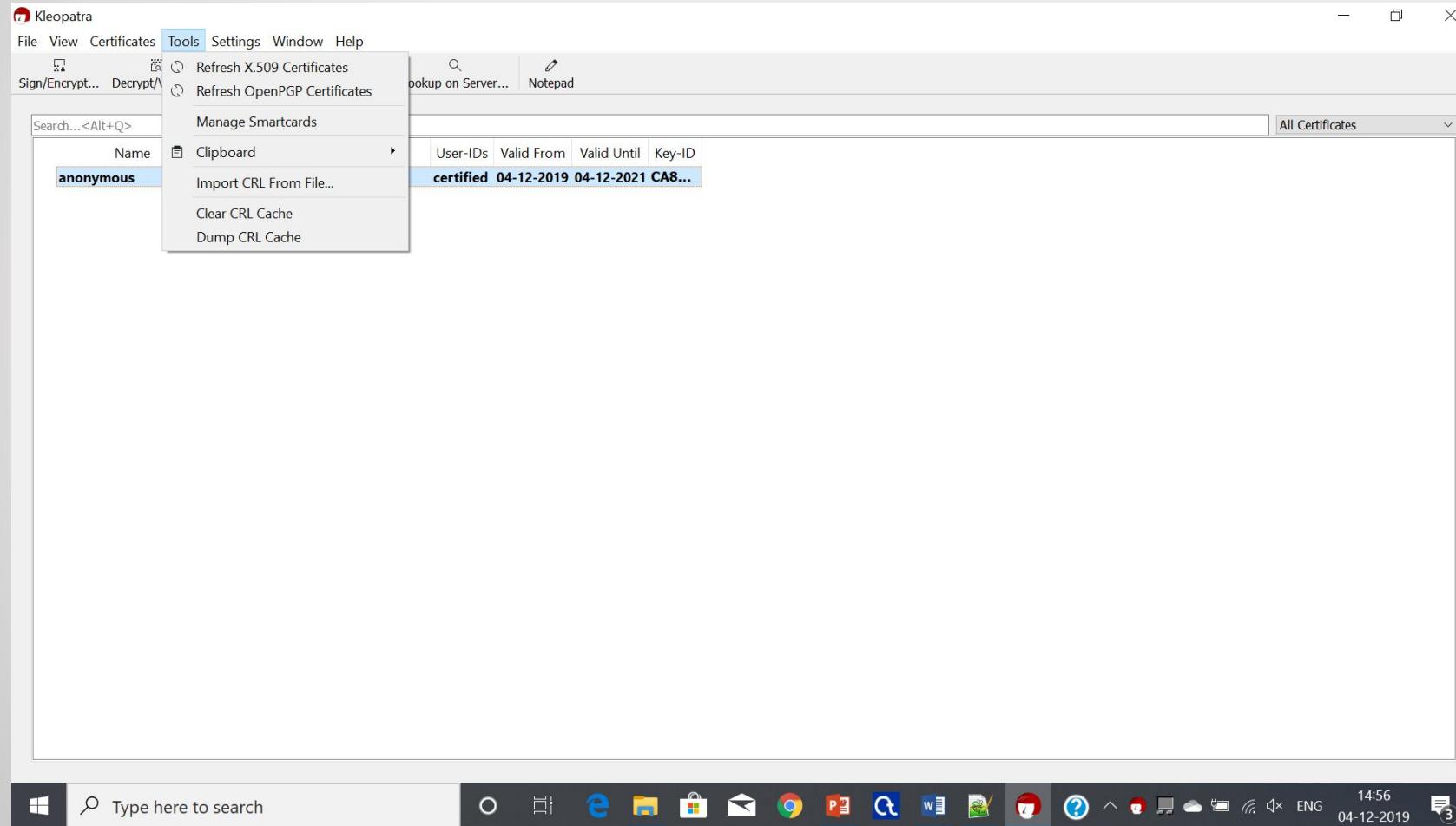
The screenshot shows a Notepad++ window titled "message - Notepad++". The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Tools, Macro, Run, Plugins, Window, and Help. The toolbar contains various icons for file operations like Open, Save, Print, and Find. The status bar at the bottom displays "Normal text file", "length : 870 lines : 18", "Ln : 5 Col : 51 Sel : 0 | 0", "Windows (CR LF)", "UTF-8", and "INS". The main text area contains the following message:

```
1 Women and child Safety
2 For child at age 6 -9
3 □ Make them remember about them like name address parents name or prepare the bag that contains all detail about family.
4 □ Teach them difference between safe and unsafe touch.
5 □ Teach them the routes to their relatives or mainly about their home.
6 For 10 -18
7 □ Self defence
8 □ Self-awareness
9 □ Say no
10 □ Open communication
11 At school:-
12 □ Deploy Digital Surveillance system.
13 □ Install firewall .
14 □ Isolate Internet access from other school Network.
15 □ Aware the teachers and other school staffs about Internet safety norms.
16 Apps and wearable devices.
17) Ekavach: The App was developed at Delhi on 22.9.2015 version 2.1.5 available. It is an app that ensures the child safety. Provides safe br
18
```

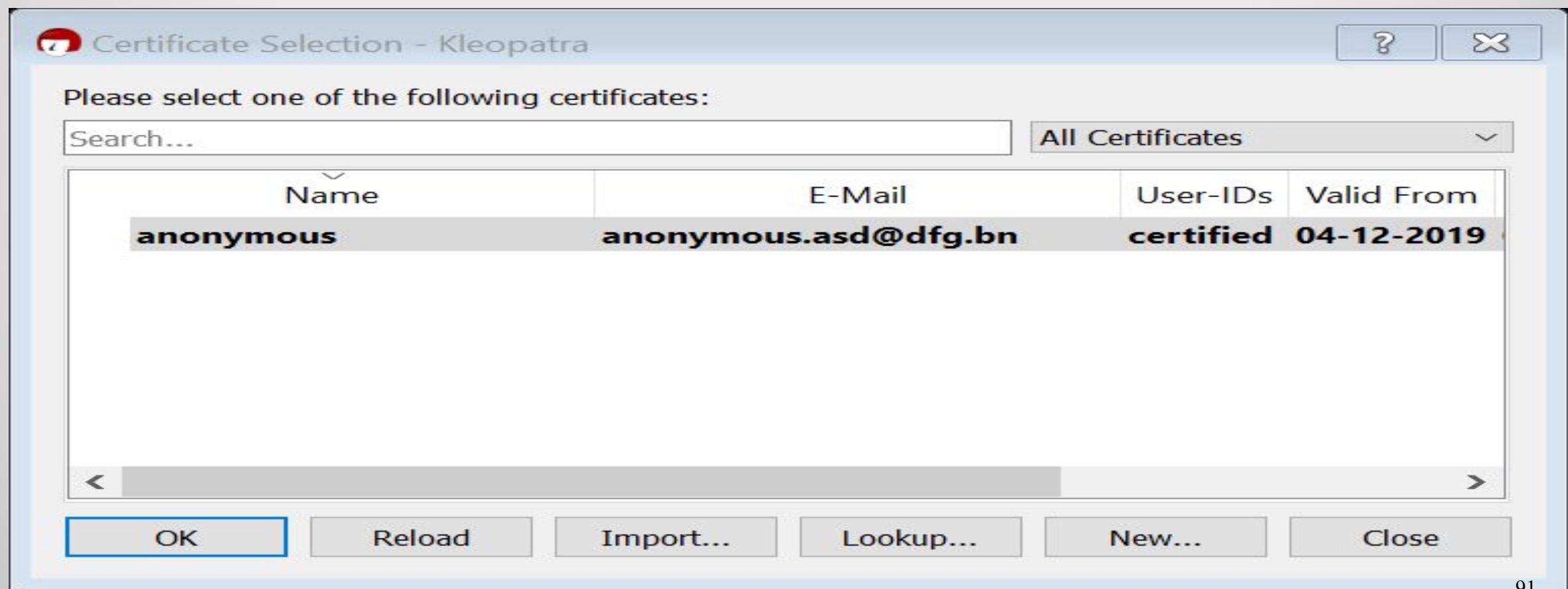
TO ENCRYPT THE MESSAGE

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

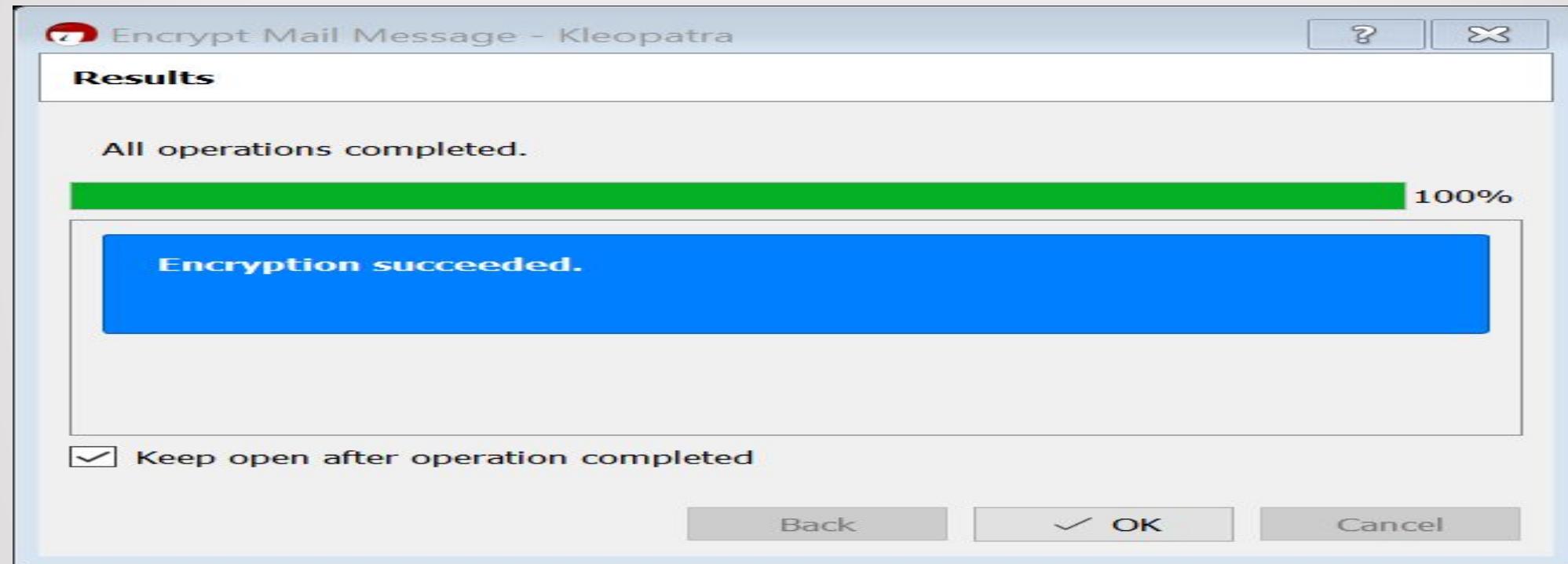
STEP 12:- CLICK ON THE TOOLS OF THE WIZARD AND CLICK ENCRYPT



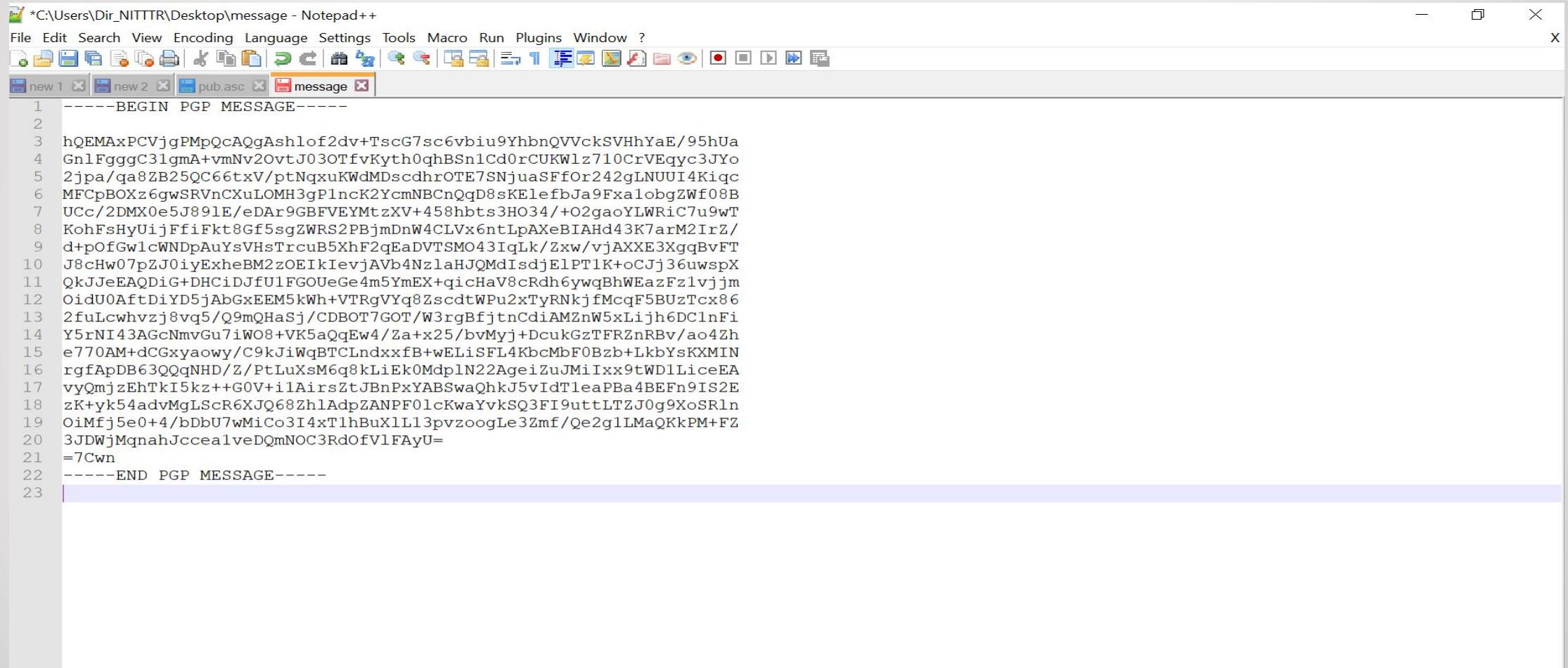
STEP13:- THEN ADD THE RECIPIENT



THEN THE MESSAGE IS SUCCESSFULLY ENCRYPTED



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



The screenshot shows a Notepad++ window with the title bar "C:\Users\Dir_NITTTR\Desktop\message - Notepad++". The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Tools, Macro, Run, Plugins, Window, and Help. The toolbar below has icons for file operations like Open, Save, Print, and Find. Below the toolbar, there are tabs for "new 1", "new 2", "pub.asc", and "message". The main text area contains a PGP message:

```
1 -----BEGIN PGP MESSAGE-----
2
3 hQEMAxPCVjgPMpQcAQgAshlof2dv+TscG7sc6vbiu9YhbnQVVckSVHhYaE/95hUa
4 Gn1FgggC31gmA+vmNv20vtJ03OTfvKyth0qhBSn1Cd0rCUKwlz710CrVEqyc3JYo
5 2jpa/qa8ZB25QC66txV/ptNqxuKWDMDscdhrOTE7SNjuaSFFor242gLNUUI4Kiqc
6 MFCpBOXz6gwSRVnCXuLOMH3gP1ncK2YcmNBCnQqD8sKElefJa9FxalobgZWf08B
7 UCC/2DMX0e5J891E/eDAr9GBFVEYMtzXV+458hbts3HO34/+O2gaoYLWRiC7u9wT
8 KohFsHyUi jFFiFkt8Gf5sgZWRs2PBjmDnW4CLVx6ntLpAXeBIAh43K7arM2IrZ/
9 d+pOfGw1cWNDpAuYsVHsTrcuB5XhF2qEaDVTSMO43IqLk/Zxw/vjAXXE3XgqBvFT
10 J8cHw07pZJ0iyExheBM2zOEIkIevjAvB4Nz1aHJQMdIsdjElPT1K+oCJj36uwspX
11 QkJJeEAQDiG+DHCiDJfU1FGOUeGe4m5YmEX+qicHaV8cRdh6ywqBhWEazFz1vjjm
12 OidU0AftDiYD5jAbGxEEM5kWh+VTRgVYq8ZscdtWPu2xTyRNkjfMcqF5BUzTcx86
13 2fuLcwhvzj8vq5/Q9mQHaSj/CDBOT7GOT/W3rqBfjtnCdiAMZnW5xLijh6DC1nFi
14 Y5rNI43AGcNmvgu7iW08+VK5aQqEw4/Za+x25/bvMyj+DcukGzTFRZnRBv/ao4Zh
15 e770AM+dCGxyaowy/C9kJiWqBTCLndxxfb+wELiSFL4KbcMbF0Bzb+LkbYsKXMIN
16 rgfApDB63QQqNHD/Z/PtLuXsM6q8kLiEkOMdp1N22AgeiZuJMiIxx9tWD1LiceEA
17 vyQmjzEhTkI5kz++GOV+i1AirsZtJBnPxYABSwahkJ5vIdT1eaPBa4BEFn9IS2E
18 zK+yk54advMgLScR6XJQ68ZhlAdpZANPF01cKwaYvkSQ3FI9uttLTZJ0g9XoSRLn
19 OiMfj5e0+4/bDbU7wMiCo3I4xT1hBuXlL13pvzoogLe3Zmf/Qe2g1LMaQKkPM+FZ
20 3JDWjMqnahJccealveDQmNOC3RdOfV1FAyU=
21 =7Cwn
22 -----END PGP MESSAGE-----
23
```

THANK YOU