

## [Exit Lab](#)

### InstructionsResources

### Module 20: Cryptography

#### Scenario

With the increasing adoption of the Internet for business and personal communication, securing sensitive information such as credit-card and personal identification numbers (PINs), bank account numbers, and private messages is becoming increasingly important, and yet, more difficult to achieve. Today's information-based organizations extensively use the Internet for e-commerce, market research, customer support, and a variety of other activities. Thus, data security is critical to online businesses and privacy of communication.

Cryptography and cryptographic ("crypto") systems help in securing data from interception and compromise during online transmissions. Cryptography enables one to secure transactions, communications, and other processes performed in the electronic world, and is additionally used to protect confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, etc.

As an ethical hacker or penetration tester, you should suggest to your client proper encryption techniques to protect data, both in storage and during transmission. The labs in this module demonstrate the use of encryption to protect information systems in organizations.

#### Objective

The objective of the lab is to use encryption to conceal data and perform other tasks that include, but is not limited to:

- Generate hashes and checksum files
- Calculate the encrypted value of the selected file
- Use encrypting/decrypting techniques
- Perform file and data encryption
- Create self-signed certificates
- Perform email encryption
- Perform disk encryption

- Perform cryptanalysis

## Overview of Cryptography

"Cryptography" comes from the Greek words *kryptos*, meaning "concealed, hidden, veiled, secret, or mysterious," and *graphia*, "writing"; thus, cryptography is "the art of secret writing."

Cryptography is the practice of concealing information by converting plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme: it is the process of the conversion of data into a scrambled code that is sent across a private or public network.

There are two types of cryptography, determined by the number of keys employed for encryption and decryption:

- **Symmetric Encryption:** Symmetric encryption (secret-key, shared-key, and private-key) uses the same key for encryption as it does for decryption
- **Asymmetric Encryption:** Asymmetric encryption (public-key) uses different encryption keys for encryption and decryption; these keys are known as public and private keys

## Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform cryptography to protect confidential data. Recommended labs that will assist you in learning various cryptography techniques include:

1. Encrypt the information using various cryptography tools
  - Calculate one-way hashes using HashCalc
  - Calculate MD5 hashes using MD5 Calculator
  - Calculate MD5 hashes using HashMyFiles
  - Perform file and text message encryption using CryptoForge
  - Encrypt and decrypt data using BCTextEncoder
2. Create a self-signed certificate
  - Create and use self-signed certificates
3. Perform email encryption

- Perform email encryption using RMail
- 4. Perform disk encryption
  - Perform disk encryption using VeraCrypt
  - Perform disk encryption using BitLocker Drive Encryption
  - Perform disk encryption using Rohos Disk Encryption
- 5. Perform cryptanalysis using various cryptanalysis tools
  - Perform cryptanalysis using CrypTool
  - Perform cryptanalysis using AlphaPeeler

1 Hr 28 Min Remaining

## **Lab 1: Encrypt the Information using Various Cryptography Tools**

### **Lab Scenario**

As a professional ethical hacker and penetration tester, you should use various cryptography techniques or tools to protect confidential data against unauthorized access. Cryptography protects confidential data such as email messages, chat sessions, web transactions, personal data, corporate data, e-commerce applications, and many other kinds of communication. Encrypted messages can at times be decrypted by cryptanalysis (code breaking), although modern encryption techniques are virtually unbreakable.

The labs in this exercise demonstrate how you can use various cryptography tools to encrypt important information in the system.

### **Lab Objectives**

- Calculate one-way hashes using HashCalc
- Calculate MD5 hashes using MD5 Calculator
- Calculate MD5 hashes using HashMyFiles
- Perform file and text message encryption using CryptoForge
- Encrypt and decrypt data using BCTextEncoder

### **Overview of Cryptography Tools**

System administrators use cryptography tools to encrypt system data within their network to prevent attackers from modifying the data or misusing it in other ways. Cryptography tools can also be used to calculate or decrypt hash functions available in MD4, MD5, SHA-1, SHA-256, etc.

Cryptography tools are used to convert the information present in plain text (readable format) into cipher text (unreadable format) using a key or encryption scheme. The converted data are in the form of a scrambled code that is encrypted and sent across a private or public network.

#### **Task 1: Calculate One-way Hashes using HashCalc**

Hash functions calculate a unique fixed-size bit string representation, called a message digest, of any arbitrary block of information. Message digest (One-way Hash) functions distill the information contained in a file (small or large) into a single fixed-length number, typically between 128 and 256 bits. If any given bit of the function's input is changed, every output bit



has a 50% chance of changing. Given an input file and its corresponding message digest, it should be nearly impossible to find another file with the same message digest value, as it is computationally infeasible to have two files with the same message digest value.

HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports the Secure Hash Algorithm family: MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in the peer-to-peer file sharing applications, eDonkey and eMule.

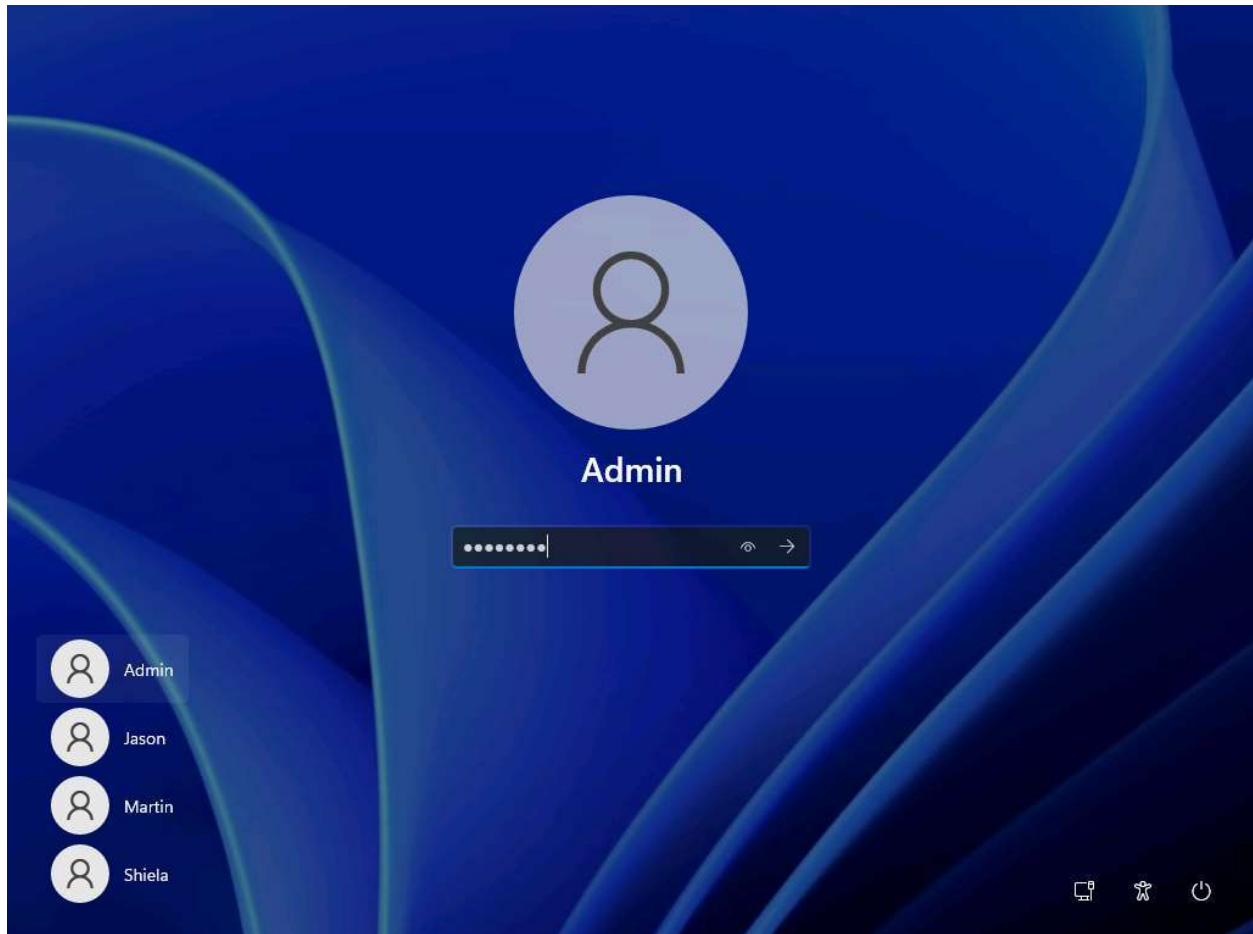
Here, we will use the HashCalc tool to calculate one-way hashes.

1. Click [Windows 11](#) to switch to the **Windows 11** machine. click [Ctrl+Alt+Delete](#) to activate it. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa\$\$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.

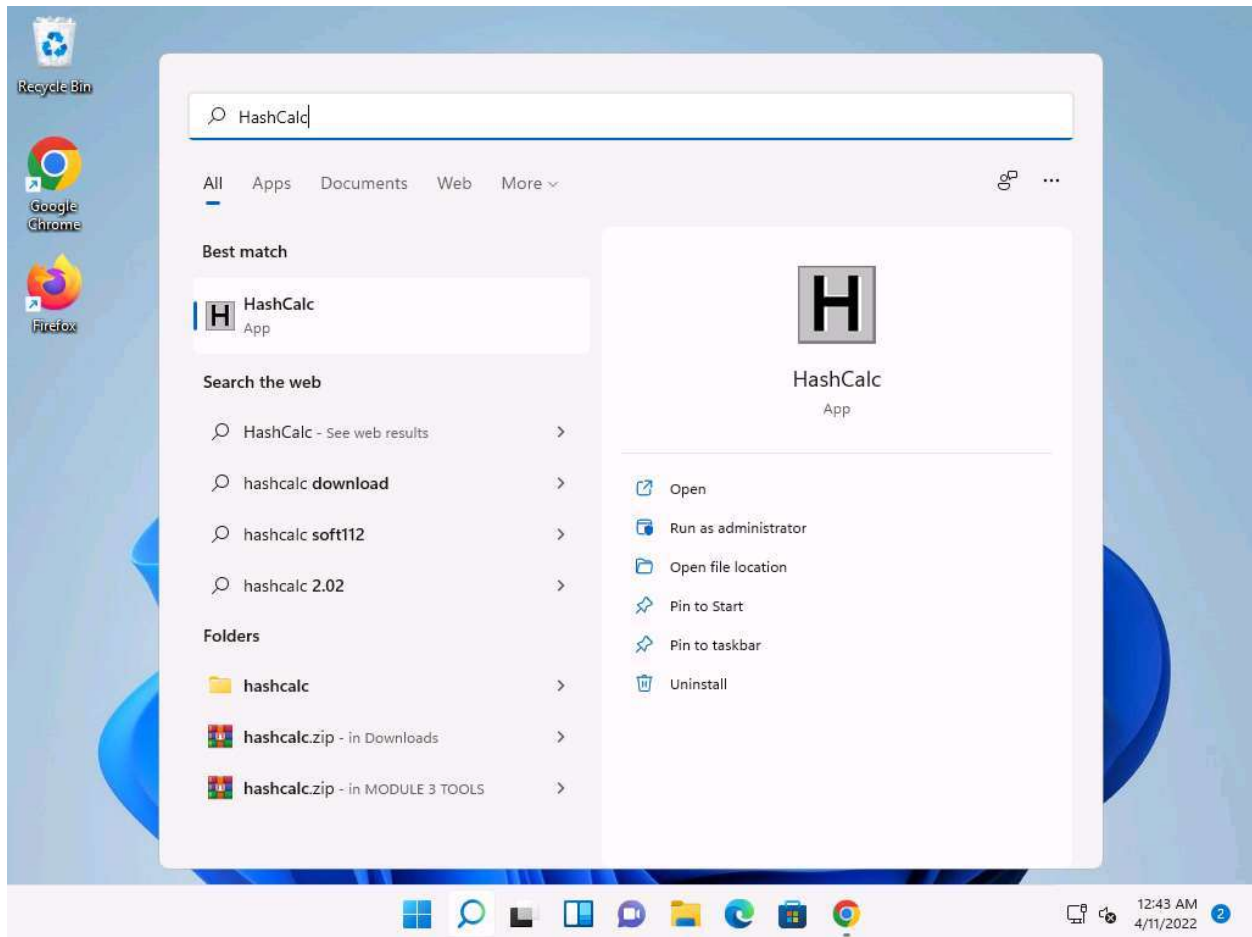
If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** wizard, click **Cancel**.

Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

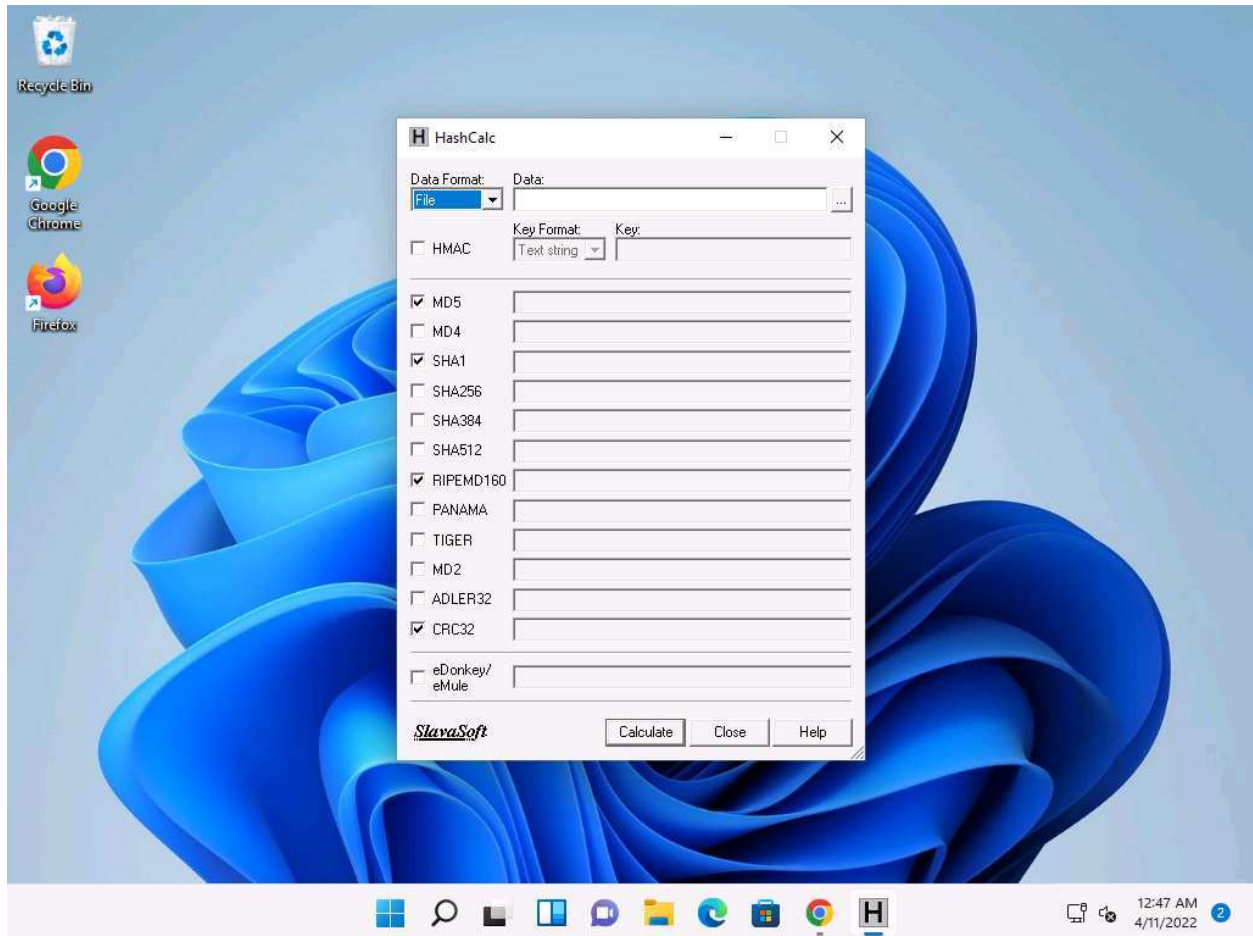


2. Click **Search** icon (  ) on the **Desktop**. Type **HashCalc** in the search field, the **HashCalc** appears in the results, click **Open** to launch it.

If the **User Account Control** pop-up appears, click **Yes**.



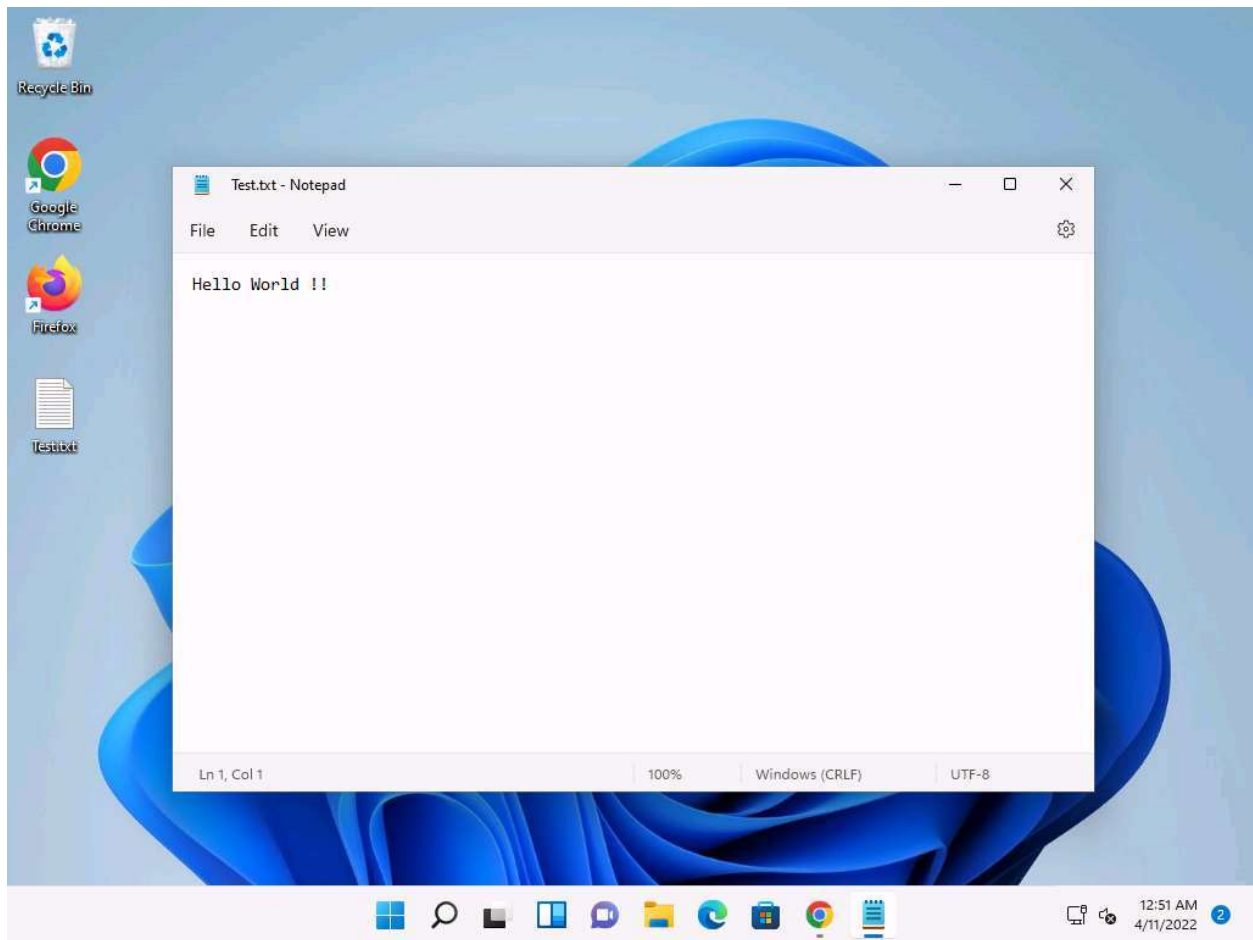
3. The **HashCalc** main window appears, as shown in the screenshot.



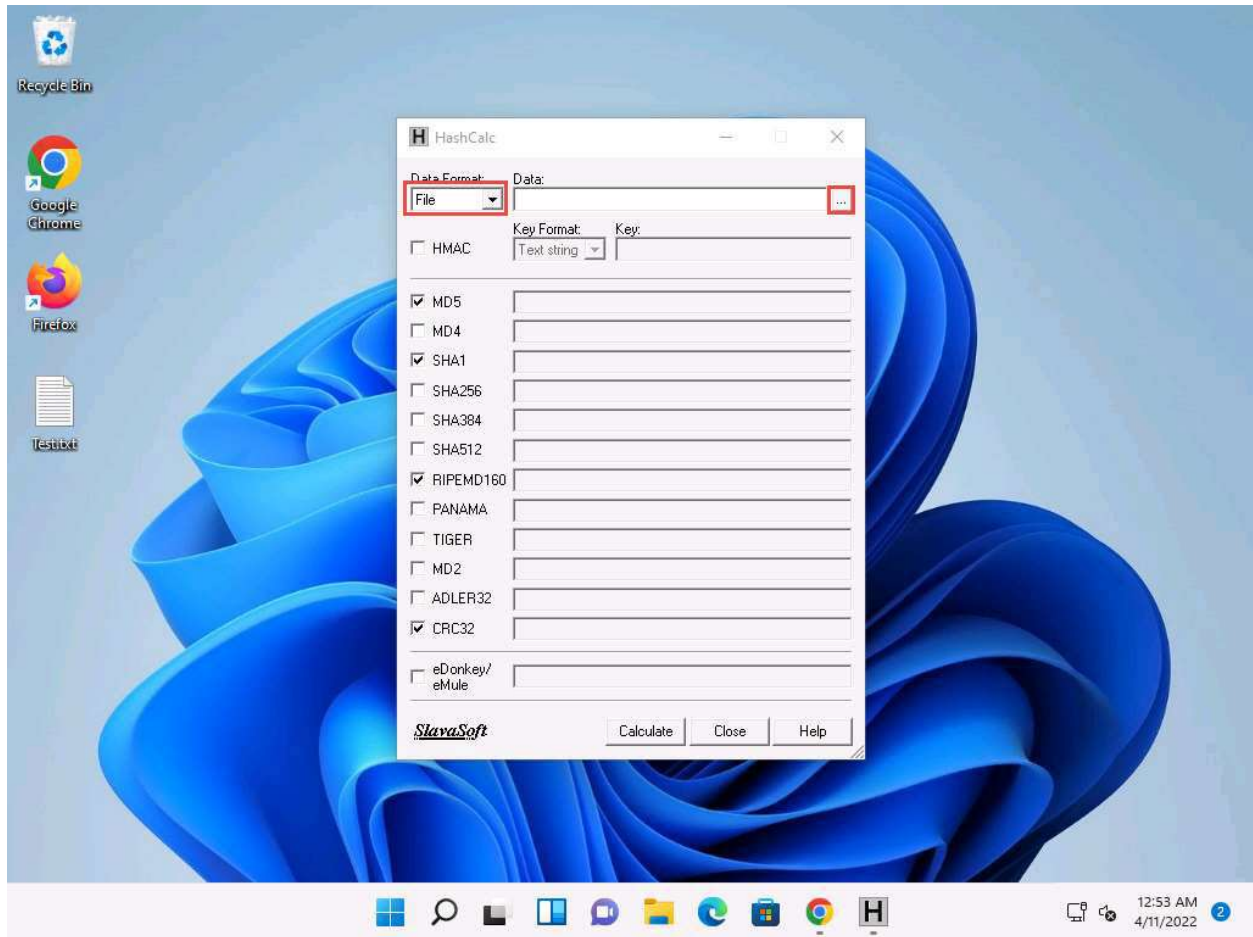
4. Minimize the **HashCalc** window. Navigate to **Desktop**, right-click on the **Desktop** window, and navigate to **New --> Text Document** to create a new text file.

You can create a text file at any location of your choice.

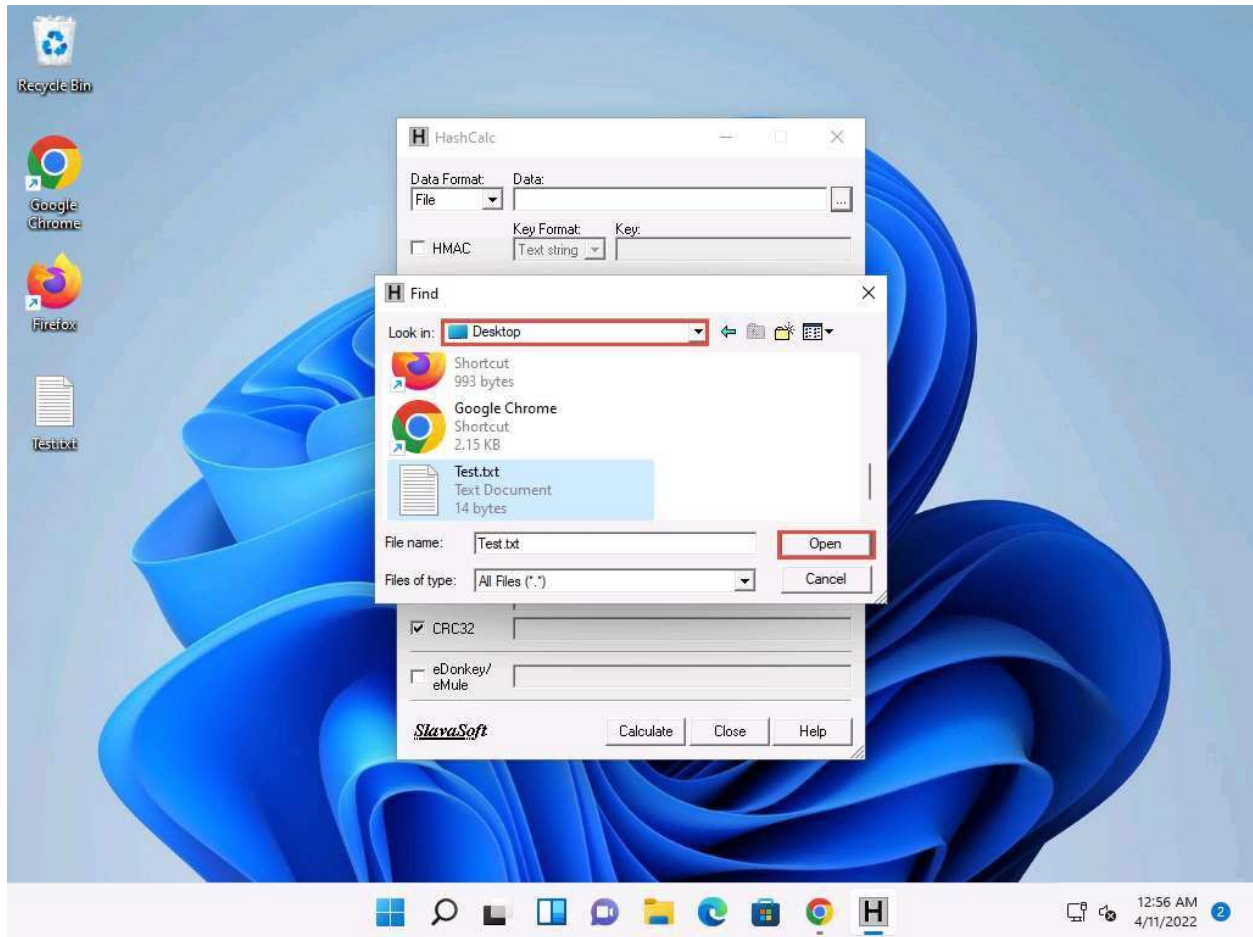
5. A newly created text file appears; rename it to **Test.txt** and open it. Write some text in it (here, **Hello World !!**) and press **Ctrl+S** to save the file. Close the text file.



- Now, switch back to the **HashCalc** window; ensure that the **File** option is selected in the **Data Format** field and click ellipsis icon under the **Data** field.

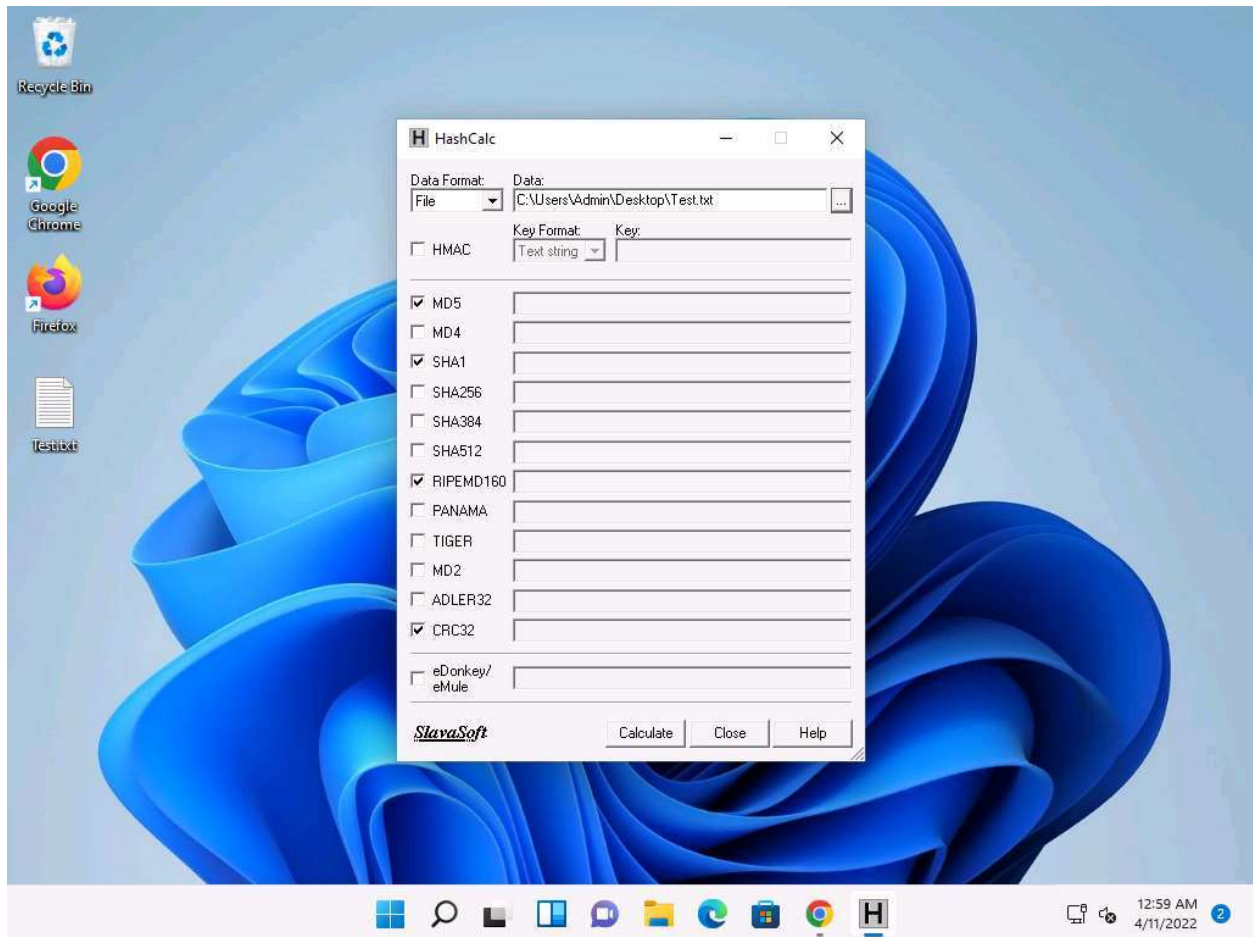


7. The **Find** window appears, navigate to the location where you saved the **Test.txt** file (here, **Desktop**) and click **Open**.



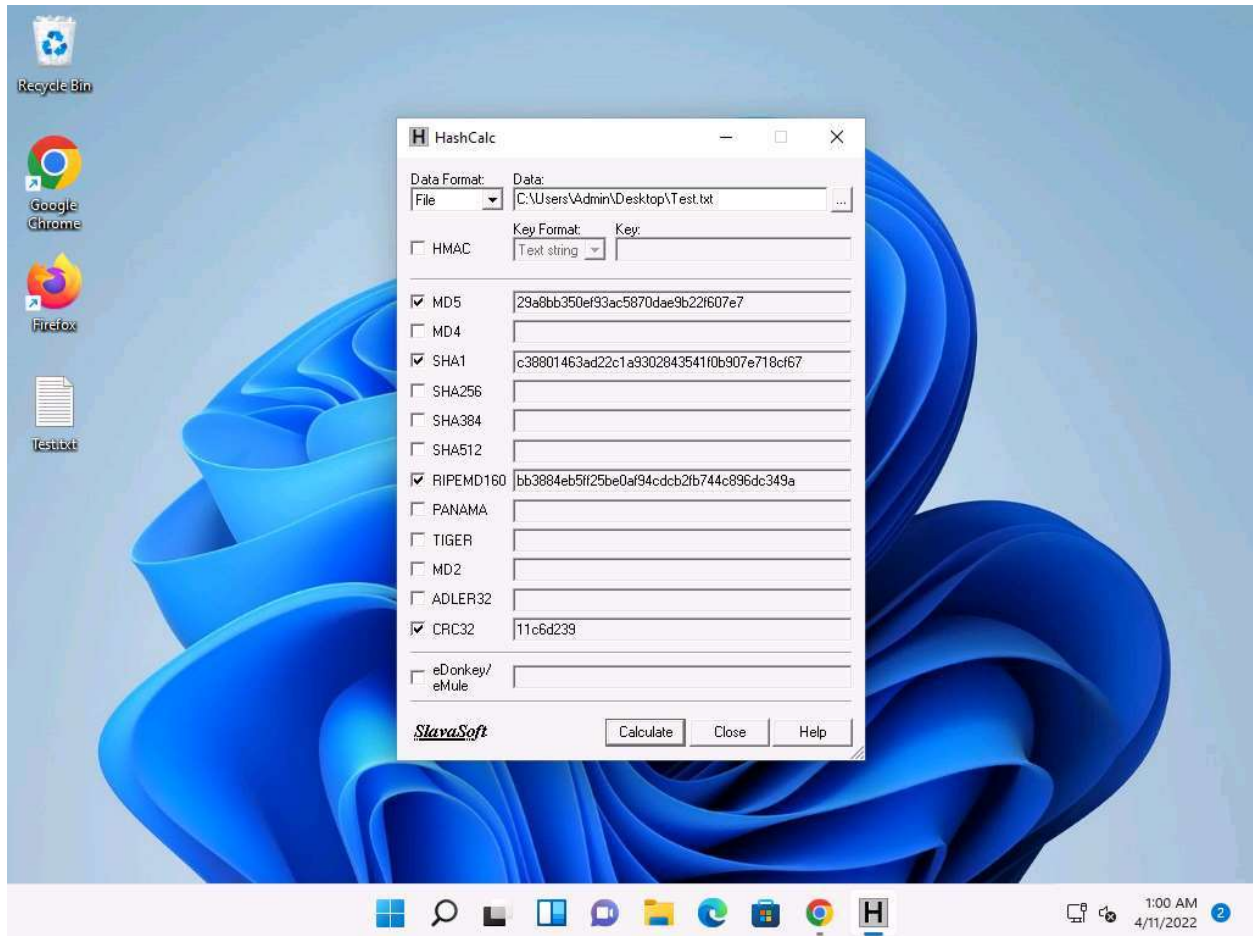


8. The path of the selected file (**Test.txt**) appears under the **Data** field. Ensure that the **MD5**, **SHA1**, **RIPEMD160**, and **CRC32** hash functions are selected. Click the **Calculate** button.

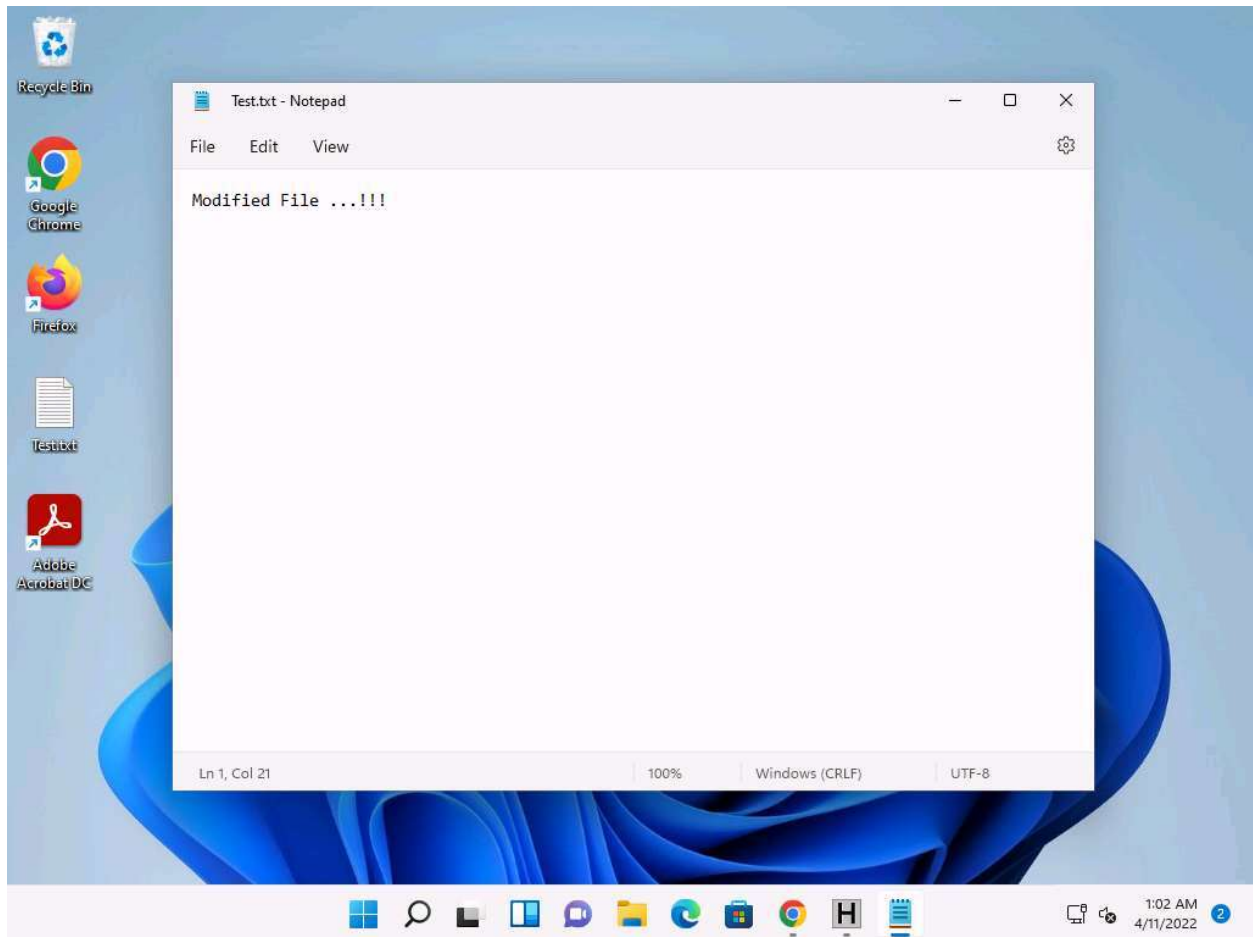




9. The calculated hash values of the **Test.txt** file appears, as shown in the screenshot.



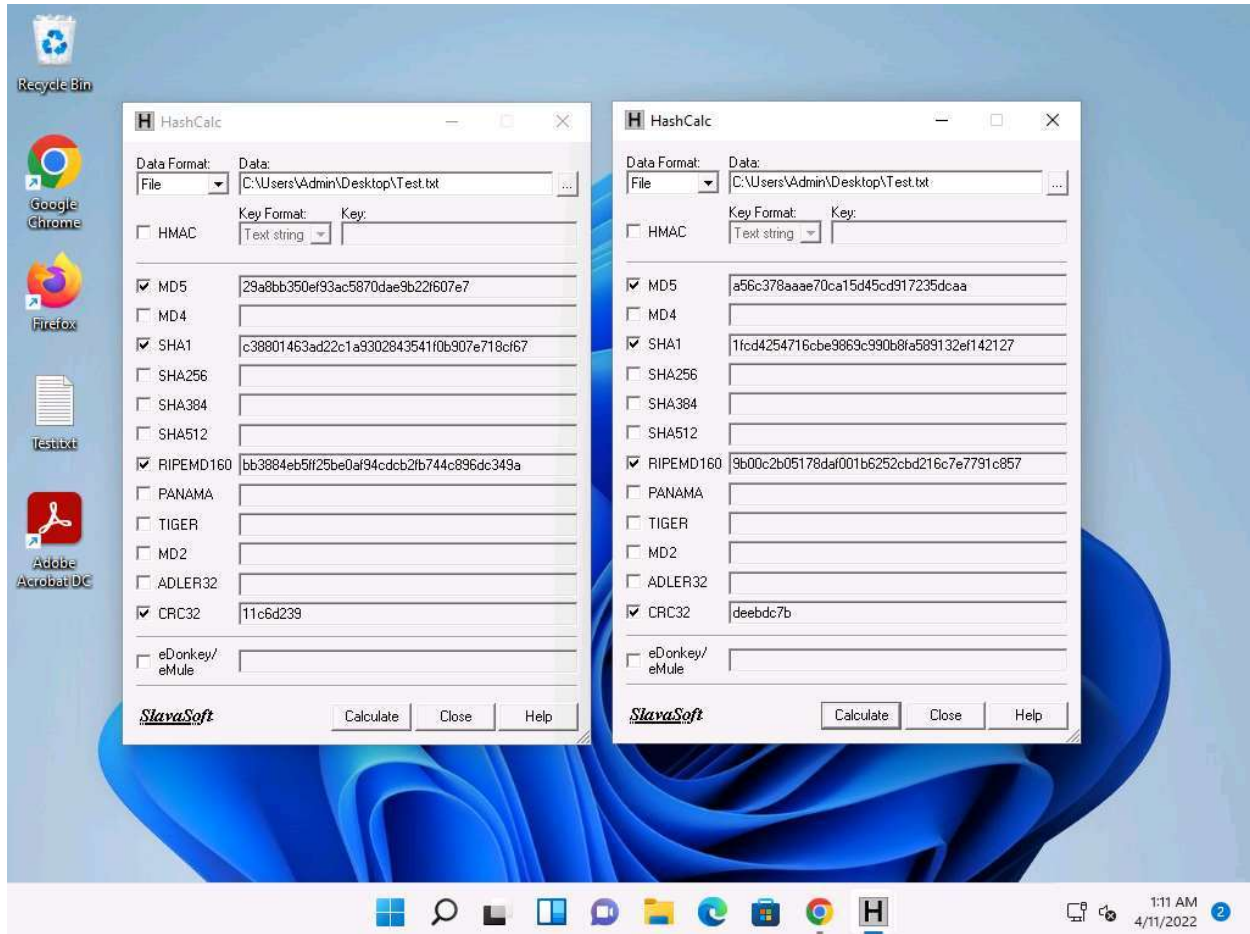
10. Minimize the **HashCalc** window, navigate to **Desktop**, and double-click the **Test.txt** file to open it. Modify the file content by writing some text (here, **Modified File ...!!!**) and press **Ctrl+S** to save it. Close the text file.



11. Click **Search** icon (  ) on the **Desktop**. Type **HashCalc** in the search field, the **HashCalc** appears in the results, click **Open** to launch it.

12. A new **HashCalc** window appears, perform **Steps #6-9**

13. Now, maximize the first **HashCalc** window and place it beside the second **HashCalc** window. You can observe changes in the hash values of the text file (**Test.txt**) before and after the modification, as shown in the screenshot.



In real-time, the HashCalc tool is used to check the integrity of a file where the changes in the hash values indicate that the file content has been modified.

14. This concludes the demonstration of calculating one-way hashes using HashCalc.

15. Close all open windows and document all the acquired information.

#### **Question 20.1.1.1**

Use HashCalc to find the CRC32 hash value of the file E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashCalc\setup.exe on the Windows 11 machine.


## Task 2: Calculate MD5 Hashes using MD5 Calculator

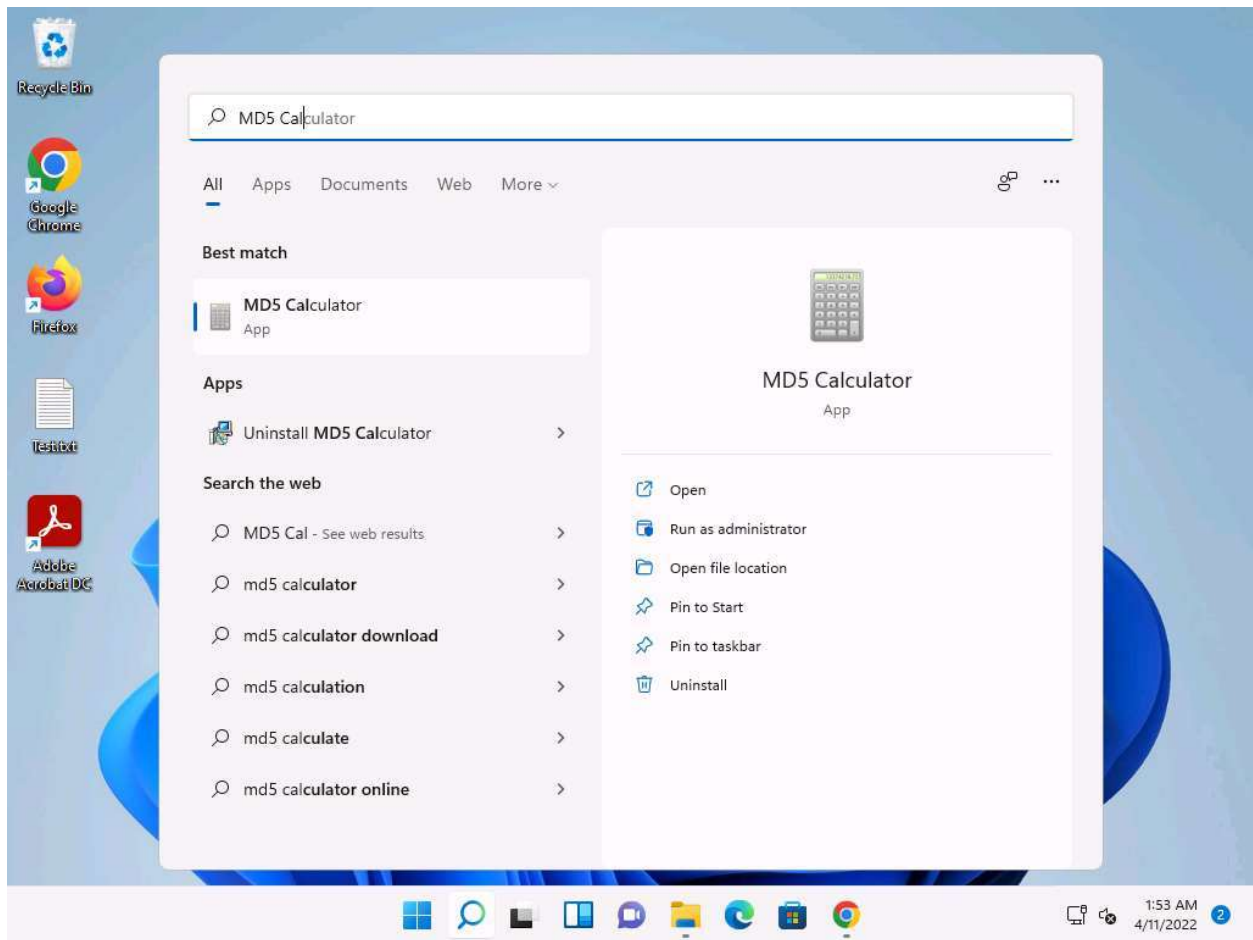
MD2, MD4, MD5, and MD6 are message digest algorithms used in digital signature applications to compress documents securely before the system signs it with a private key. The algorithms can be of variable length, but the resulting message digest is always 128 bits.

The MD5 algorithm is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the input. The MD5 algorithm is used in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords.

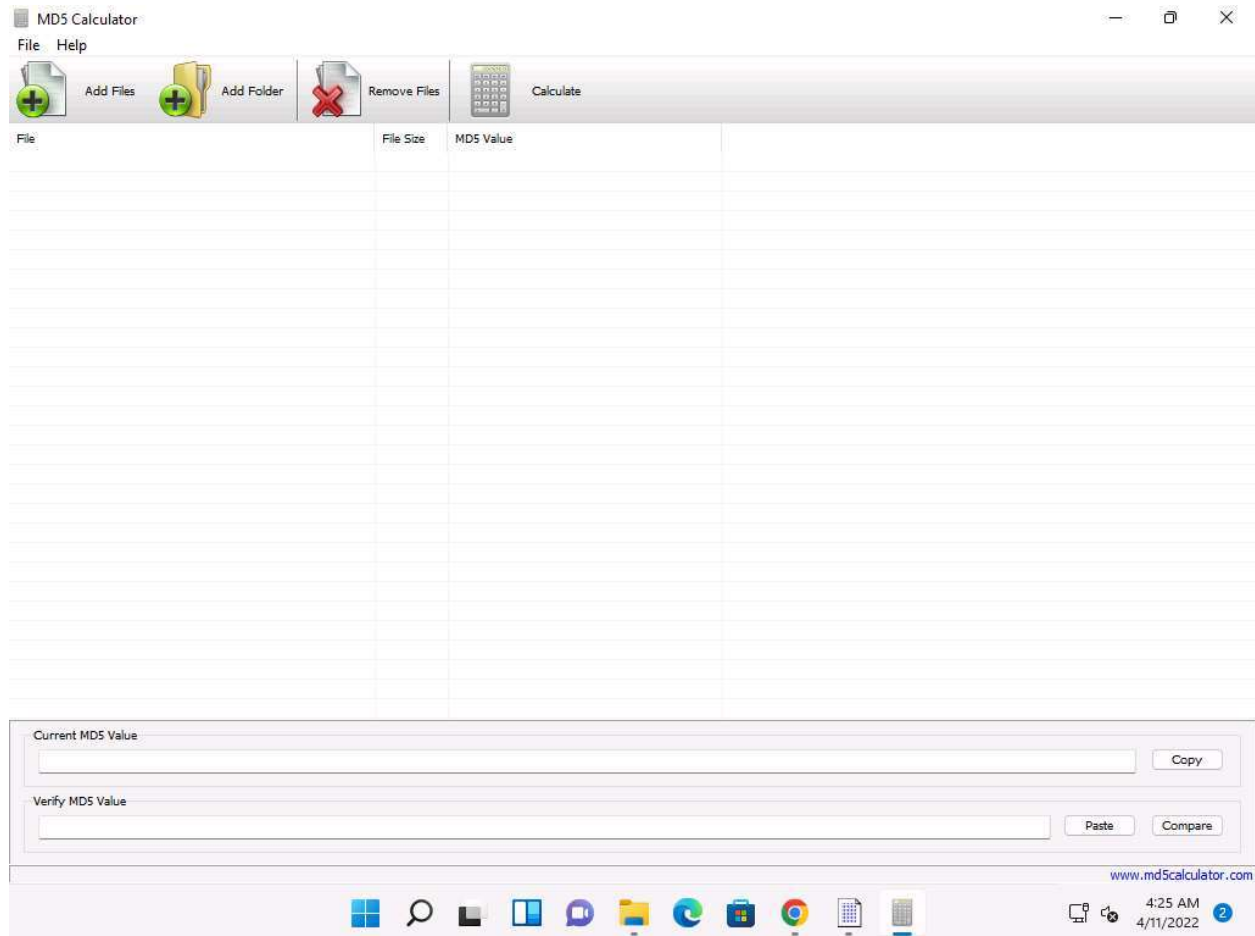
MD5 Calculator is a simple application that calculates the MD5 hash of a given file, and it can be used with large files (e.g., multiple gigabytes). It features a progress counter and a text field from which the final MD5 hash can be easily copied to the clipboard. MD5 calculator can be used to check the integrity of a file.

Here, we will use the MD5 Calculator tool to calculate MD5 hashes.

1. Click **Search** icon (  ) on the **Desktop**. Type **MD5 Cal** in the search field, the **MD5 Calculator** appears in the results, click **Open** to launch it.

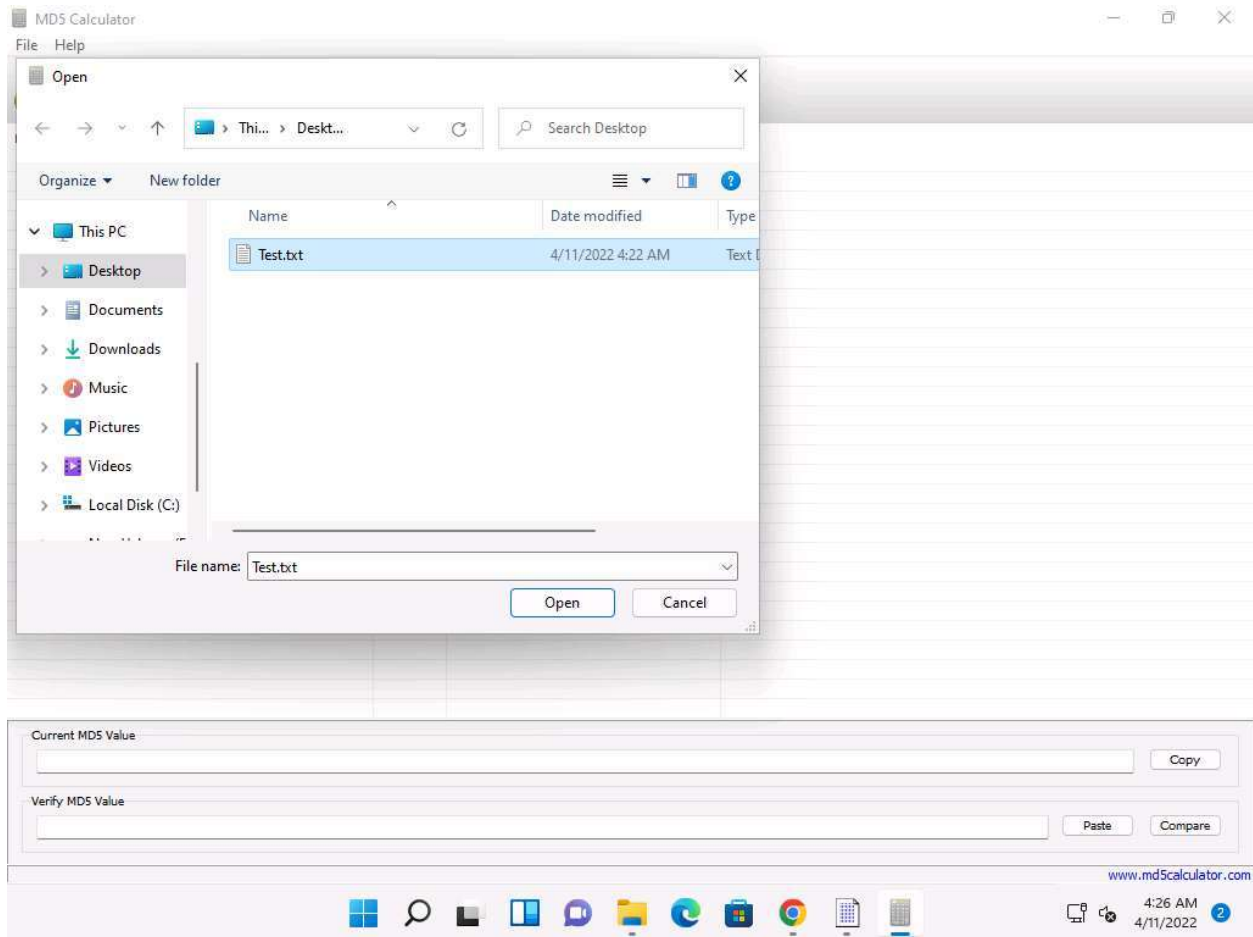


2. The **MD5 Calculator** main window appears, as shown in the screenshot.



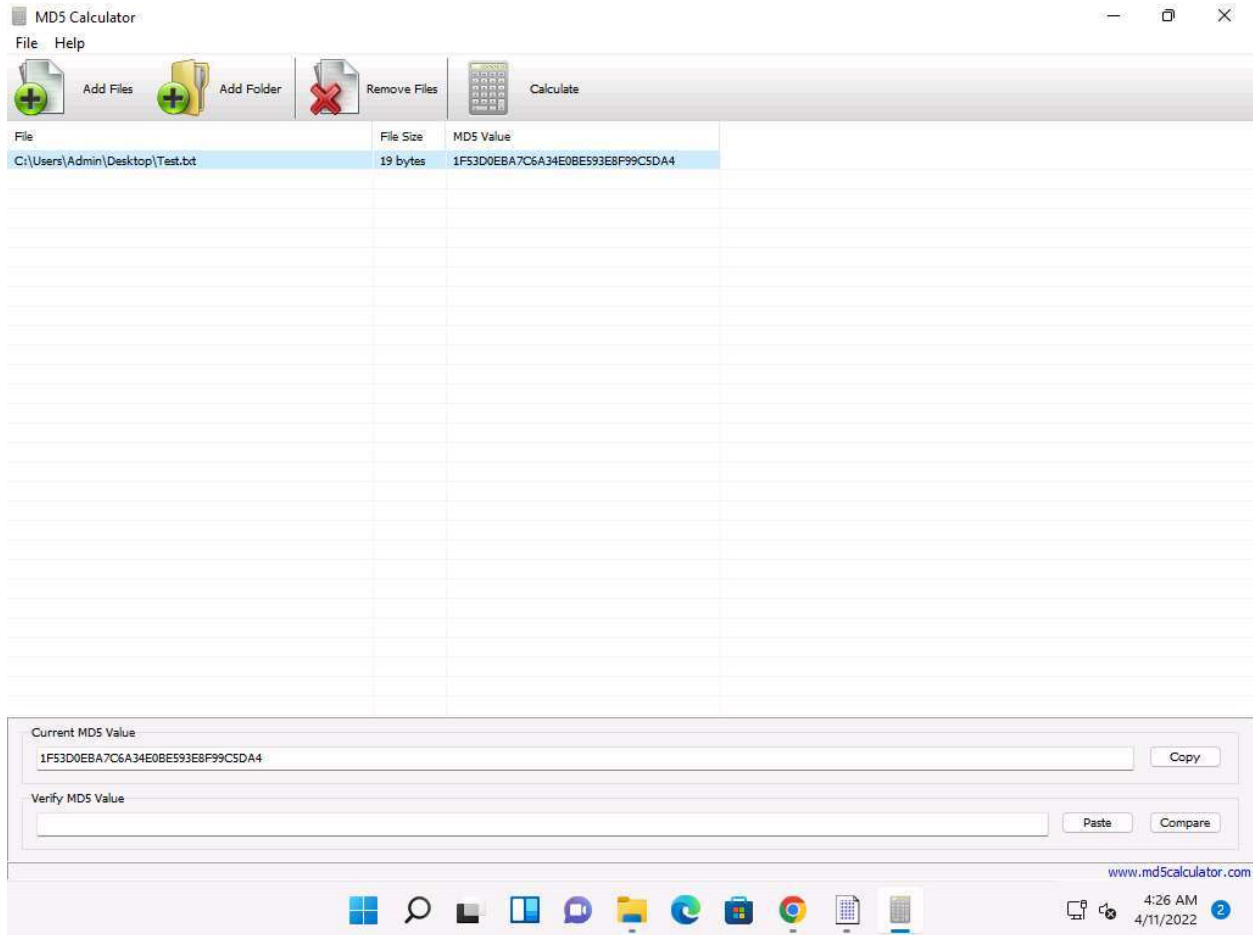
3. Click on **Add Files** in **MD5 Calculator** window.

4. In the **Open** window, navigate to the Desktop and select **Test.txt** file and click **Open**.

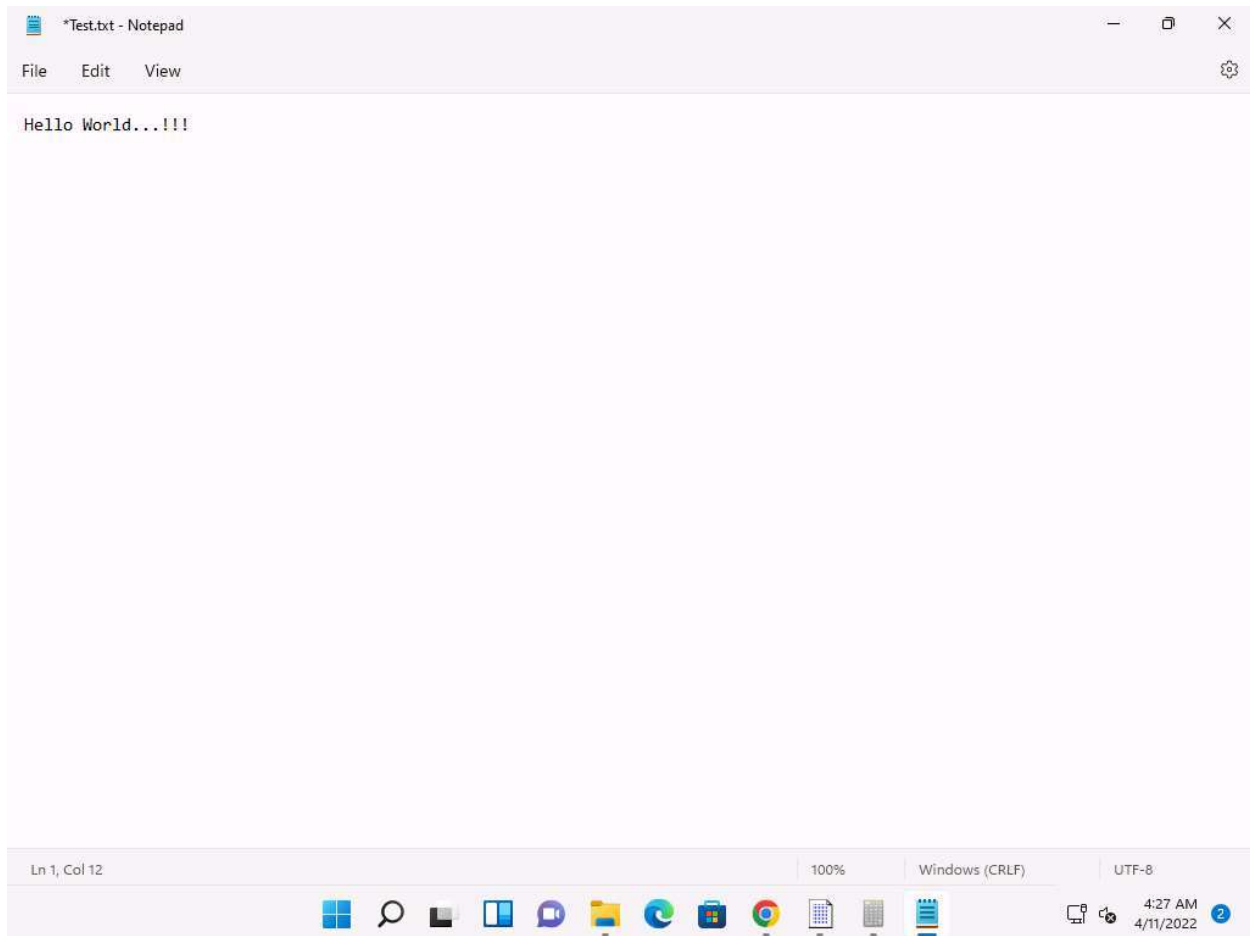




5. You can observe the uploaded file path under **File** section, click on **Calculate** to get the hash value in **Current MD5 value** field at the bottom of the window.

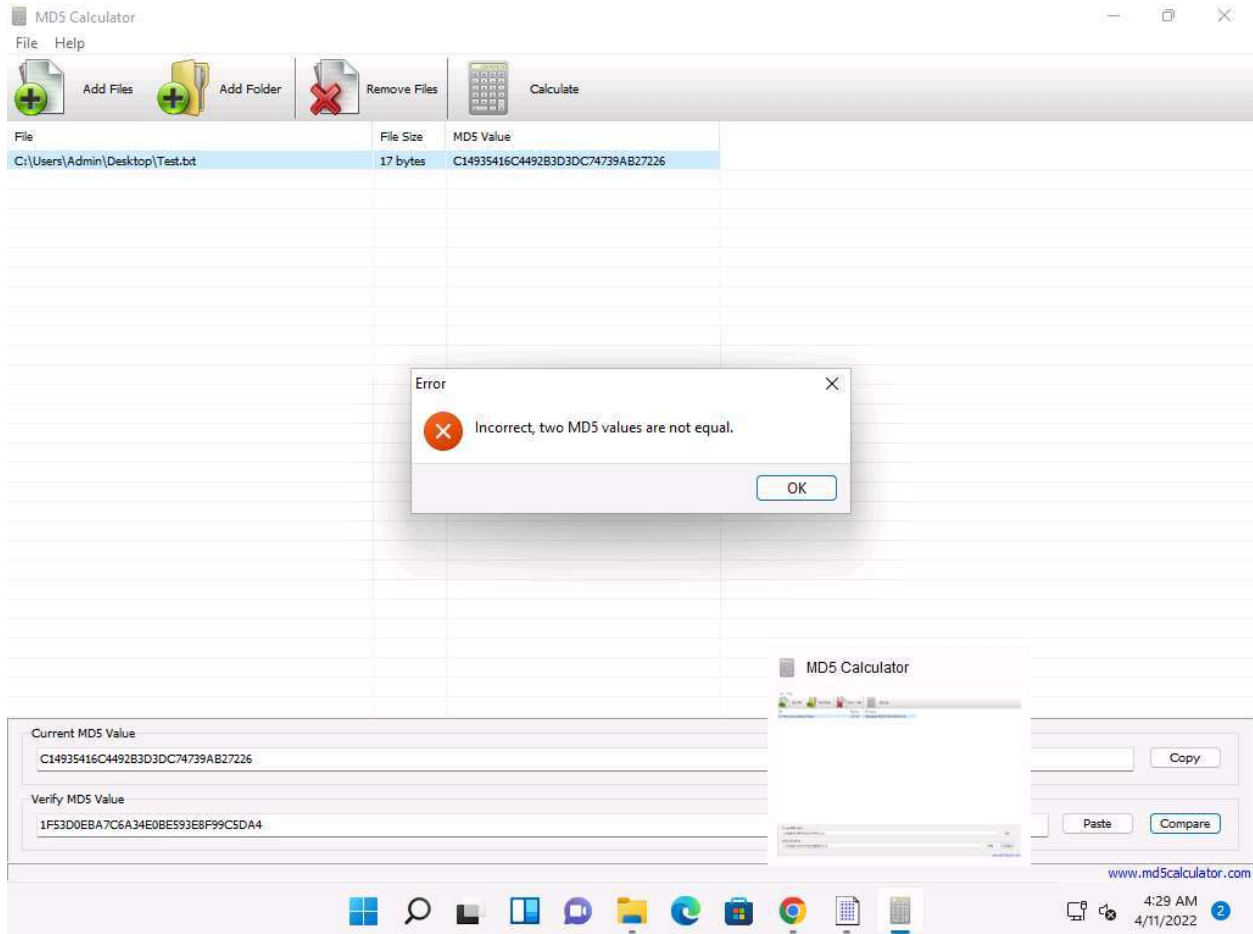


6. Now, click on **Copy** beside the MD5 value, to copy the hash value from **Current MD5 Value** field and click on **Remove Files** to clear the MD5 value.
7. Now, double-click the **Test.txt** file from **Desktop** to open it and change the content of the file by modifying text within (here, **Hello World...!!!**). Save and close the **Test.txt** file.



8. In **MD5 Calculator** perform **Steps #2-5**.

9. Now, paste the previous hash value in the **Verify MD5 Value** field and click on **Compare** to compare the MD5 values.



10. We can see that the MD5 hash values of the file before modification is not equal to the MD5 hash value of the file after modification.

If a person wants to send a file to another person via a medium, they will calculate its hashes and send the file (along with the hash value) to the intended person. When the intended person receives the email, they will download the file and calculate its value using the MD5 Calculator.

The recipient compares the generated hash value with the hash value that was sent through email: if both tally, it is evident that they received the file without any modifications by a third person and that the integrity of the file is intact.

11. This concludes the demonstration of calculating MD5 hashes using MD5 Calculator.

12. Close all open windows and document all the acquired information.

### **Question 20.1.2.1**

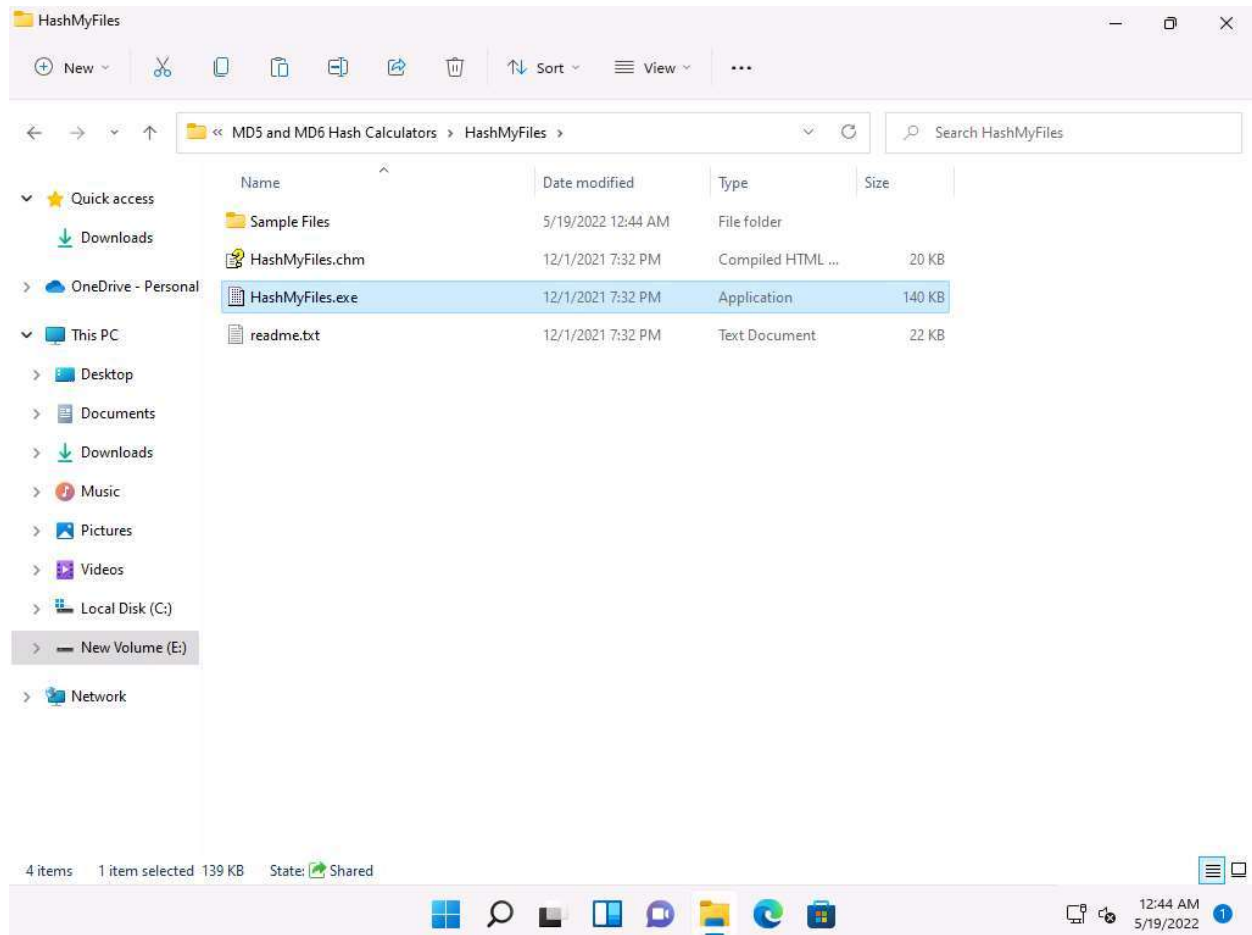
Use MD5 Calculator to find the MD5 hash value of the file E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\MD5 Calculator\md5calc(1.0.0.0).msi on the Windows 11 machine.

### Task 3: Calculate MD5 Hashes using HashMyFiles

HashMyFiles is a small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system: you can easily copy the MD5/SHA1 hashes list into the clipboard, or save them into text/html/xml file. HashMyFiles can also be launched from the context menu of Windows Explorer, and can display the MD5/SHA1 hashes of the selected file or folder.

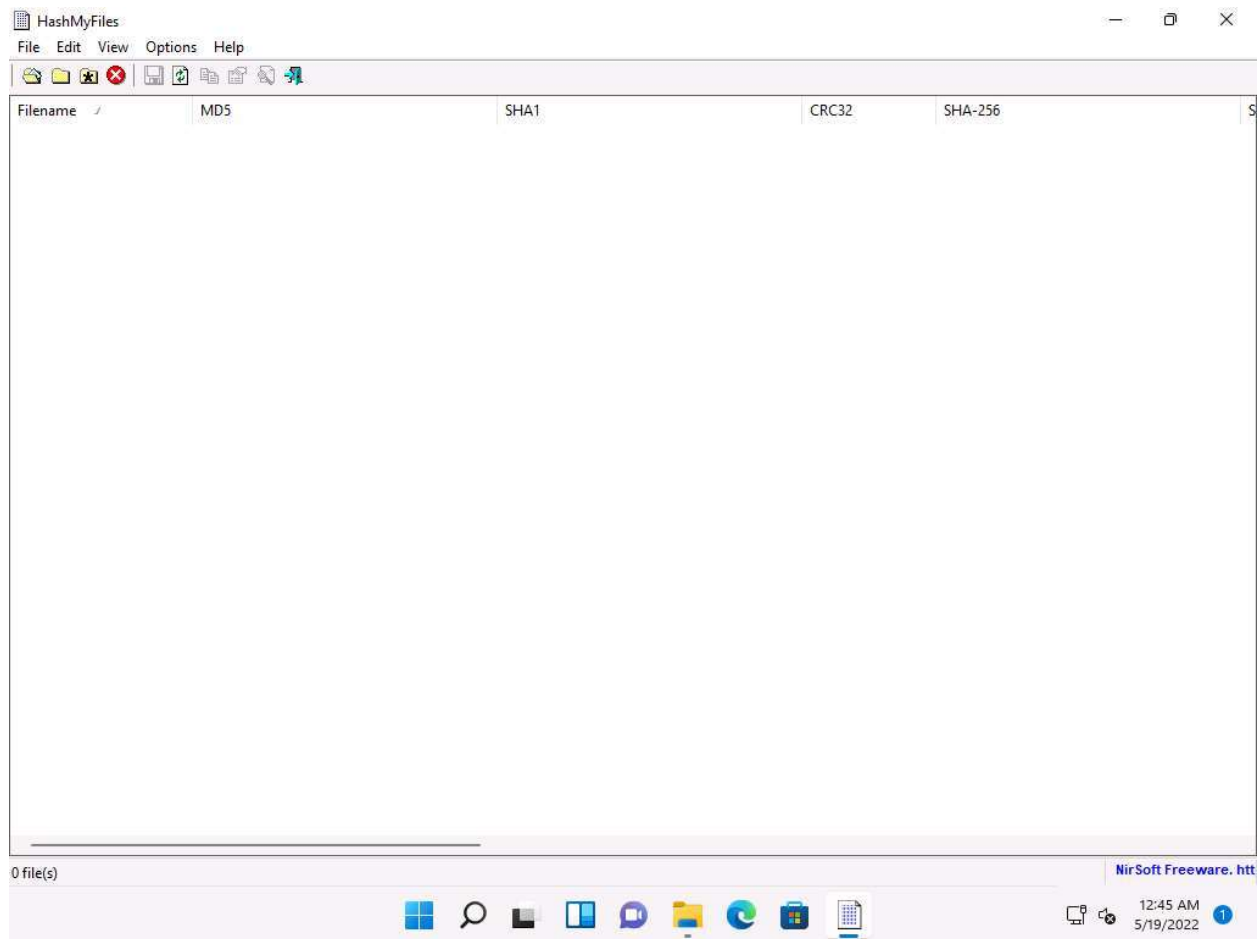
Here, we will use the HashMyFiles tool to calculate MD5 hashes.

1. In **Windows 11** machine navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and double click **HashMyFiles.exe**.



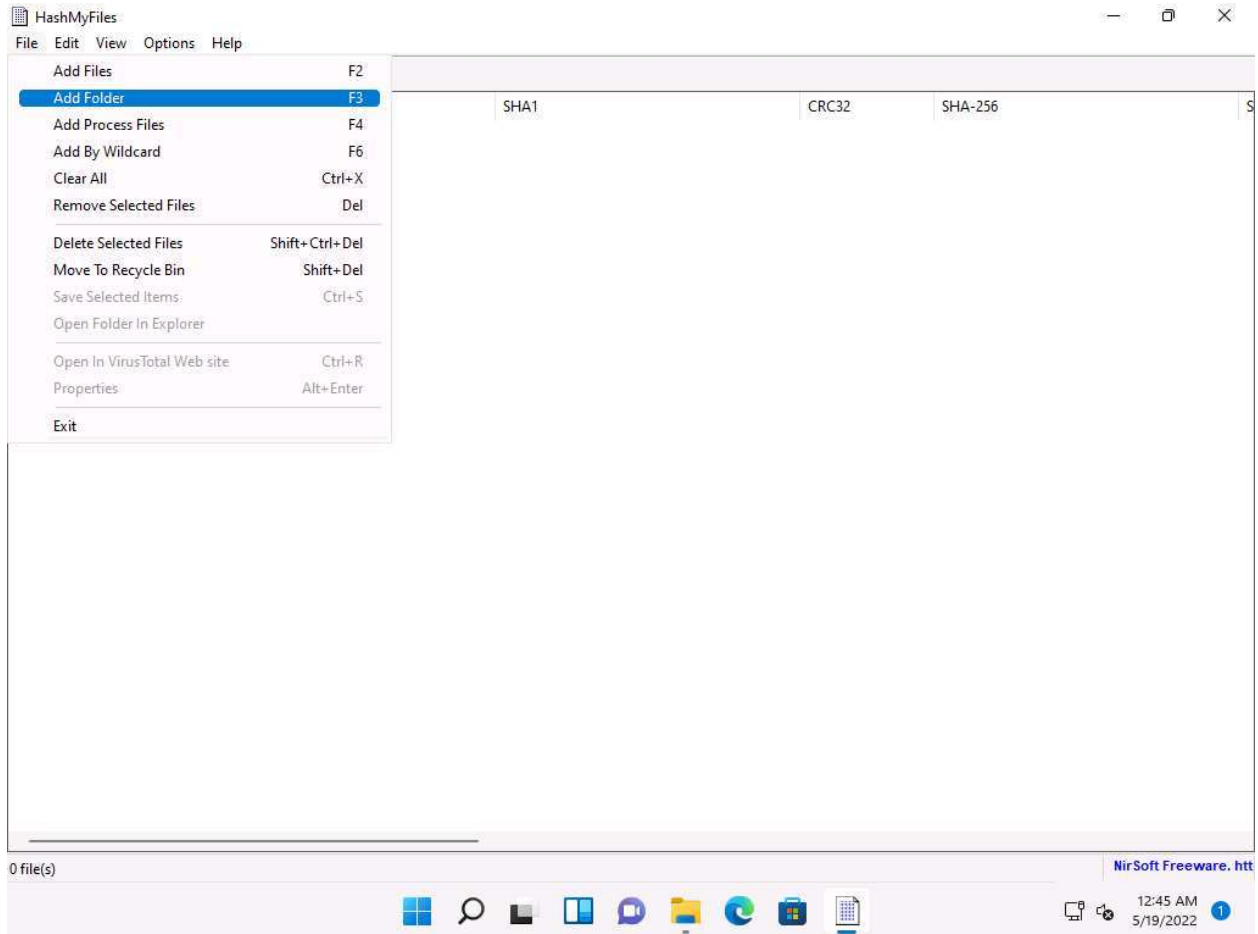
If the **Open File - Security Warning** pop-up appears, click **Run**.

2. The **HashMyFiles** main window appears, as shown in the screenshot.



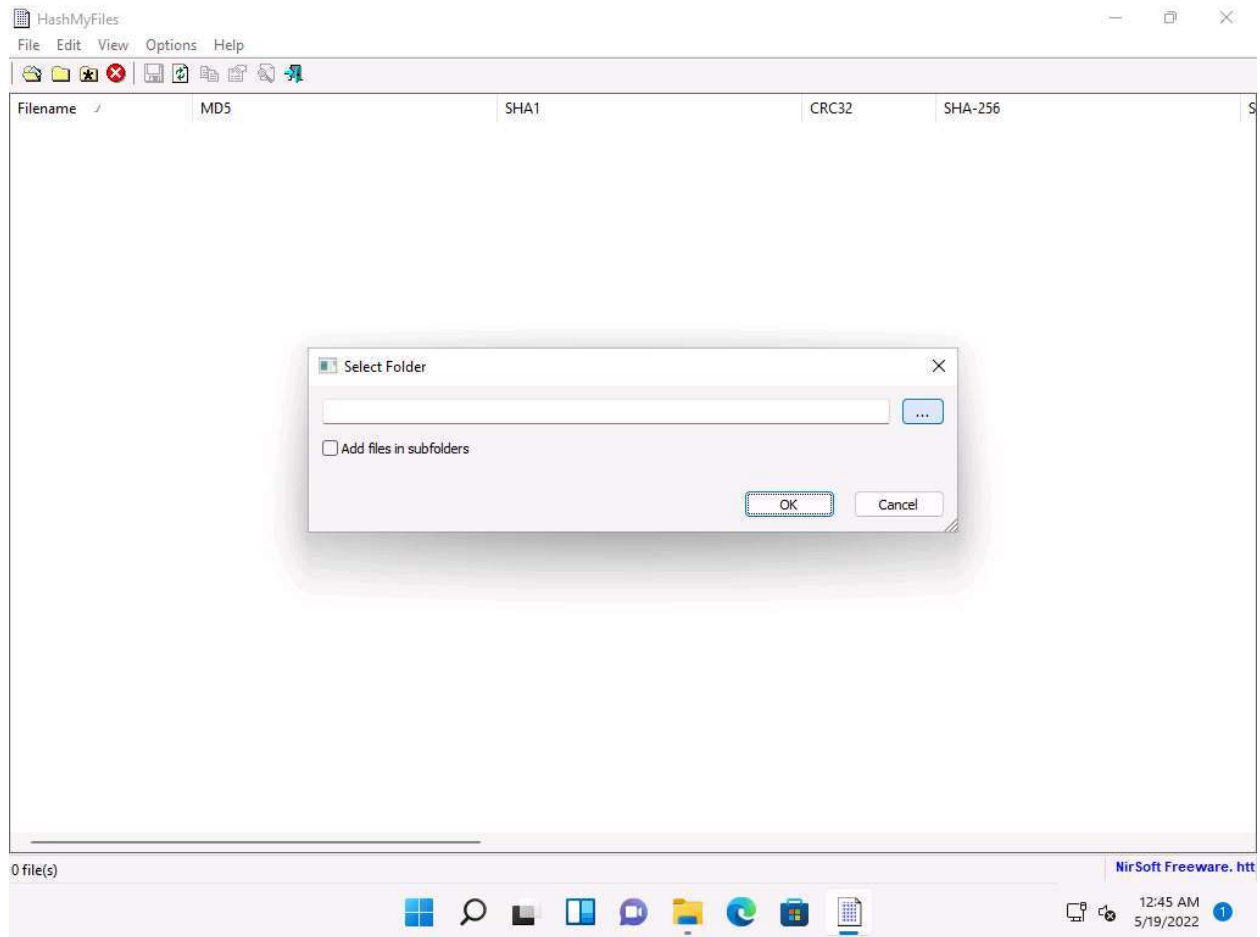
3. In the **HashMyFiles** window, click **File** from the menu bar. From the drop-down list, click the **Add Folder** option.

You can also use the **Add Files** option to add multiple files.



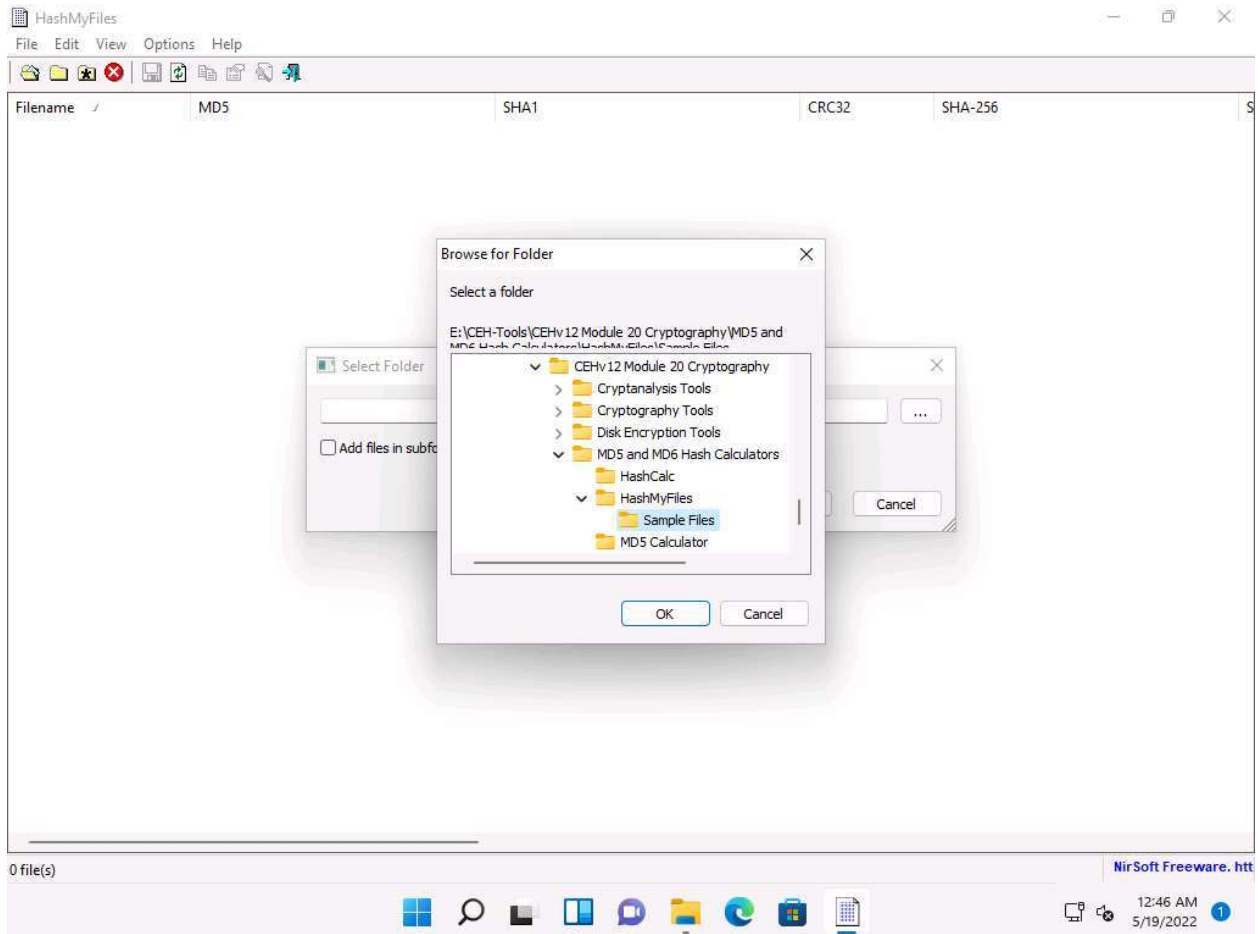


4. The **Select Folder** pop-up appears; click on the ellipsis icon to select the folder you want to encrypt.

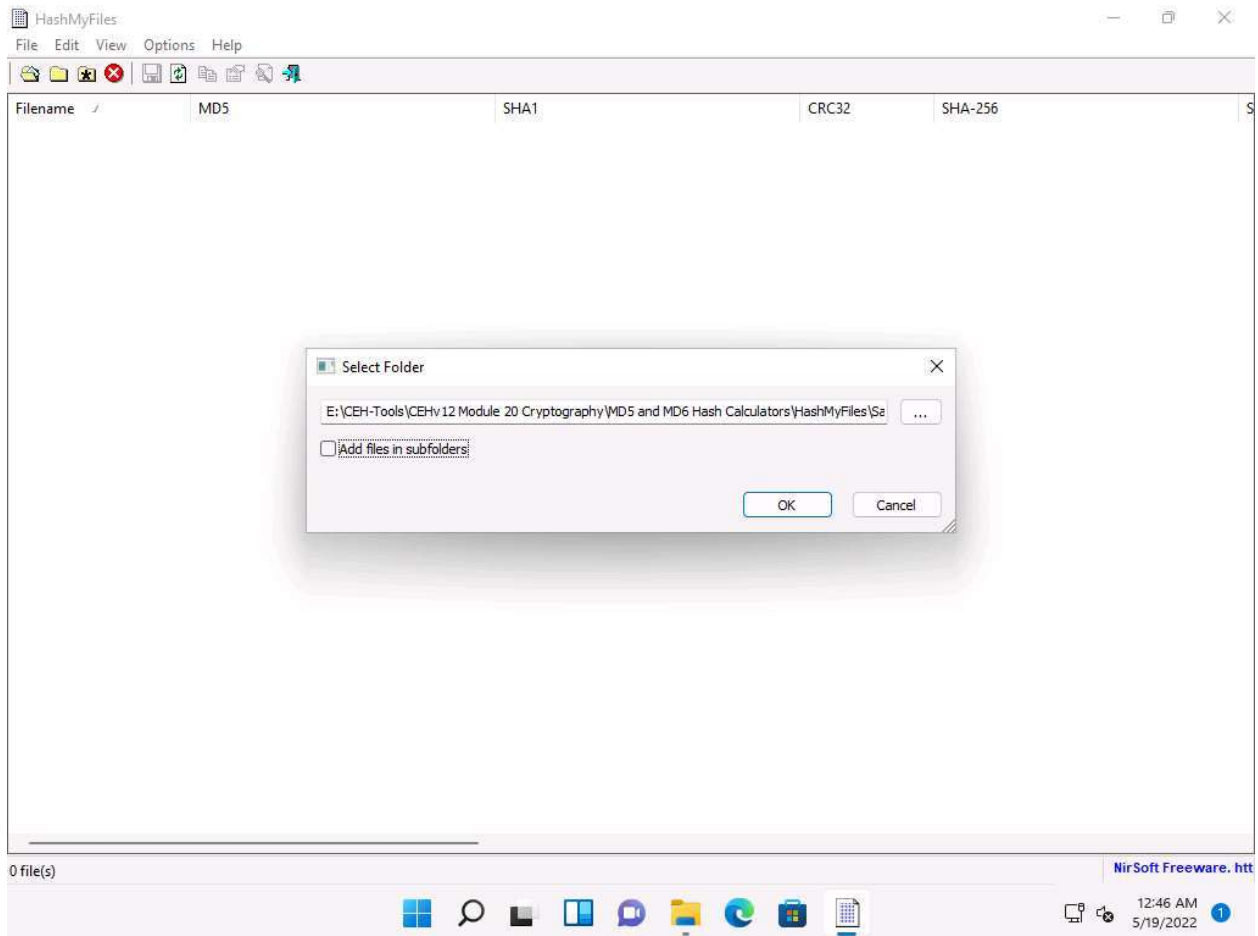


5. The **Browse for Folder** window appears; navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles** and select the **Sample Files** folder; then, click **OK**.

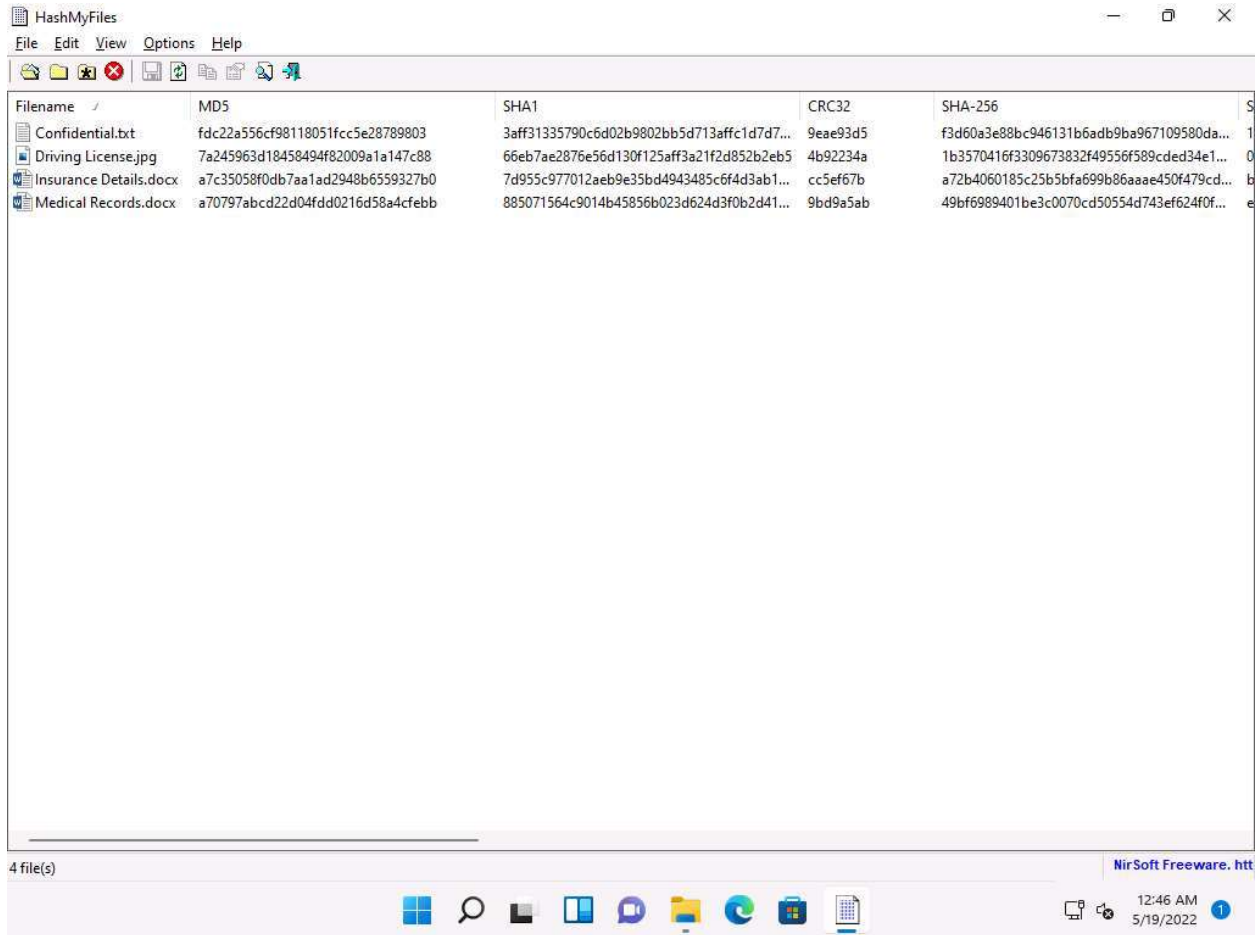
You can select any folder of your choice that you wish to encrypt.



6. The location of the selected folder appears in the field; click **OK**.



7. A list of files contained in the folder appears, along with their various hash values such as **MD5**, **SHA1**, **CRC32**, etc.

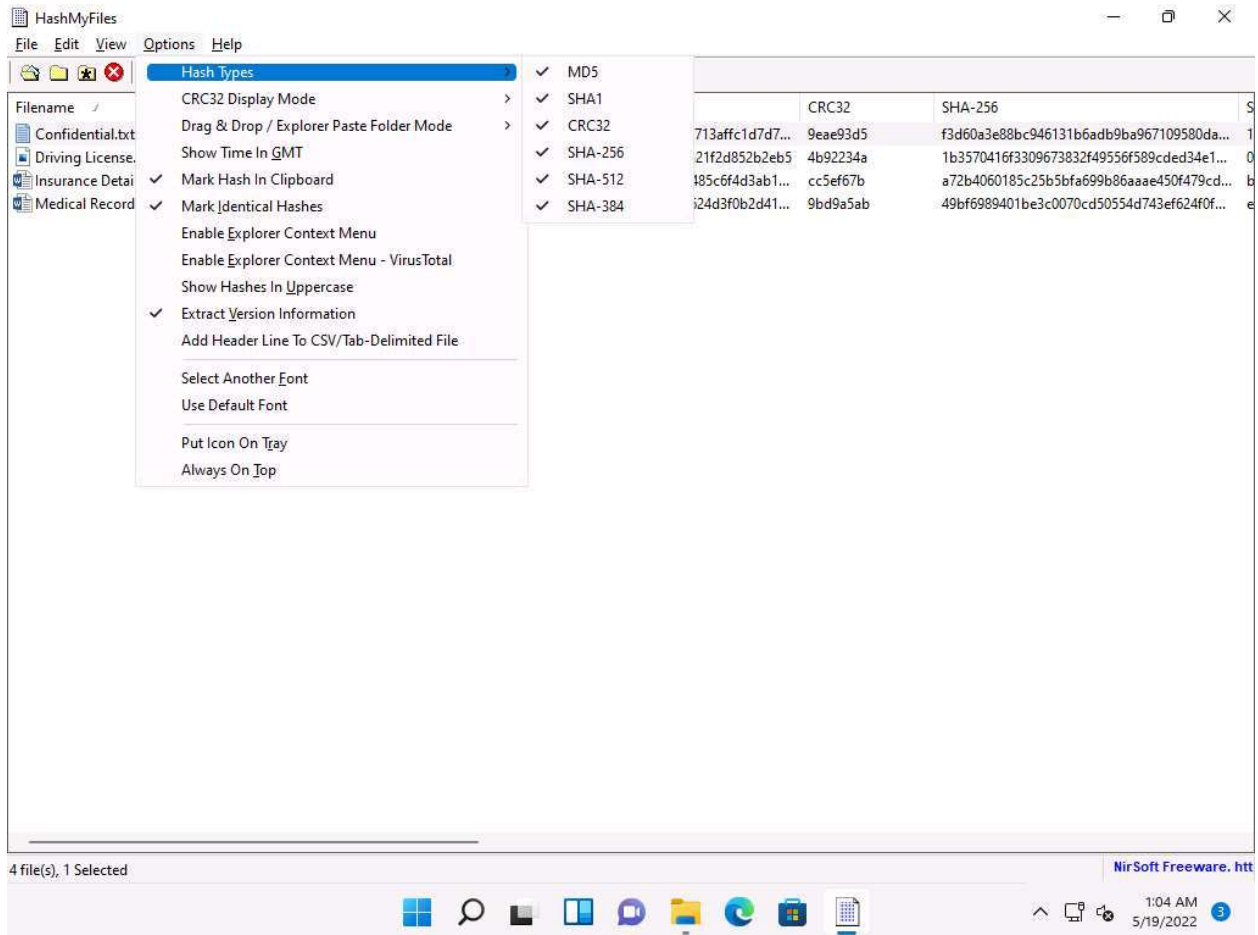


The screenshot shows the HashMyFiles application window. The title bar reads "HashMyFiles". The menu bar includes "File", "Edit", "View", "Options", and "Help". The toolbar contains icons for file operations. The main window displays a table with the following data:

Filename	MD5	SHA1	CRC32	SHA-256
Confidential.txt	fdc22a556cf98118051fcc5e28789803	3aff31335790c6d02b9802bb5d713affc1d7d7...	9eae93d5	f3d60a3e88bc946131b6adb9ba967109580da...
Driving License.jpg	7a245963d18458494f82009a1a147c88	66eb7ae2876e56d130f125aff3a21f2d852b2eb5	4b92234a	1b3570416f3309673832f49556f589cded34e1...
Insurance Details.docx	a7c35058f0db7aa1ad2948b6559327b0	7d955c977012aeb9e35bd4943485c6f4d3ab1...	cc5ef67b	a72b4060185c25b5bfa699b86aaae450f479cd...
Medical Records.docx	a70797abcd22d04fdd0216d58a4cfebb	885071564c9014b45856b023d624d3f0b2d41...	9bd9a5ab	49bf6989401be3c0070cd50554d743ef624f0f...

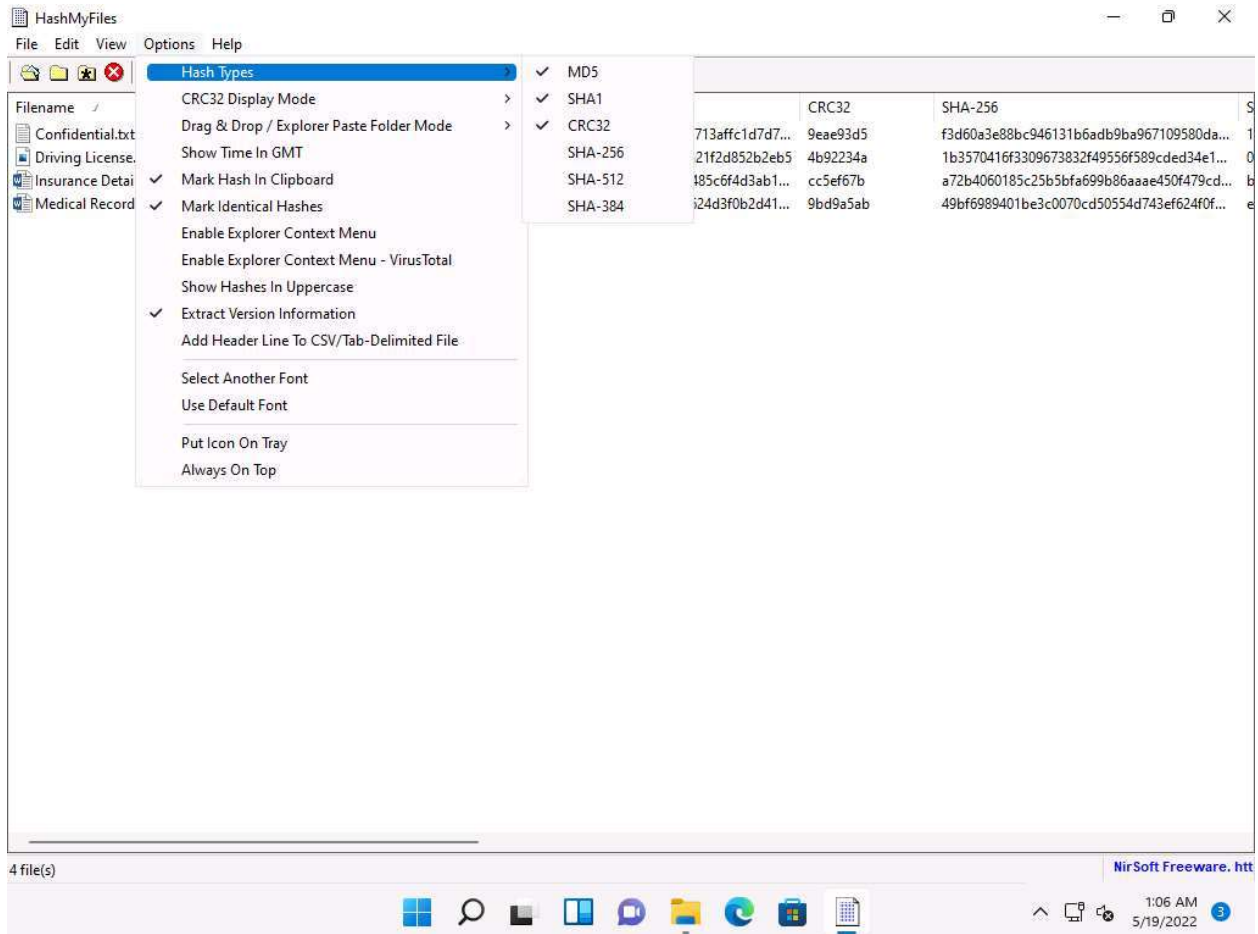
At the bottom of the window, it says "4 file(s)". The taskbar at the bottom shows the Windows Start button, search icon, and several application icons. The system clock in the bottom right corner displays "12:46 AM 5/19/2022". A small notification bubble with the number "1" is also visible.

8. In the **HashMyFiles** window, click **Options** from the menu bar and choose **Hash Types** from the options. You can observe a list of hash functions such as **MD5**, **SHA1**, **CRC32**, **SHA-256**, **SHA-512**, and **SHA-384**.




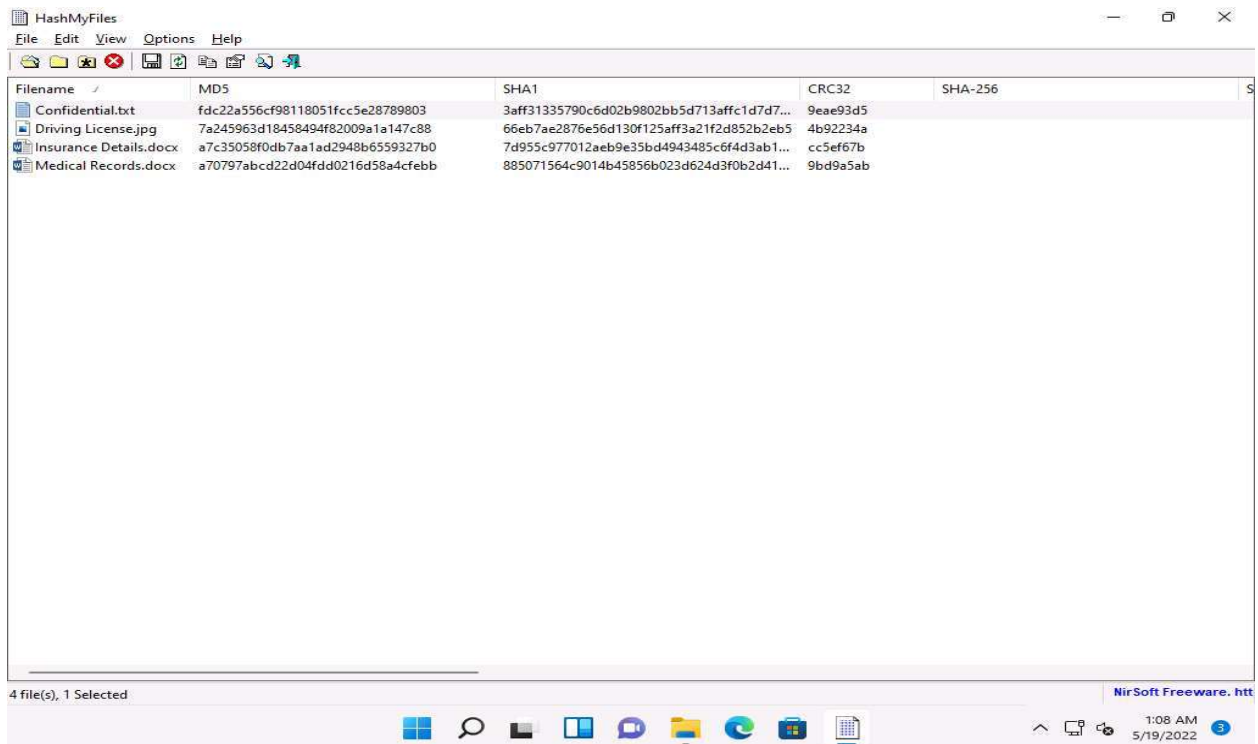
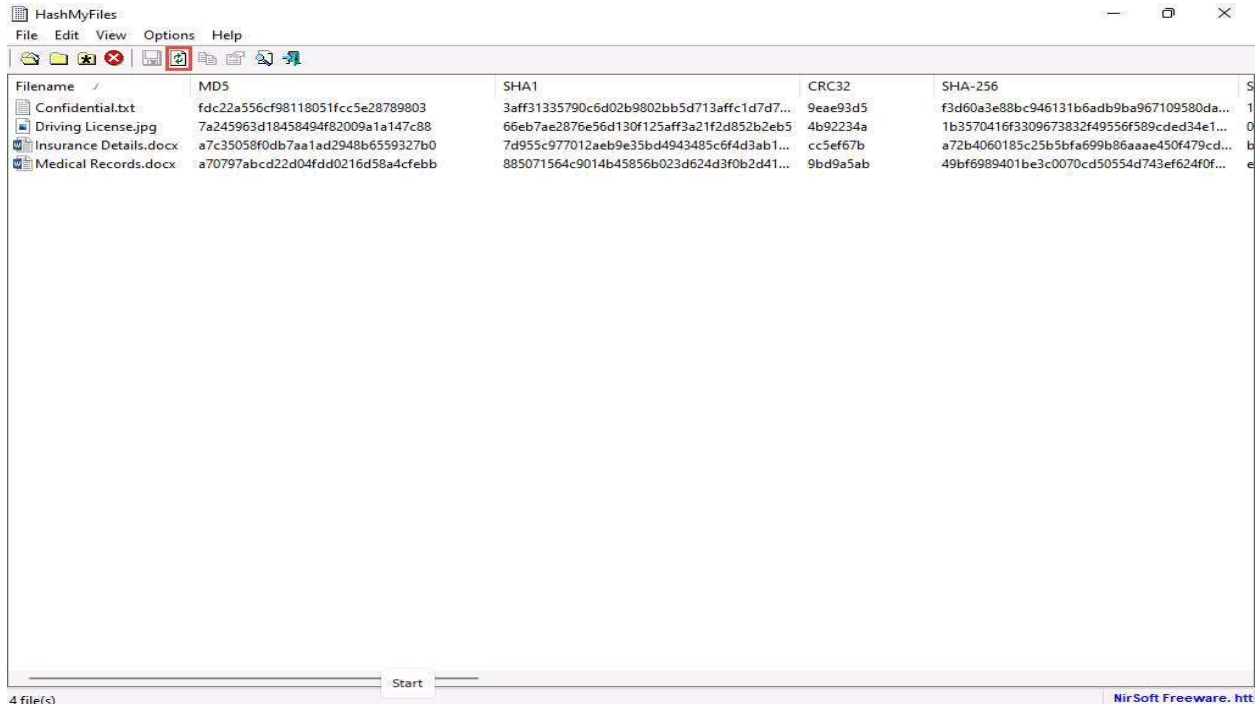
In real-time, you may share confidential information in the folder in an encrypted form to maintain its integrity.

- From the list of hash functions, unselect **SHA-256**, **SHA-512** and **SHA-384** hash types one by one.



Here, we will calculate **MD5**, **SHA1** and **CRC32 Hash Types**.

10. After selecting the hash functions to be displayed, click **Refresh** icon  from the menu bar to view the selected hash functions.



11. This concludes the demonstration of calculating MD5 hashes using HashMyFiles.

12. You can also use other MD5 and MD6 hash calculators such as **MD6 Hash Generator** (<https://www.browserling.com>), **All Hash Generator** (<https://www.browserling.com>), **MD6 Hash Generator** (<https://convert-tool.com>), and **md5 hash calculator** (<https://onlinehashtools.com>) to calculate MD5 and MD6 hashes.

13. Close all open windows and document all the acquired information.

#### **Question 20.1.3.1**

Use HashMyFiles to find the MD5 hash value of the file E:\CEH-Tools\CEHv12 Module 20 Cryptography\MD5 and MD6 Hash Calculators\HashMyFiles\Sample Files\Medical Records.docx on the Windows 11 machine.



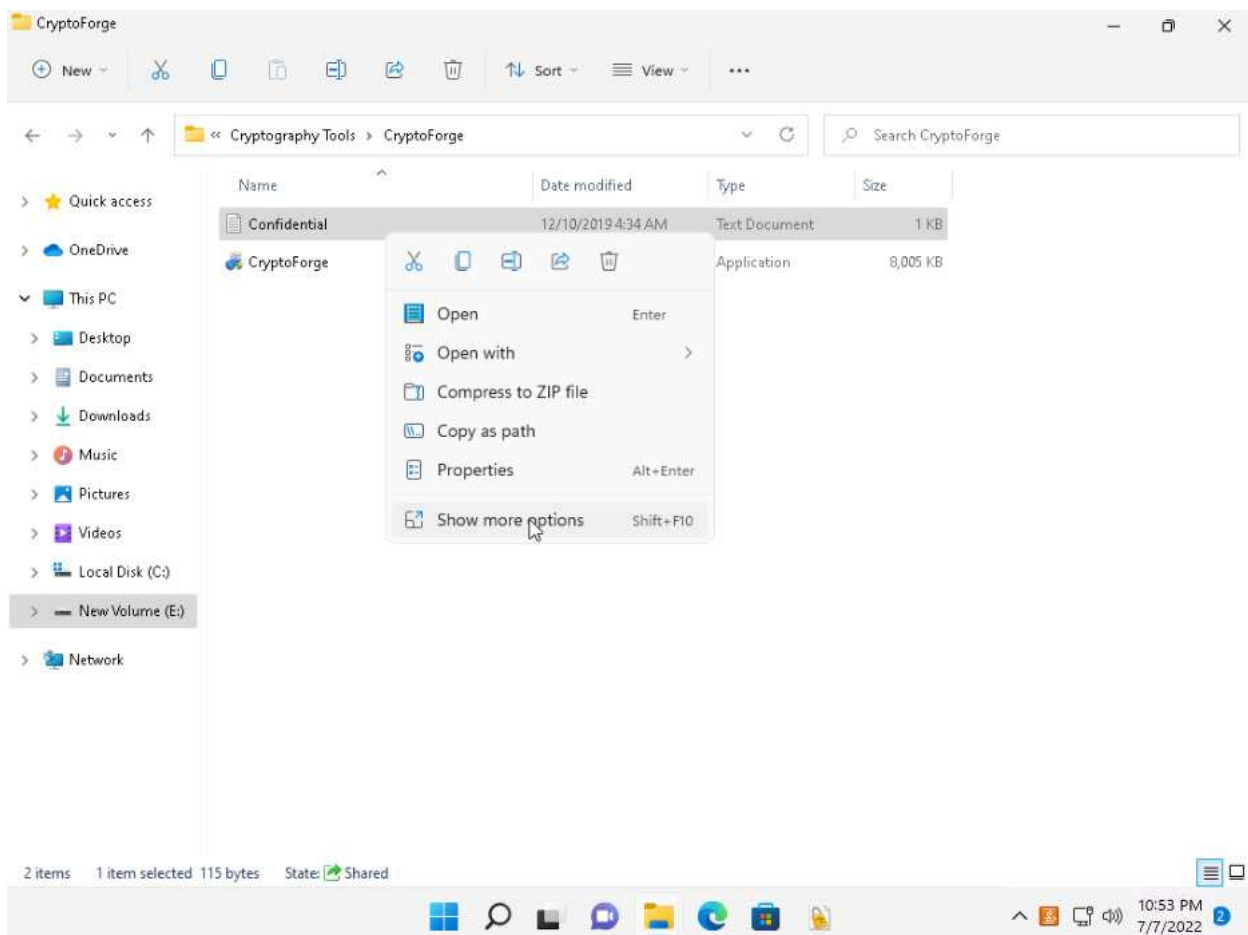
#### Task 4: Perform File and Text Message Encryption using CryptoForge

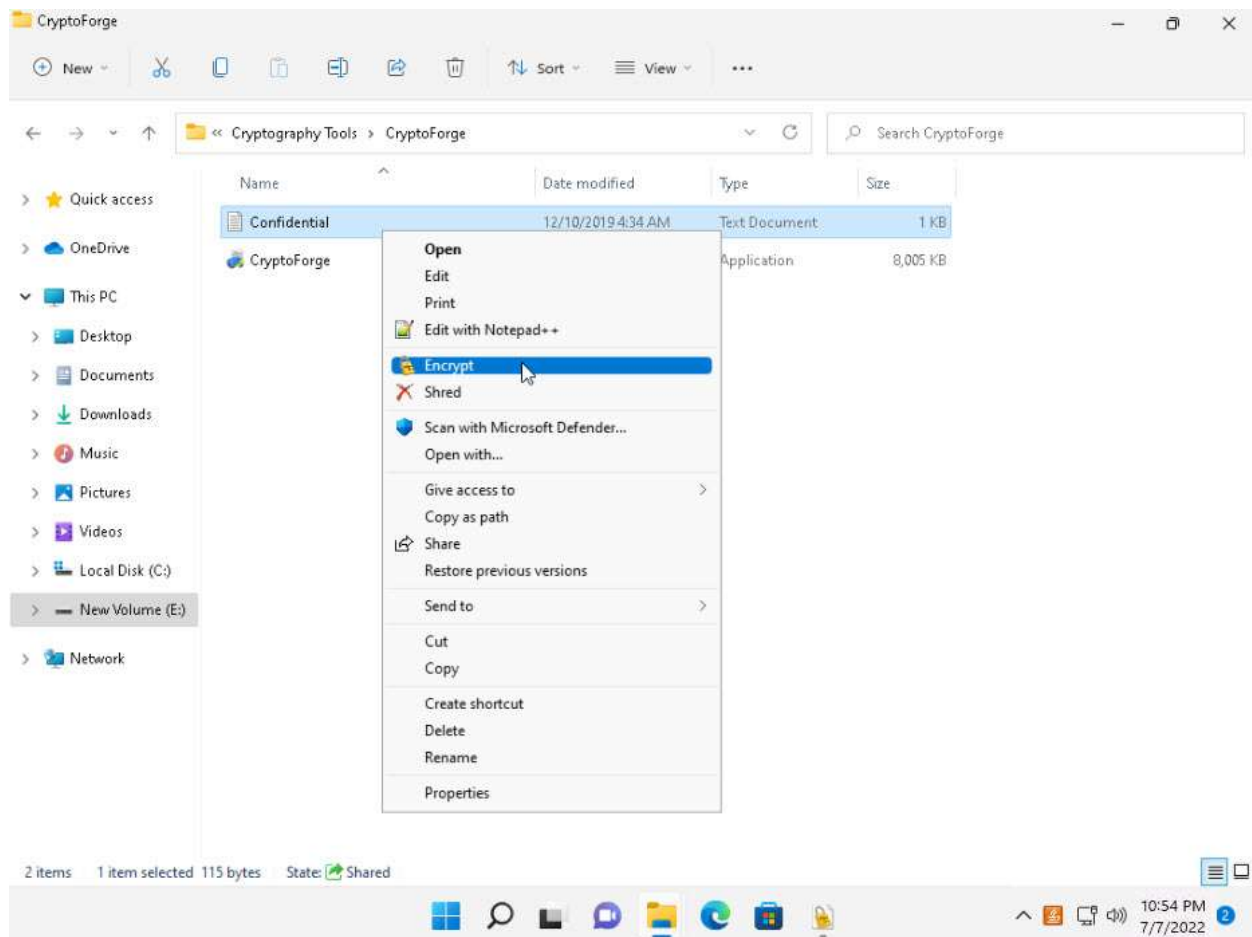
CryptoForge is a file encryption software for personal and professional data security. It allows you to protect the privacy of sensitive files, folders, or email messages by encrypting them with strong encryption algorithms. Once the information has been encrypted, it can be stored on insecure media or transmitted on an insecure network-such as the Internet-and remain private. Later, the information can be decrypted into its original form.

Here, we will use the CryptoForge tool to encrypt a file and text message.

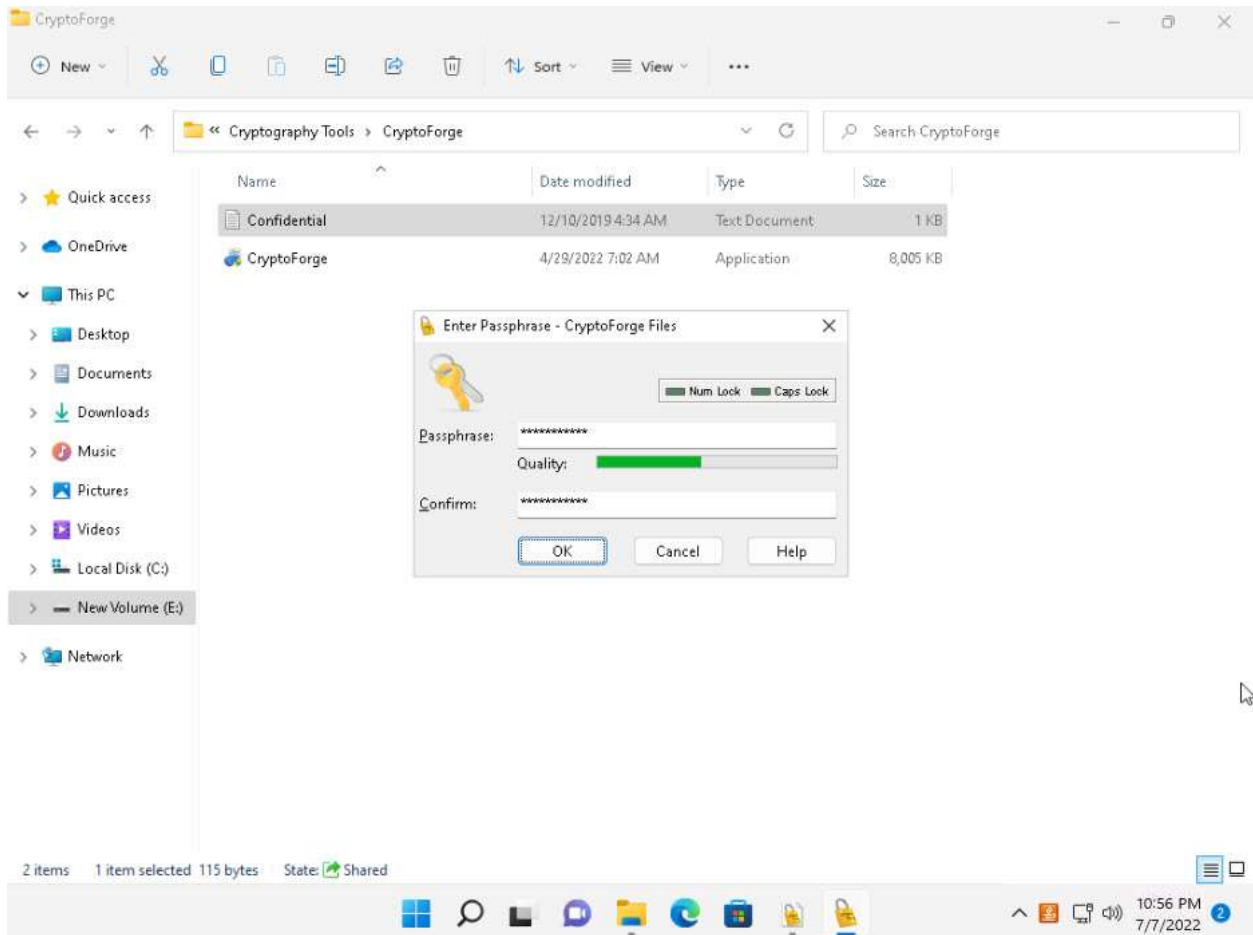
1. Click on [Windows 11](#) to switch to the **Windows 11** machine. Navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**. Right-click the **Confidential.txt** file and click **Show more options** and select **Encrypt** from the context menu

In this task, we are encrypting the **Confidential.txt** file, although you can encrypt any file of your choice.



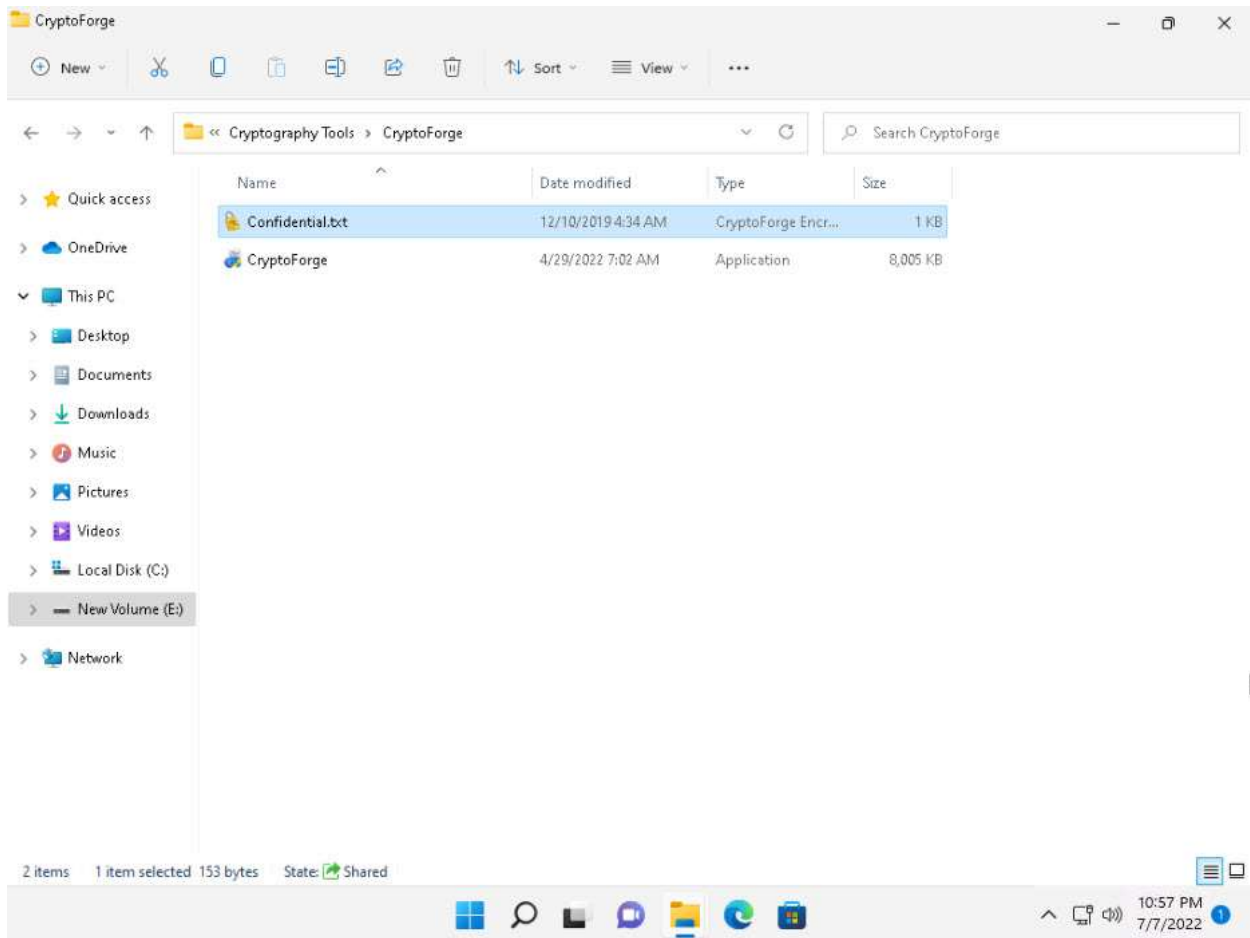


2. The **Enter Passphrase - CryptoForge Files** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **qwerty@1234**.

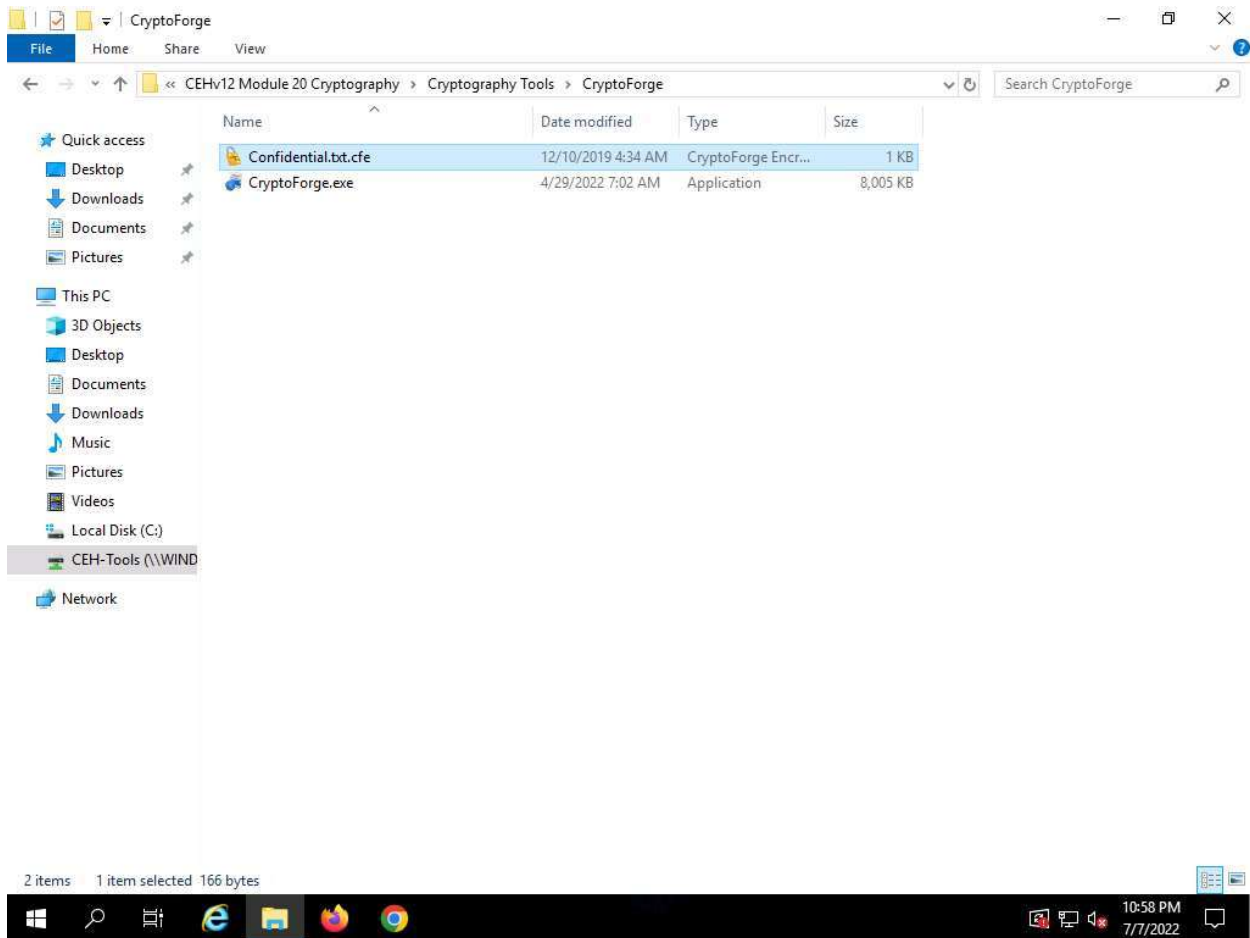


- Now, the file will be encrypted in the same location, and the old file will be deleted automatically, as shown in the screenshot.

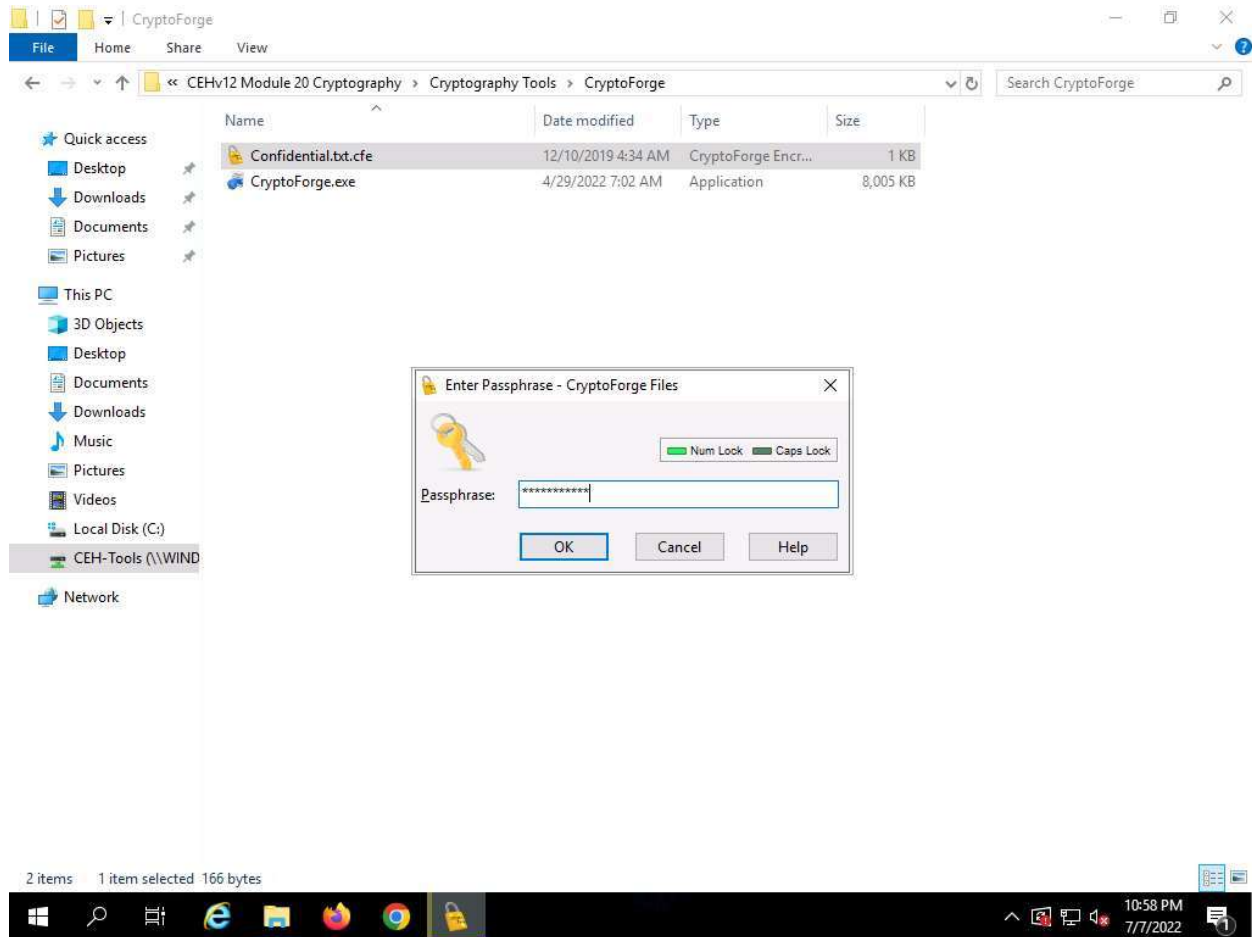
No one can access this file unless the user provides the password for the encrypted file. You will have to share the password with the user through message, email, or any other means.



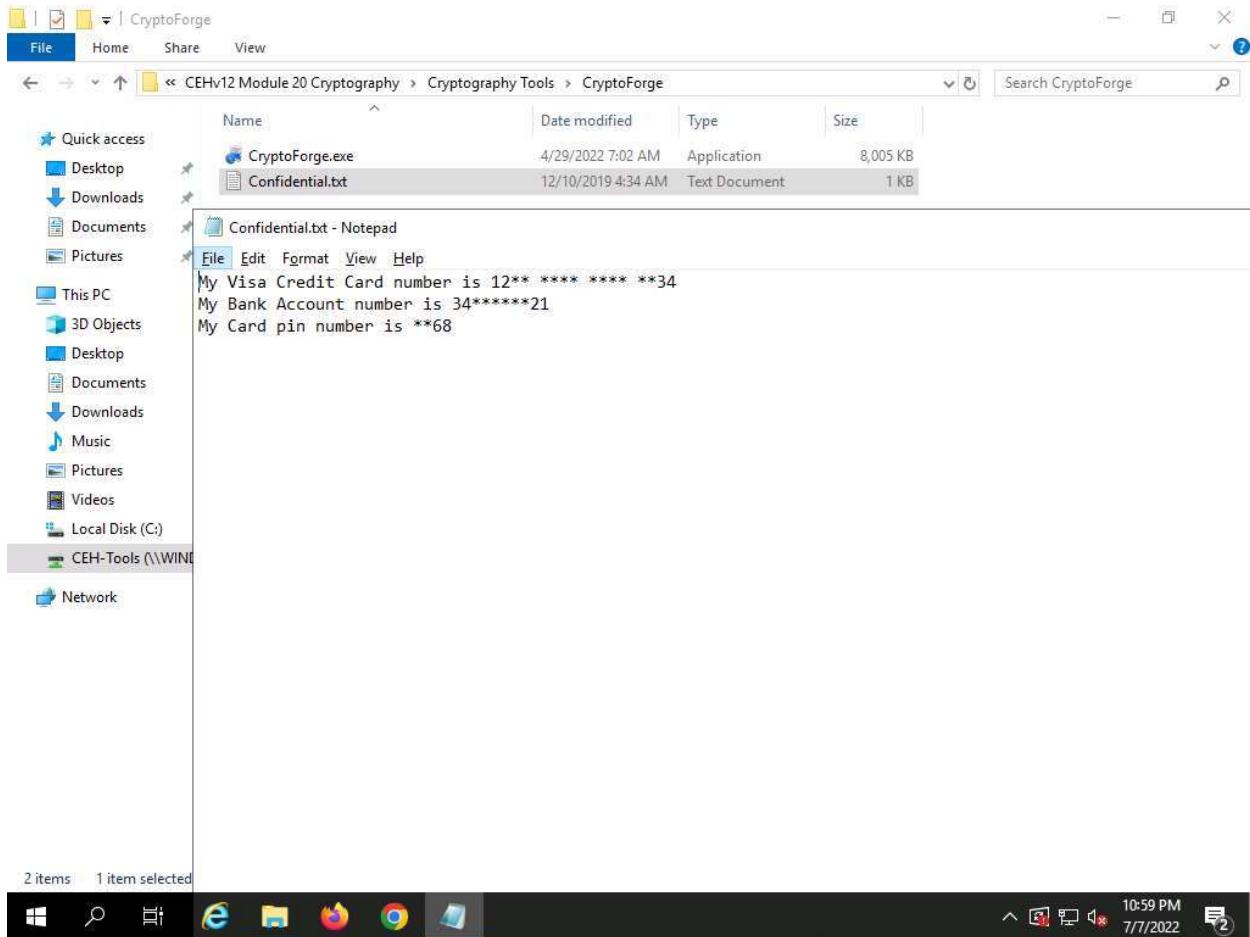
4. Let us assume that you shared this file through a shared network drive.
5. Now, click on [Windows Server 2019](#) to switch to the **Windows Server 2019**, click **Ctrl+Alt+Delete** to activate the machine. By default, **Administrator** profile is selected, type **Pa\$\$w0rd** to enter password in the Password field and press **Enter** to login.
6. Navigate to **Z:\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**. You will observe the encrypted file in this location.
7. Double-click the encrypted file to decrypt it and view its contents.



8. The **Enter Passphrase - CryptoForge Files** dialog-box appears; enter the password that you have provided in **Step#2** to encrypt the file and click **OK**.

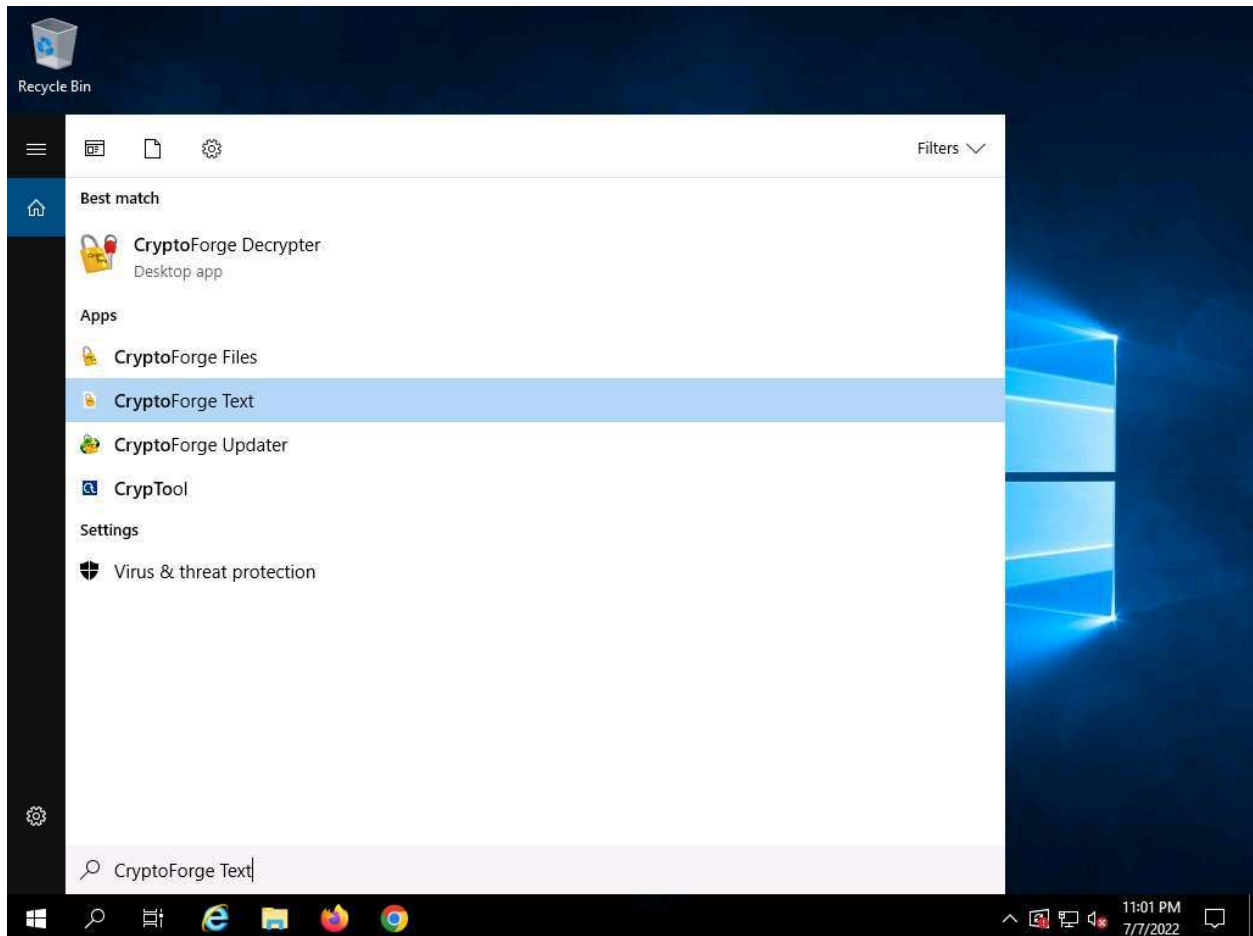


9. Upon entering the password, the file will be successfully decrypted. You may now double-click the text file to view its contents.



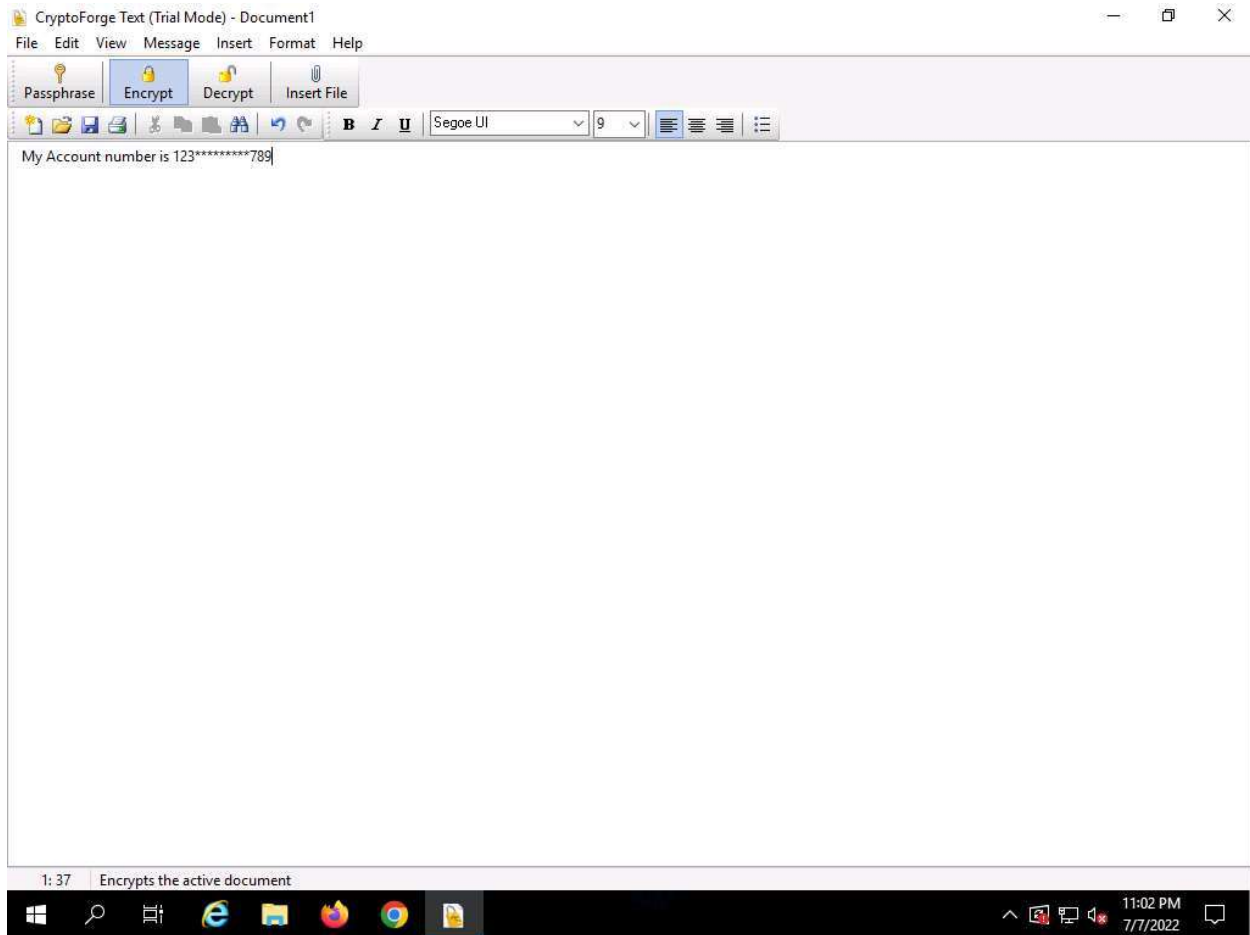
10. So far, you have seen how to encrypt a file and share it with the intended user. Now, we shall share an encrypted message with a user.

11. In the **Windows Server 2019** machine, click the **Type here to search** icon present in the bottom-left corner of **Desktop**, type **crypto** in the search field and click **CryptoForge Text** from the apps to launch the application.

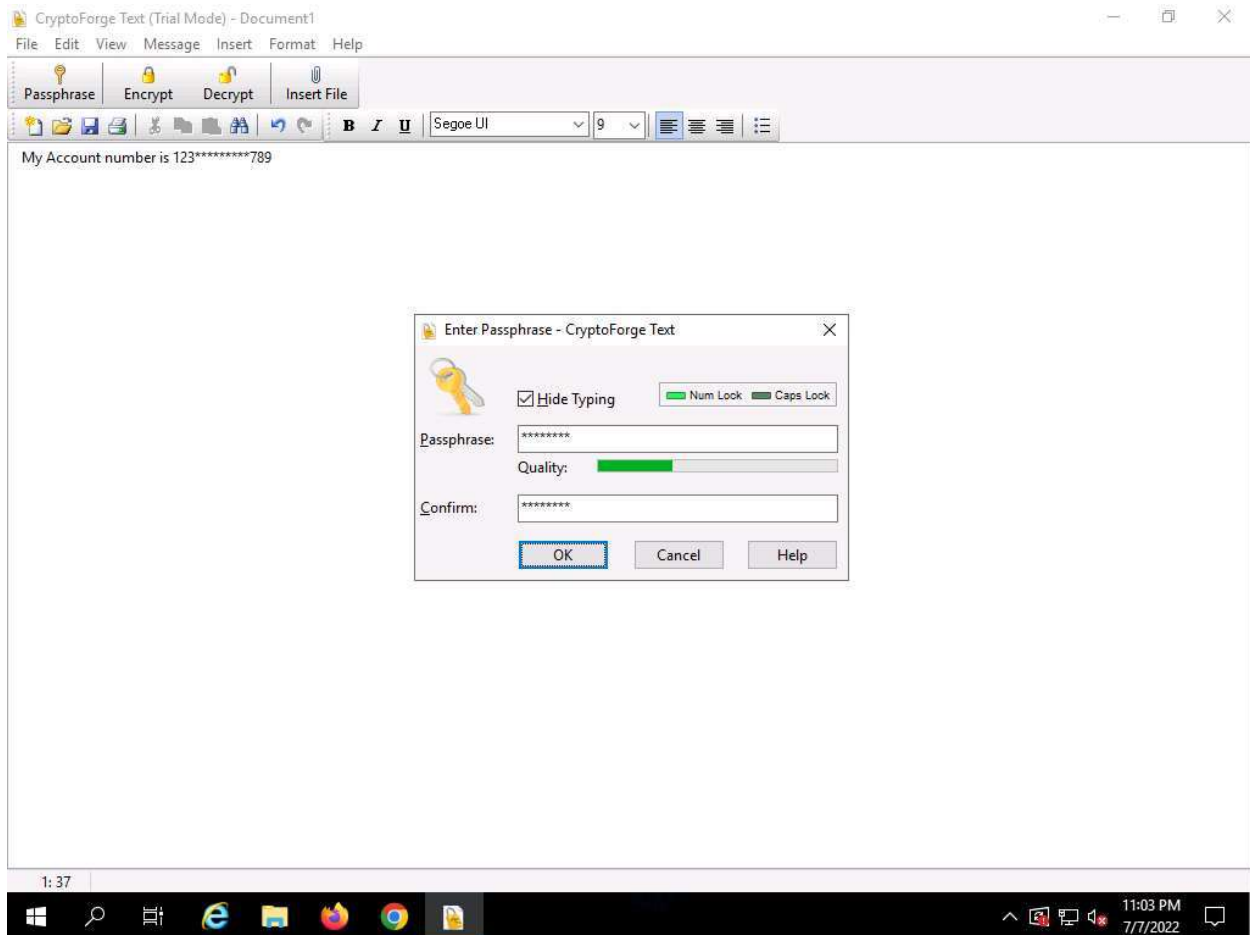




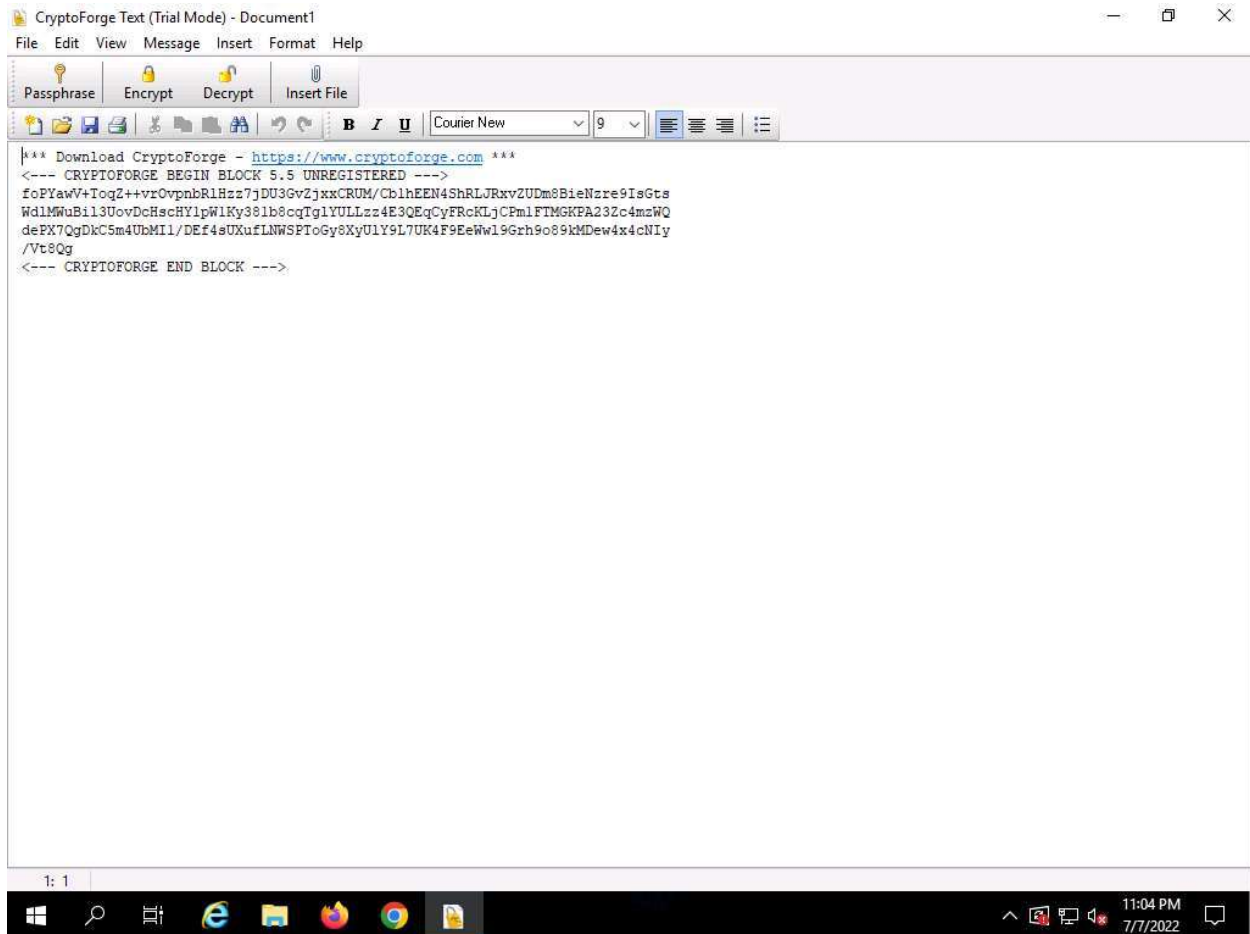
12. The **CryptoForge Text** window appears; type a message and click **Encrypt** from the toolbar.



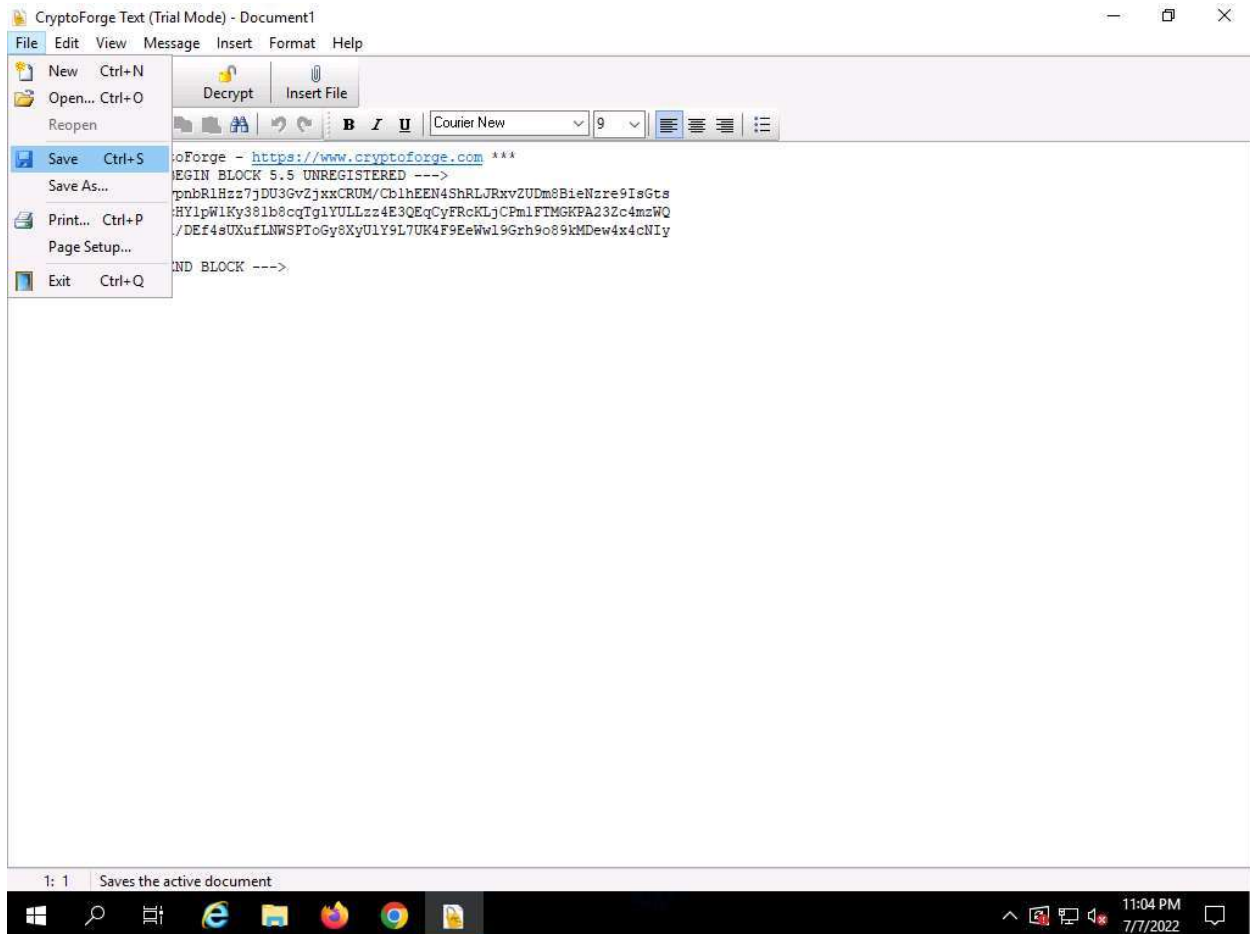
13. The **Enter Passphrase - CryptoForge Text** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **test@123**.



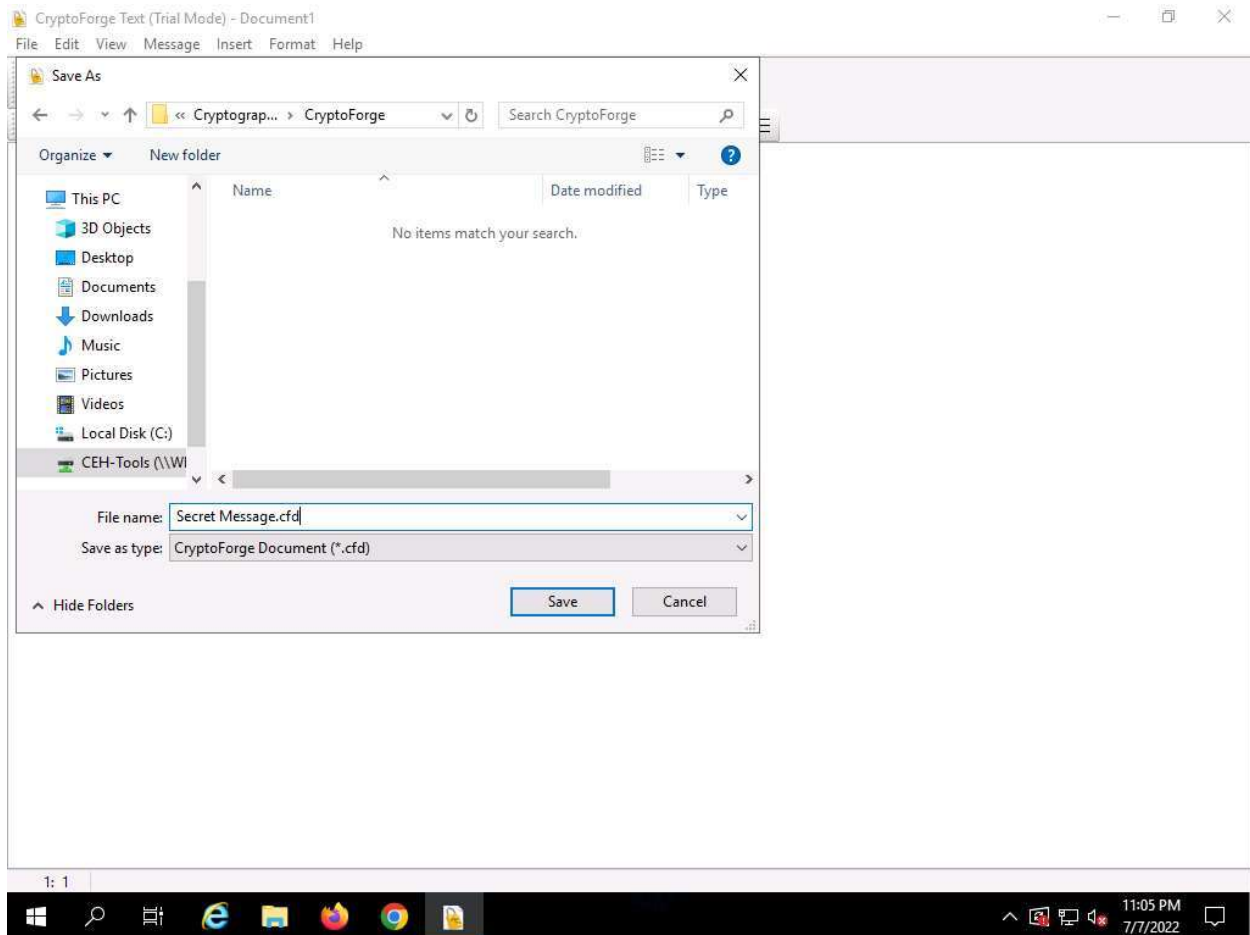
14. The message that you have typed will be encrypted, as shown in the screenshot.



15. Now, you need to save the file. Click **File** in the menu bar and click **Save**.



16. The **Save As** window appears; navigate to **Z:\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**, specify the file name as **Secret Message.cfd**, and click **Save**.

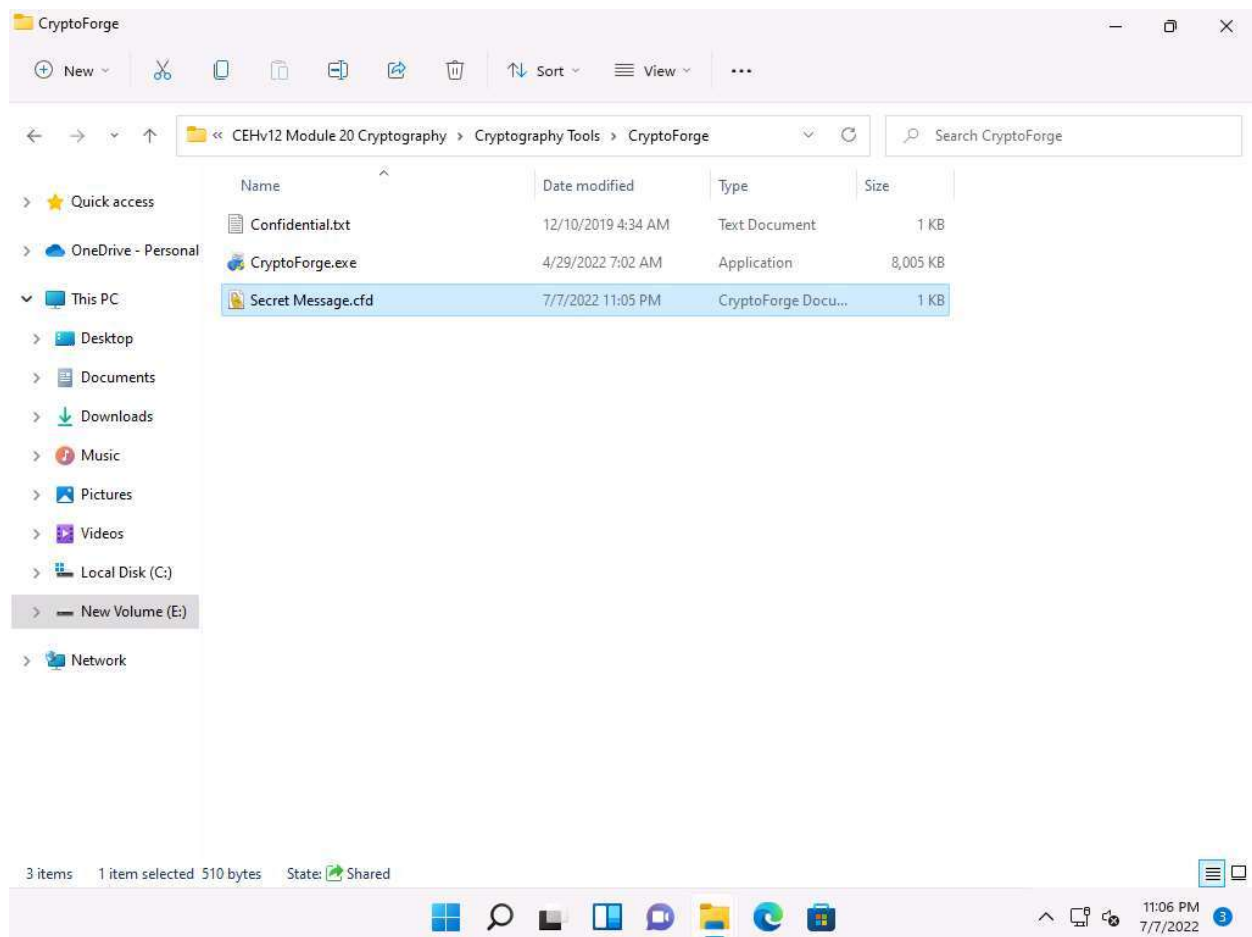


17. Close the **CryptoForge Text** window.

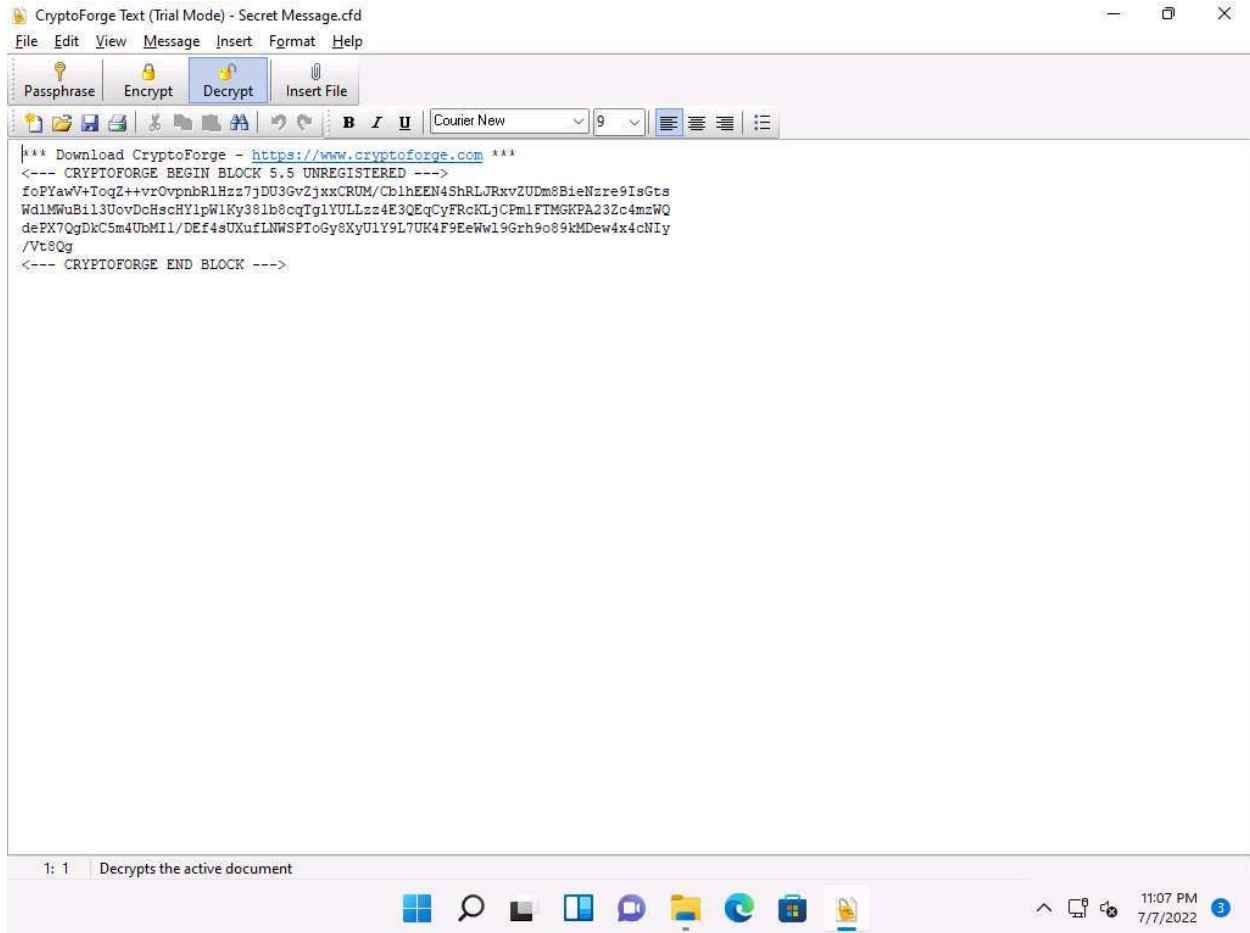
18. Now, let us assume that you shared the file through the mapped network drive and shared the password to decrypt the file in an email message or through some other means.

19. Click on [Windows 11](#) to switch to the **Windows 11** machine and navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge**.

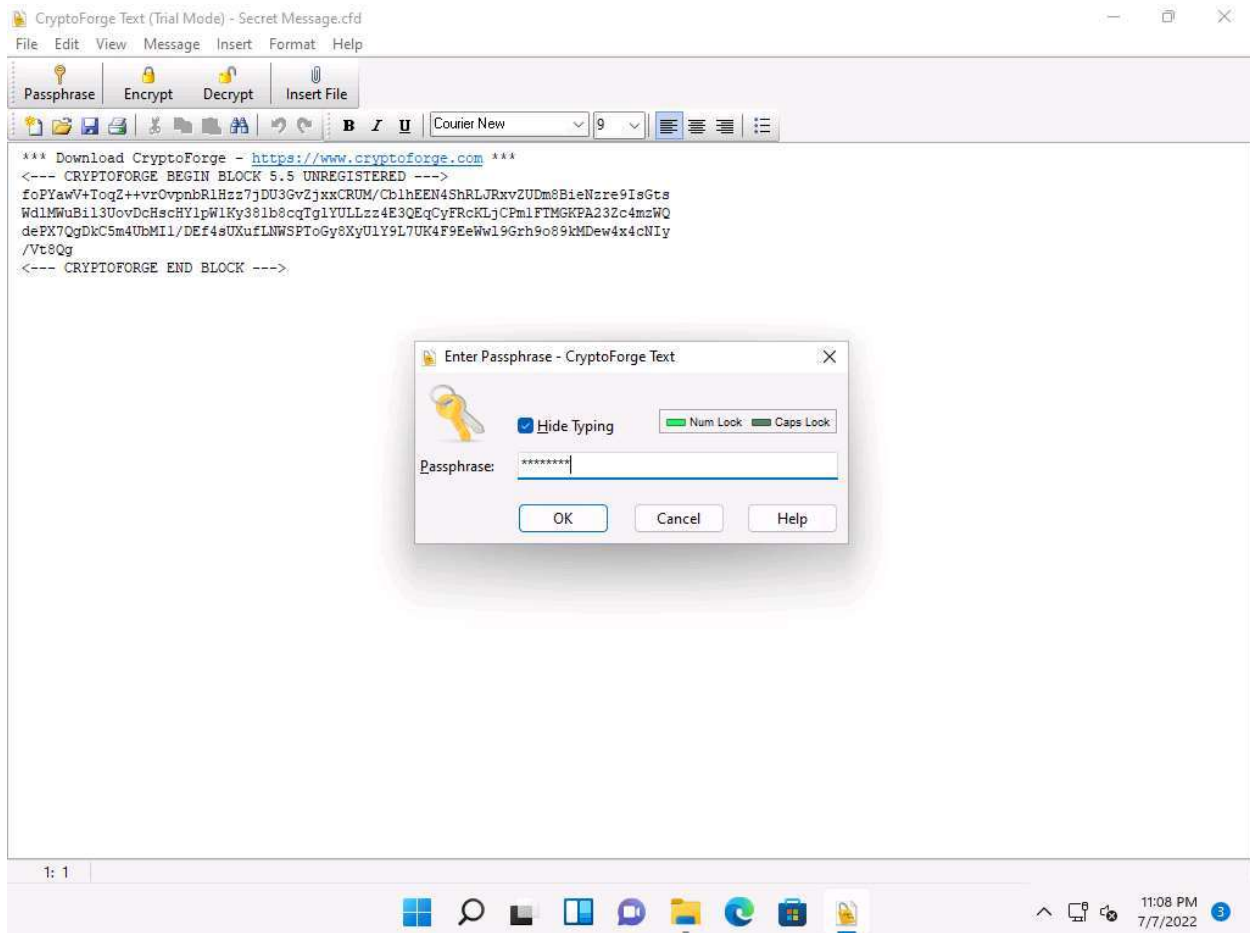
20. You will observe the encrypted file in this location; double-click the file **Secret Message.cfd**.



21. The **CryptoForge Text** window appears, displaying the message in an encrypted format. Click **Decrypt** from the toolbar to decrypt it.



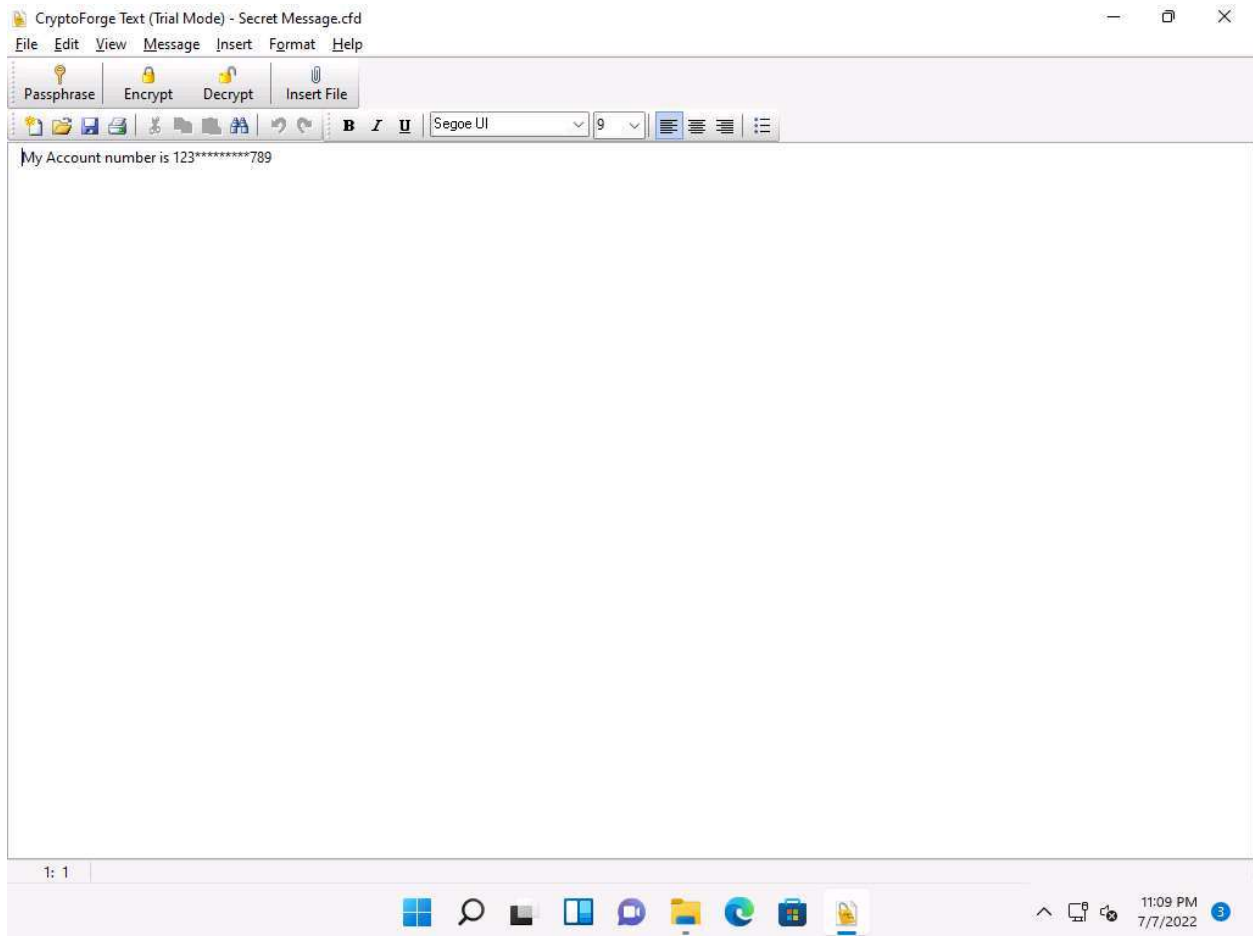
22. The **Enter Passphrase - CryptoForge Text** dialog-box appears; enter the password you provided in **Step#13** to decrypt the message in the **Passphrase** field and click **OK**.





23. The **CryptoForge Text** window appears, displaying the message in plain-text format, as shown in the screenshot.

In real-time, you may share sensitive information through email by encrypting data using CryptoForge.



24. This concludes the demonstration of performing file and text message encryption using CryptoForge.

25. Close all open windows and document all the acquired information.

**Question 20.1.4.1**

Use CryptoForge to encrypt the file E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\CryptoForge\Confidential.txt on the Windows 11 machine. What is the extension of the encrypted file?

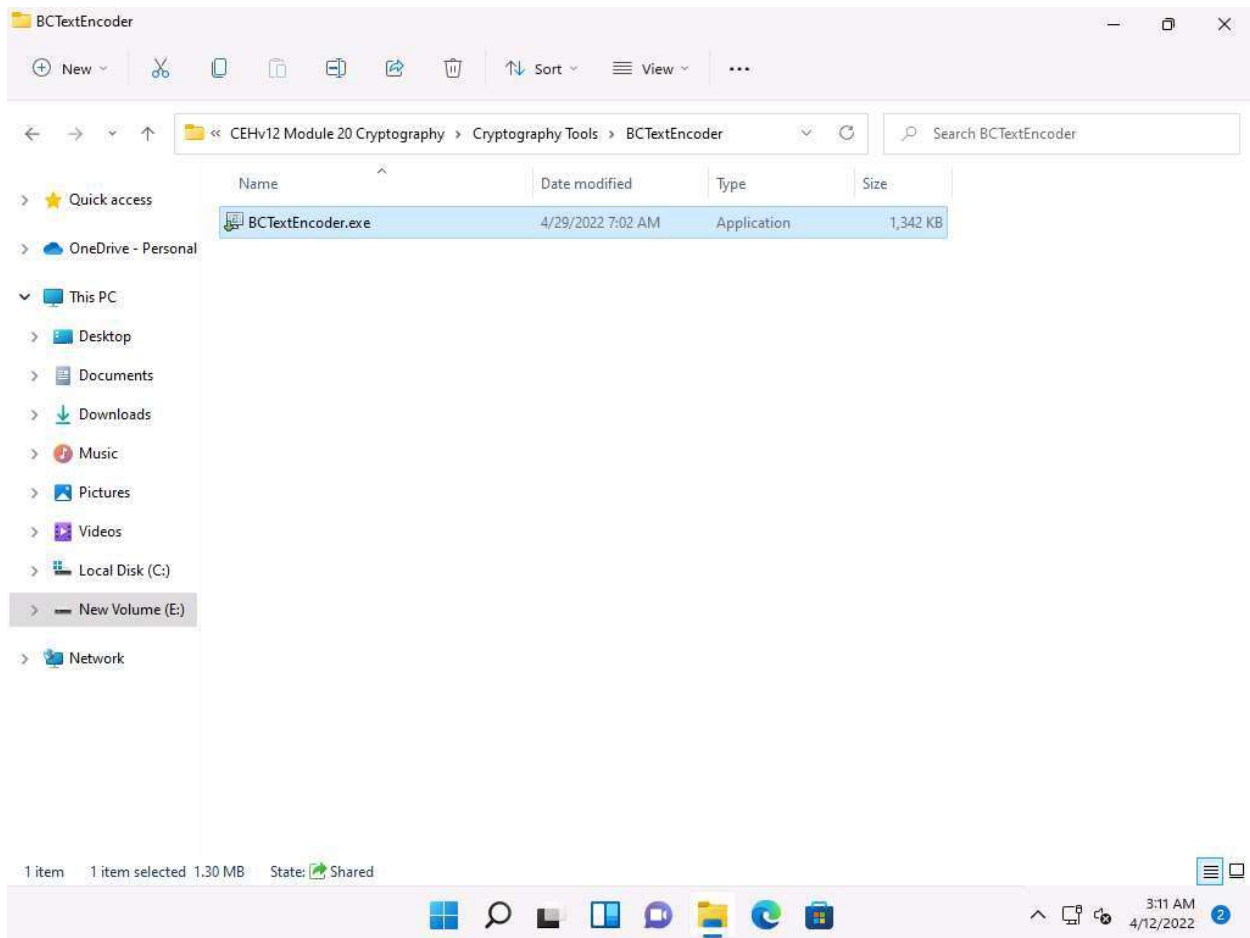
---

## Task 5: Encrypt and Decrypt Data using BCTextEncoder

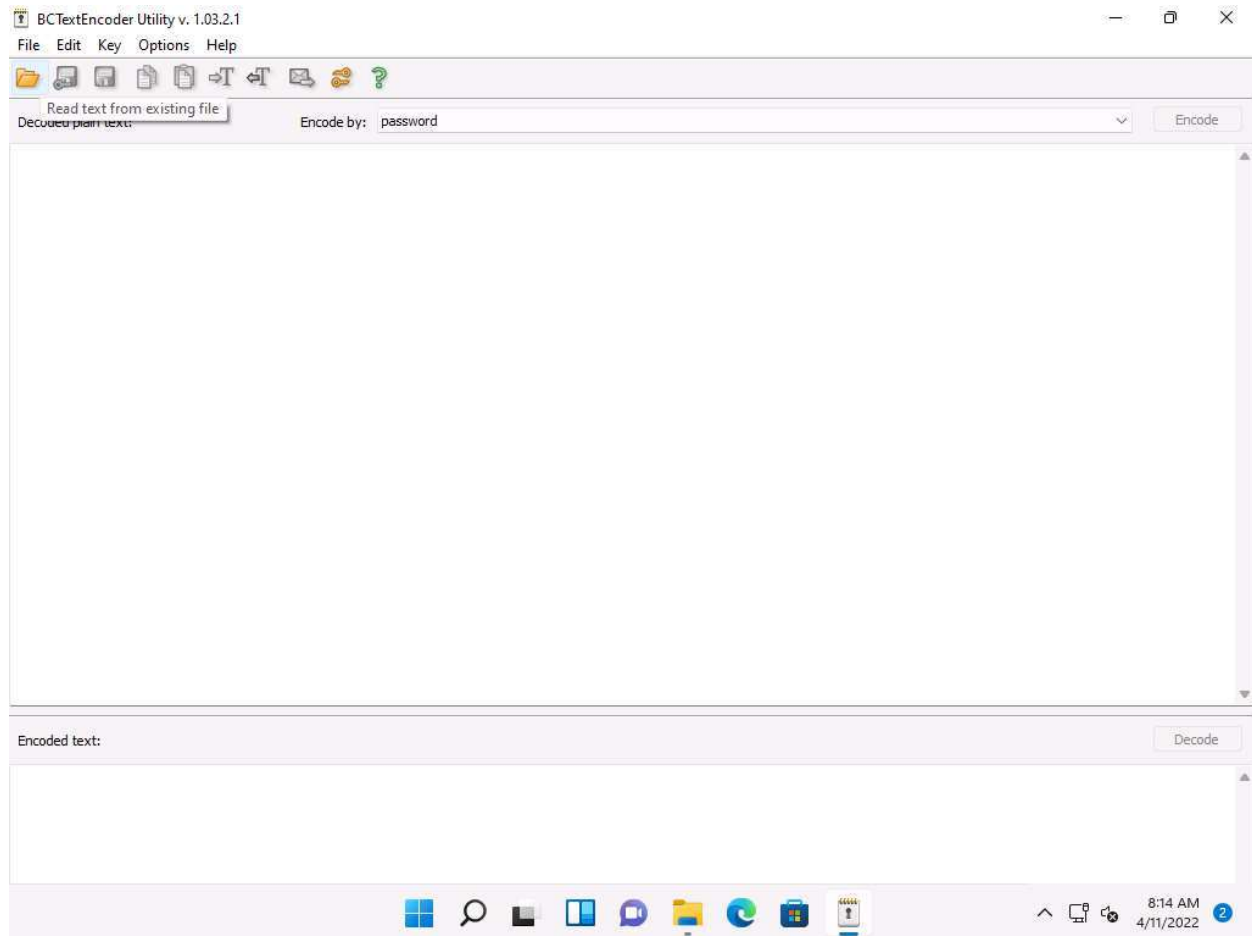
BCTextEncoder simplifies encoding and decoding text data. Plain text data are compressed, encrypted, and converted to text format, which can then be easily copied to the clipboard or saved as a text file. This utility software uses public key encryption methods and password-based encryption, as well as strong and approved symmetric and public key algorithms for data encryption.

Here, we will use the BCTextEncoder tool to encrypt and decrypt data.

1. In **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptography Tools\BCTextEncoder** and double click **BCTextEncoder.exe**.



2. The **BCTextEncoder Utility** window appears, as shown in the screenshot.

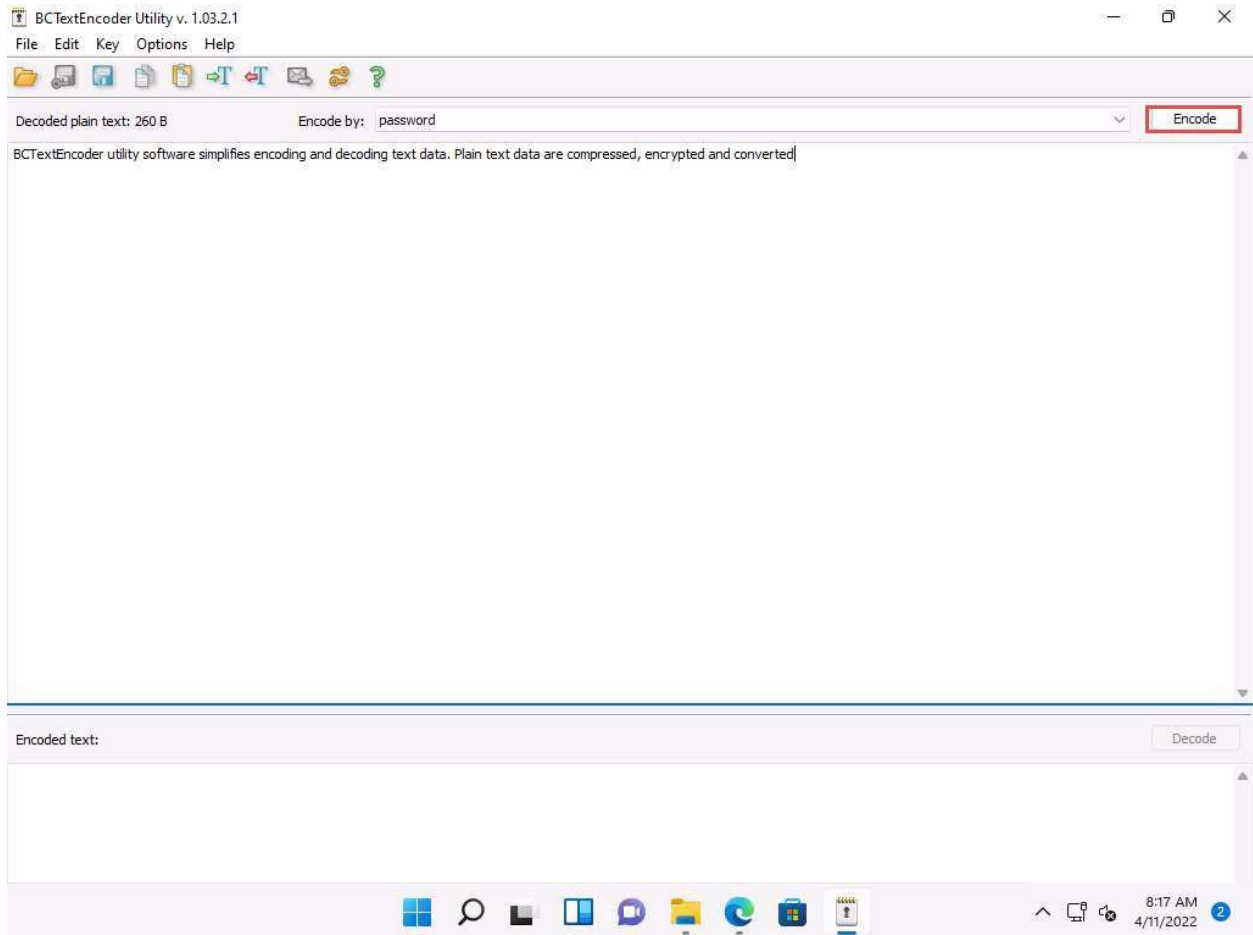


3. To encrypt the text, insert text in the clipboard.

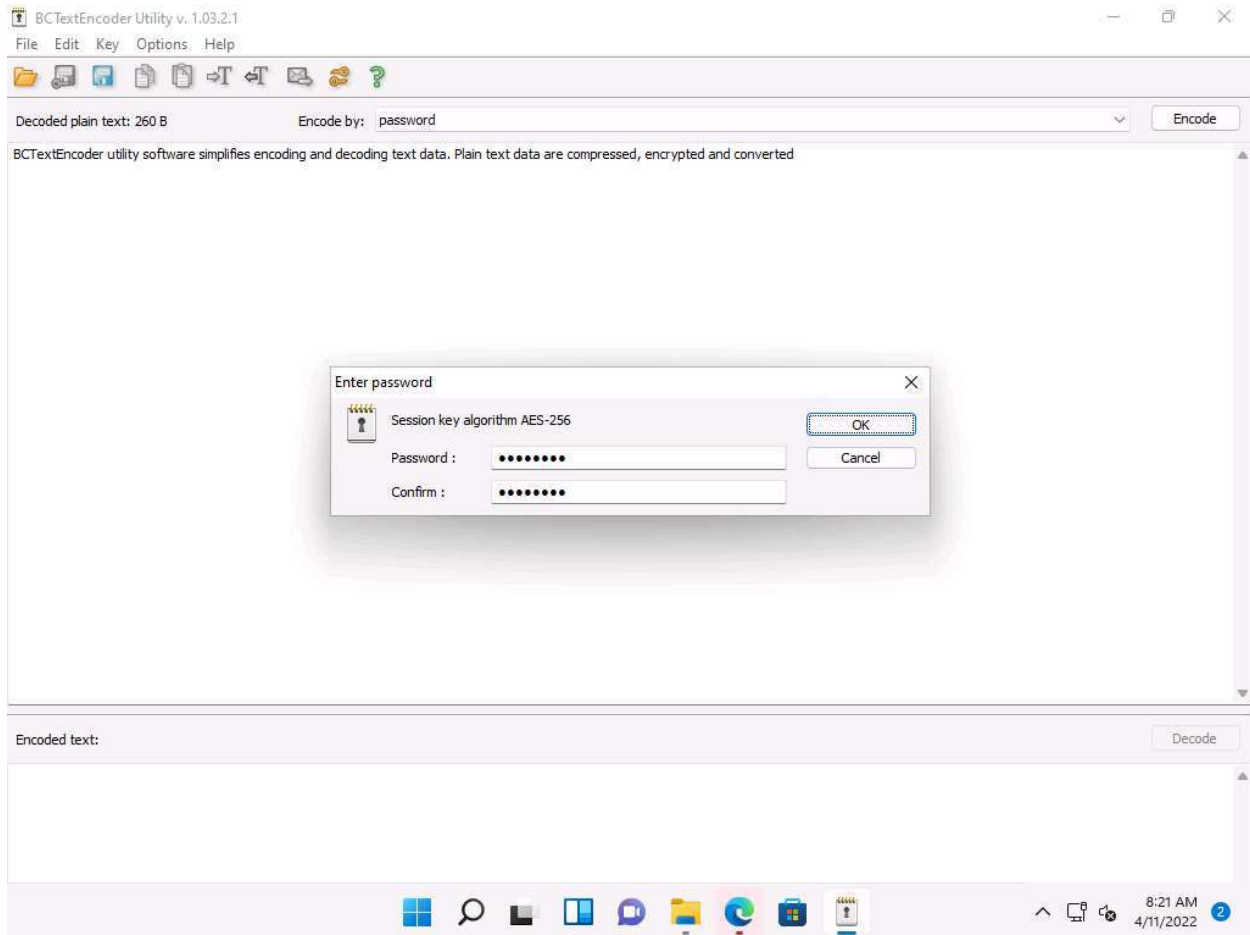
Or

Select the data that you want to encode and paste it to the clipboard by pressing **Ctrl+V**.

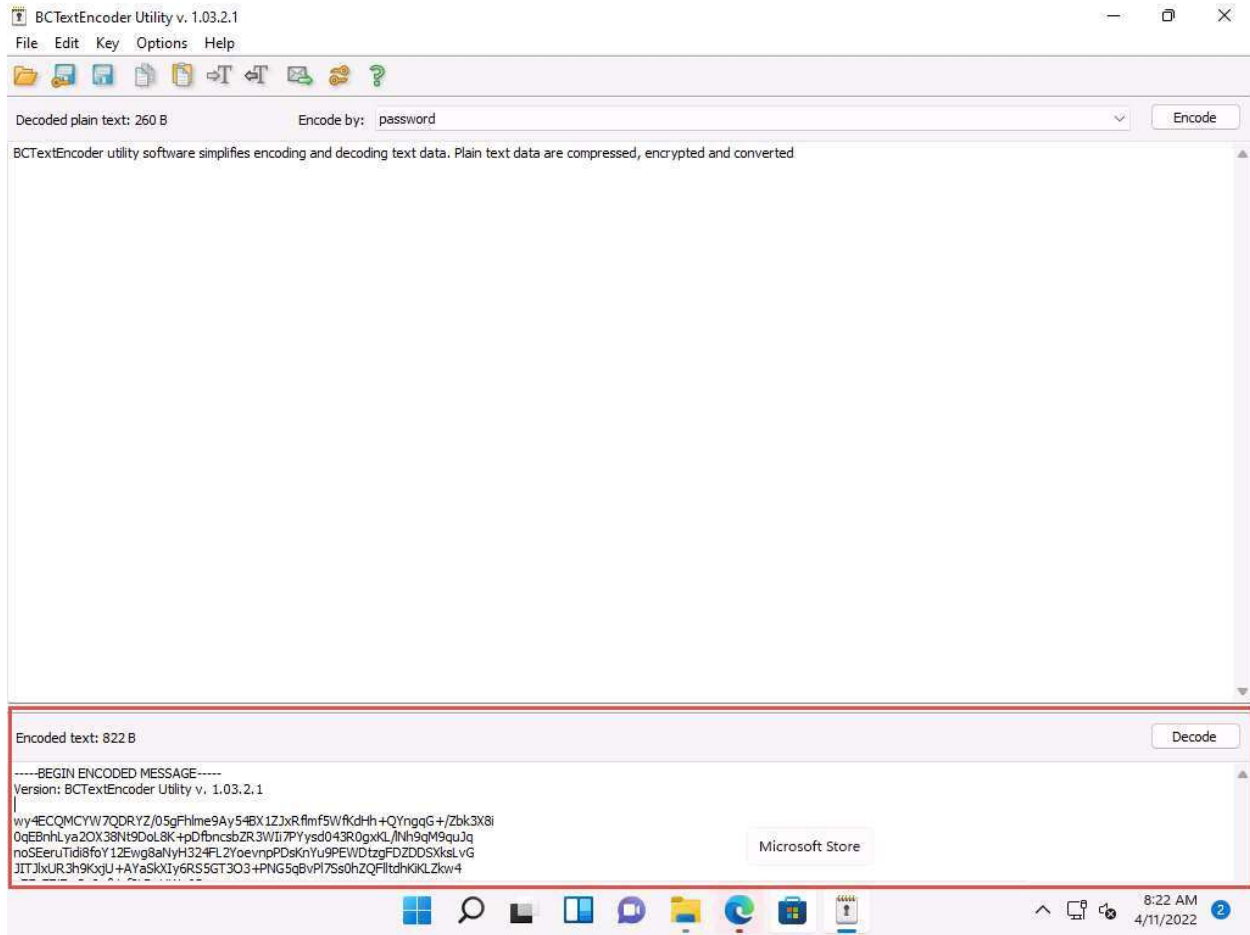
4. Ensure that the **password** option is selected in the **Encode by** field and click **Encode**.



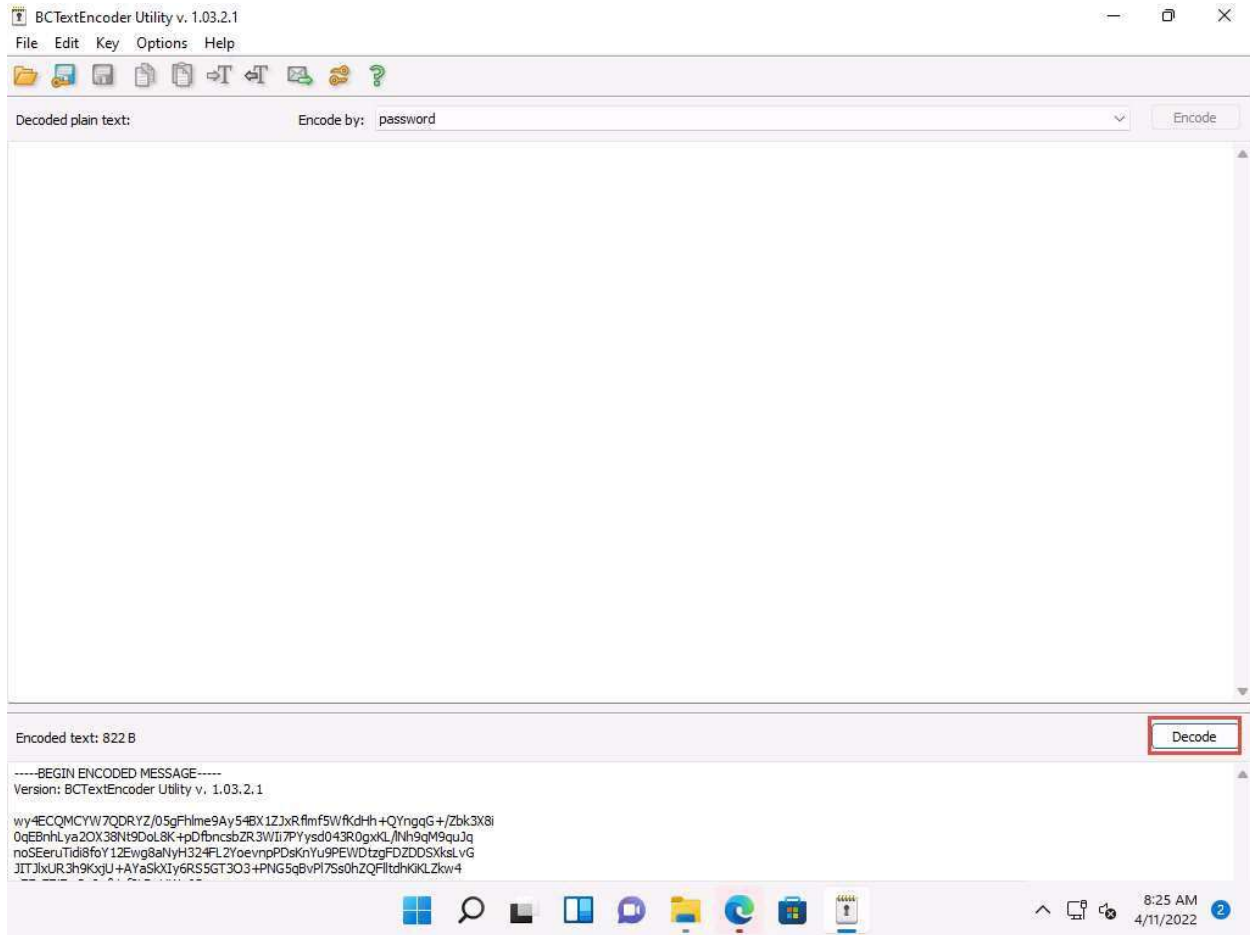
5. The **Enter password** pop-up appears; enter the password into the **Password** field and retype it in the **Confirm** field; then, click **OK**. (Here, we use the password **test@123**).



6. **BCTextEncoder** encodes the text and displays it in under the **Encoded text** section, as shown in the screenshot.

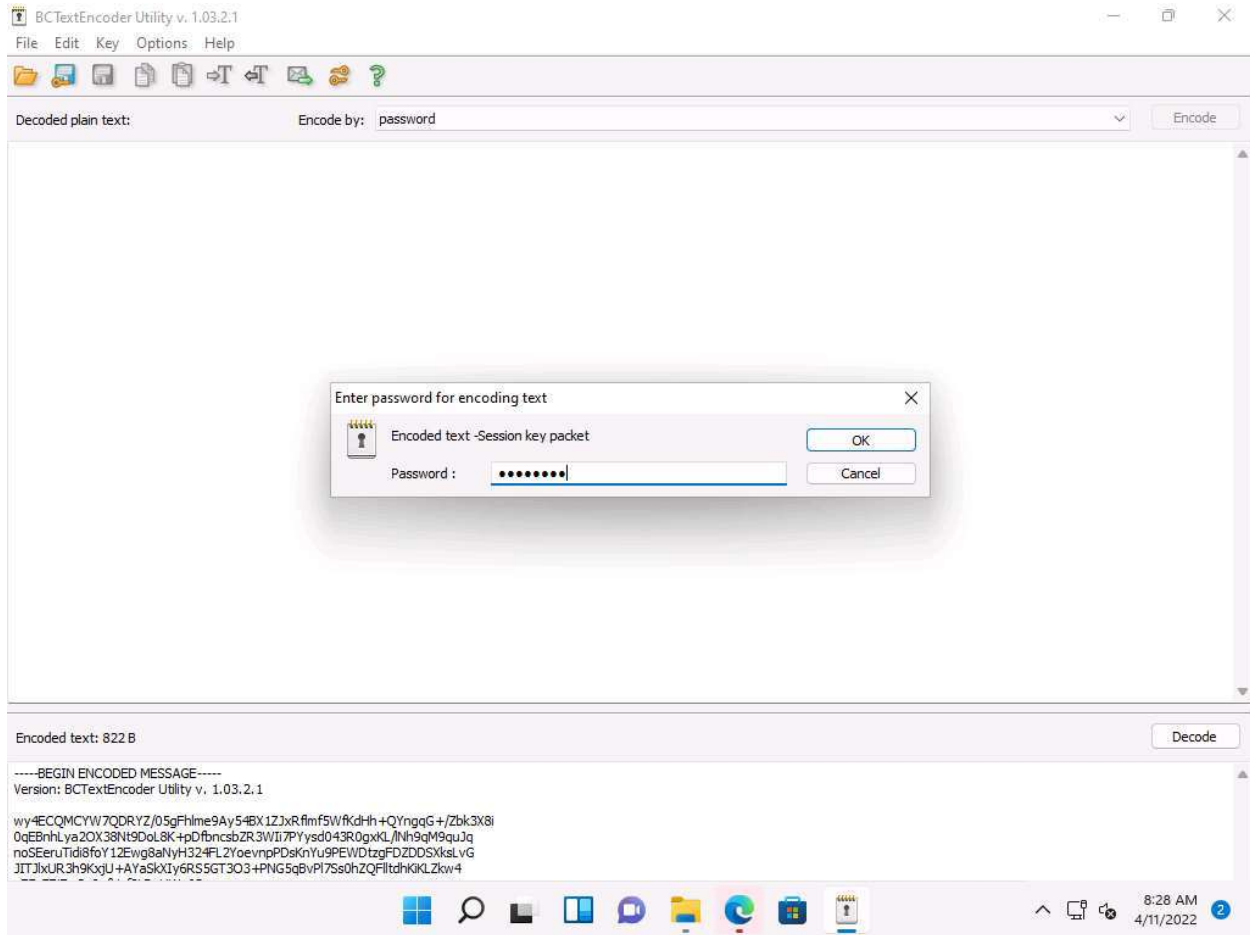


7. To decrypt the data, first, you need to clean the **Decoded plain text** in the clipboard, and then click the **Decode** button.

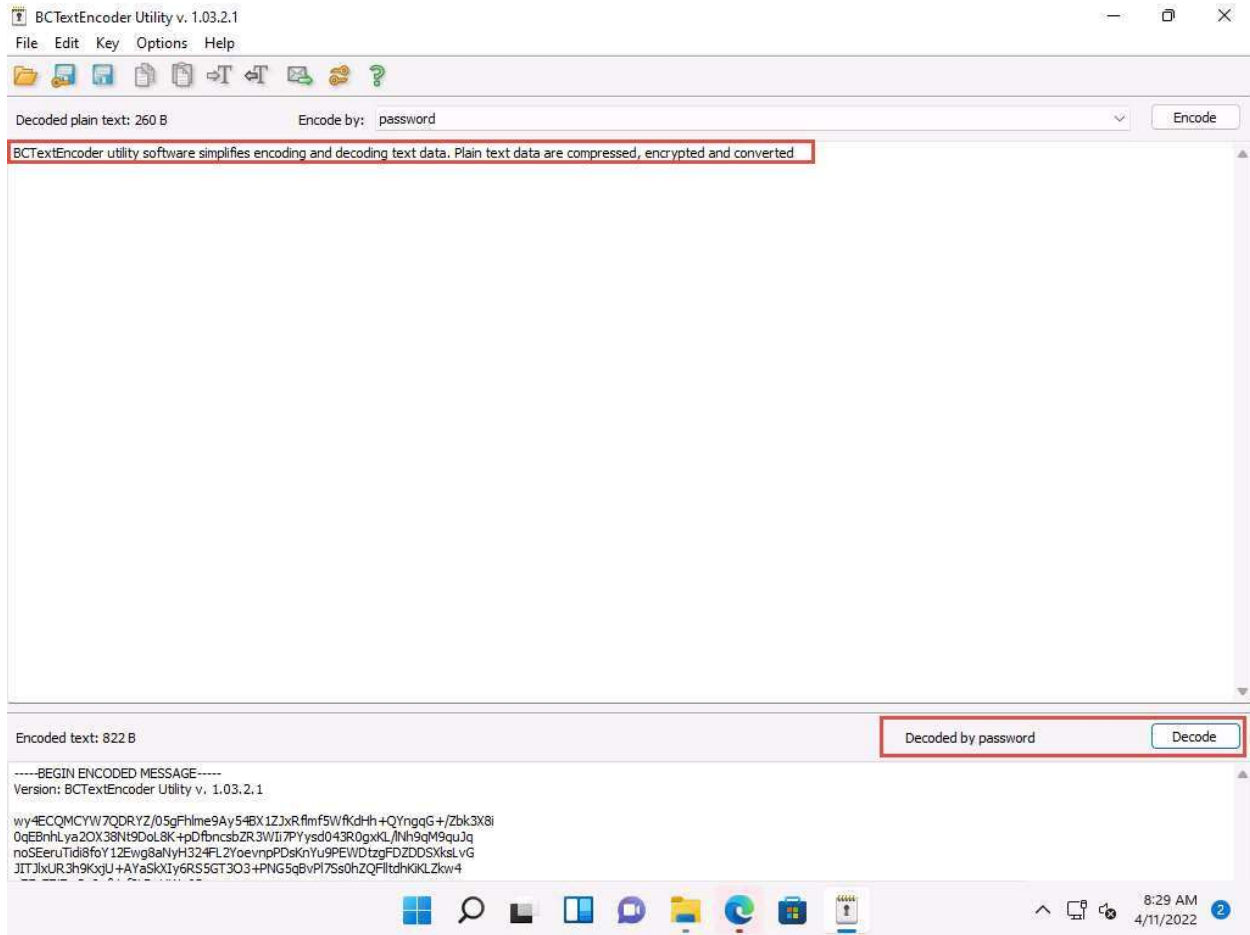




8. The **Enter password for encoding text** dialog-box appears; insert the **Password (test@123)** into the password field and click **OK**.



9. The decoded plain text appears under the **Decoded plain text** section, as shown in the screenshot.



In real-time, using this procedure, you can encode the text while sending it to the intended user along with the password used for encryption. The user for whom the text is intended should have the BCTextEncoder application installed on his/her machine. He/she will have to paste the encoded text into the **Encoded text** section and use the password you shared, to decode it to plain text.

10. This concludes the demonstration of encrypting and decrypting the data using BCTextEncoder.

11. You can also use other cryptography tools such as **AxCrypt** (<https://www.axcrypt.net>), **Microsoft Cryptography Tools** (<https://docs.microsoft.com>), and **Concealer** (<https://www.belightsoft.com>) to encrypt confidential data.

12. Close all open windows and document all the acquired information.

1 Hr 27 Min Remaining

## **Lab 2: Create a Self-signed Certificate**

### **Lab Scenario**

As a professional ethical hacker and penetration tester, you must possess a proper knowledge of creating this certificate as it validates the public key contained within the certificate belonging to the person, company, server, or other entity mentioned. The labs in this exercise demonstrate the creation of a self-signed certificate.

### **Lab Objectives**

- Create and use self-signed certificates

### **Overview of Self-signed Certificate**

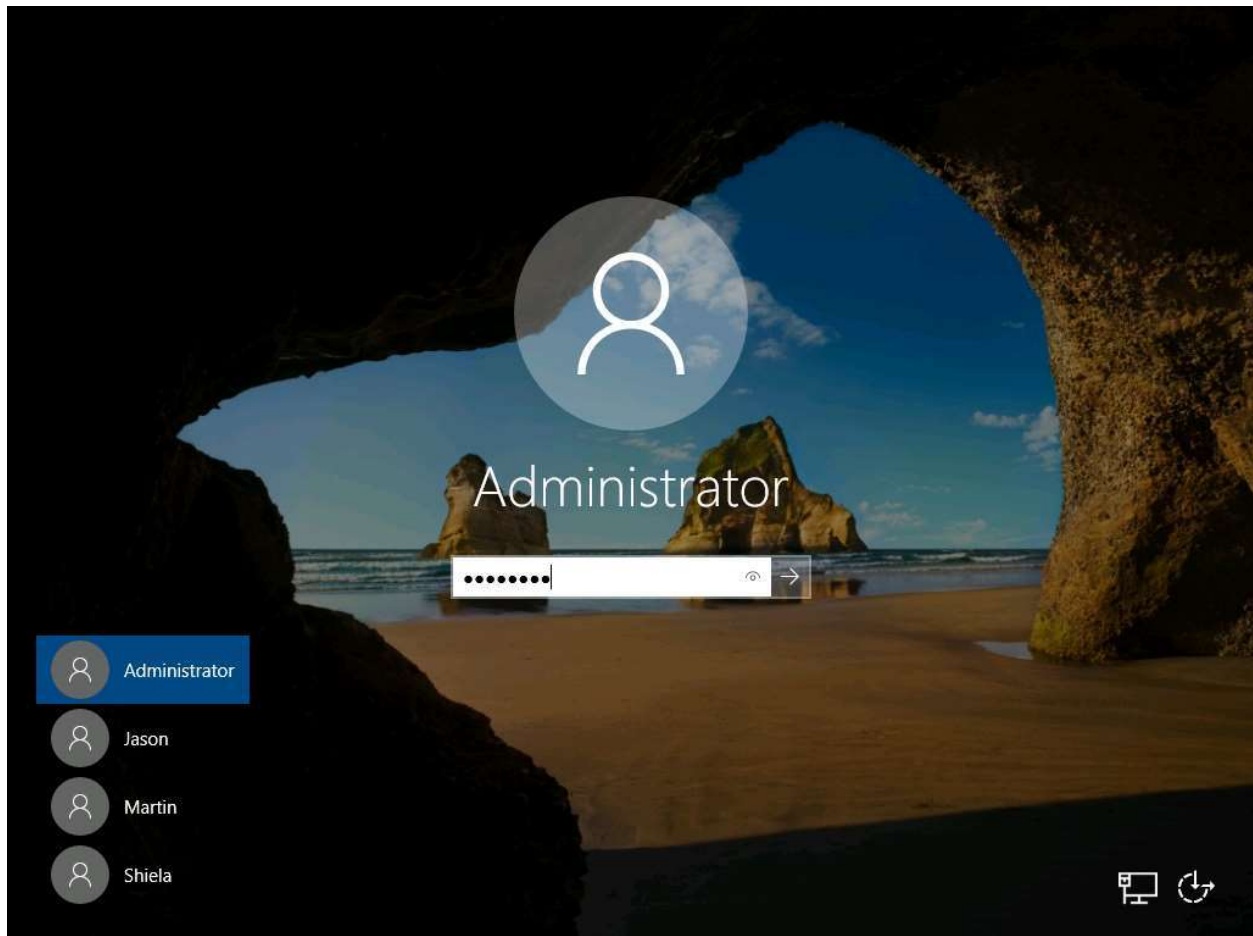
In cryptography and computer security, a self-signed certificate is an identity certificate signed by the same entity whose identity it verifies. However, the term is unrelated to the identity of the person or organization that actually performs the signing procedure.

#### **Task 1: Create and Use Self-signed Certificates**

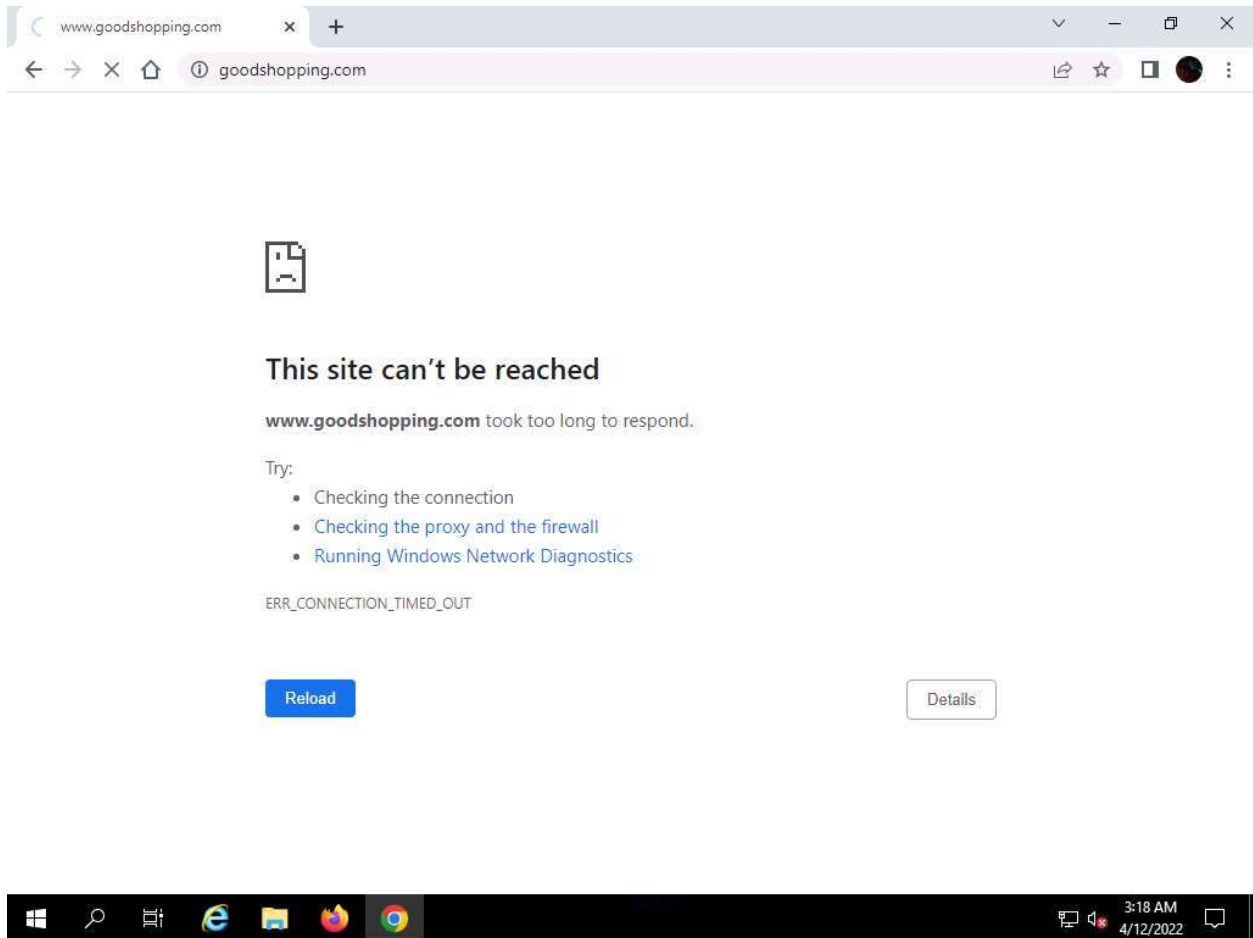
Self-signed certificates are widely used for testing servers. In self-signed certificates, a user creates a pair of public and private keys using a certificate creation tool such as Adobe Acrobat Reader, Java's keytool, Apple's Keychain, etc. and signs the document with the public key. The recipient requests the private key from the sender in order to verify the certificate. However, certificate verification rarely occurs due to the necessity of disclosing the private key: this makes self-signed certificates useful only in a self-controlled testing environment.

Here, we will create a self-signed certificate in Windows Server 2019.

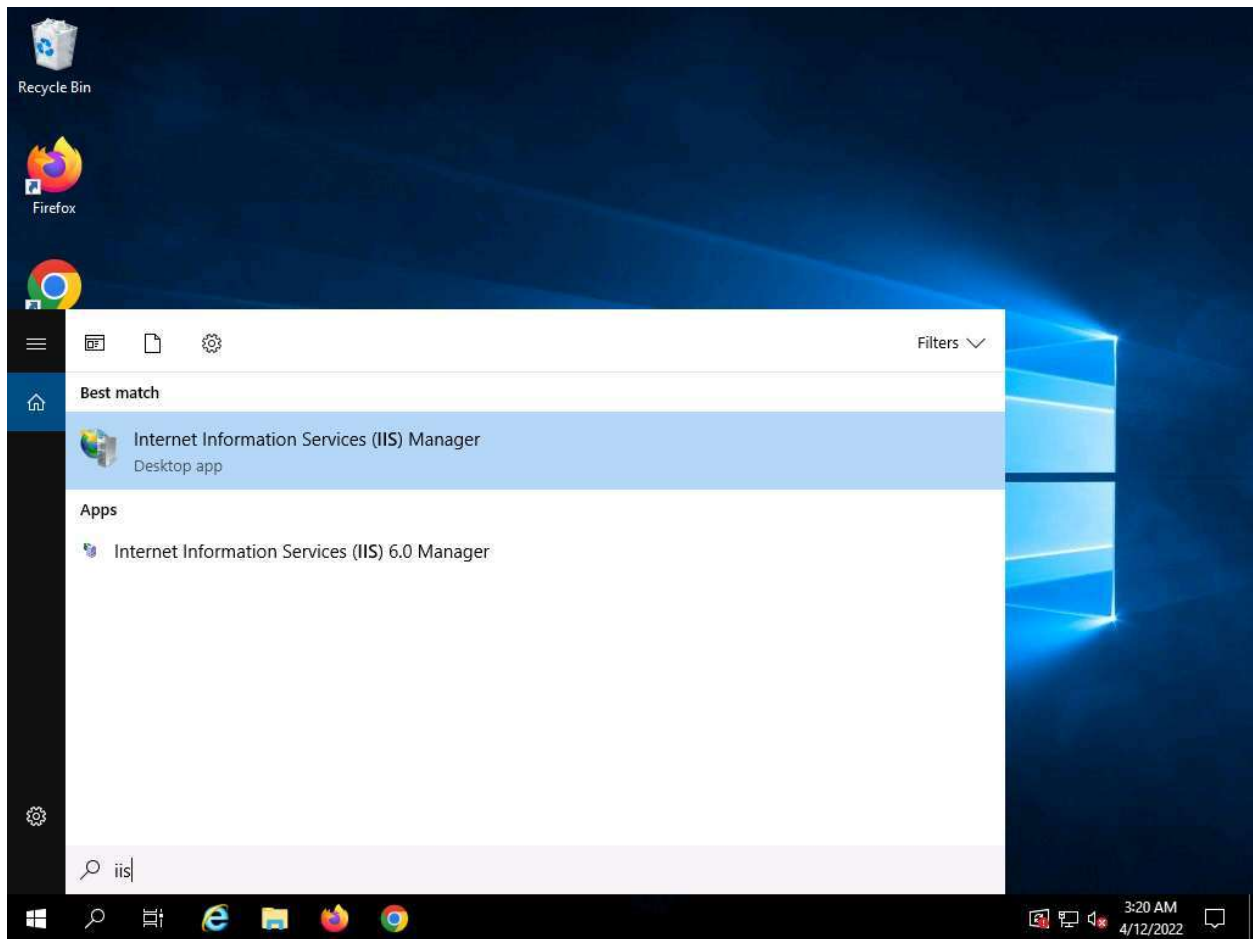
1. Click on [Windows Server 2019](#) to switch to the **Windows Server 2019**, click [Ctrl+Alt+Delete](#) to activate the machine. By default, **Administrator** profile is selected, type **Pa\$\$word** to enter password in the Password field and press **Enter** to login.



2. Before you start this task, you will need to check with your local sites whether they include a self-signed certificate.
3. Launch any web browser (here, **Google Chrome**), place the cursor in the address bar and type **https://www.goodshopping.com**, and press **Enter**.
4. As you are using an https channel to browse the website, it displays a page stating that **This site can't be reached**.
5. As the site does not have a self-signed certificate, it displays a connection refused message, as shown in the screenshot. Close the web browser.

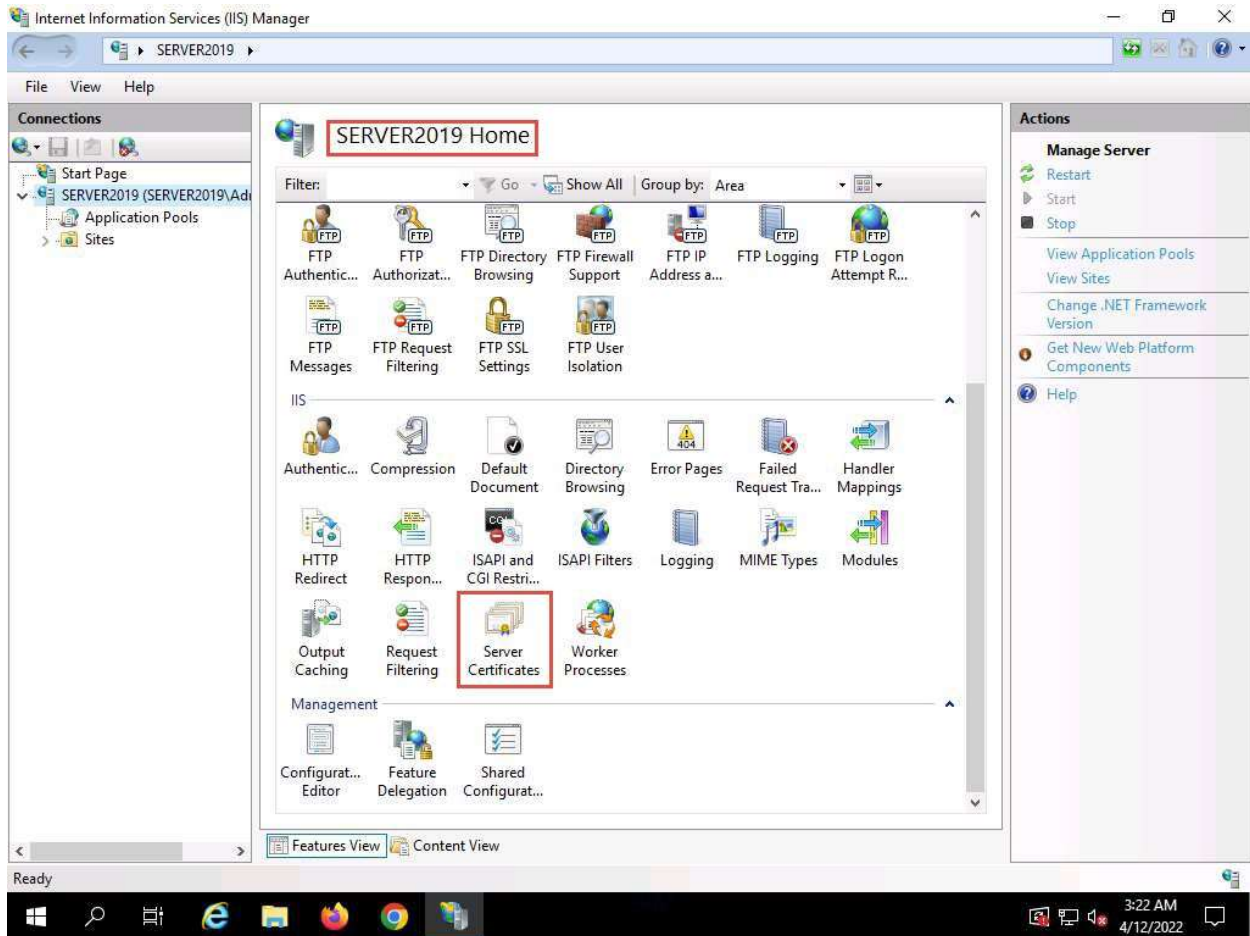


- Click the **Type here to search** icon present in the bottom-left of **Desktop** and type **iis**. Select **Internet Information Services (IIS) Manager** from the results.



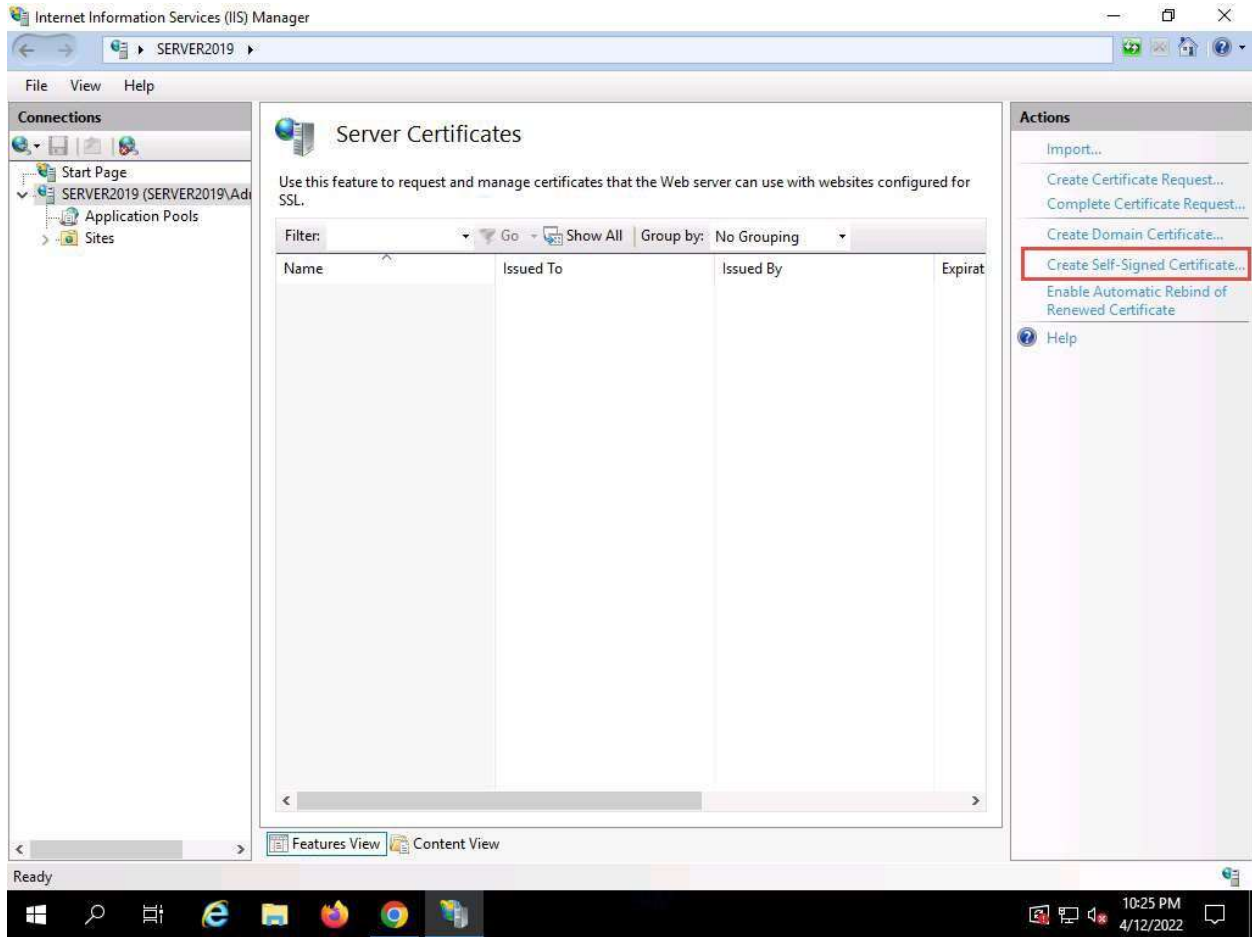
7. The **Internet Information Services (IIS) Manager** window appears; click the machine name (**SERVER2019 (SERVER2019\Administrator)**) under the **Connections** section from the left-hand pane.

8. In **SERVER2019 Home**, double-click **Server Certificates** in the **IIS** section.

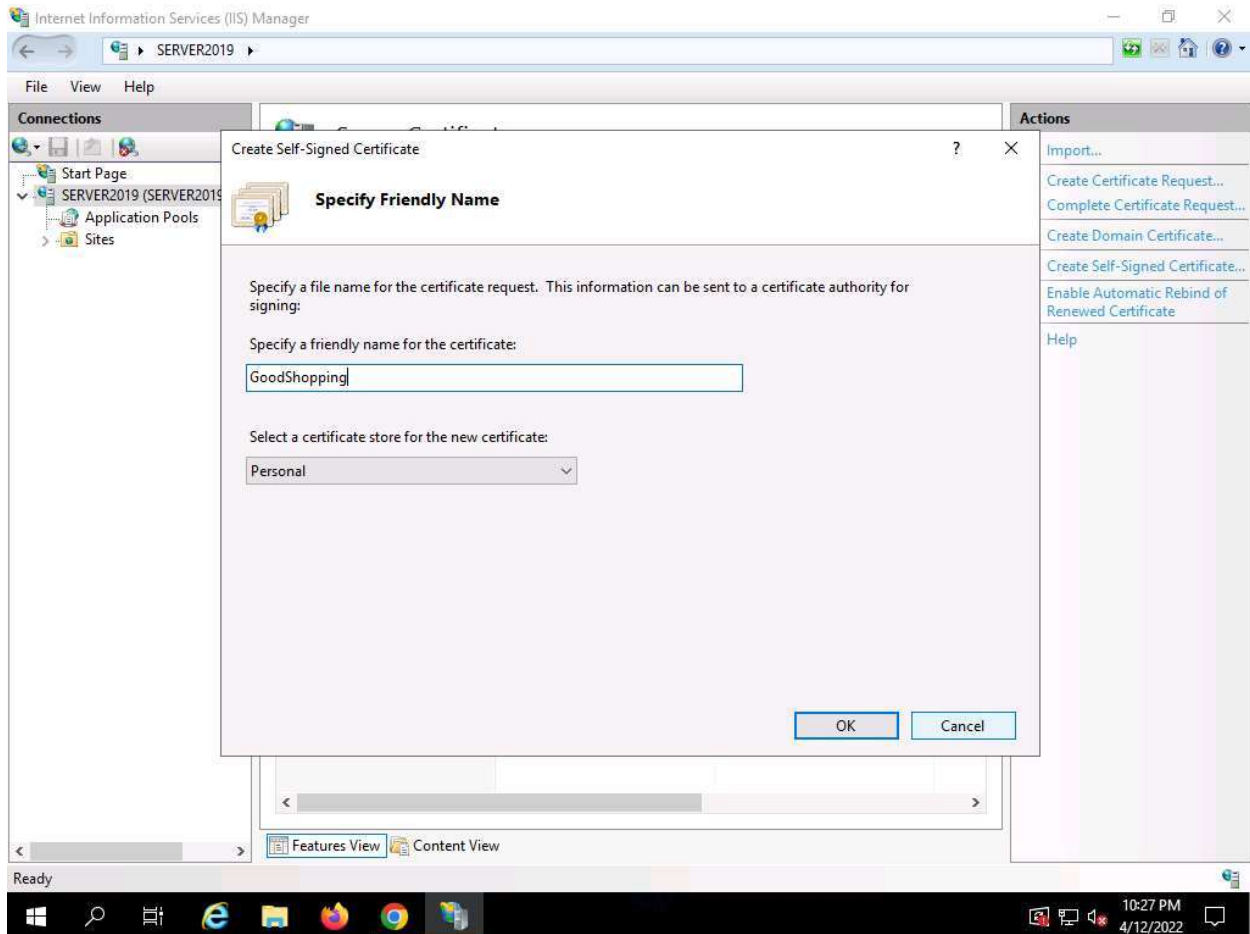




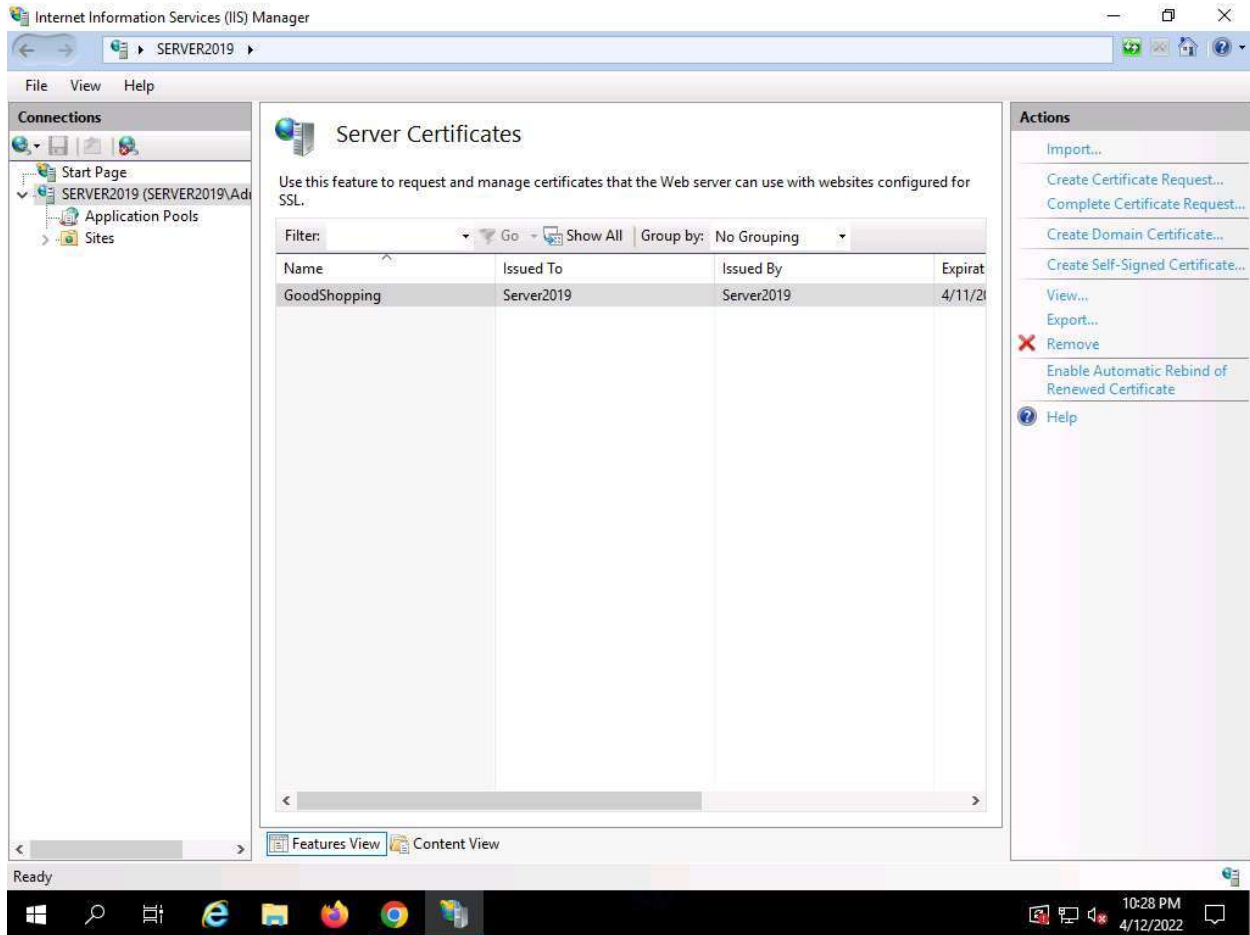
9. The **Server Certificates** wizard appears; click **Create Self-Signed Certificate...** from the right-hand pane in the **Actions** section.



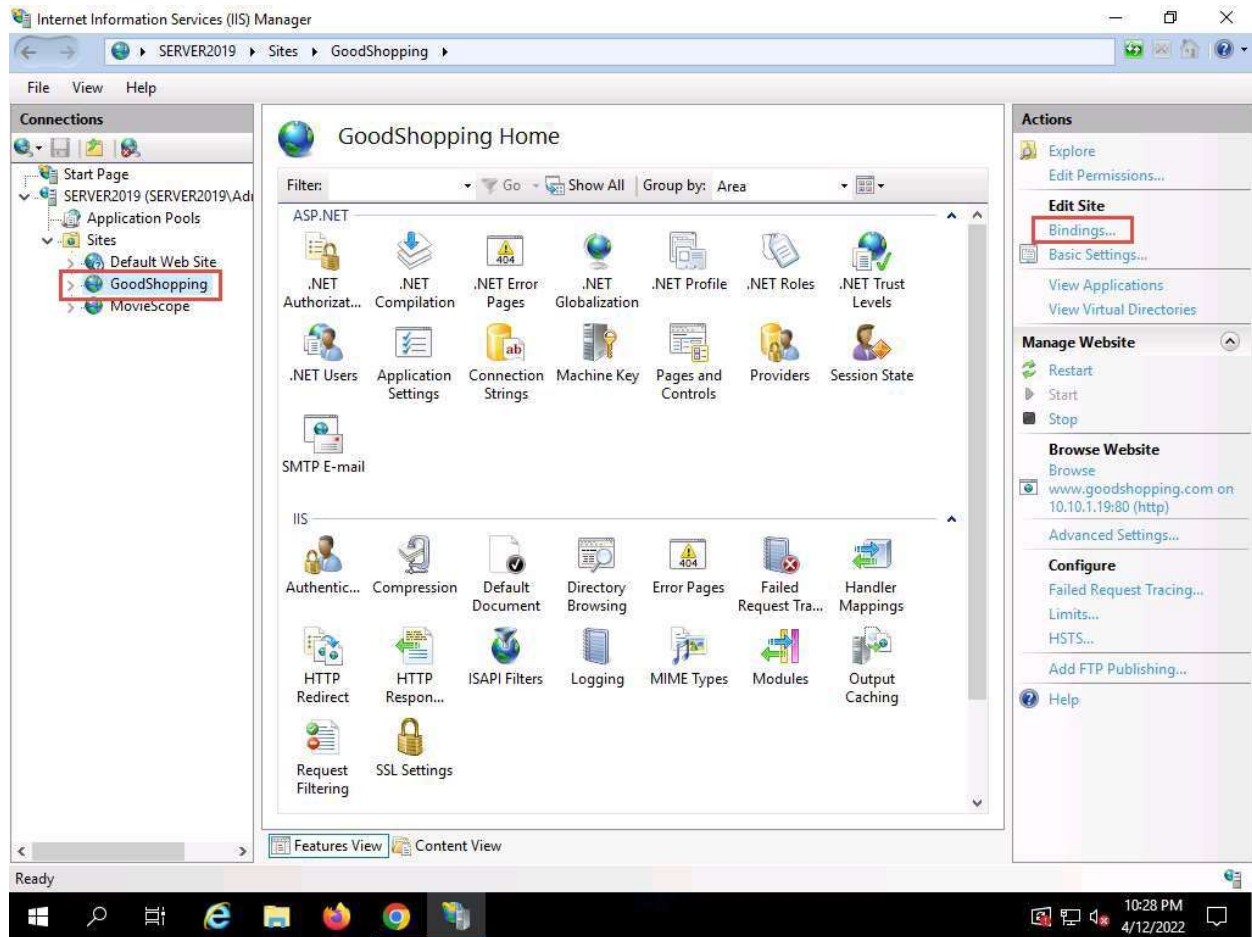
10. The **Create Self-Signed Certificate** window appears; type **GoodShopping** in the **Specify a friendly name for the certificate** field. Ensure that the **Personal** option is selected in the **Select a certificate store for the new certificate** field; then, click **OK**.



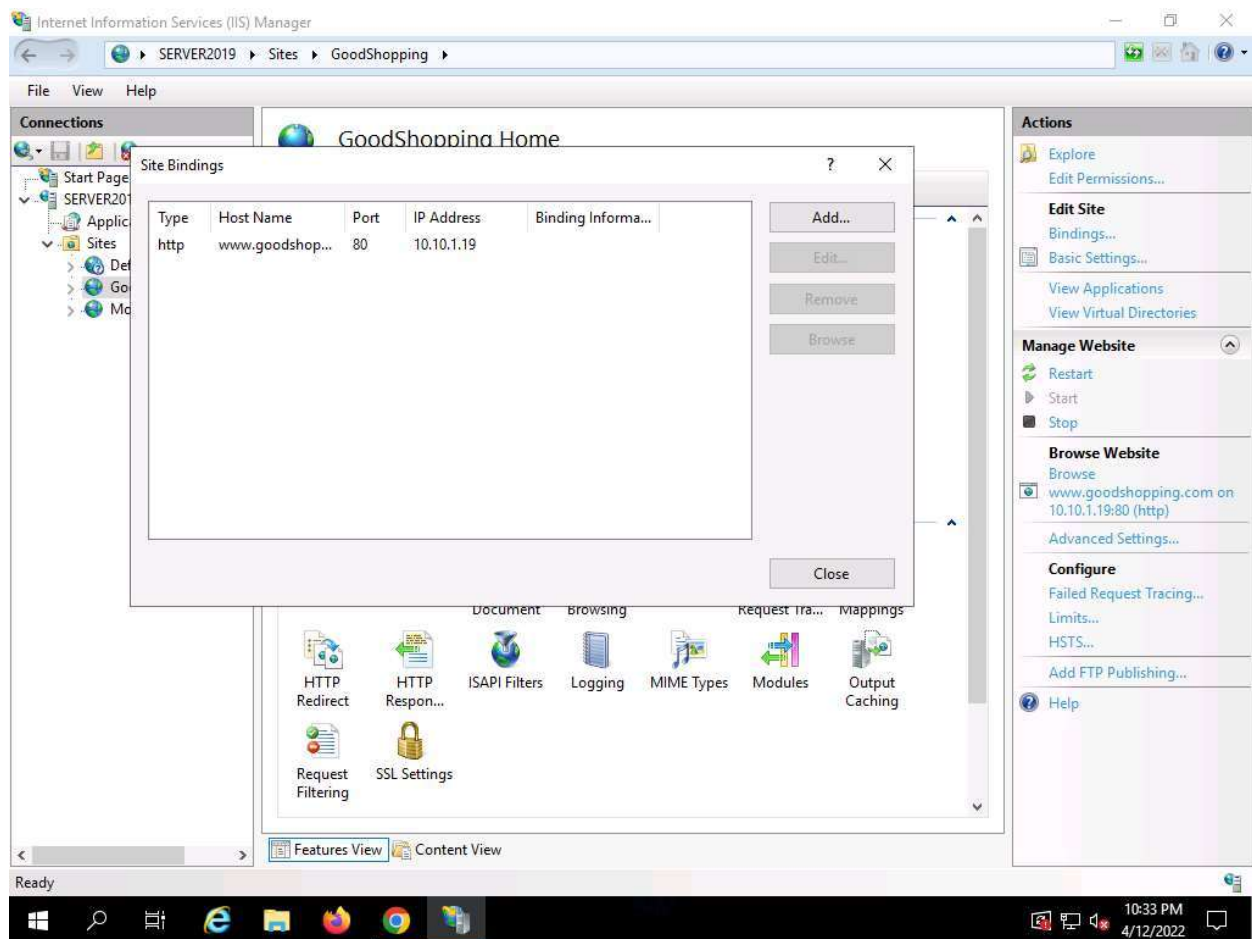
11. A newly created self-signed certificate will be displayed in the **Server Certificates** pane, as shown in the screenshot.



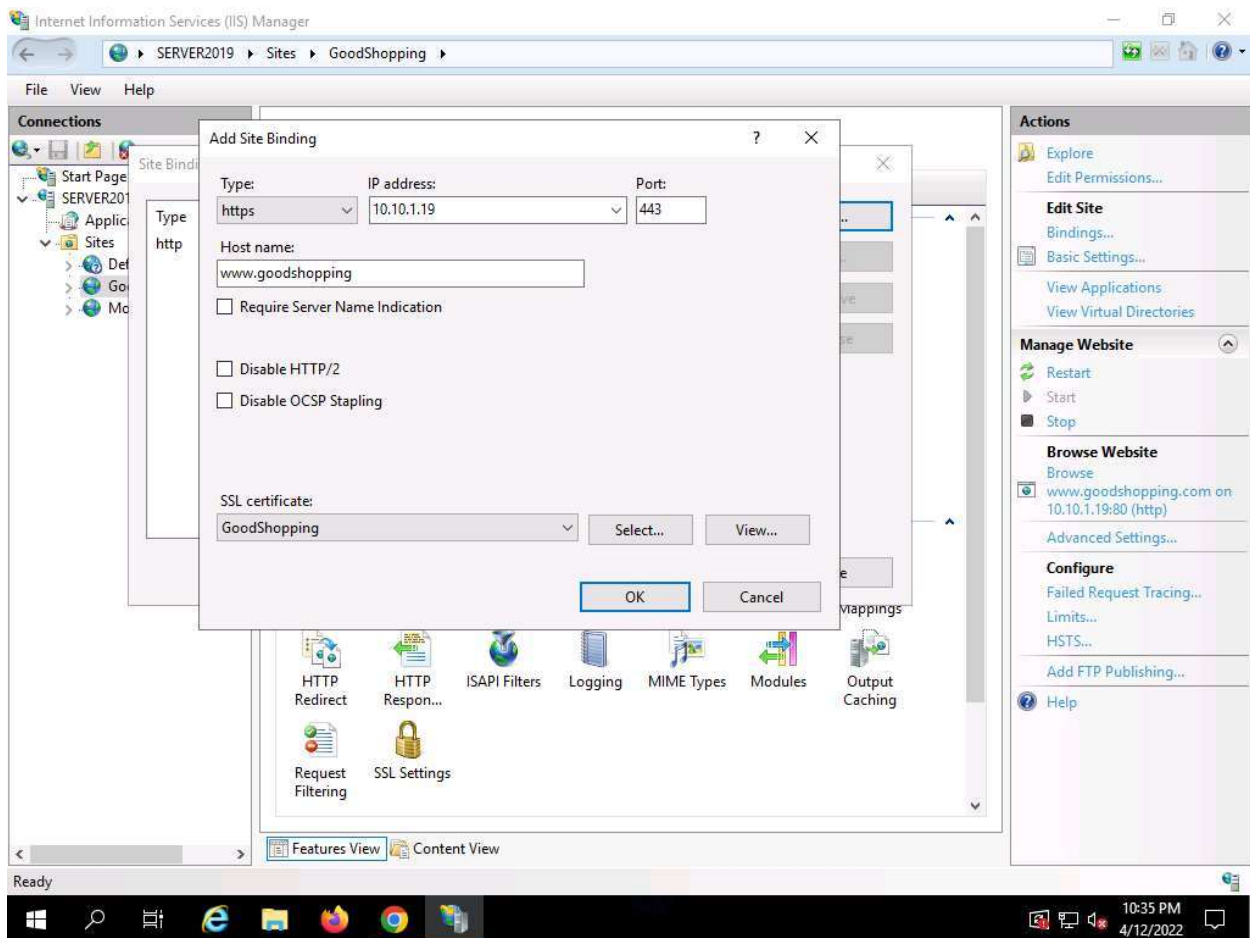
12. Expand the **Sites** node from the left-hand pane, and select **GoodShopping** from the available sites. Click **Bindings...** from the right-hand pane in the **Actions** section.



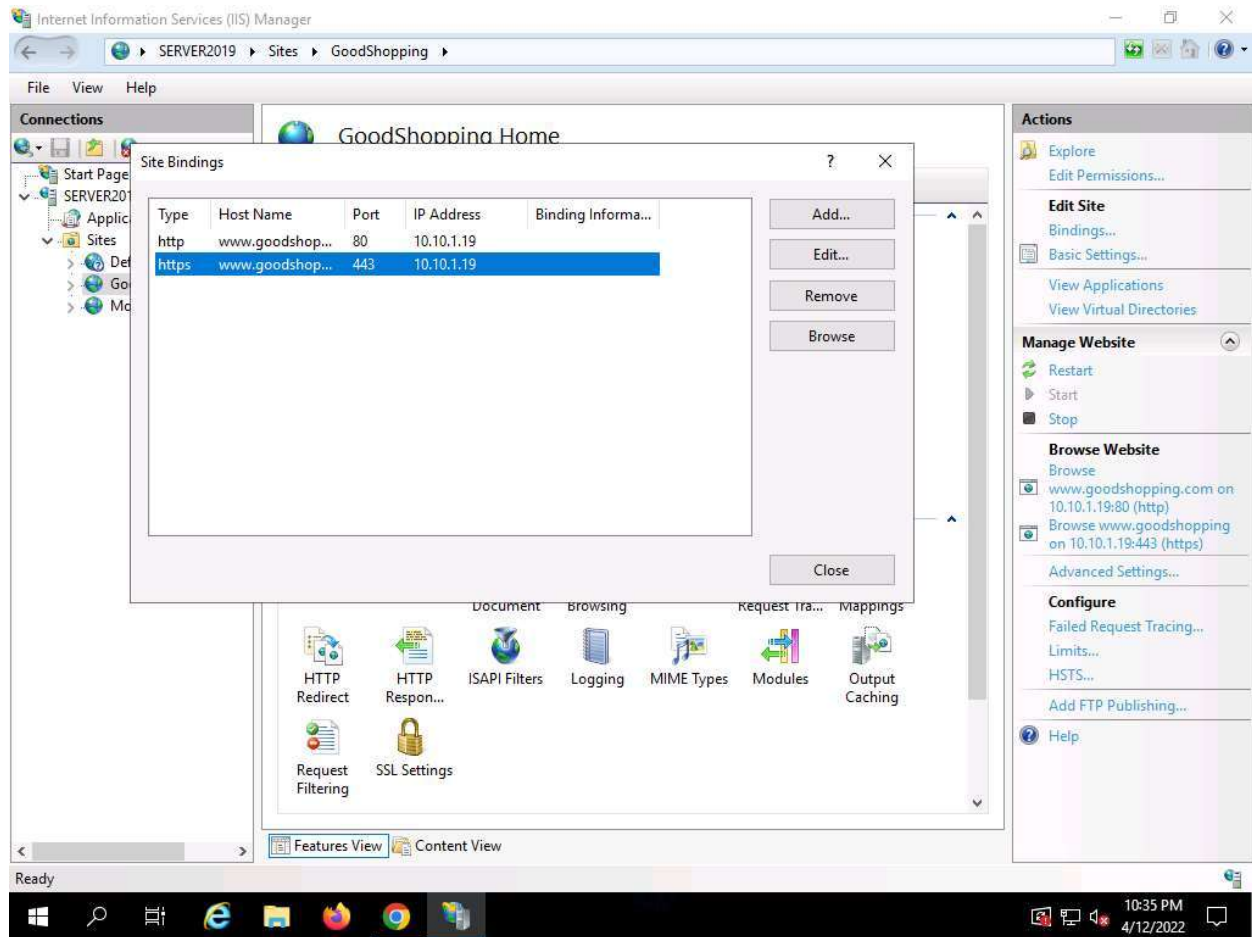
### 13. The **Site Bindings** window appears; click **Add...**



14. The **Add Site Binding** window appears; choose **https** from the **Type** field drop-down list. Once you choose the https type, the port number in the **Port** field automatically changes to **443** (the channel on which HTTPS runs).
15. Choose the **IP address** on which the site is hosted (here, **10.10.1.19**).
16. Under the **Host name** field, type **www.goodshopping.com**. Under the **SSL certificate** field, select **GoodShopping** from the drop-down list, and click **OK**.

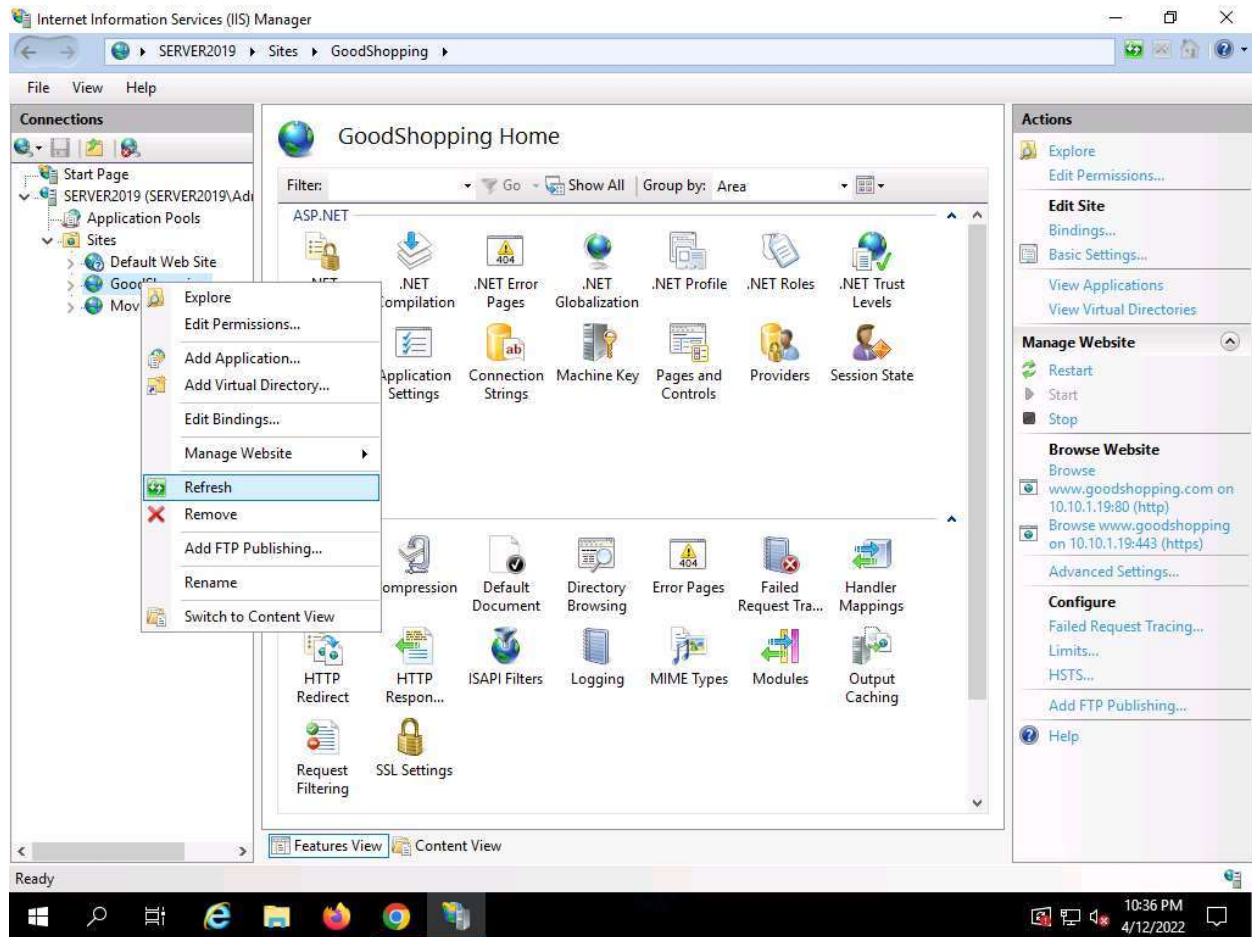


17. The newly created SSL certificate is added to the **Site Bindings** window; then, click **Close**.





18. Now, right-click the name of the site for which you have created the self-signed certificate (here, **GoodShopping**) and click **Refresh** from the context menu.

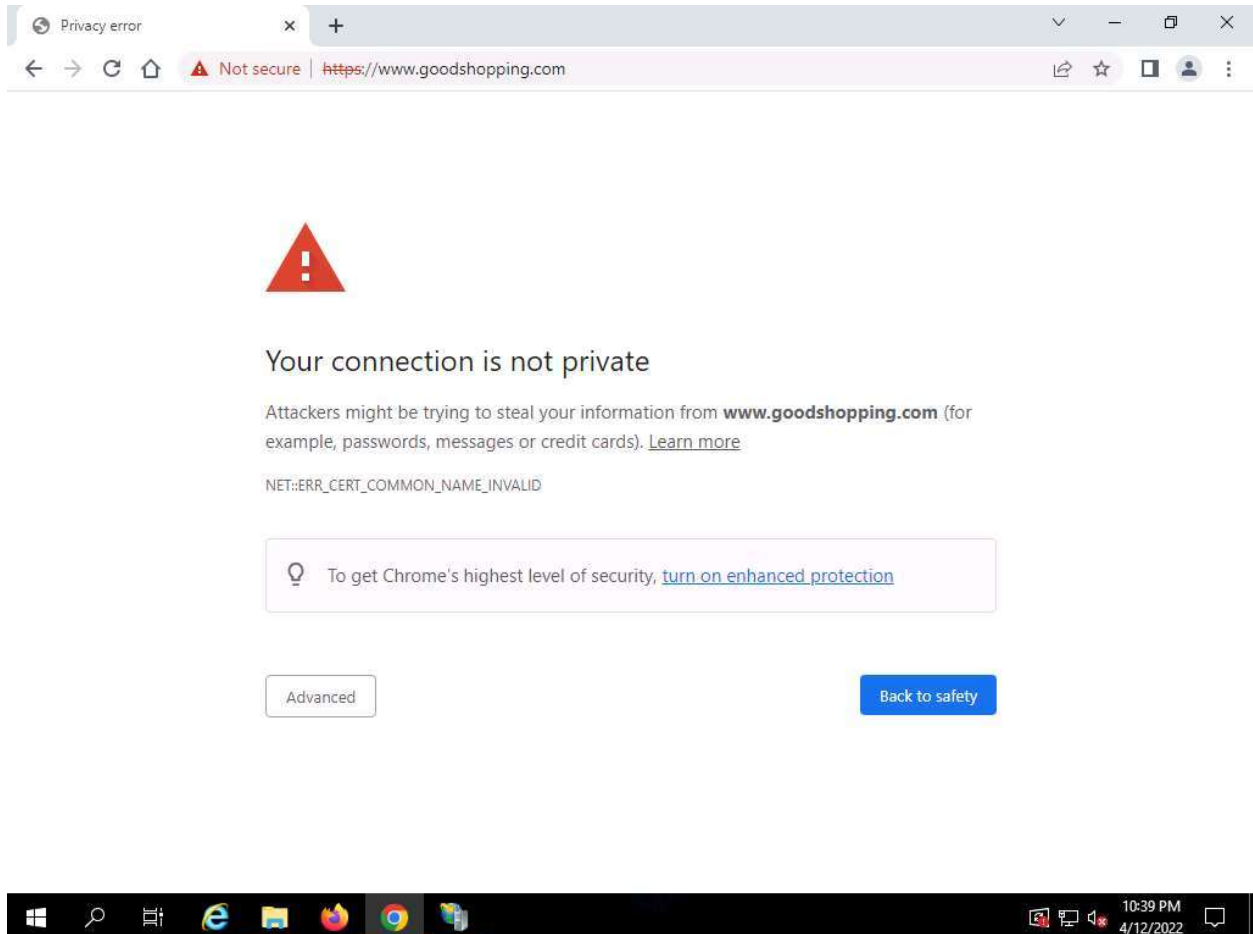




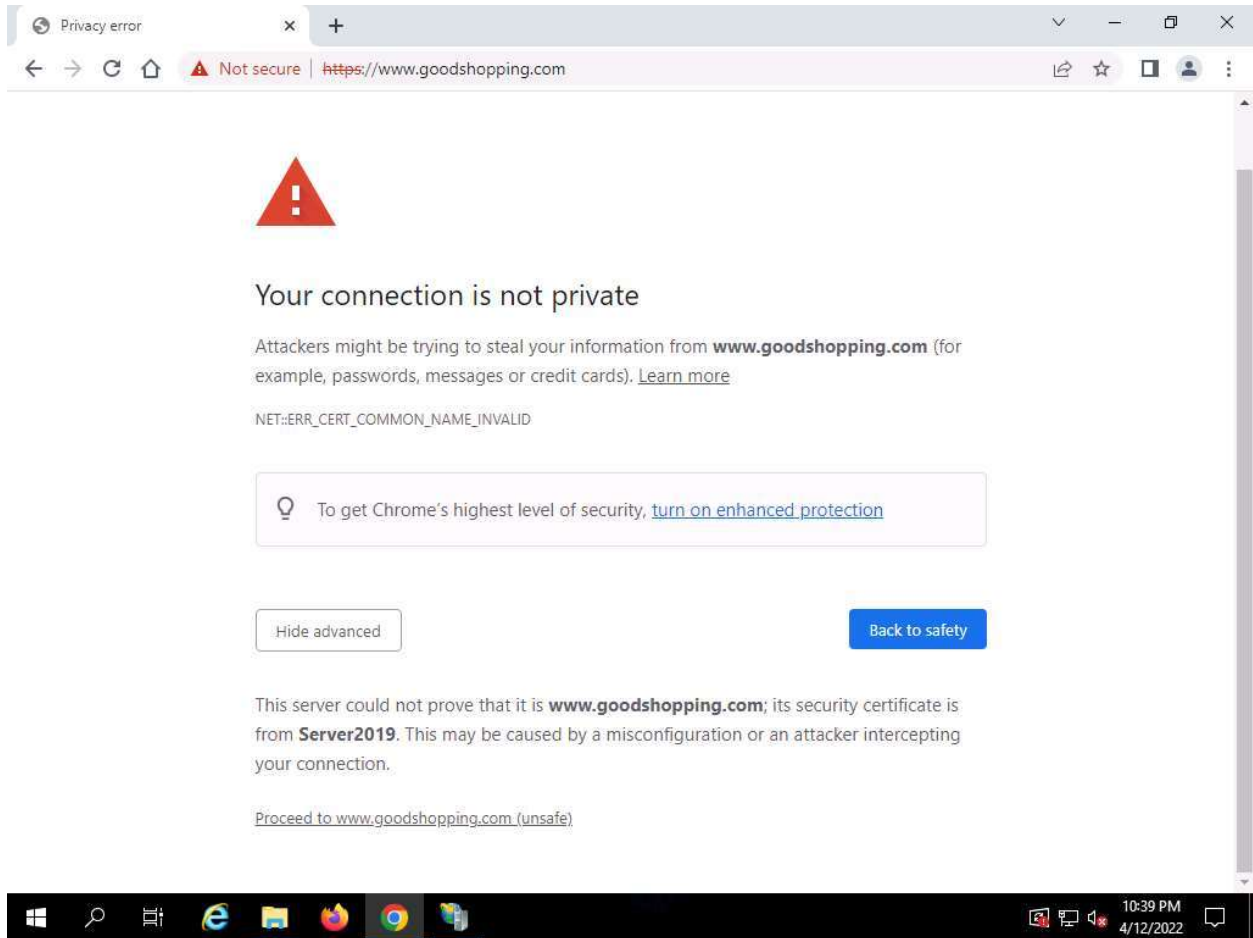
19. Minimize the **Internet Information Services (IIS) Manager** window.

20. Open the **Google Chrome** browser place the cursor in the address bar and type **https://www.goodshopping.com**, and press **Enter**.

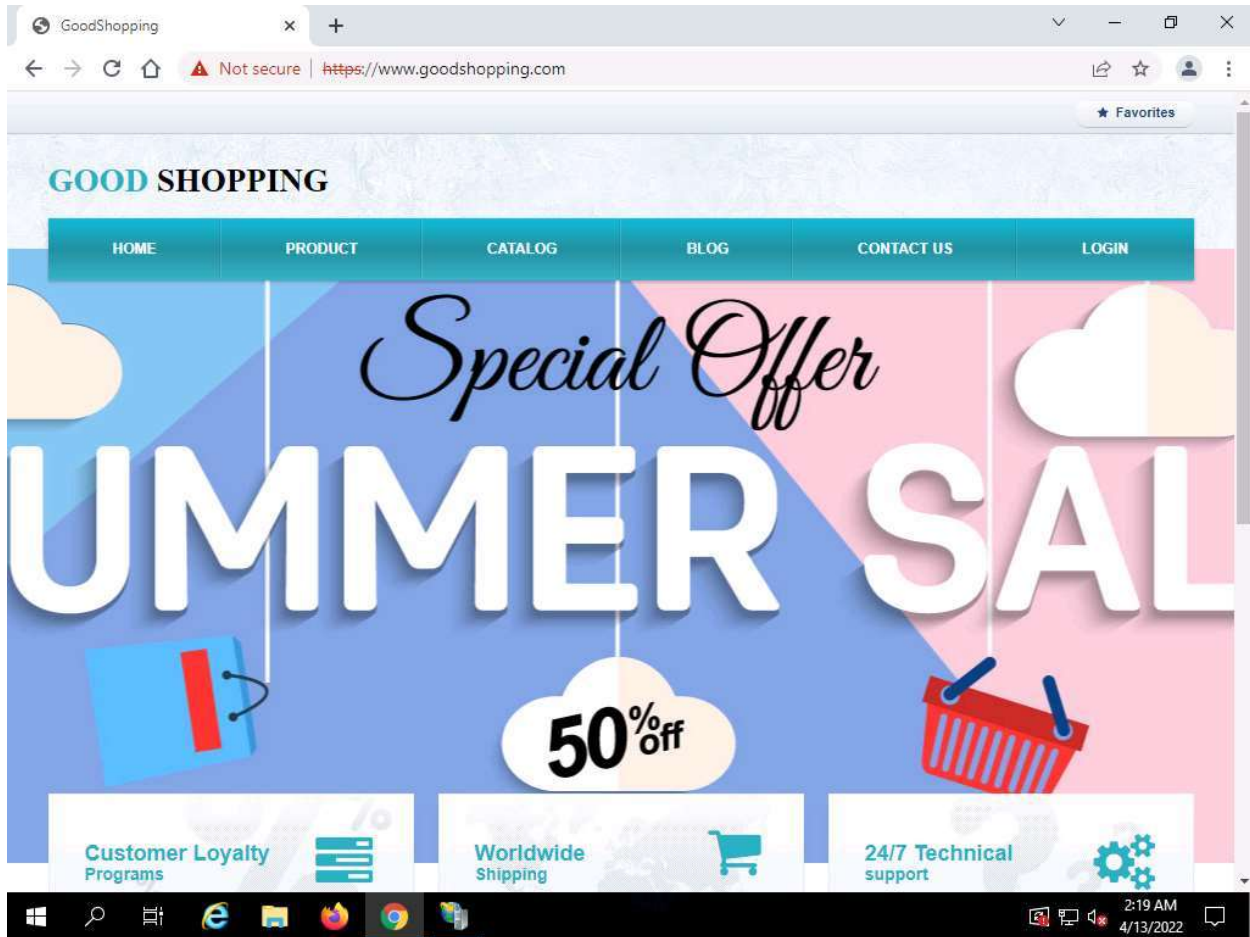
21. The **Your connection is not private** message appears, click **ADVANCED** to proceed.



22. Click **Proceed to www.goodshopping.com (unsafe)**.



23. Now you can see **Goodshopping webpage** with **ssl certificate** assigned to it, as shown in the screenshot.



24. This concludes the demonstration of creating and using a self-signed certificate.

25. Close all open windows and document all the acquired information.

## InstructionsResources

### Lab 3: Perform Email Encryption

#### Lab Scenario

Currently, the majority of businesses use email as their primary source of communication, as it is simple and easy to communicate or share information. Emails can contain sensitive information about an organization such as projects, upcoming news, and financial data, which, when accessed by the wrong person, can cause huge losses to the organization. One can protect emails containing sensitive information by encrypting them.

As a professional ethical hacker and penetration tester, you must have proper knowledge of encrypting email messages so that sensitive information sent through emails remain intact. This lab will demonstrate how to encrypt email messages using various email encryption tools.

#### Lab Objectives

- Perform email encryption using RMail

#### Overview of Email Encryption

Email encryption hides the email content from eavesdroppers by encrypting it into an unreadable form. Emails can be encrypted and decrypted by means of a digital signature mechanism that uses public and private keys: the public key is shared, while the private key is kept private.

There are numerous methods that can be employed for email encryption, including:

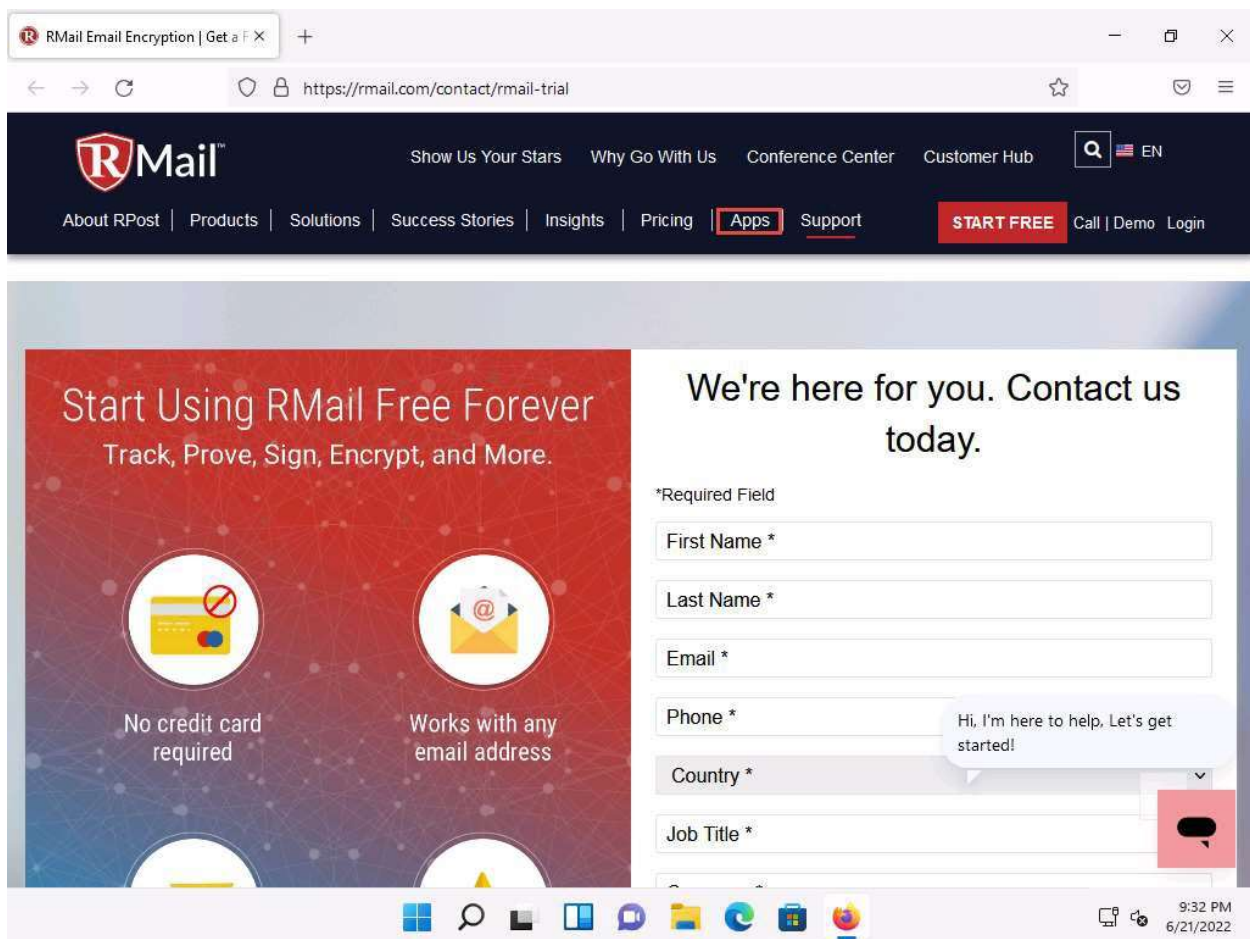
- **Digital Signature:** Uses asymmetric cryptography to simulate the security properties of a signature in digital, rather than written form
- **Secure Sockets Layer (SSL):** Uses RSA asymmetric (public key) encryption to encrypt data transferred over SSL connections
- **Transport Layer Security (TLS):** Uses a symmetric key for bulk encryption, an asymmetric key for authentication and key exchange, and message authentication codes for message integrity
- **Pretty Good Privacy (PGP):** Used to encrypt and decrypt data that provides authentication and cryptographic privacy
- **GNU Privacy Guard (GPG):** Software replacement of PGP and free implementation of the OpenPGP standard that is used to encrypt and decrypt data

## Task 1: Perform Email Encryption using RMail

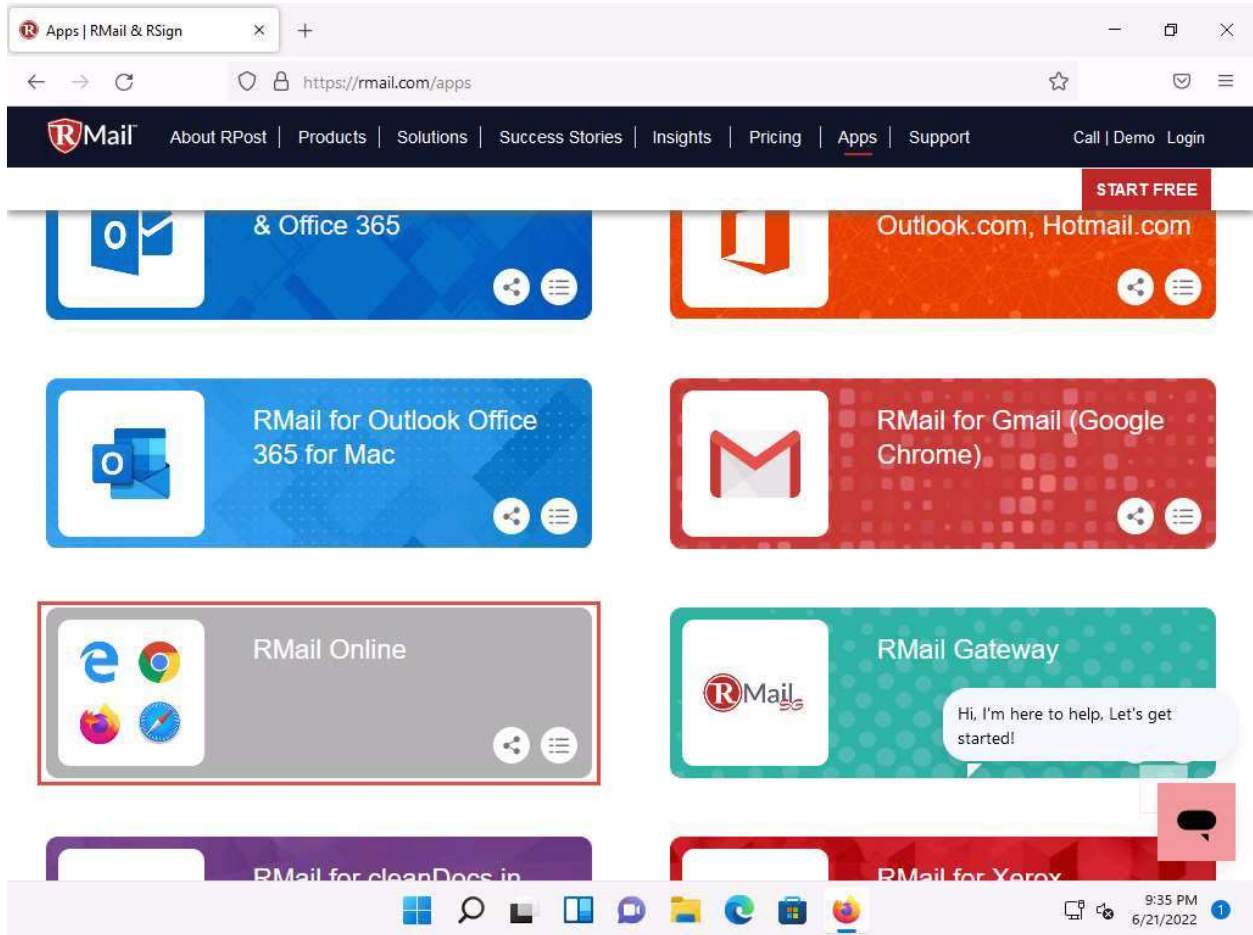
RMail is an email security tool that provides open tracking, proof of delivery, email encryption, electronic signatures, large file transfer functionality, etc. RMail works seamlessly with users' existing email platforms, including Microsoft Outlook and Gmail, amongst others. Using this tool, you can encrypt sensitive emails and attachments for security or legal compliance.

Here, we will use the RMail tool to perform email encryption.

1. Click [Windows 11](#) to switch to the **Windows 11** machine.
2. Launch any web browser (here, **Mozilla Firefox**), Place the cursor in the address bar and click <https://www.rmail.com/free-trial/>, and press **Enter**.
3. The **RMail FREE TRIAL** webpage appears, click on **Apps** from the menu to navigate to the Apps page.



4. In the **Get Started with Rmail. Select an App** page scroll down and select **RMail Online**.



5. The **Rmail Online for Desktop & Mobile Browsers** window appears, scroll down and click on **CLICK HERE TO GET STARTED**.

The screenshot shows a web browser window with the address bar displaying <https://rmail.com/apps/rmail-online>. The page features a dark blue header with the RMail logo and navigation links: About RPost, Products, Solutions, Success Stories, Insights, Pricing, Apps, Support, Call, Demo, and Login. A red 'START FREE' button is positioned in the top right corner of the header. The main content area has a light gray background and includes the following text: 'RMail Online works alongside one's existing email account as an alternate compose and send pane. There is no need to set up a new email address or new email inbox.' Below this, under the heading 'Main Services:', there is a bulleted list of features: 'Track & Prove' (sends a Registered Email™ message with a court-admissible receipt), 'Encrypt' (delivers encrypted files and text), and 'E-Sign' (allows for electronic signatures on documents). Under the heading 'Installation Tips:', it states 'There is no installation required.' A large red button with the text 'CLICK HERE TO GET STARTED' is prominently displayed. A chat bubble on the right side of the page says 'Hi, I'm here to help. Let's get started!'. The Windows taskbar at the bottom shows various application icons and the system clock indicating 9:38 PM on 6/21/2022.

RMail Email Encryption, Register X

← → ↻ 🔒 <https://rmail.com/apps/rmail-online> 📄 ☆ 📧 ☰

**RMail** About RPost | Products | Solutions | Success Stories | Insights | Pricing | Apps | Support Call | Demo Login

**START FREE**

RMail Online works alongside one's existing email account as an alternate compose and send pane. There is no need to set up a new email address or new email inbox.

**Main Services:**

- **Track & Prove:** Sends a Registered Email™ message. A Registered Receipt™ email record is then returned to the sender with court-admissible time-stamped proof of the content delivered and advanced open tracking.
- **Encrypt:** Delivers files and email message body text and attachments encrypted direct to the recipient's inbox with no need for recipients to register or click links, returning auditable proof of compliance and privacy.
- **E-Sign:** Attach a document and send as a Registered Email™ message with the e-sign feature. The message auto-formats so the recipient can use their mouse to electronically draw or type their signature on the document, which returns a legally signed contract to both sender and recipient.

**Installation Tips:**

There is no installation required.

**CLICK HERE TO GET STARTED**

Hi, I'm here to help. Let's get started!

9:38 PM 6/21/2022



6. The **RMail** webpage appears, click on **CREATE AN ACCOUNT**.

RMail Email Encryption, Register... RMail Online

https://app.rmail.com/home

RMail English

CREATE AN ACCOUNT LOGIN

# EMPOWER YOUR EMAIL

Security Compliance Productivity

CREATE AN ACCOUNT

## RMail

Track. Prove. Sign. Encrypt.  
Share.

RMail® makes it easy to encrypt email, certify, track and prove e-delivery, e-sign, and share large files, all-in-one.

Relied on worldwide for more than a decade by governments and businesses of all sizes.

Sign-up now by clicking the [Create an Account](#)

Windows taskbar: 9:40 PM 6/21/2022



7. **Let's get started!** page appears, as well as the registration form. Fill in the required personal details and click on **Sign up**.

The screenshot shows a web browser window with two tabs: 'RMail Email Encryption, Register...' and 'RMail Online'. The address bar shows 'https://app.rmail.com/account'. The page features the RMail logo in the top left and a 'POST R' logo in the top right. On the left, a red sidebar contains the text: 'RMail & RSign: Feature-Rich. More affordable. Elegantly easy. We're here for you.', 'Track. Prove. E-Sign. Encrypt. Share. Certify.', 'The Global Standard in Secure & Certified E-communications. Award winning, since 2000.', and social media icons for Facebook, Twitter, and LinkedIn. The main content area is titled 'Let's get started!' and contains a registration form with the following fields: Email (with a dropdown arrow), Phone, Password (with a strength indicator), Confirm Password (with a strength indicator), First Name, Last Name, Company (with a dropdown arrow), Country (with a dropdown arrow), and a checkbox for 'I agree to the Terms & Conditions'. A red 'Sign up' button is at the bottom of the form. The Windows taskbar at the bottom shows the time as 9:45 PM on 6/21/2022.

RMail Email Encryption, Register... RMail Online

https://app.rmail.com/account

RMail

POST R

**Let's get started!**

Email: [email address] @gmail.com Phone: [phone number]

Password: [password] Confirm Password: [password]

First Name: [first name] Last Name: [last name]

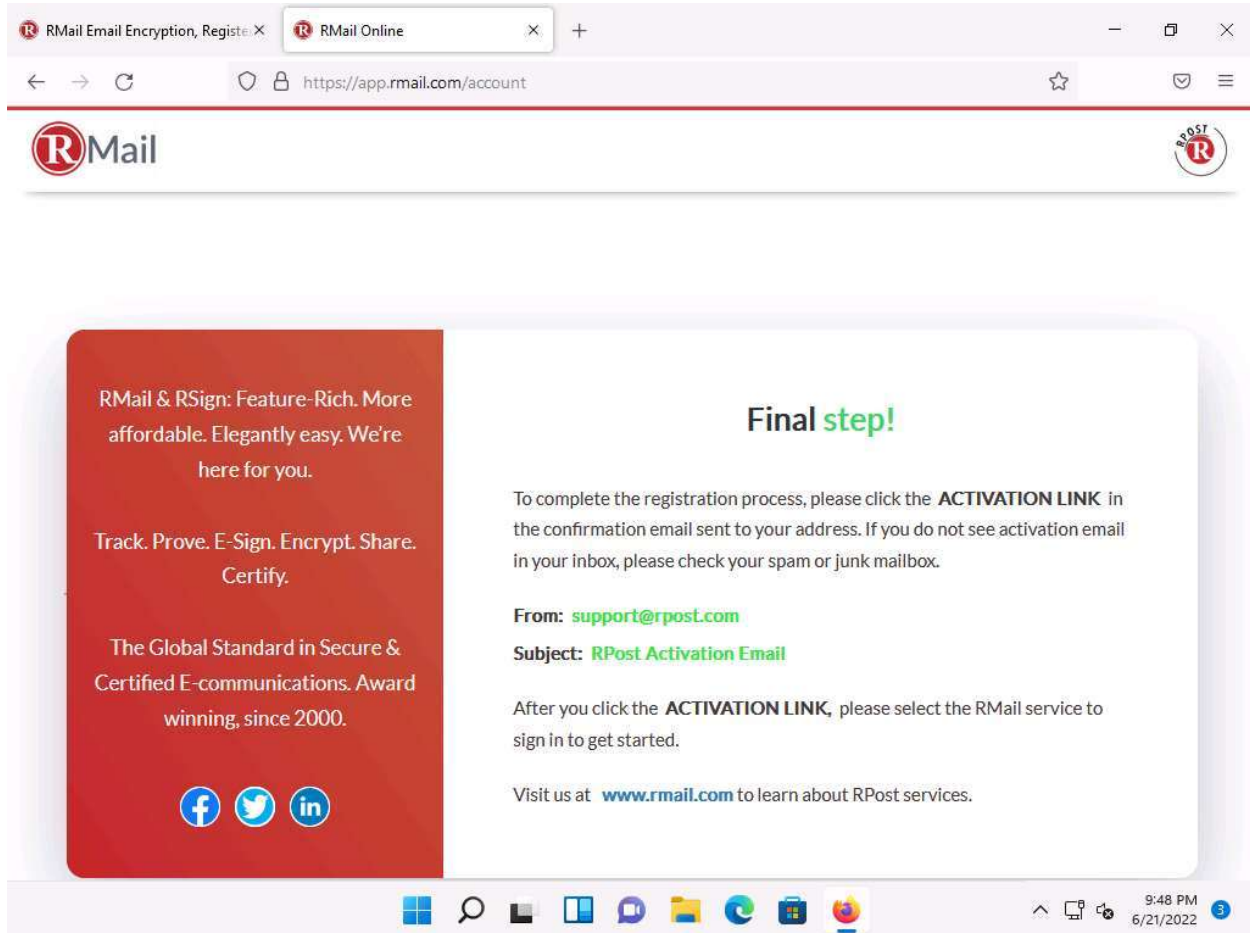
Company: [company] Country: [country]

☒ I agree to the Terms & Conditions

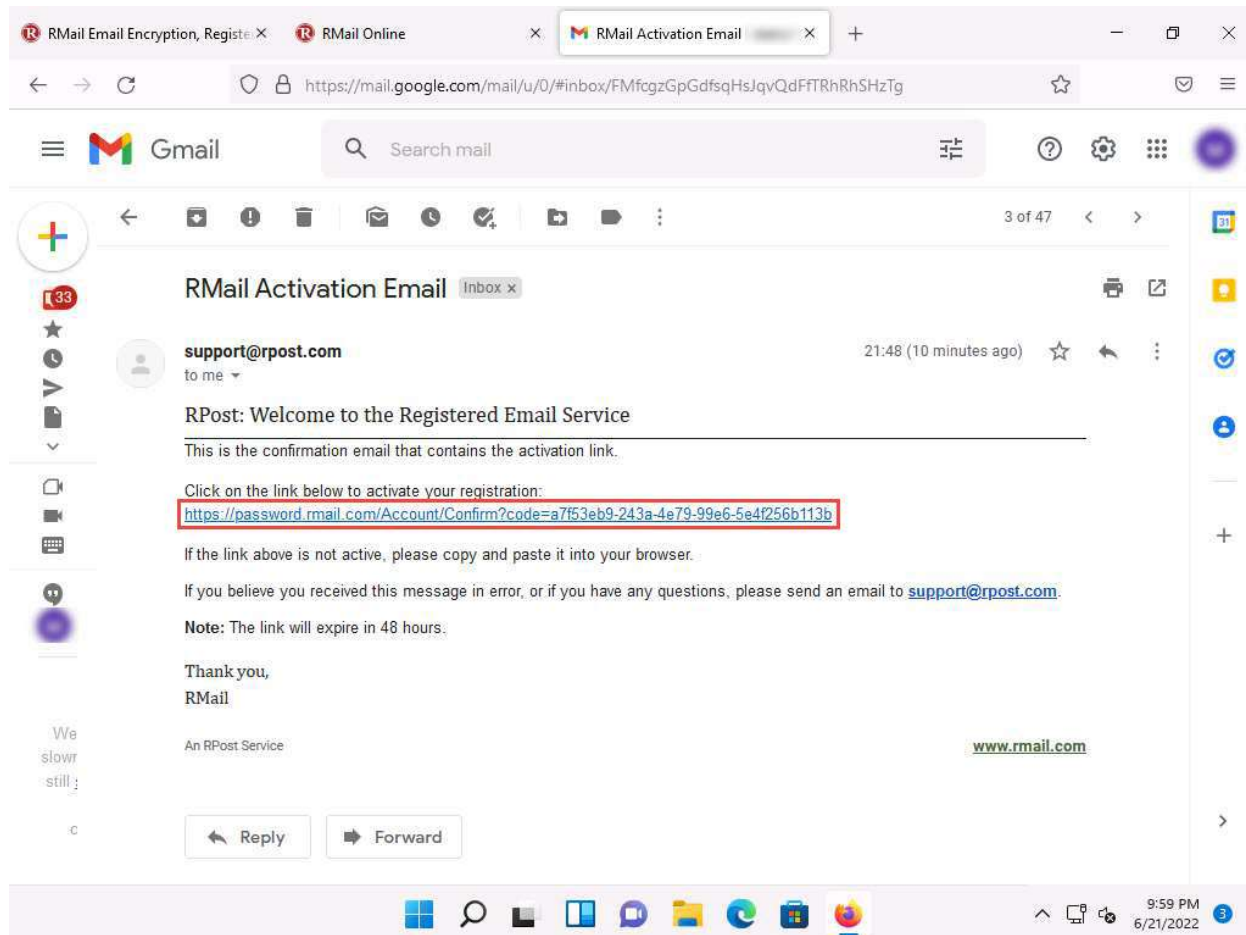
**Sign up**

Windows taskbar: 9:45 PM 6/21/2022

8. **Final step!** page appears displaying that the activation link has been sent to the registered email address.



9. Now, open a new tab in the browser and open the **Gmail** account which you have used to create the RMail account.
10. Open the email from **support@rpost.com** and click the activation link to activate the account.



11. **support.rpost.com** page appears, scroll down and click on **https://app.rmail.com/** link.

The screenshot shows a web browser window with multiple tabs. The active tab is titled "Onboarding Guide for RMail® Services". The address bar shows the URL <https://support.rpost.com/hc/en-us/articles/360046286514>. The page has a header with a cityscape image and a breadcrumb trail: "Help Center / RMail 101 / RMail Basics - What, Why & How". On the left, a sidebar menu under "RMail 101" includes "RMail Basics - What, Why & How" (expanded), "Onboarding Guide for RMail® Services" (selected), "How to add your own signature to any electronic document using RMail", "How to pick the right RMail Sending Application", "RMail for Beginners - FAQs", "Why do I need to use RMail?", and "RMail - Features at a glance". The main content area is titled "Onboarding Guide for RMail® Services" with a sub-header "Last updated on 04/13/2022". The content begins with "CONGRATULATIONS!" and "You are ready to start using RMail." It then states: "If you are using **RMail Online** you can now sign into the service from this link <https://app.rmail.com/>". Below this, it describes RMail features: "What's included in RMail? RMail is packed with powerful features to help you track, prove, encrypt, e-sign and send large files. You can see a quick overview of these features at the Features section on our website ([www.rmail.com/features](http://www.rmail.com/features))". It then mentions training videos and lists five features: "Track and Prove", "Encryption", "E-signatures and signing documents", "Include private notes on documents", and "Convert documents to PDFs while sending". The Windows taskbar at the bottom shows the time as 10:02 PM on 6/21/2022.

Help Center / RMail 101 / RMail Basics - What, Why & How

**RMail 101** ▼

- RMail Basics - What, Why & How ▼
  - Onboarding Guide for RMail® Services
  - How to add your own signature to any electronic document using RMail
  - How to pick the right RMail Sending Application
  - RMail for Beginners - FAQs
  - Why do I need to use RMail?
  - RMail - Features at a glance

## Onboarding Guide for RMail® Services

Last updated on 04/13/2022

### CONGRATULATIONS!

You are ready to start using RMail.

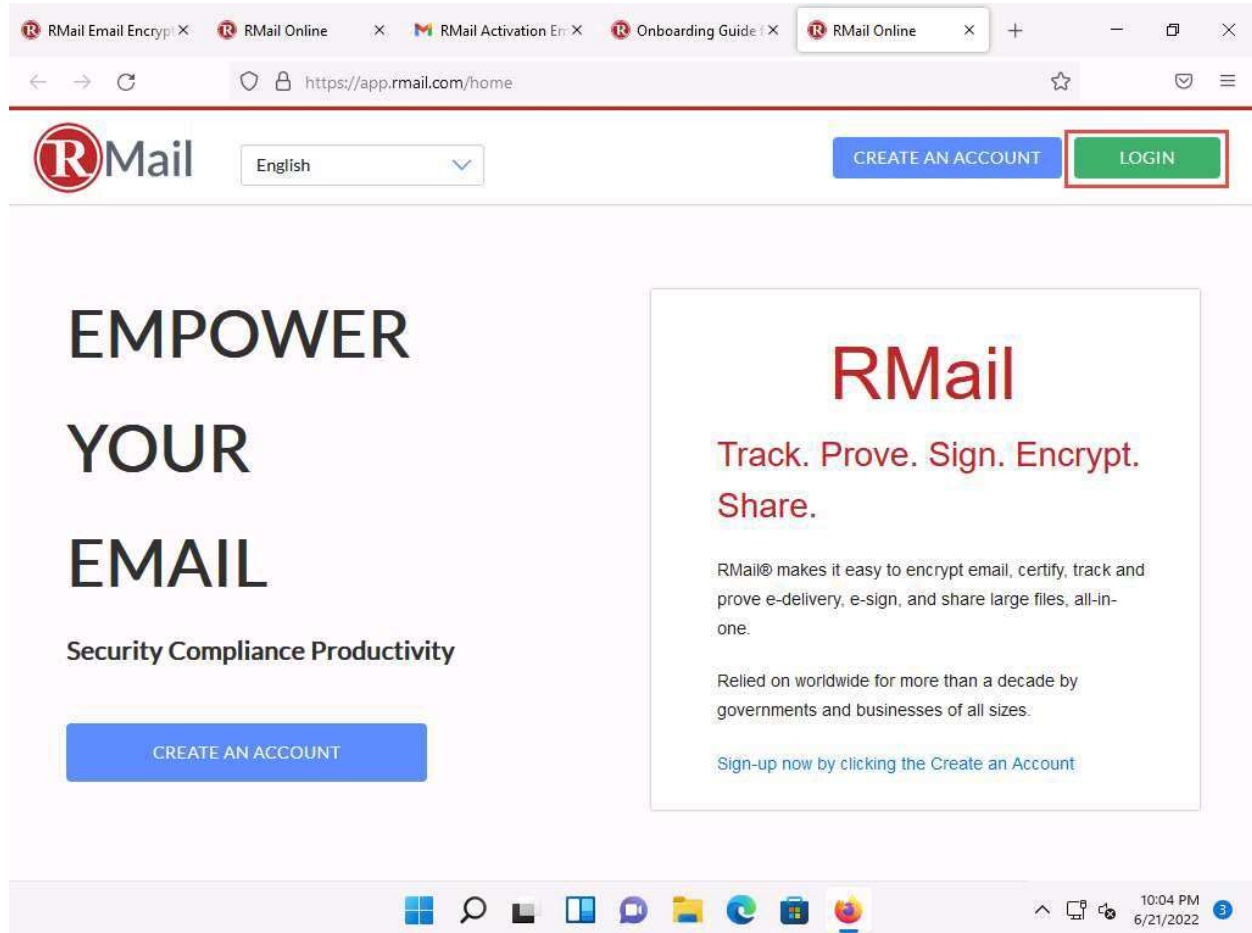
If you are using **RMail Online** you can now sign into the service from this link <https://app.rmail.com/>

What's included in RMail? RMail is packed with powerful features to help you track, prove, encrypt, e-sign and send large files. You can see a quick overview of these features at the Features section on our website ([www.rmail.com/features](http://www.rmail.com/features))

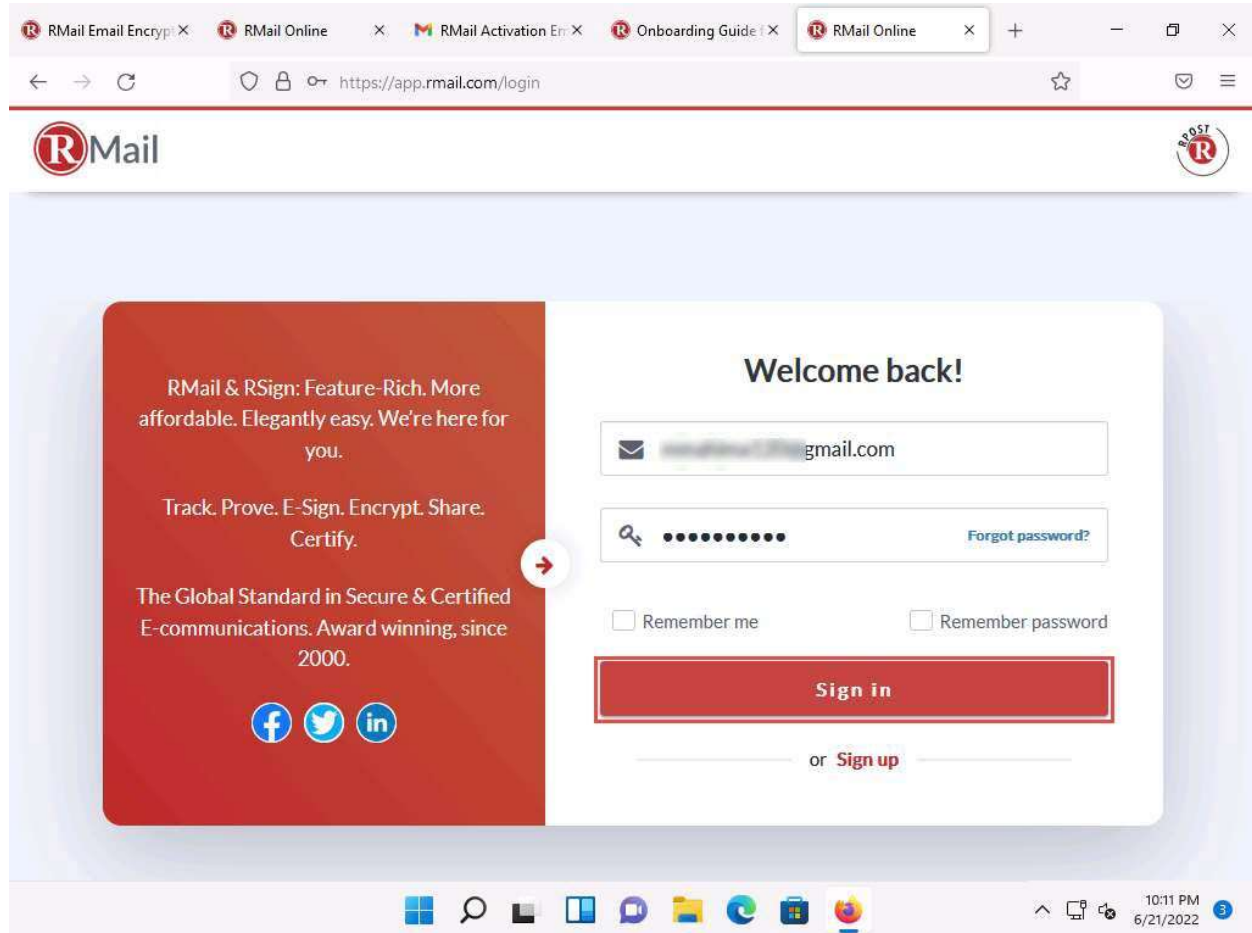
We have provided short training videos guides below which explain how to use each of the main features of RMail and the benefits of the service.

- Track and Prove
- Encryption
- E-signatures and signing documents
- Include private notes on documents
- Convert documents to PDFs while sending

12. The **app.rmail.com** page appears, click on **LOGIN** at the top right corner of the web page.



13. In the **Welcome back!** page, enter the email address and password that was used during registration and click on **Sign in**.



The screenshot shows a web browser window with the URL <https://app.rmail.com/login>. The page features the RMail logo in the top left and a 'POST R' logo in the top right. The main content area is divided into two sections. On the left, a red box contains the text: 'RMail & RSign: Feature-Rich. More affordable. Elegantly easy. We're here for you.', 'Track. Prove. E-Sign. Encrypt. Share. Certify.', and 'The Global Standard in Secure & Certified E-communications. Award winning, since 2000.' Below this text are icons for Facebook, Twitter, and LinkedIn. On the right, a white box titled 'Welcome back!' contains a login form. The form has two input fields: the first for an email address (partially filled with 'gmail.com') and the second for a password (masked with dots). A 'Forgot password?' link is located to the right of the password field. Below the input fields are two checkboxes: 'Remember me' and 'Remember password'. A large red 'Sign in' button is positioned below the checkboxes. At the bottom of the white box, there is a link 'or Sign up'. The browser's taskbar at the bottom shows various application icons and the system clock indicating 10:11 PM on 6/21/2022.

RMail & RSign: Feature-Rich. More affordable. Elegantly easy. We're here for you.

Track. Prove. E-Sign. Encrypt. Share. Certify.

The Global Standard in Secure & Certified E-communications. Award winning, since 2000.

Facebook Twitter LinkedIn

### Welcome back!

Email:

Password:  [Forgot password?](#)

☐ Remember me ☐ Remember password

**Sign in**

or [Sign up](#)

10:11 PM 6/21/2022

14. The RMail Online page appears, in the **To** field enter the recipient address. Ensure that **Marked as** is selected under **Track & Prove** section in the right-pane. Check the **Encrypt - select primary receiving experience** option and ensure that the **Transmission-auto-decrypts for receiver** radio button is selected. Ensure that **E-Sign - send for signature** check-box is checked, and **Web Sign** radio button is selected.

The screenshot displays the RMail Online web interface in a browser window. The address bar shows the URL <https://app.rmail.com/rmail>. The page header includes the RMail logo and the text "RMail Online". Below the header is a navigation bar with buttons for "SEND REGISTERED", "SAVE AS DRAFT", and "ATTACH FILE", along with an "Upgrade" link and "Units Remaining: 5".

The main composition area includes fields for "From:", "To:", "Cc:", "Bcc:", and "Subject:". The "To:" field contains a placeholder email address. To the right of the "From:" field is a "Copy Me" checkbox and a "more\_vert" link.

Below the address fields is a rich text editor with a toolbar containing options for font style (Sans Serif), font size (Normal), bold (B), italic (I), underline (U), link, text color, background color, bulleted list, numbered list, and indent. The editor area contains the placeholder text "Enter message here".

On the right side of the interface is a "Track & Prove" section with several options, each highlighted with a red box:

- Track & Prove**: A section header.
- Marked as**: A radio button option, currently selected.
- Unmarked**: A radio button option.
- Encrypt - select primary receiving experience**: A checkbox option, currently checked.
- Transmission - auto-decrypts for receiver**: A radio button option, currently selected.
- Message Level - decrypts with password**: A radio button option.
- Random password (click to)**: A button to generate a random password.
- Send Password**: A checkbox option.
- E-Sign - send for signature**: A checkbox option, currently checked. A link "RSign" is visible next to it.
- Web Sign**: A radio button option, currently selected.
- Email Sign**: A radio button option.

The Windows taskbar at the bottom shows the time as 10:16 PM on 6/21/2022.

15. After selecting the options, enter a message to be sent to the recipient, and click on **SEND REGISTERED** button.

The screenshot displays the RMail Online web application interface. At the top, there's a browser window with multiple tabs, including 'RMail Online'. The address bar shows 'https://app.rmail.com/rmail'. The RMail logo is on the left, and 'RMail Online' is centered. On the right, there's a 'POST' icon and a 'Units Remaining: 5' indicator.

The main interface has a dark header bar with three buttons: 'SEND REGISTERED' (red), 'SAVE AS DRAFT' (green), and 'ATTACH FILE' (green). To the right of these buttons are links for 'Upgrade' and 'Units Remaining: 5'.

The email composition form includes fields for 'From:', 'To:', 'Cc:', 'Bcc:', and 'Subject:'. The 'From:' field is pre-filled with a redacted email address. The 'To:' field is also pre-filled with a redacted email address. The 'Subject:' field contains the text 'Business Strategy model'. There is a 'Copy Me' checkbox and a 'more\_vert' link next to the 'From:' field.

Below the form fields is a rich text editor with a toolbar containing options for font face (Sans Serif), font size (Normal), bold (B), italic (I), underline (U), link (G), text color (A), background color, bulleted list, numbered list, indent, link, and image. The text area contains the message: 'Hi, I have completed the Business Strategy Model, enclosing the same. Please provide your feedback.'

On the right side, there's a sidebar with several sections:

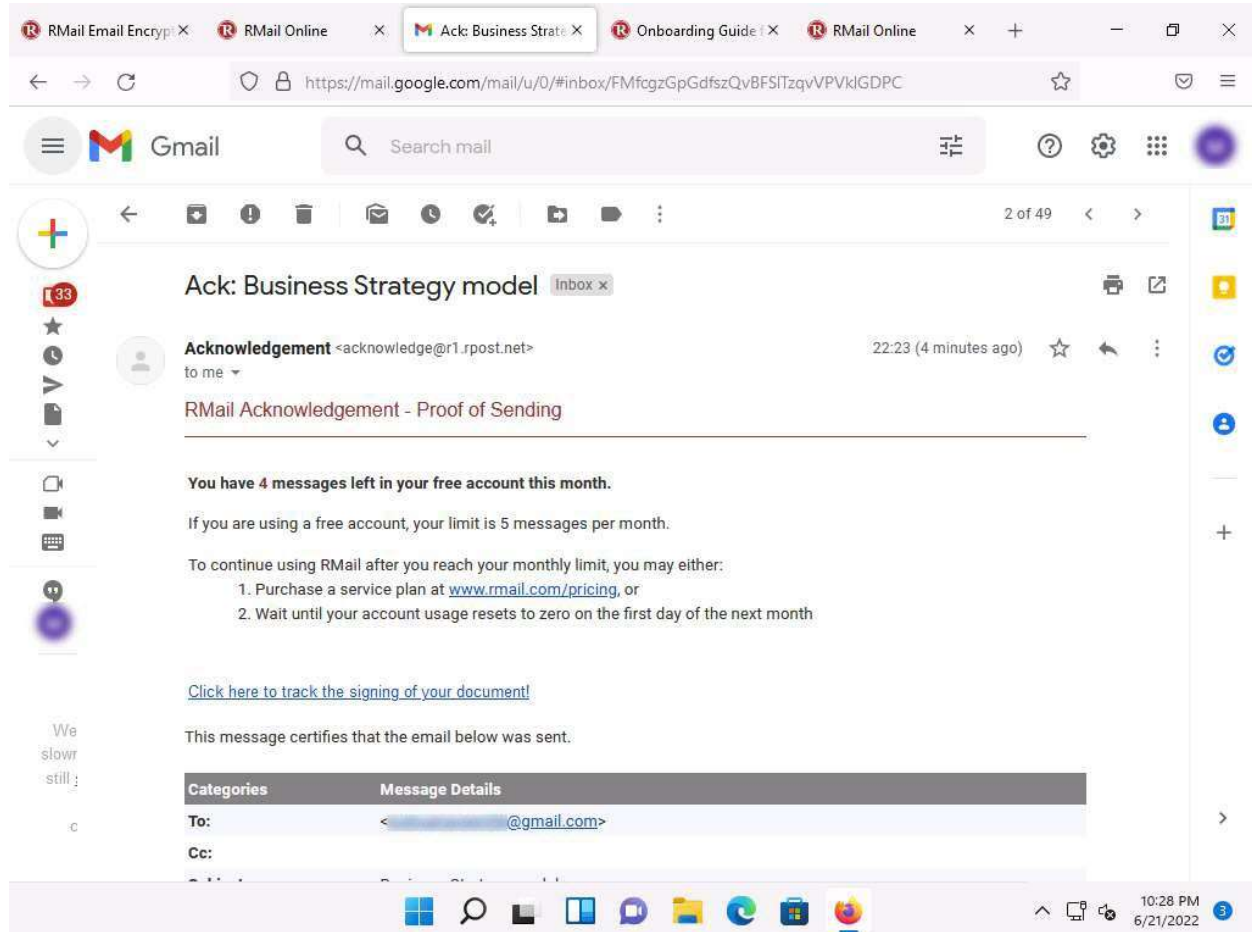
- Track & Prove**: Includes radio buttons for 'Marked as' (selected) and 'Unmarked'.
- Encrypt - select primary receiving experience**: Includes a checked checkbox and options for 'Transmission - auto-decrypts for receiver' (selected) and 'Message Level - decrypts with password' (unselected).
- Random password (click to)**: A button to generate a random password, with a 'Send Password' checkbox.
- E-Sign - send for signature**: Includes a checked checkbox and a link to 'RSign'.
- Web Sign**: Includes a radio button.
- Email Sign**: Includes a radio button.

The bottom of the screen shows a Windows taskbar with various application icons and a system clock indicating 10:21 PM on 6/21/2022.

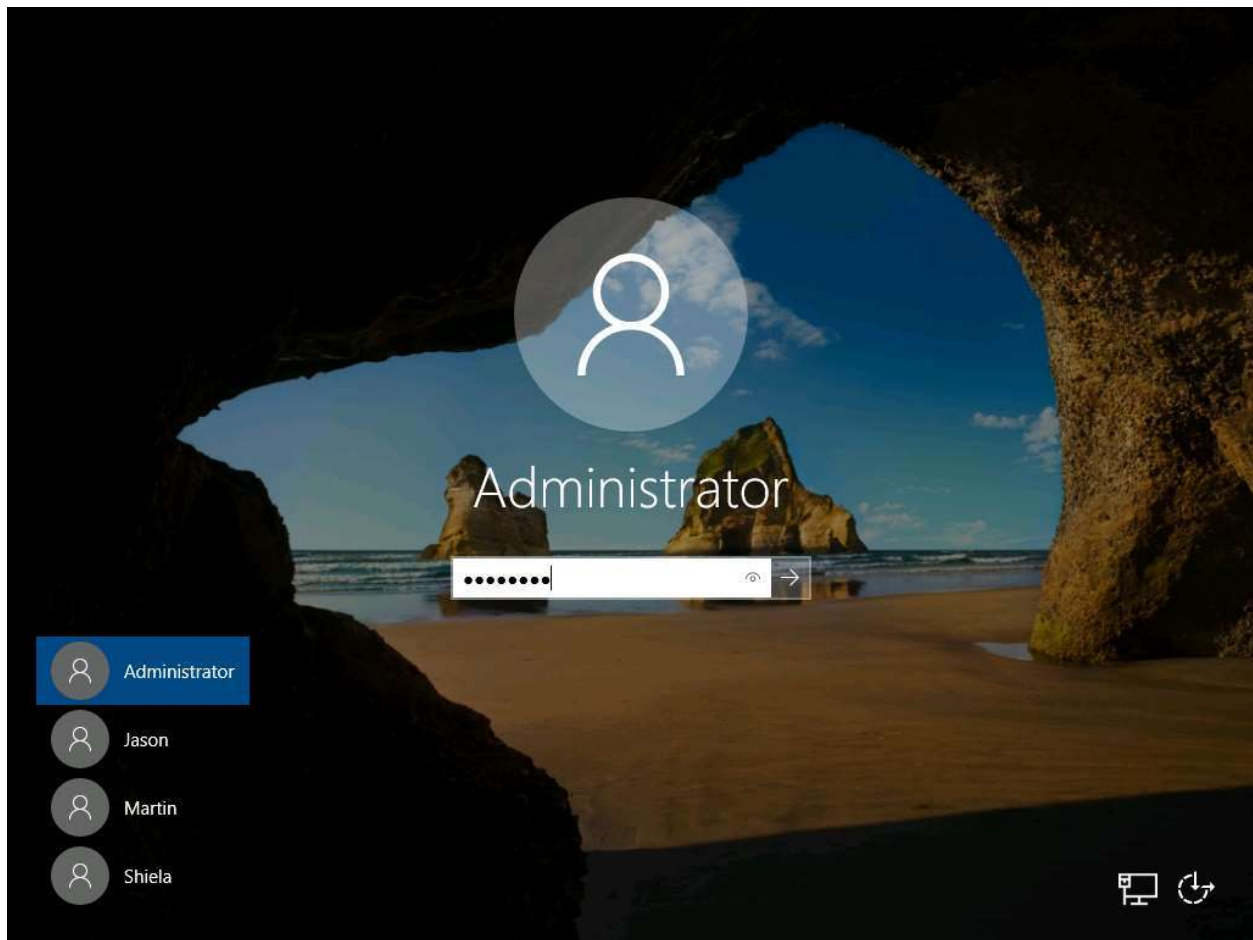


16. Upon clicking **SEND REGISTERED** button, **Email Sent** pop-up appears.

17. Now, navigate to the tab in which Gmail account that was opened previously, you can observe an **Acknowledgement** email with **Proof of Sending**.



18. In this task, for the purpose of demonstration, we will open the recipient's account and view the email.
19. To do so, click on [Windows Server 2019](#) to switch to the **Windows Server 2019**, click [Ctrl+Alt+Delete](#) to activate the machine. By default, **Administrator** profile is selected, click on Pa\$\$w0rd to enter password in the password field and press **Enter** to login.

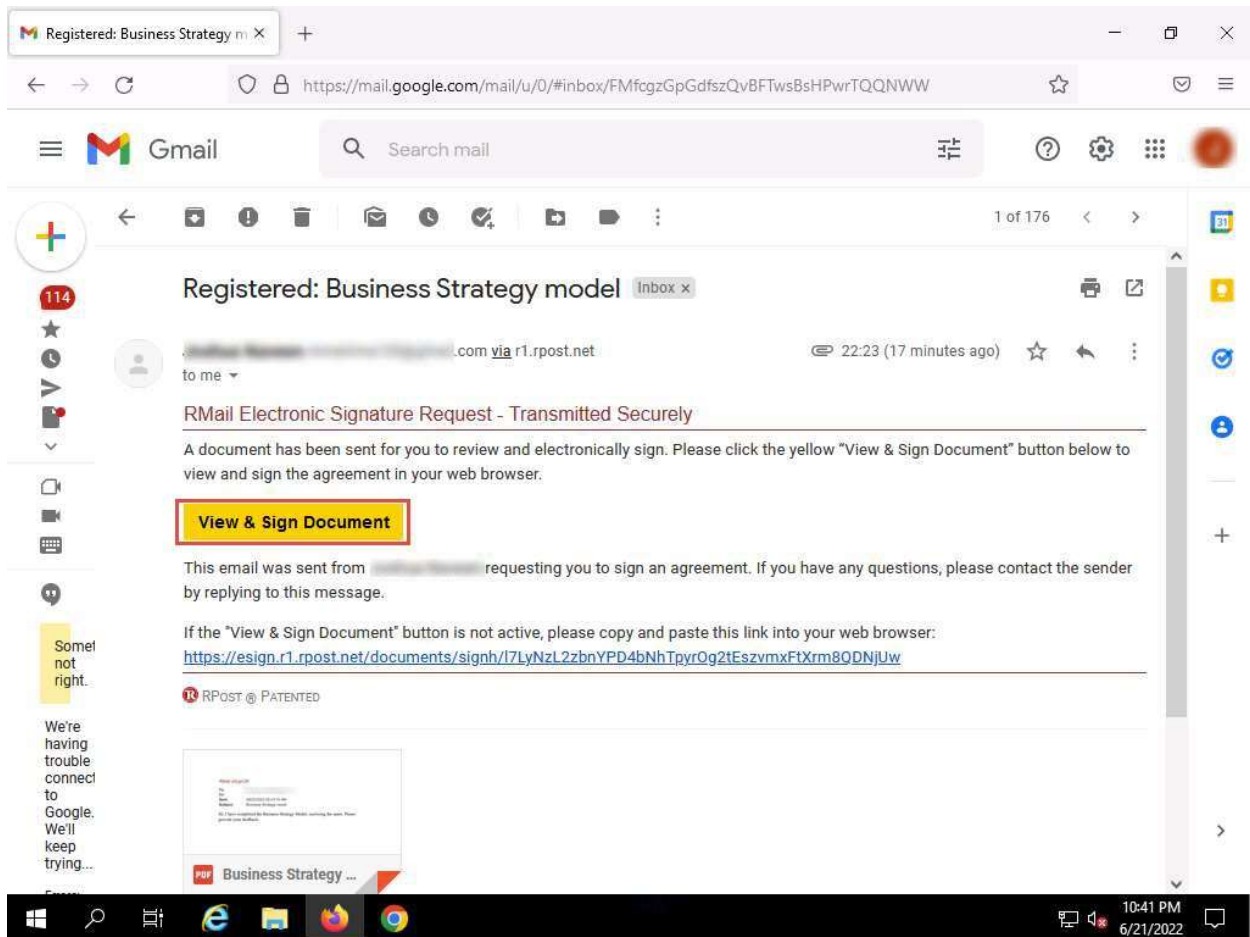


20. Open any web browser (here, **Mozilla Firefox**) and log in to the **Gmail** account of the recipient. Open the email from the sender.

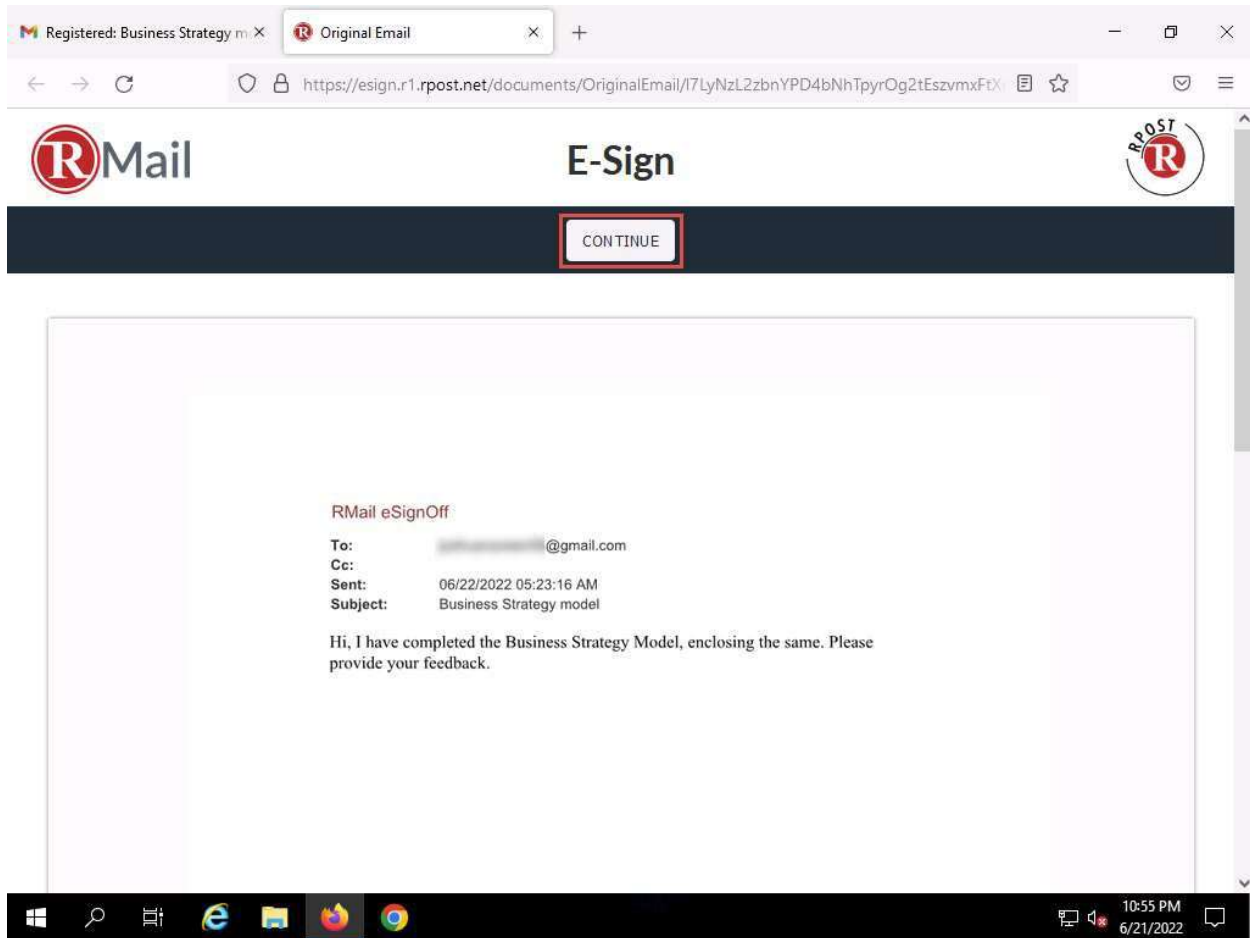
21. You can observe that the email received is tagged as a registered email wherein a document has been sent for the recipient to review and electronically sign to confirm his/her identity.

You might receive an email in the spam folder.

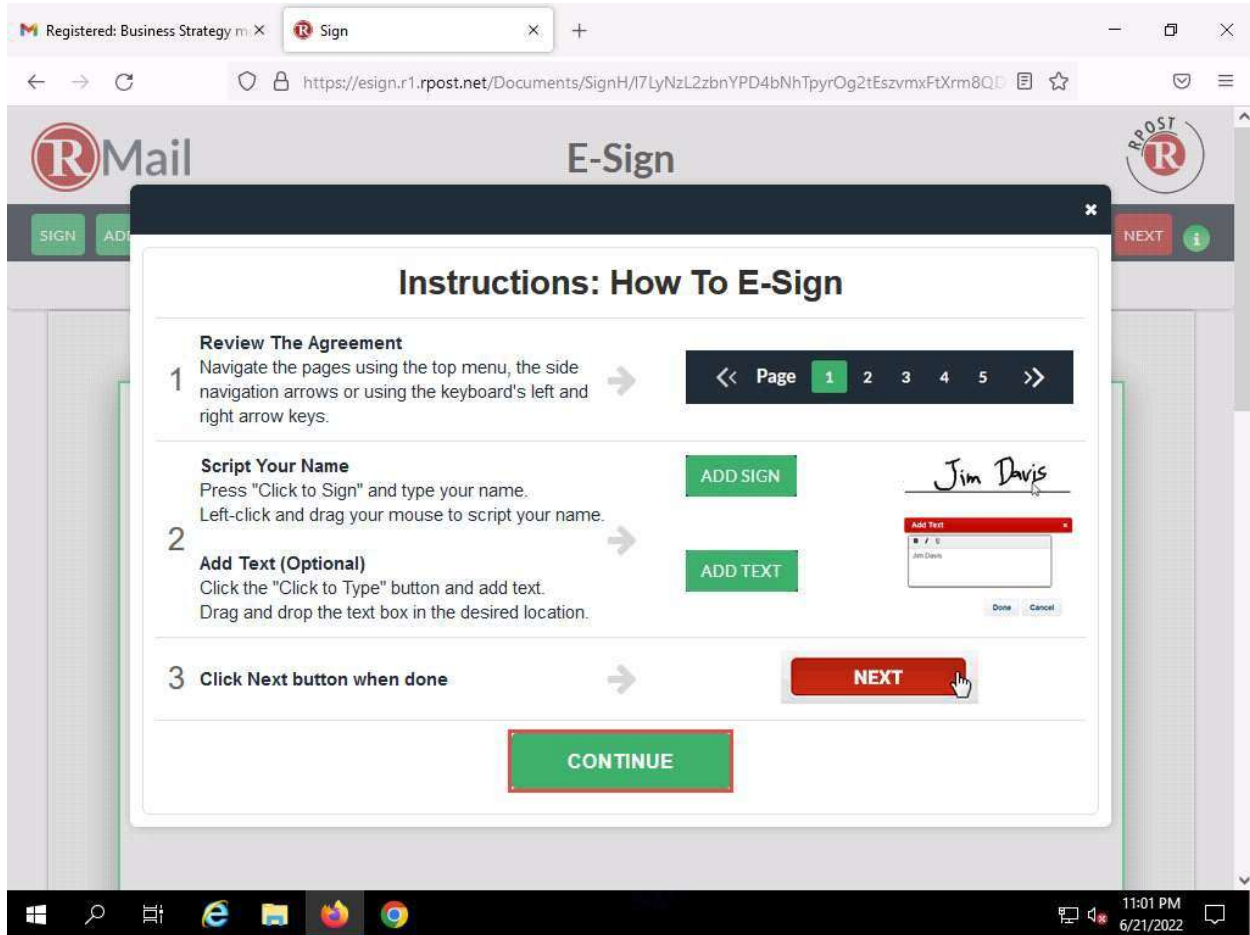
22. Click the **View & Sign Document** button to sign an agreement.



23. A new **E-Sign** webpage appears displaying the email content; click **CONTINUE**.




24. The **Instructions: How To E-Sign** page appears; read the instructions carefully and click **CONTINUE**.




25. After viewing the email content, click **NEXT**.

Registered: Business Strategy m...Sign

https://esign.r1.rpost.net/Documents/SignH/17LyNzL2zbnYPD4bNhTpyrOg2tEszvmxFTXrm8QID

RMail

E-Sign



SIGNADD TEXTCLEAR DOCUMENTVIEW PDFDECLINENEXT

<<Page 1>>Session Timeout: 20 Minutes

RMail eSignOff


To: [REDACTED]@gmail.com

Cc:

Sent: 06/22/2022 05:23:16 AM

Subject: Business Strategy model

Hi, I have completed the Business Strategy Model, enclosing the same. Please provide your feedback.



11:02 PM  
6/21/2022

26. The **Final Step - Please Complete the Information Below** page appears with the **Document Signature** form. In the **Please enter your name** field, enter your name (Recipient's name) and leave the **Initials** and **Title** field as blank and click the **Click to Sign** button.

The screenshot shows a web browser window with two tabs: 'Registered: Business Strategy m...' and 'Final Signature'. The address bar shows the URL: <https://esign.r1.rpost.net/documents/finalsig/17LyNzL2zbnYPD4bNhTpyrOg2tEszvmxFtXrm8Q>. The main content area displays the 'Document Signature' form. The form has a title 'Document Signature' with a pencil icon. Below the title is the instruction 'Please enter your name\*'. There are two text input fields for the name, both containing the placeholder text 'John Doe'. Below these are two optional fields: 'Initials (optional)' and 'Title (optional)', both of which are empty. A prominent red button labeled 'Click to Sign' is positioned below the optional fields. At the bottom of the form, there is a consent statement: 'I agree with the content of the e-mail, the contract and any attachment(s) and I further agree to use electronic signature and sign here.' The browser's taskbar at the bottom shows the Windows logo, search icon, and several application icons. The system clock in the bottom right corner indicates the time is 11:04 PM on 6/21/2022.

**Document Signature**

Please enter your name\*

John Doe

John Doe

Initials (optional)

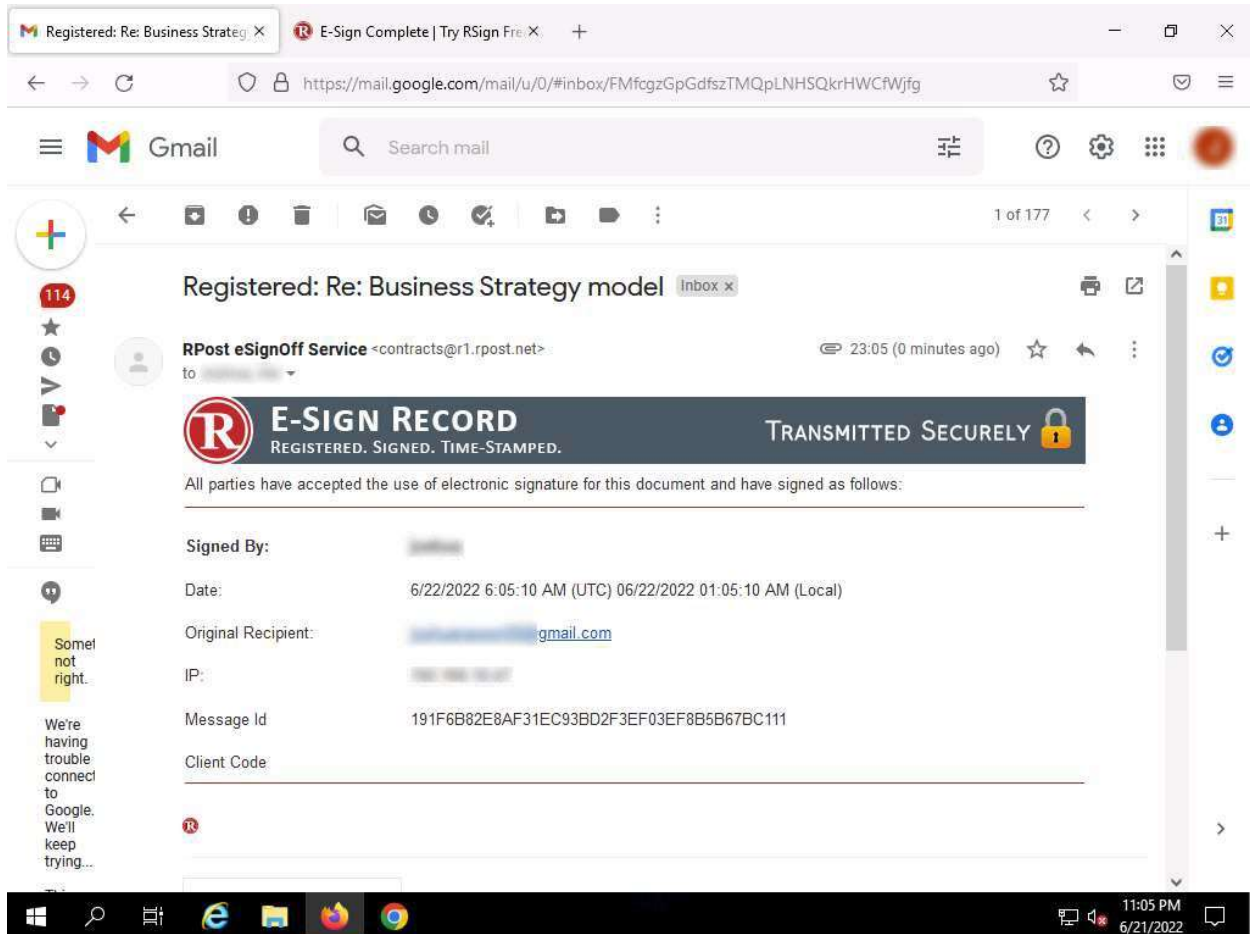
Title (optional)

**Click to Sign**

I agree with the content of the e-mail, the contract and any attachment(s) and I further agree to use electronic signature and sign here.

27. The **YOU'RE ALL DONE!** page appears; close the current tab to return to the opened email. Click **Inbox** from the left-hand pane to navigate to the inbox.

28. Open an email from **RPost eSignOff Service**. You can observe that it is an acknowledgment email from RPost along with various details such as **Signed By**, **Date**, **Time**, **Original Recipient**, **IP**, **Message Id**, etc.





29. Now, click on [Windows 11](#) to return to the **Windows 11** machine, where the sender's account is opened. In **Inbox**, you can observe two emails (**Receipt** and **RPost eSignOff Service**). Click to open the **Receipt** email.

You might receive a **Receipt** mail in the **RMail Receipts** inbox folder present in the left-hand pane.

30. The **Receipt** email contains information about the **Delivery Status**, **Message Envelope**, and **Message Statistics** of the sent email, as shown in the screenshot.

31. The **Receipt** email also includes the **DeliveryReceipt** and **HtmlReceipt** attachments containing detailed information regarding the sent email.

The screenshot shows a Gmail interface with a 'REGISTERED RECEIPT' email from RMail. The email content includes a delivery status table and a message envelope section.

**REGISTERED RECEIPT**  
EVIDENCE OF DELIVERY, CONTENT & TIME

This receipt contains verifiable proof of your RPost transaction.  
The holder of this receipt has proof of delivery, message and attachment content, and official time of sending and receipt. Depending on services selected, the holder also may have proof of encrypted transmission and/or electronic signature.

To authenticate this receipt, forward this email with its attachment to '[verify@r1.rpost.net](#)' or [click here](#)

[Click here to track the signing of your document!](#)

Delivery Status					
Address	Status	Details	Delivered (UTC*)	Delivered (local)	Opened (local)
<a href="#">[redacted]@gmail.com</a>	Delivered and Opened	HTTP- [redacted] [lock icon]	06/22/2022 05:23:25 AM (UTC)	06/22/2022 12:23:25 AM (UTC-05:00)	06/22/2022 12:41:23 AM (UTC-05:00)

\*UTC represents Coordinated Universal Time: <https://www.rmail.com/resources/coordinated-universal-time/>

Message Envelope	
From:	<a href="#">[redacted]@gmail.com</a>
Subject:	Business Strategy model
To:	<a href="#">[redacted]@gmail.com</a>
Cc:	

32. Now, navigate back to the **Inbox** and open an email from **RPost eSignOff Service**. This email contains the same information as the email received from **RPost eSignOff Service** by the recipient.
33. This concludes the demonstration of performing email encryption using RMail.
34. You can also use other email encryption tools such as **Virtru** (<https://www.virtru.com>), **ZixMail** (<https://www.zixcorp.com>), **Egress Secure Email and File Transfer** (<https://www.egress.com>), and **Proofpoint Email Protection** (<https://www.proofpoint.com>) to perform email encryption.
35. Close all open windows and document all the acquired information.

#### **Question 20.3.1.1**

Use RMail to encrypt email messages. Which option is selected in the Apps page to encrypt emails.

13 Minutes Remaining

## [Exit Lab](#)

### **InstructionsResources**

#### **Lab 4: Perform Disk Encryption**

##### **Lab Scenario**

Disk encryption is a technology that protects the confidentiality of the data stored on a disk by converting it into an unreadable code using disk encryption software or hardware, thus preventing unauthorized users from accessing it. Disk encryption provides confidentiality and privacy using passphrases and hidden volumes. As a professional ethical hacker or pen tester, you should perform disk encryption in order to prevent sensitive information from unauthorized access.

Disk encryption works in a manner similar to text-message encryption and protects data even when the OS is not active. By using an encryption program for the user's disk (Blue Ray, DVD, USB flash drive, External HDD, and Backup), the user can safeguard any or all information burned onto the disk and thus prevent it from falling into the wrong hands. Disk-encryption software scrambles the information burned on the disk into an illegible code. It is only after decryption of the disk information that one can read and use it.

This lab will demonstrate the use of various disk encryption tools to perform this technique.

##### **Lab Objectives**

- Perform disk encryption using VeraCrypt
- Perform disk encryption using BitLocker Drive Encryption
- Perform disk encryption using Rohos Disk Encryption


##### **Overview of Disk Encryption**

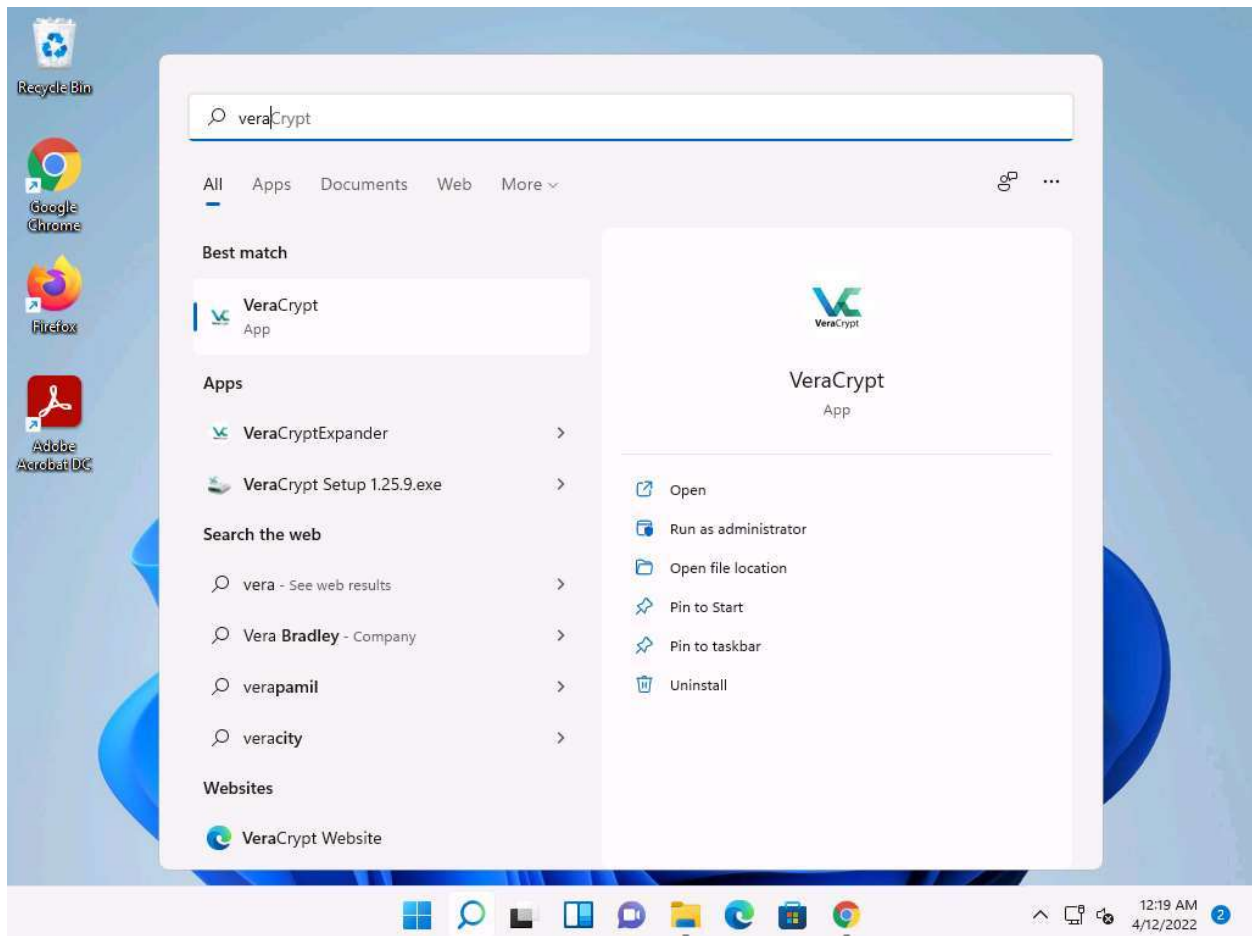
Disk encryption is useful when the user needs to send sensitive information through email. In addition, disk encryption can prevent the real-time exchange of information from threats. When users exchange encrypted information, it minimizes the chances of compromising the data; the only way an attacker could access the information is by decrypting the message. Furthermore, encryption software installed on a user's system ensures the security of the system. Install encryption software on any systems that hold valuable information or on those exposed to unlimited data transfer.

## Task 1: Perform Disk Encryption using VeraCrypt

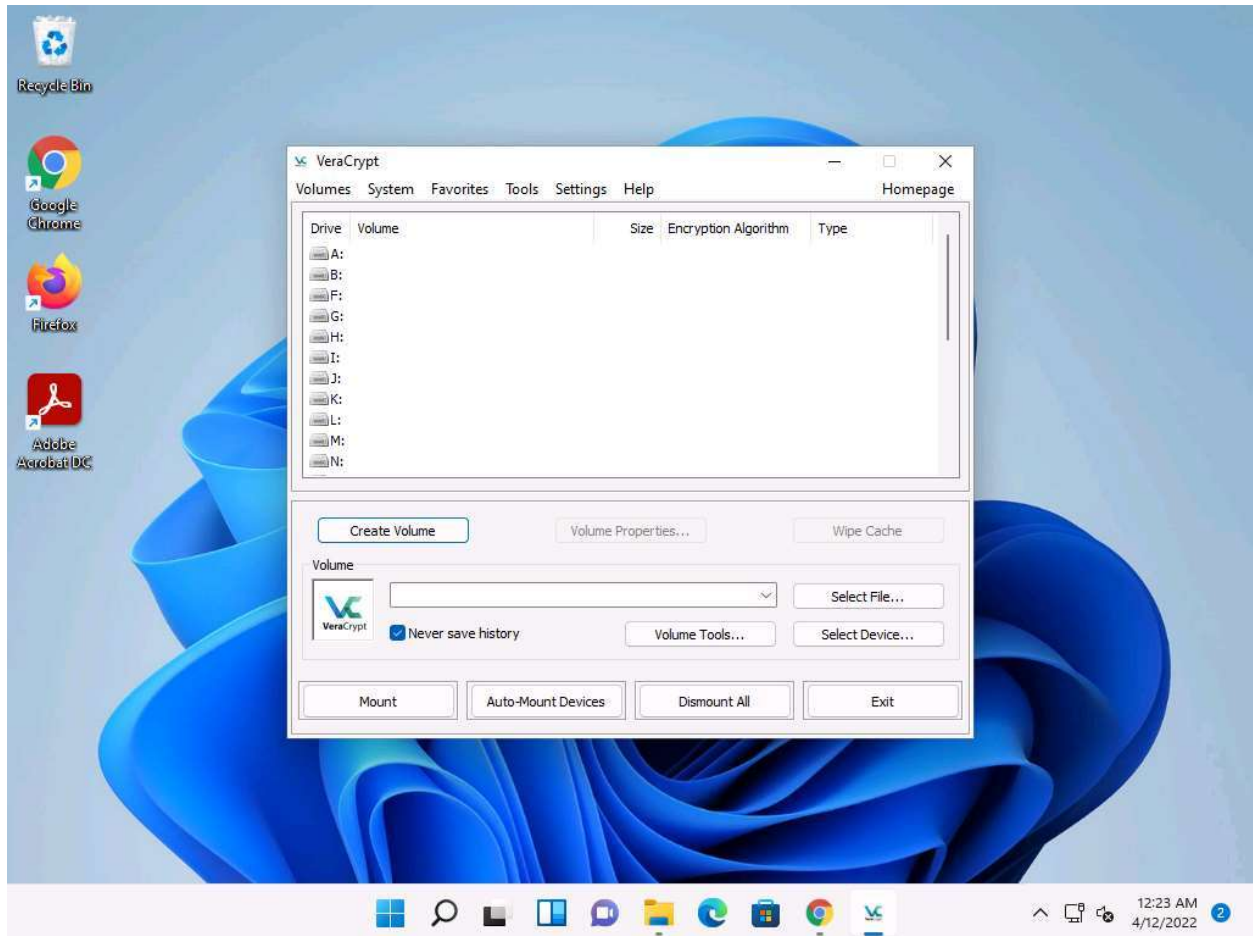
VeraCrypt is a software used for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted just before it is saved, and decrypted just after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without using the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, free space, metadata, etc.).

Here, we will use the VeraCrypt tool to perform disk encryption.

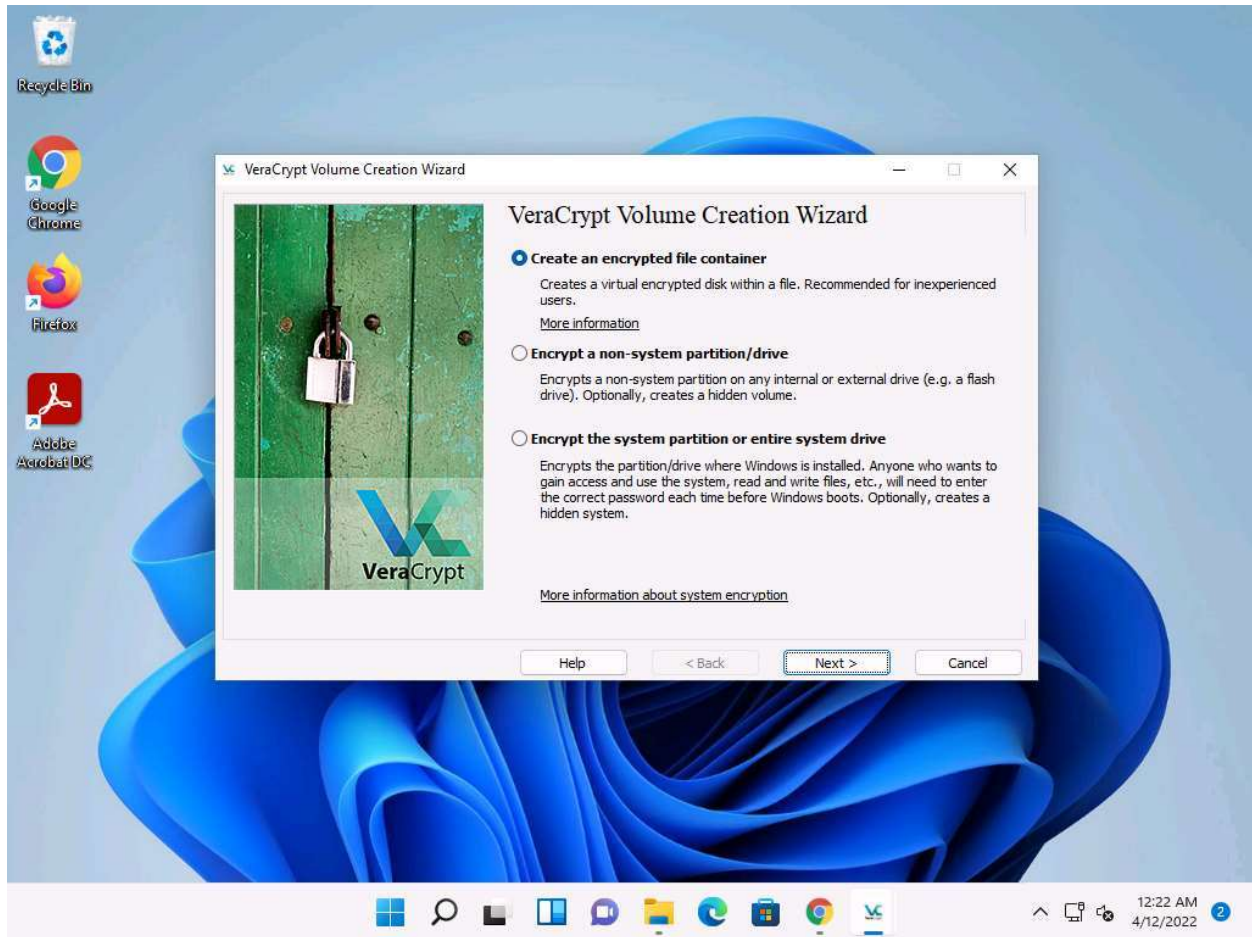
1. Click [Windows 11](#) to switch to the **Windows 11** machine.
2. Click **Search** icon (  ) on the **Desktop**. Type **vera** in the search field, the **VeraCrypt** appears in the results, click **Open** to launch it.



3. The **VeraCrypt** main window appears; click the **Create Volume** button.

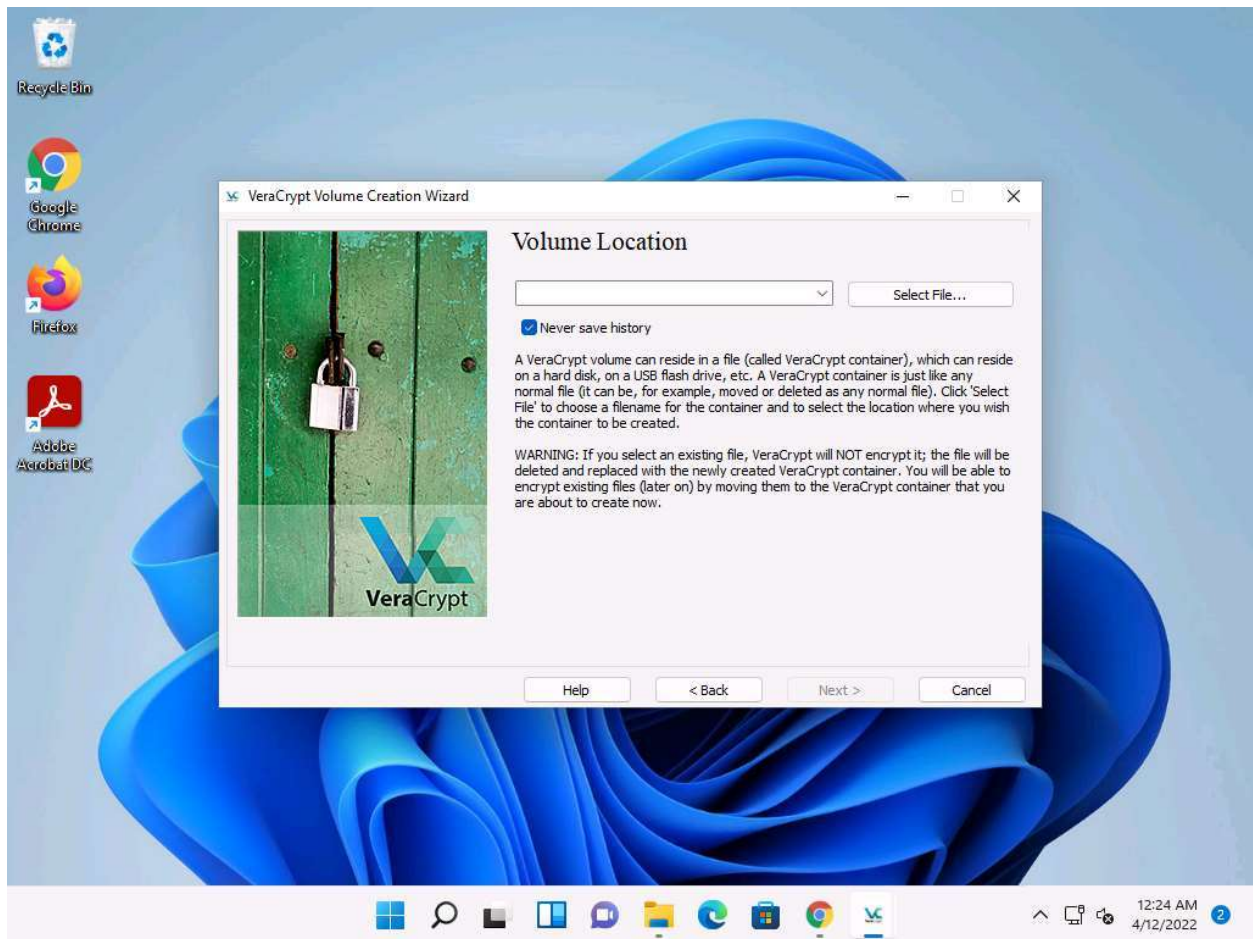


4. The **VeraCrypt Volume Creation Wizard** window appears. Ensure that the **Create an encrypted file container** radio-button is selected and click **Next** to proceed.

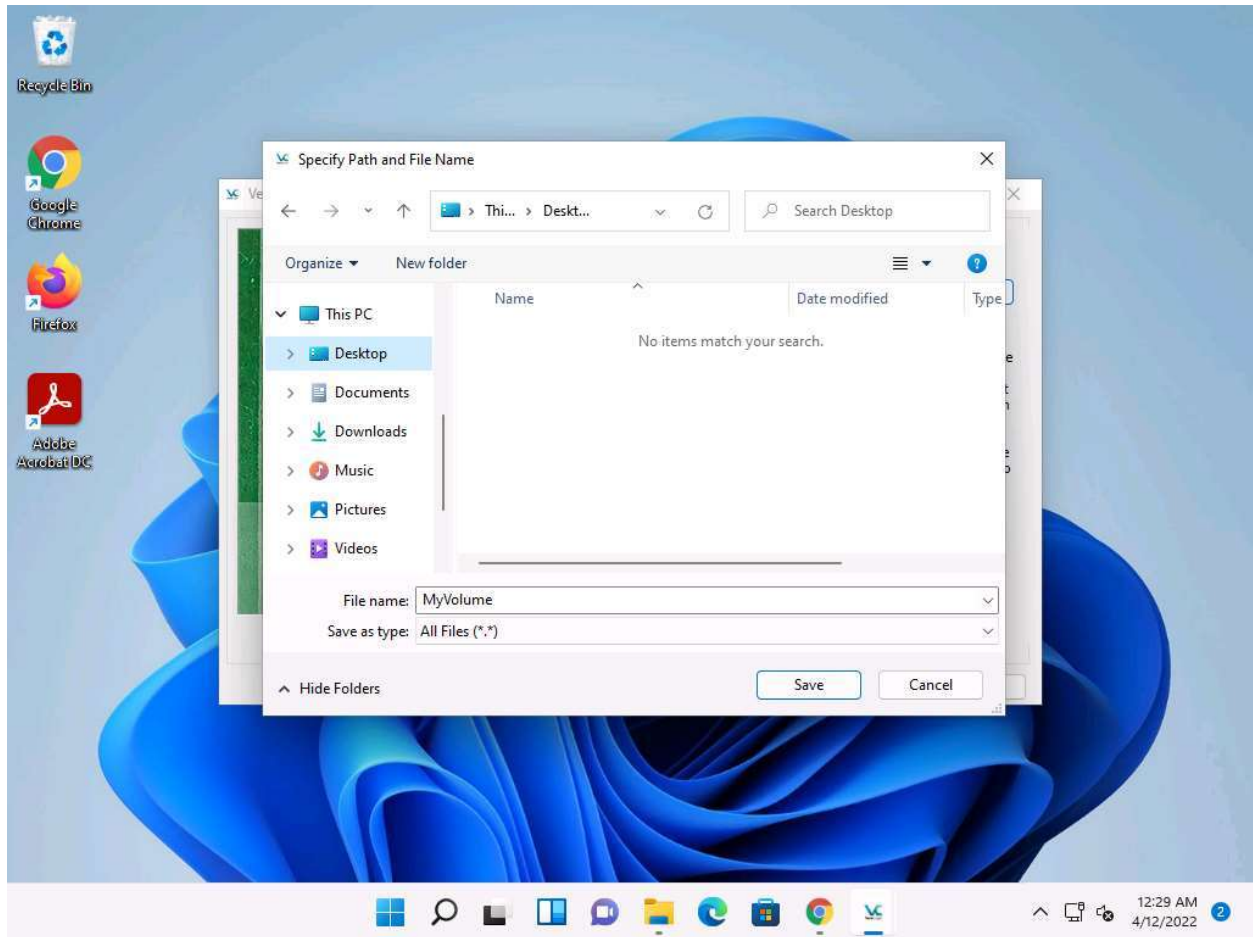




5. In the **Volume Type** wizard, keep the default settings and click **Next**.
6. In the **Volume Location** wizard, click **Select File....**

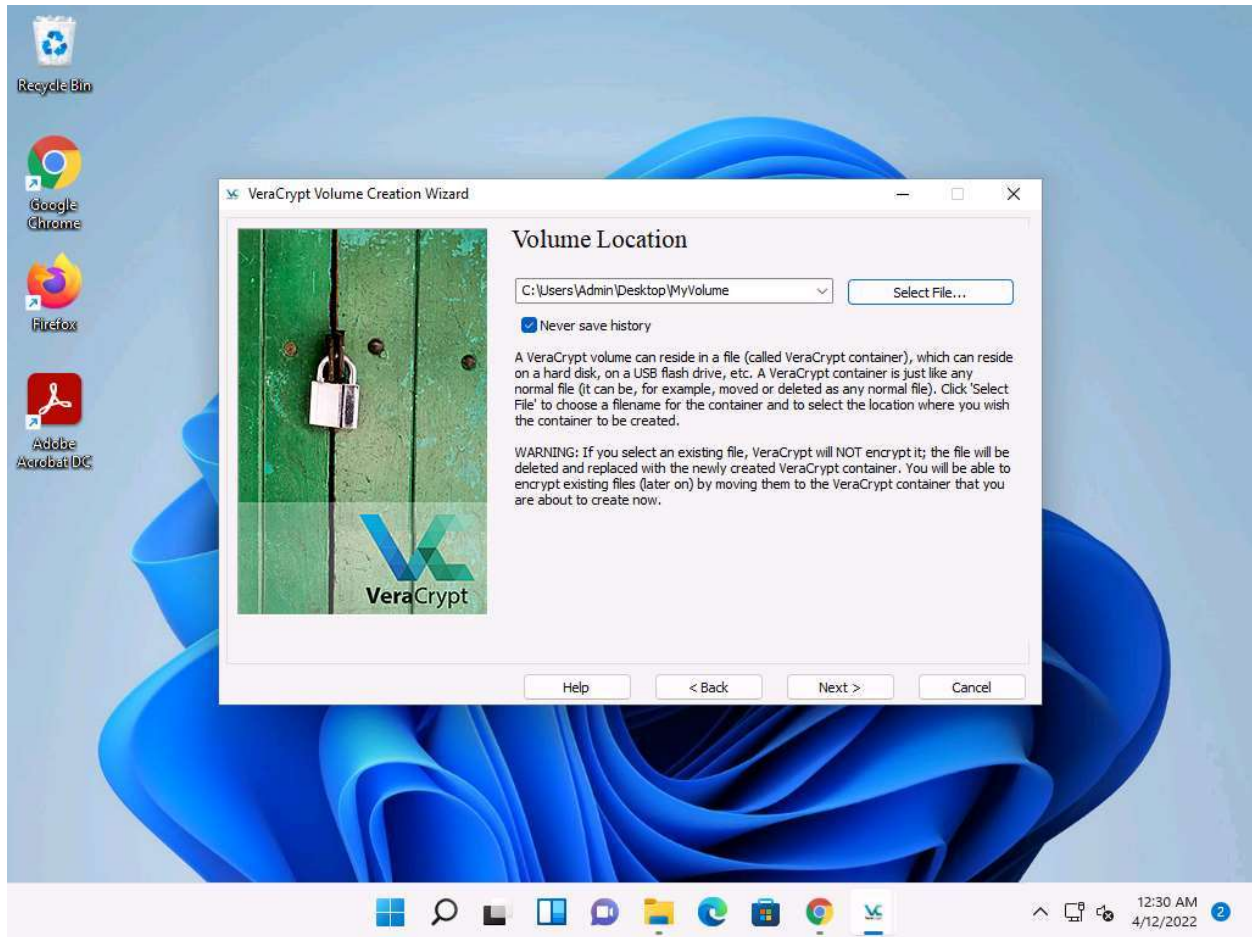


7. The **Specify Path and File Name** window appears; navigate to the desired location (here, **Desktop**), provide the **File name** as **MyVolume**, and click **Save**.



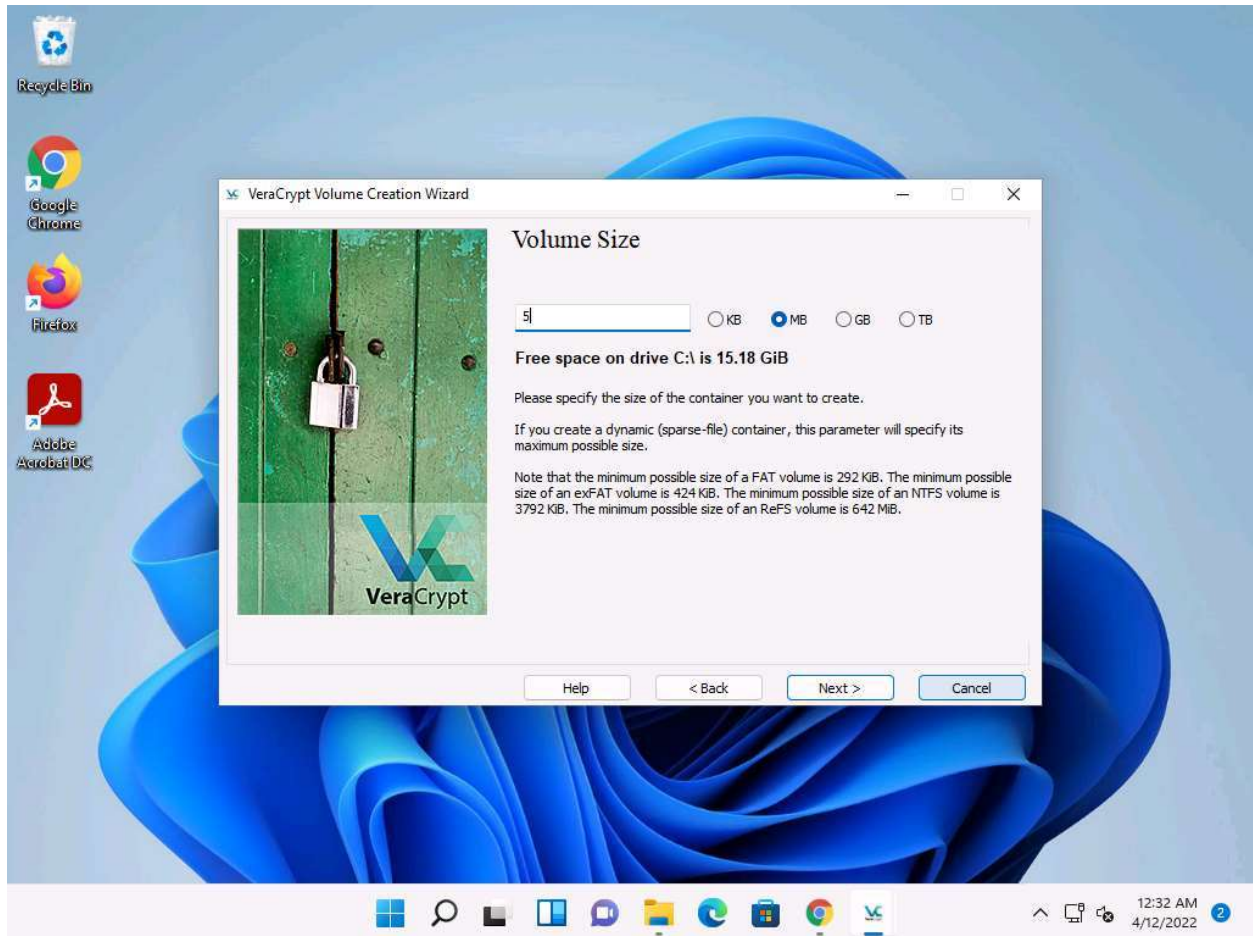


8. After saving the file, the location of a file containing the **VeraCrypt** volume appears under the **Volume Location** field; then, click **Next**.

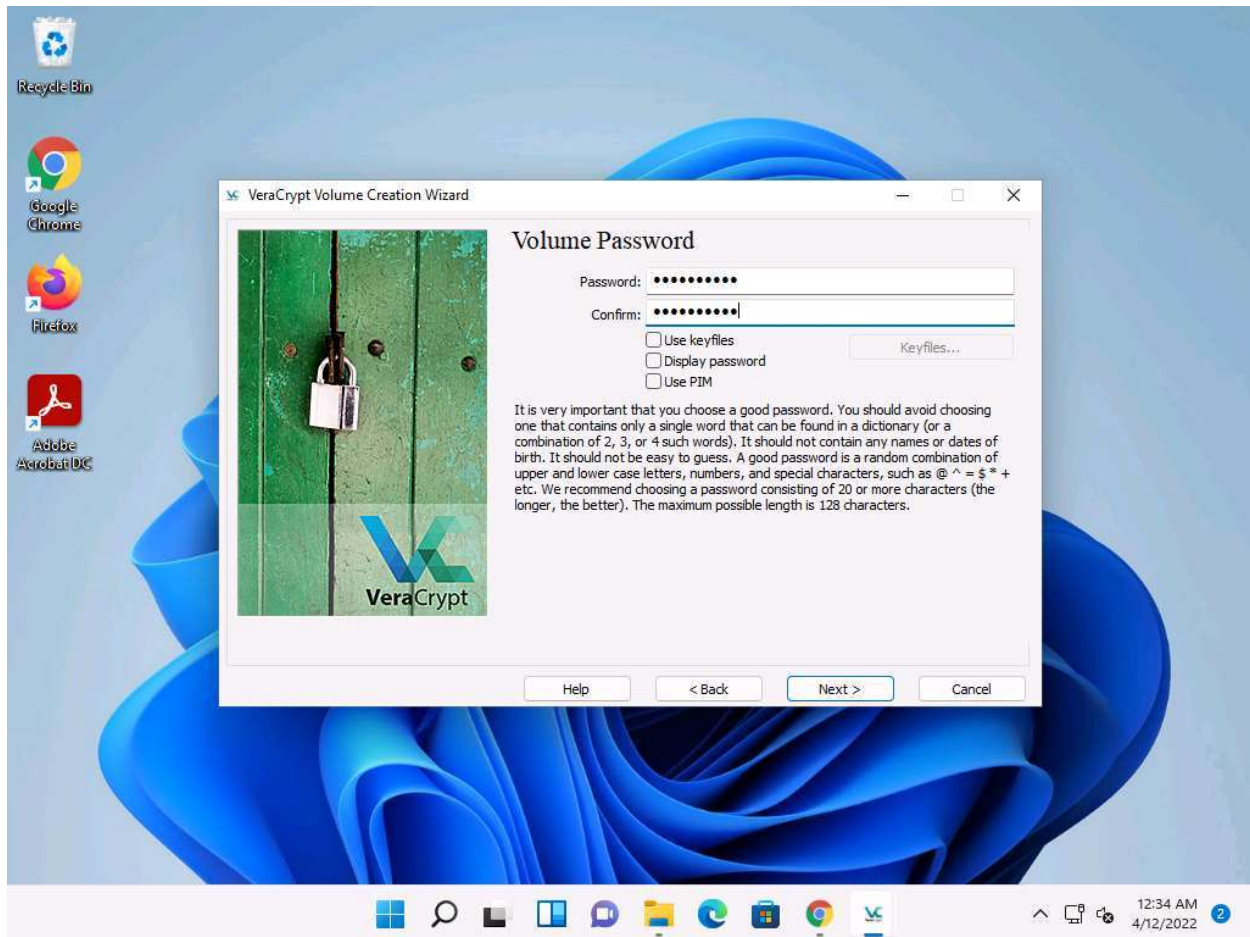


9. In the **Encryption Options** wizard, keep the default settings and click **Next**.

10. In the **Volume Size** wizard, ensure that the **MB** radio-button is selected and specify the size of the VeraCrypt container as **5**; then, click **Next**.



11. The **Volume Password** wizard appears; provide a strong password in the **Password** field, retype in the **Confirm** field, and click **Next**. The password provided in this lab is **qwerty@123**.

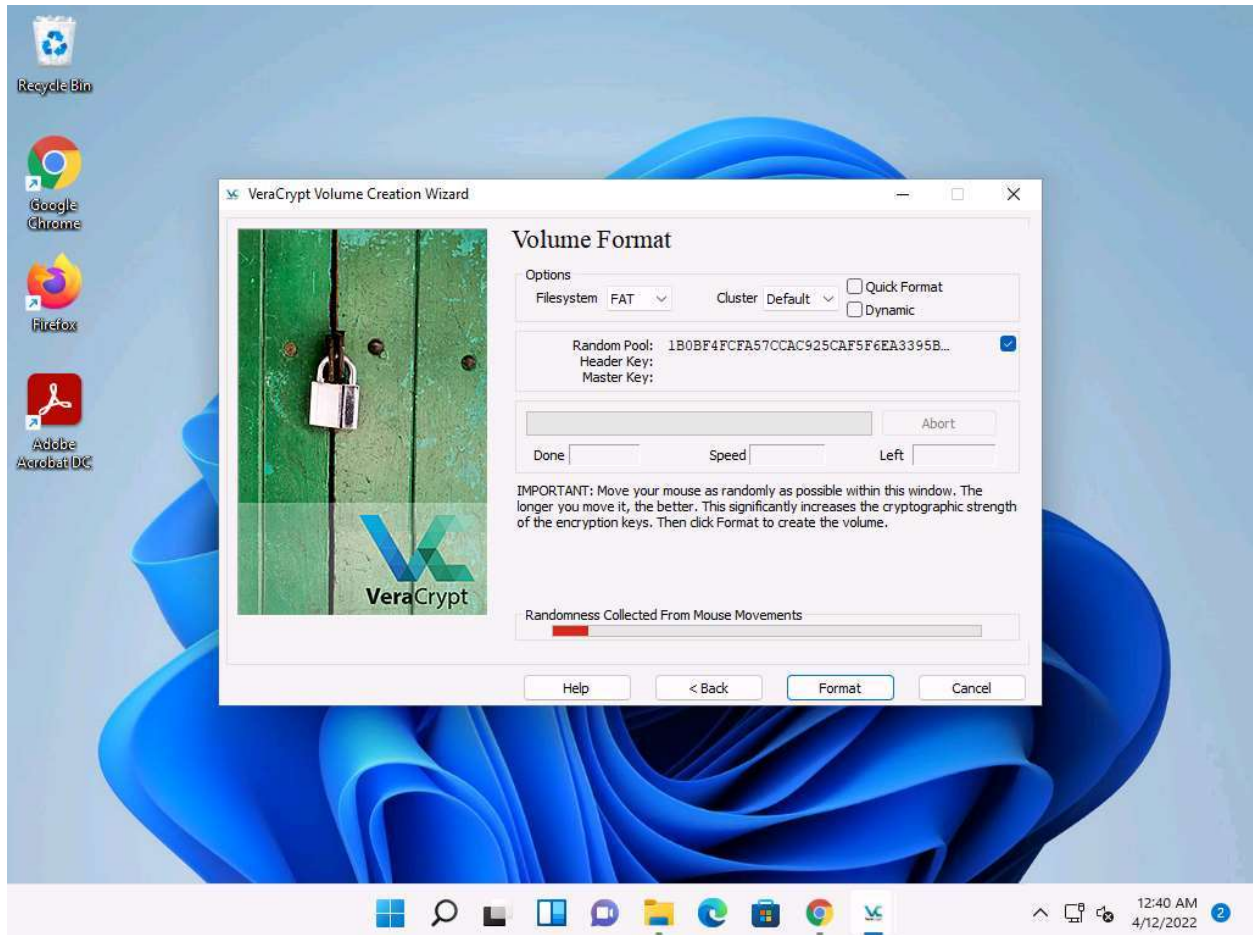


A **VeraCrypt Volume Creation Wizard** warning pop-up appears; then, click **Yes**.

12. The **Volume Format** wizard appears; ensure that **FAT** is selected in the **Filesystem** option and **Default** is selected in **Cluster** option.

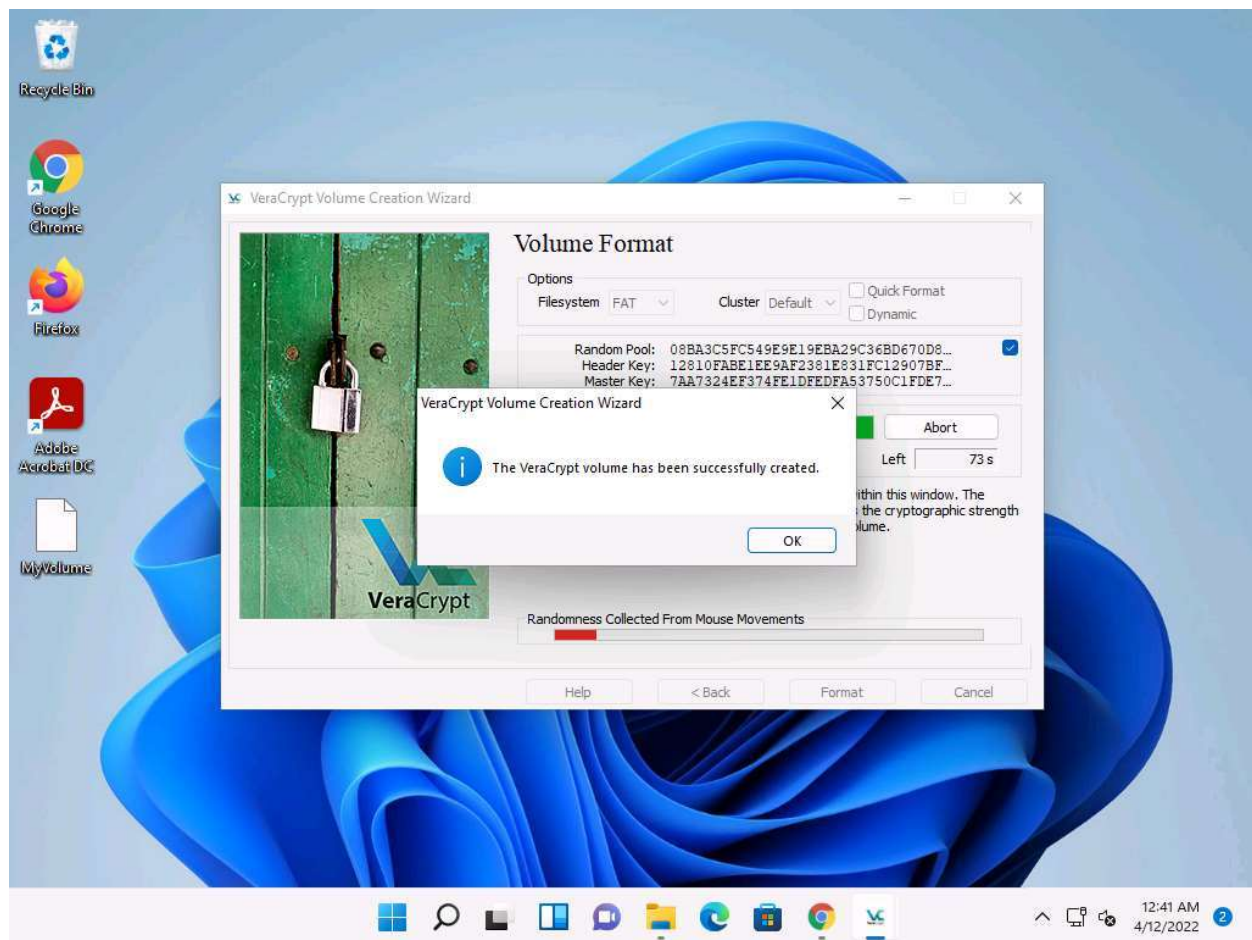
13. Check the checkbox under the **Random Pool, Header Key, and Master Key** section.

14. Move your mouse as randomly as possible within the **Volume Creation Wizard** window for at least **30 seconds** and click the **Format** button.

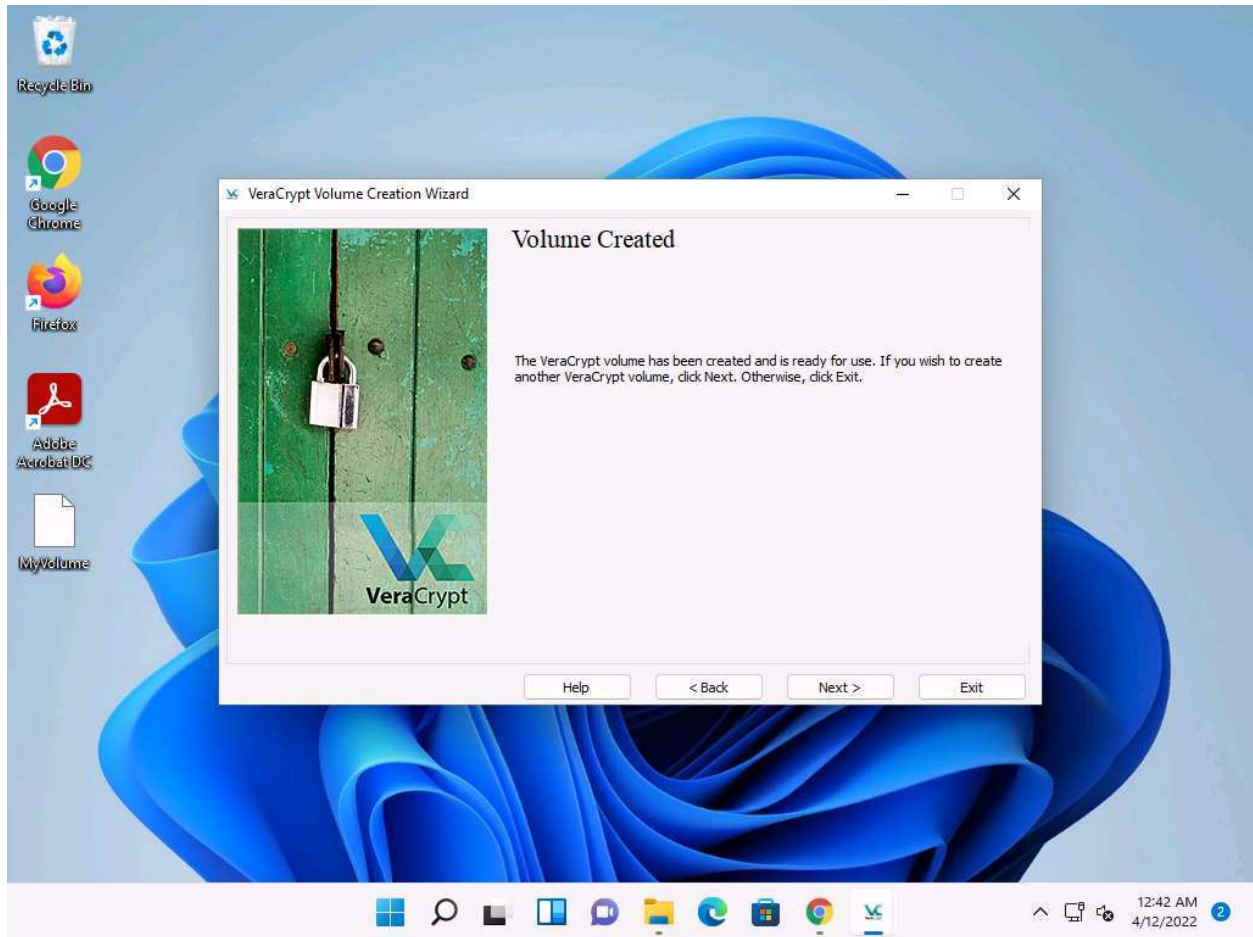




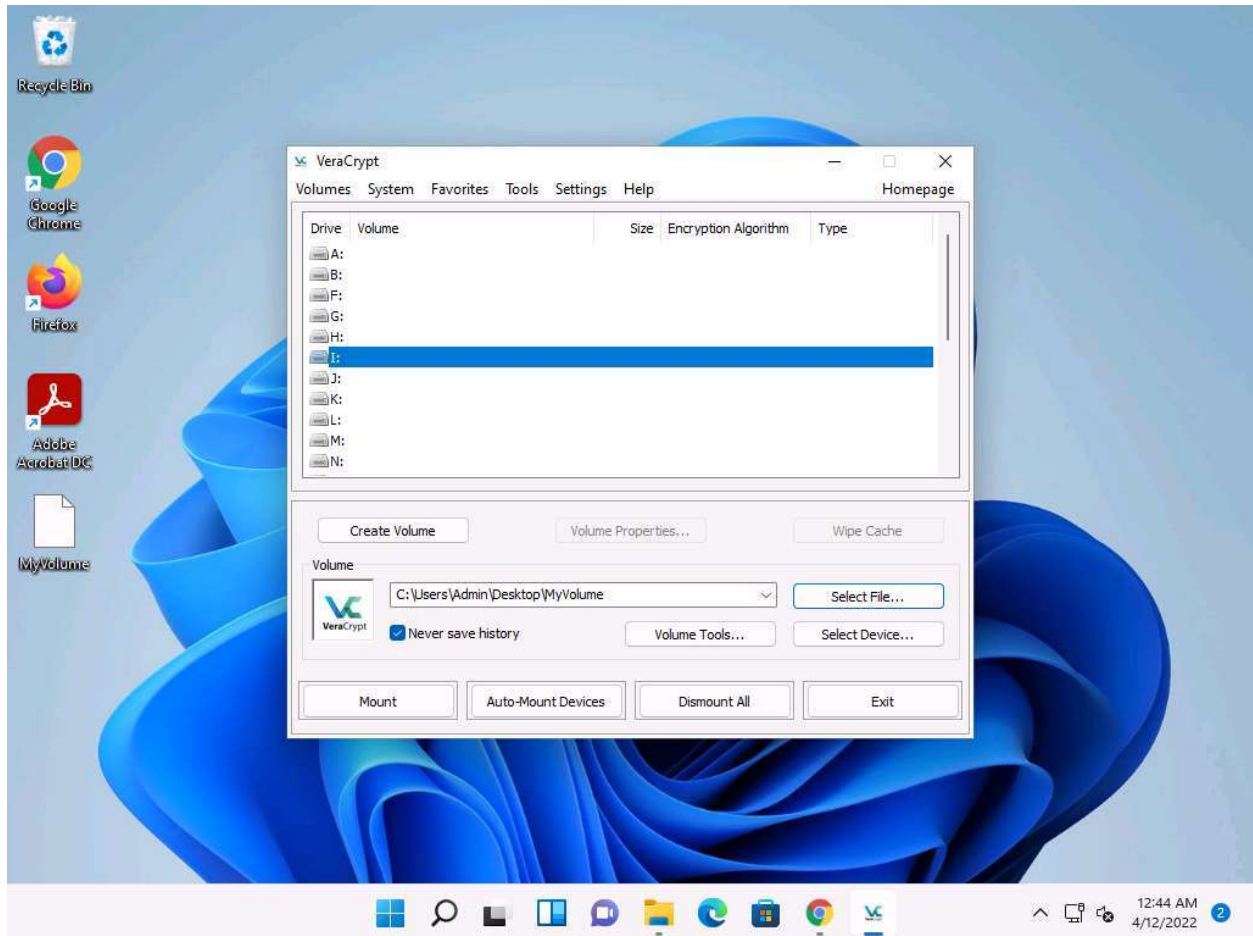
15. After clicking **Format**, VeraCrypt will create a file called **MyVolume** in the provided folder. This file depends on the VeraCrypt container (it will contain the encrypted VeraCrypt volume).
16. Depending on the size of the volume, volume creation may take some time.
17. Once the volume is created, a **VeraCrypt Volume Creation Wizard** dialog-box appears; click **OK**.



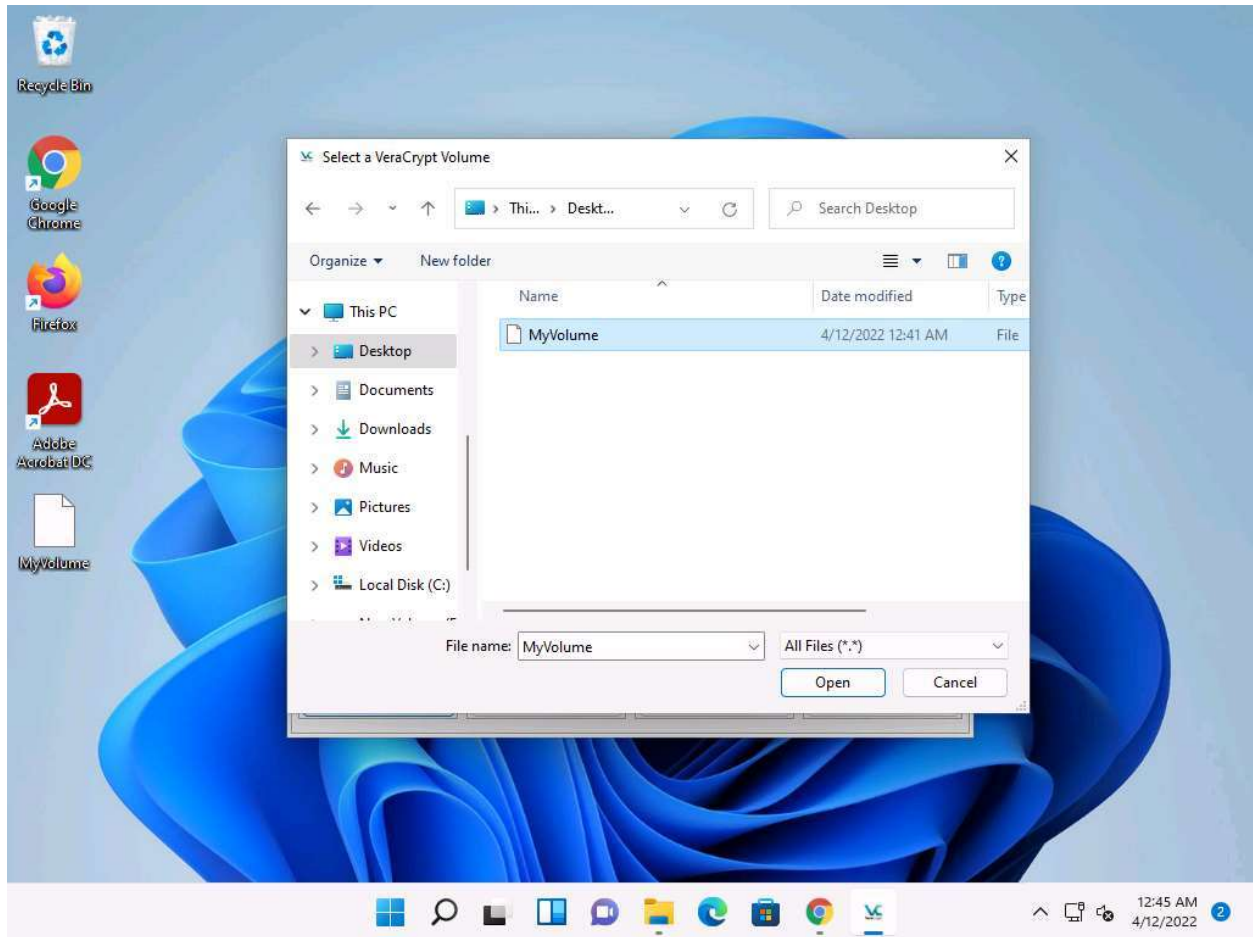
18. In the **VeraCrypt Volume Creation Wizard** window, a **Volume Created** message appears; then, click **Exit**.



19. The **VeraCrypt** main window appears; select a drive (here, **I:**) and click **Select File...**

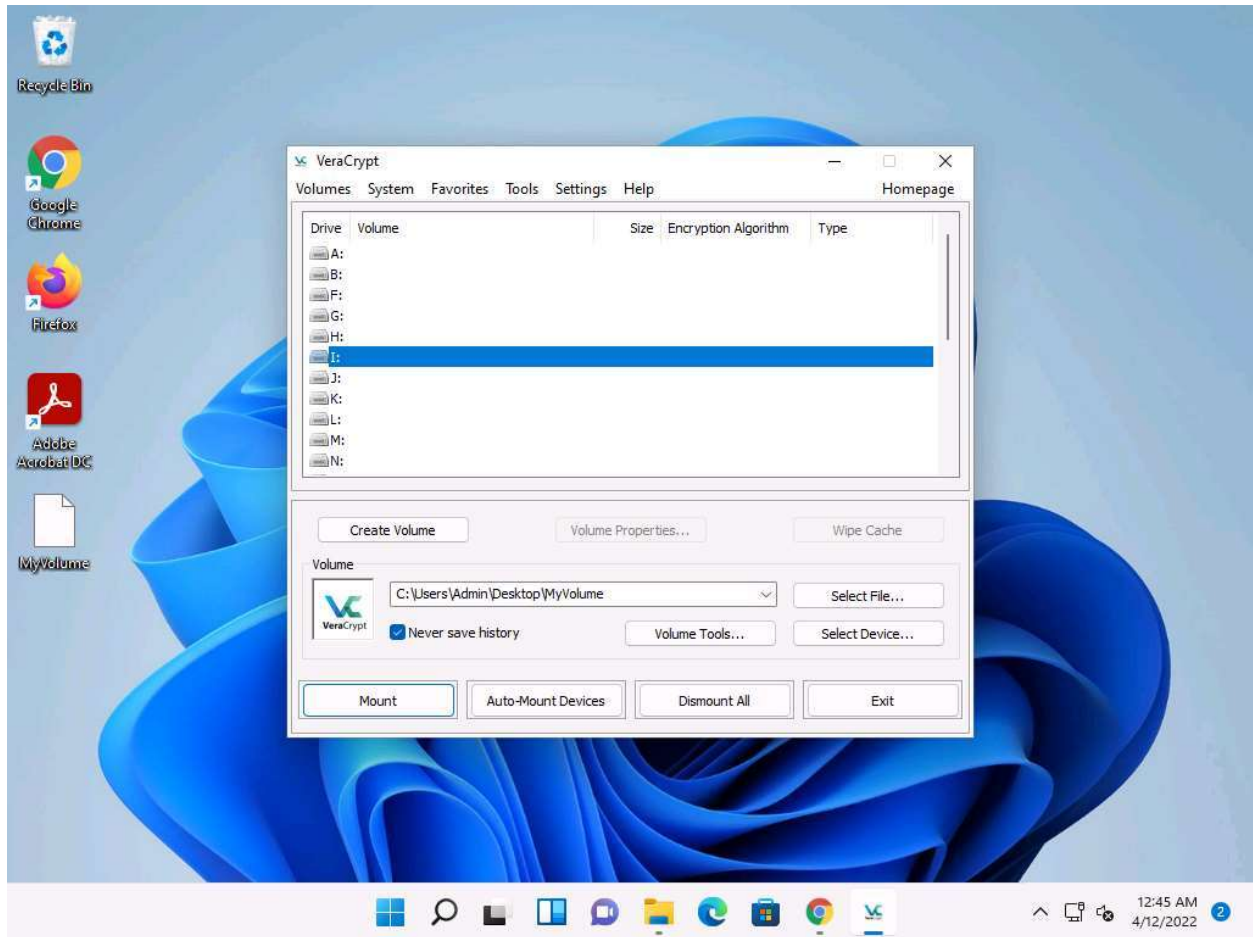


20. The **Select a VeraCrypt Volume** window appears; navigate to **Desktop**, click **MyVolume**, and click **Open**.



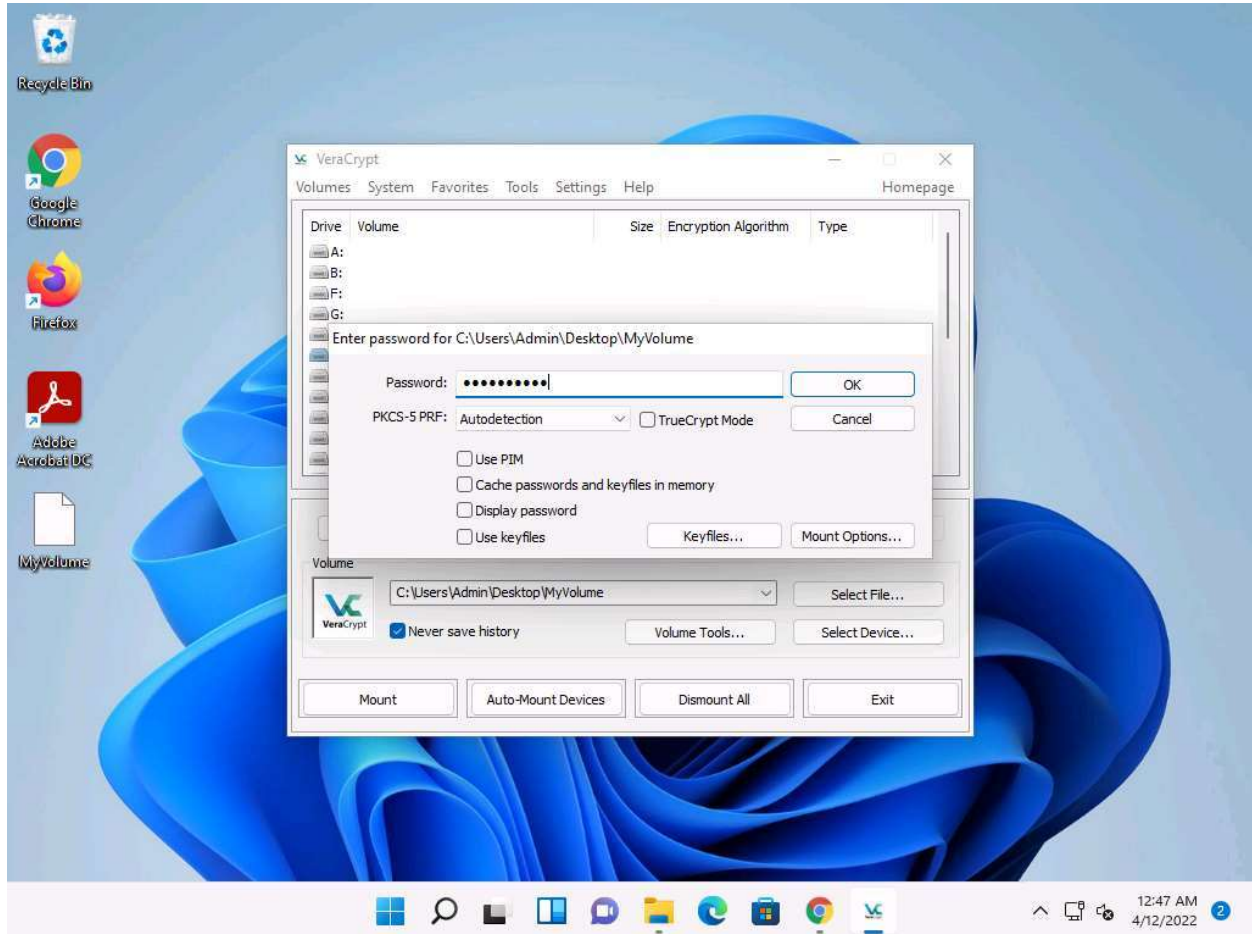


21. The window closes, and the **VeraCrypt** window appears displaying the location of selected **volume** under the Volume field; then, click **Mount**.

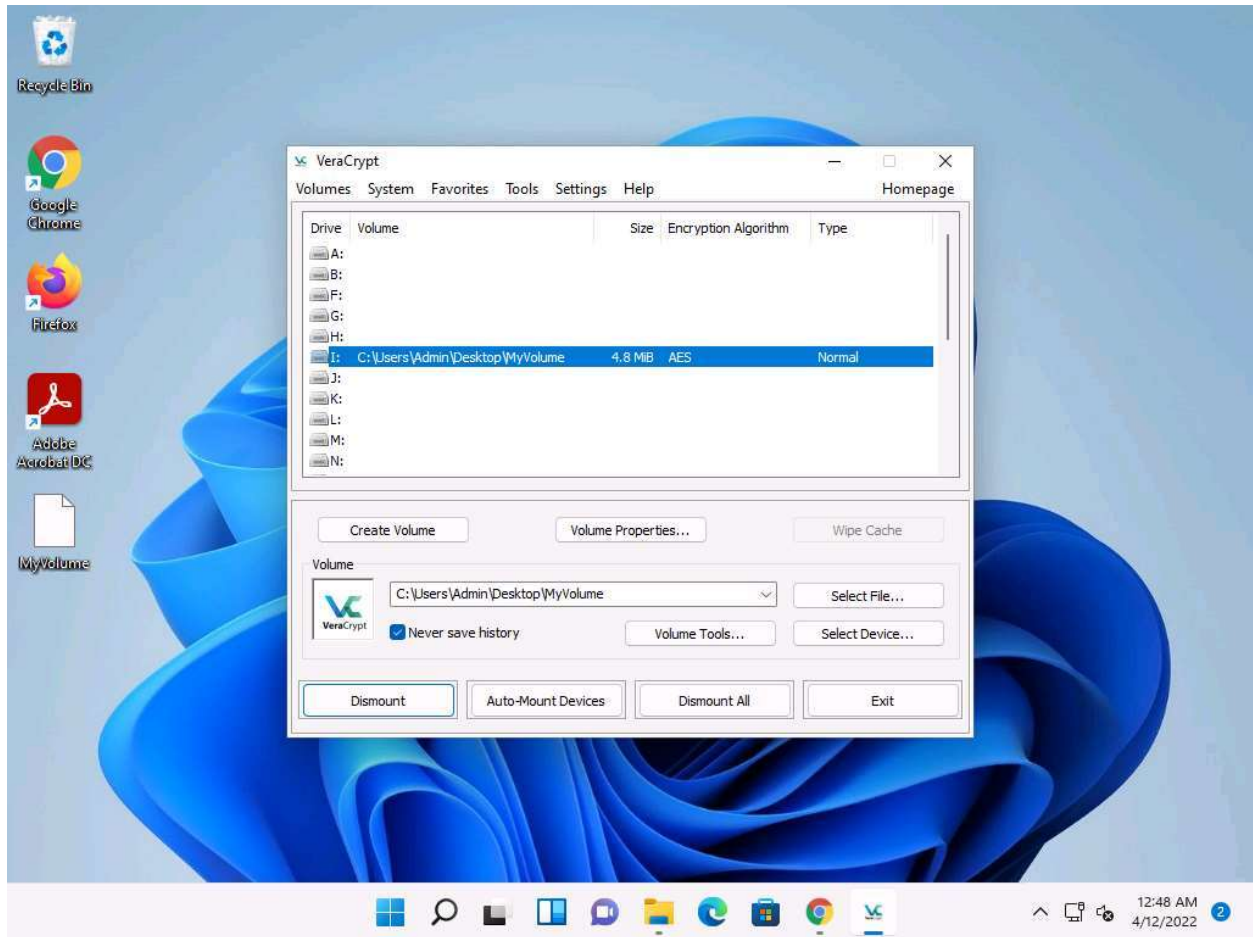


22. The **Enter password** dialog-box appears; type the password you specified in **Step#11** into the **Password** field and click **OK**.

The password specified in this task is **qwerty@123**.



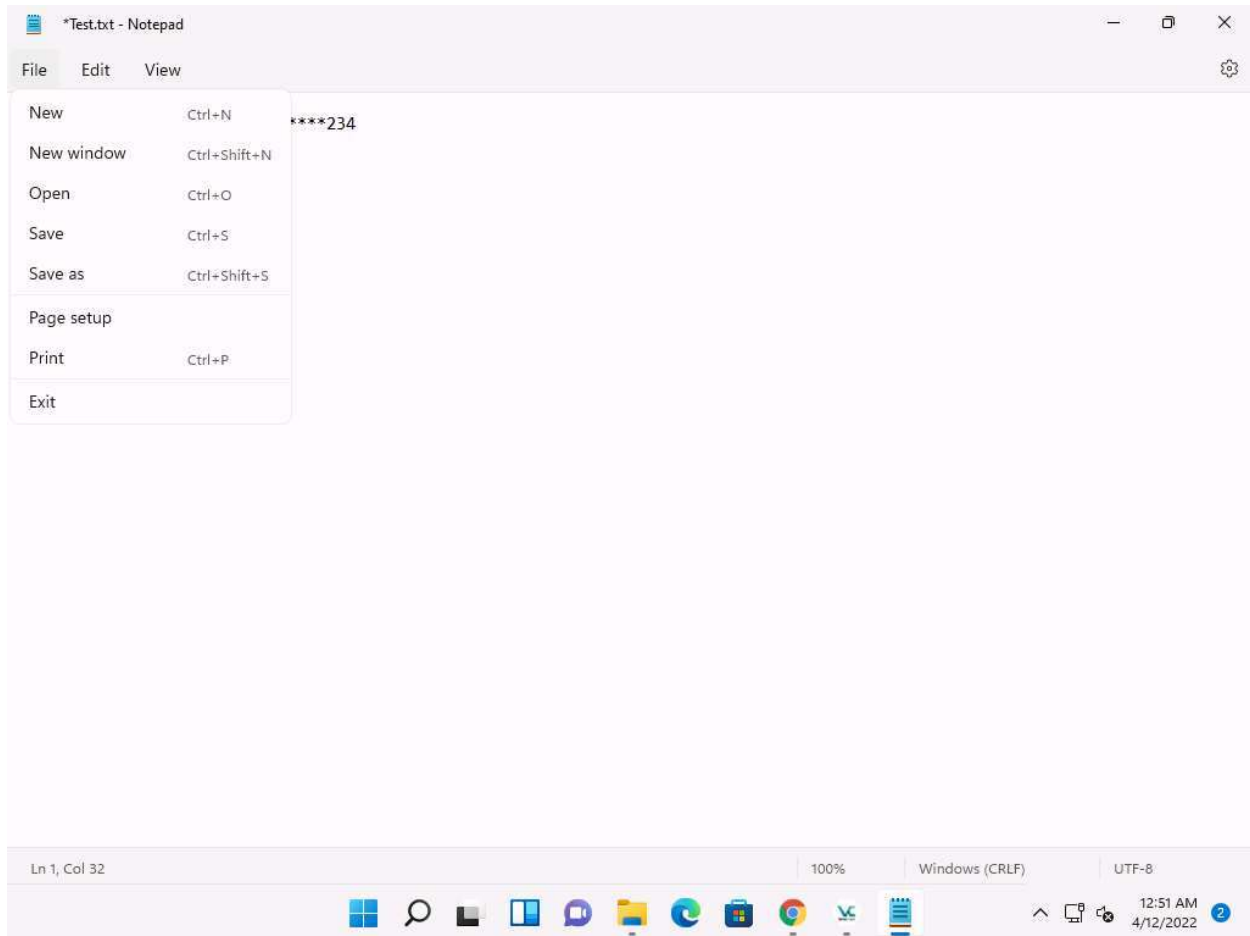
23. After the password is verified, **VeraCrypt** will mount the volume in **I:** drive, as shown in the screenshot:



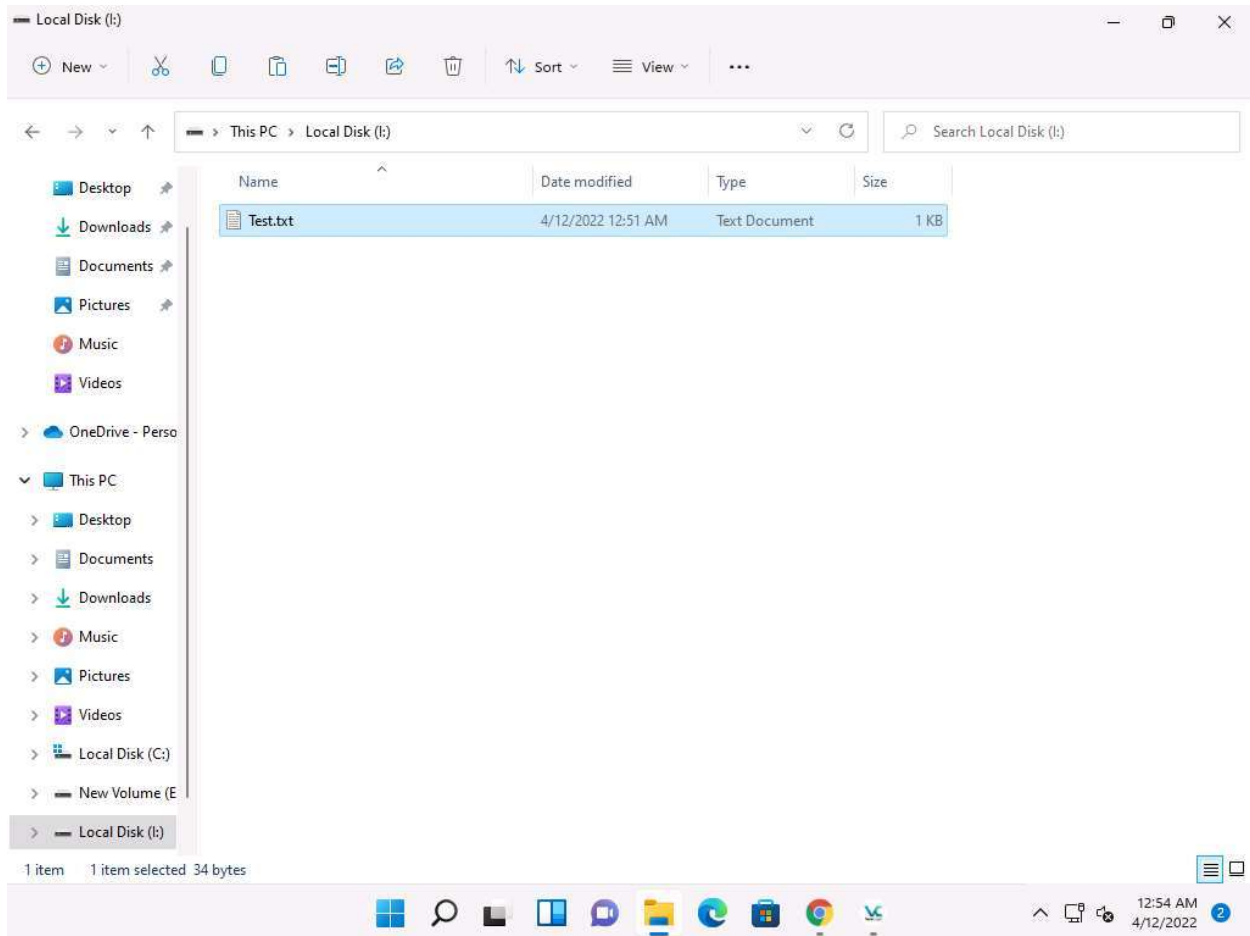
24. **MyVolume** has successfully mounted the container as a virtual disk (**I:**). The virtual disk is entirely encrypted (including file names, allocation tables, free space, etc.) and behaves similarly to a real disk. You can copy or move files to this virtual disk to encrypt them.

25. Create a text file on **Desktop** and name it **Test**. Open the text file and insert text.

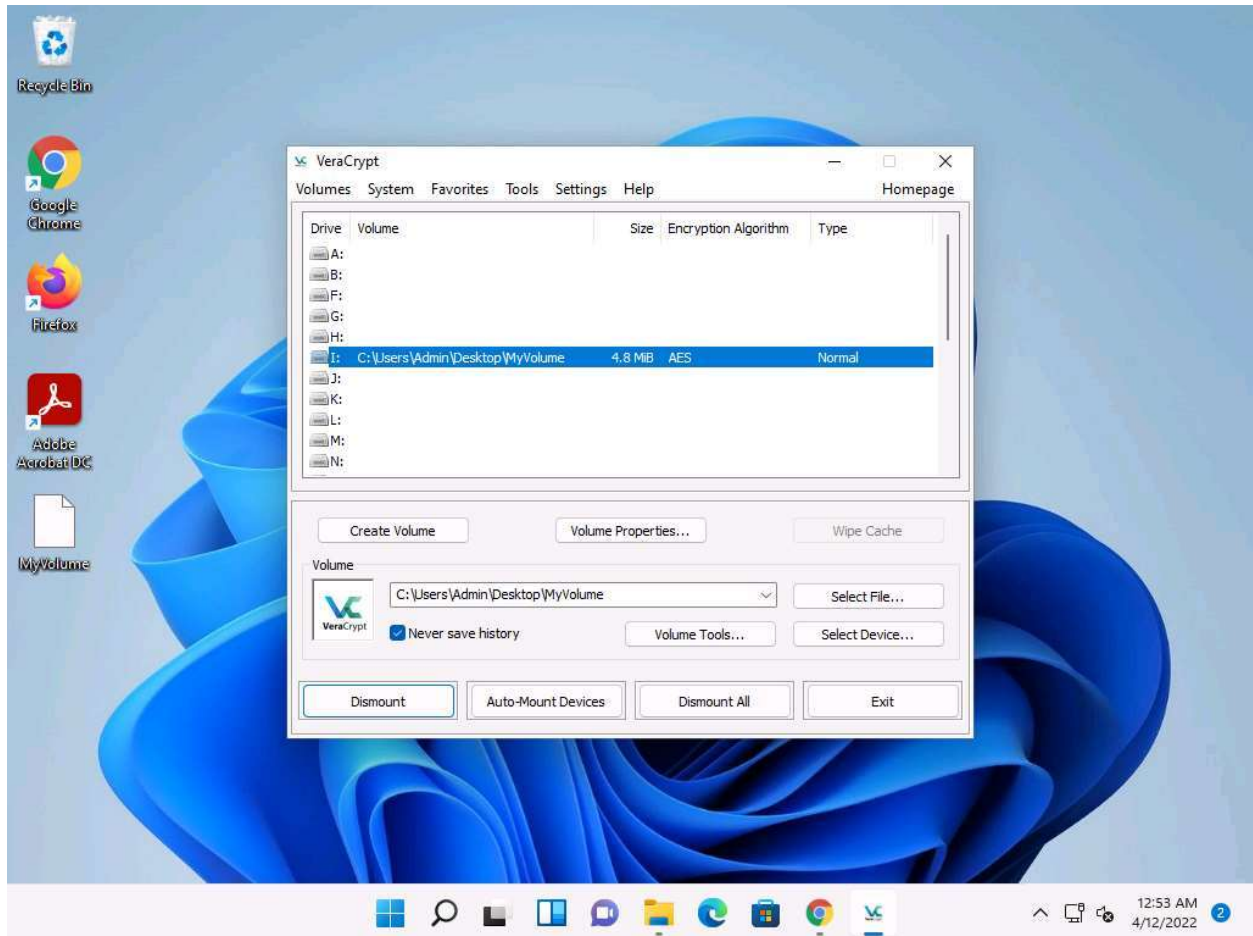
26. Click **File** in the menu bar and click **Save**.



27. Copy the file from **Desktop** and paste it into **Local Disk (I:)**. Close the window.



28. Switch to the **VeraCrypt** window, click **Dismount**, and then click **Exit**.



29. The **I:** drive located in **This PC** disappears.

This lab is used to demonstrate that, in cases of system hacks, if an attacker manages to gain remote access or complete access to the machine, he/she will not be able to find the encrypted volume-including its files-unless he/she is able to obtain the password. Thus, all sensitive information located on the encrypted volume is safeguarded.

30. This concludes the demonstration of performing disk encryption using VeraCrypt.


31. Close all open windows and document all the acquired information.

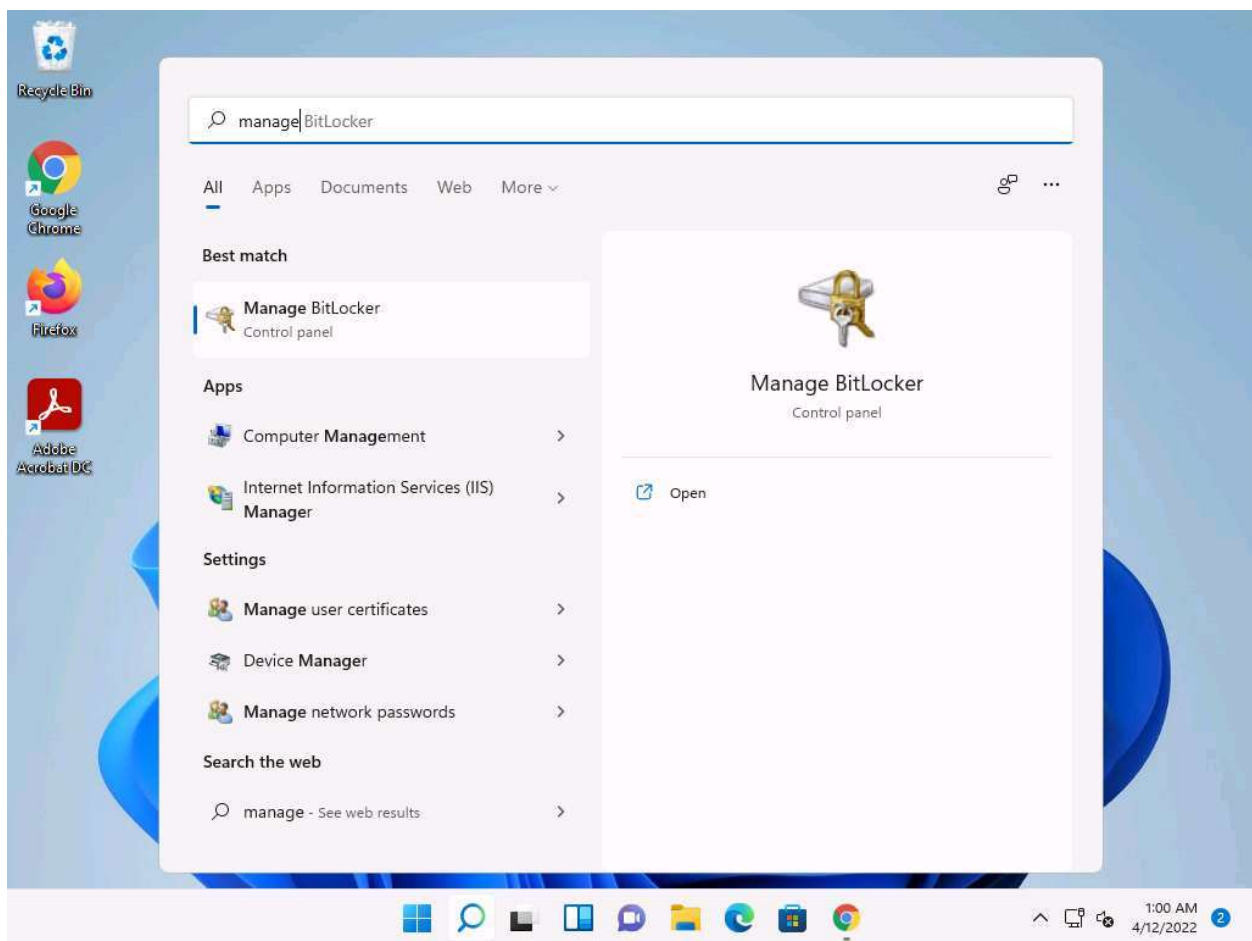
---

## Task 2: Perform Disk Encryption using BitLocker Drive Encryption

BitLocker provides offline-data and OS protection for your computer, and helps to ensure that data stored on a computer that is running Windows® is not revealed if the computer is tampered with when the installed OS is offline. BitLocker uses a microchip that is called a Trusted Platform Module (TPM) to provide enhanced protection for your data and to preserve early boot-component integrity. The TPM can help protect your data from theft or unauthorized viewing by encrypting the entire Windows volumes.

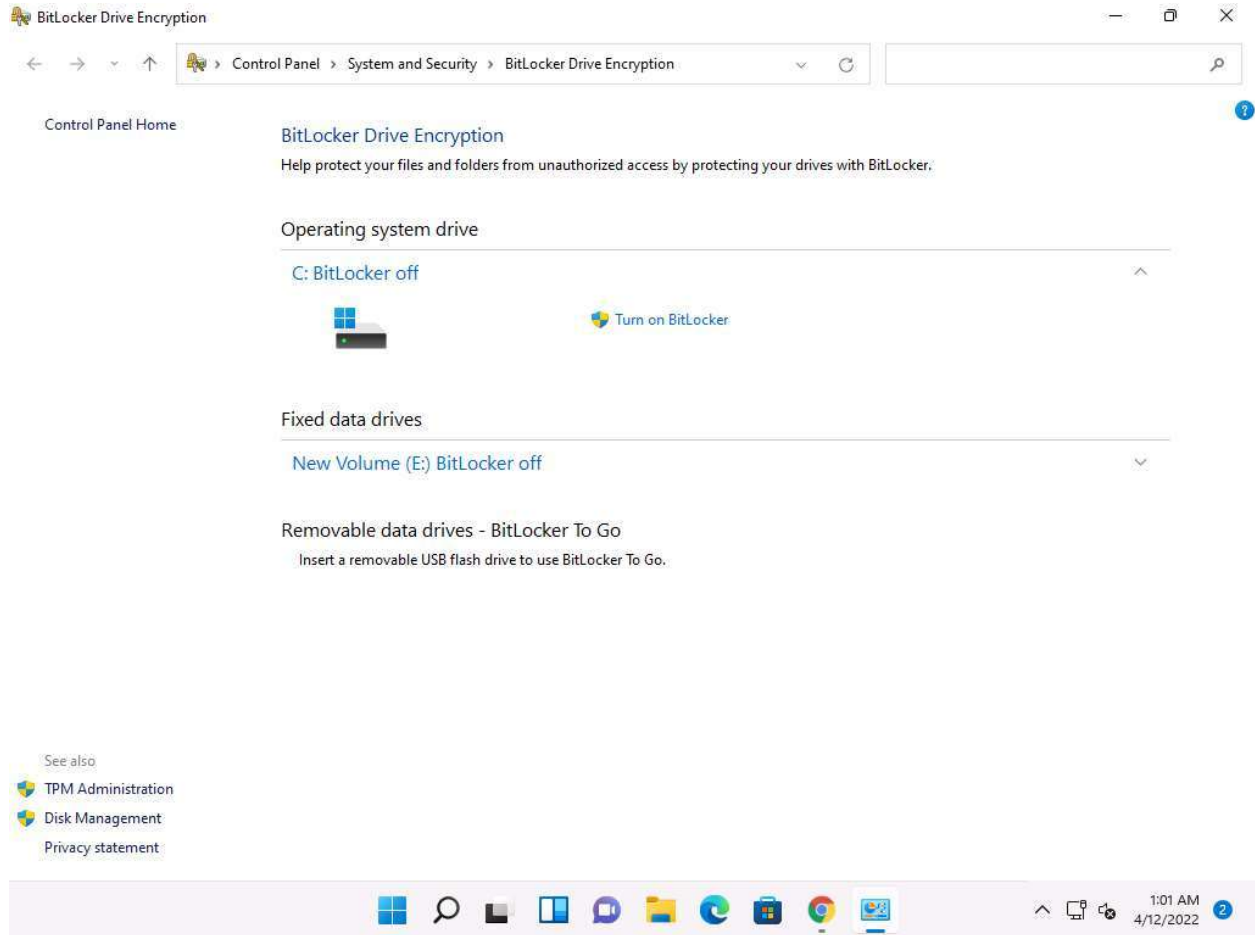
Here, we will perform disk encryption using BitLocker Drive Encryption.

1. Click **Search** icon (  ) on the **Desktop**. Type **manage** in the search field, the **Manage Bitlocker** appears in the results, click **Open** to launch it.



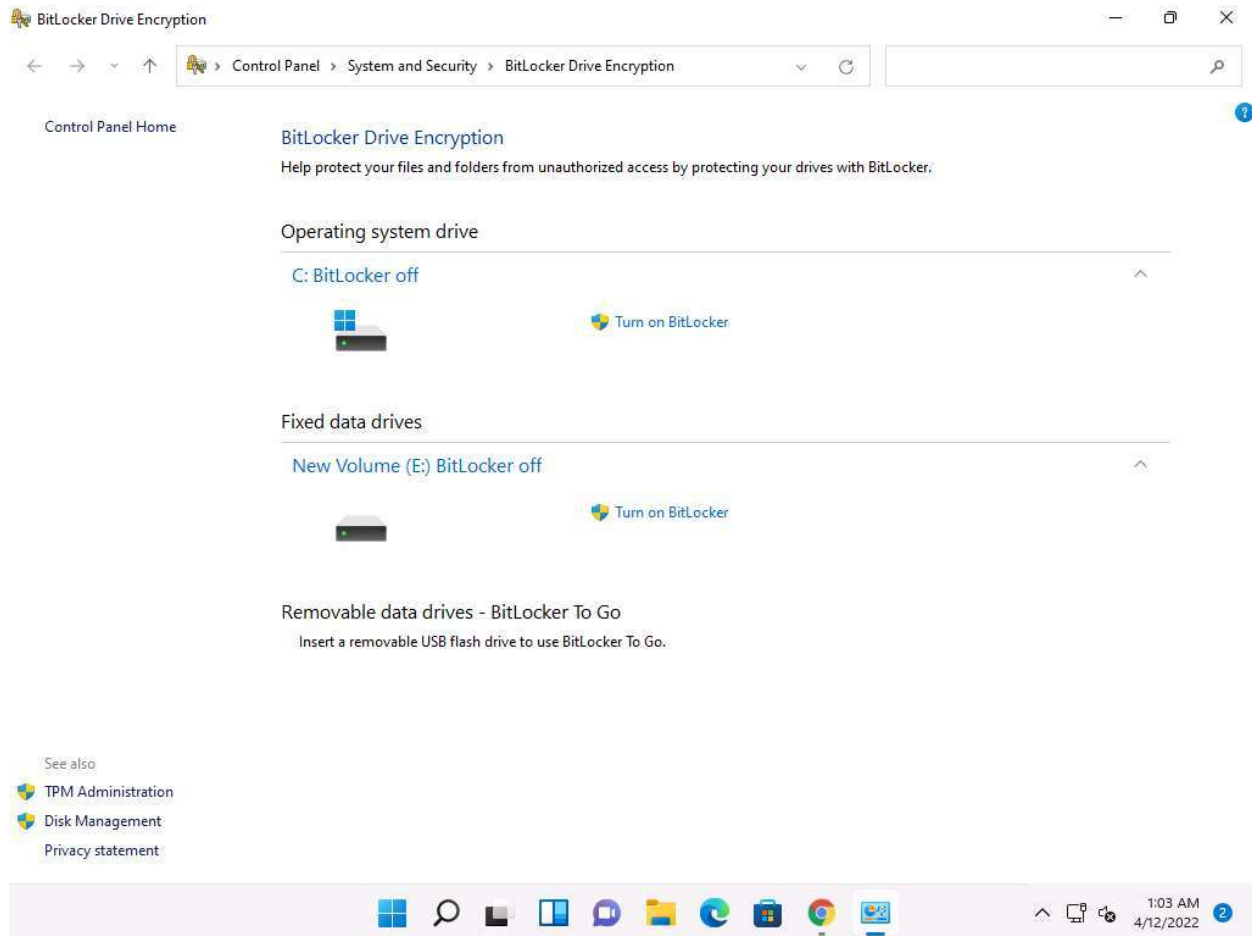


2. The **BitLocker Drive Encryption** window appears; click the **New Volume (E:) BitLocker off** option under the **Fixed data drives** section.

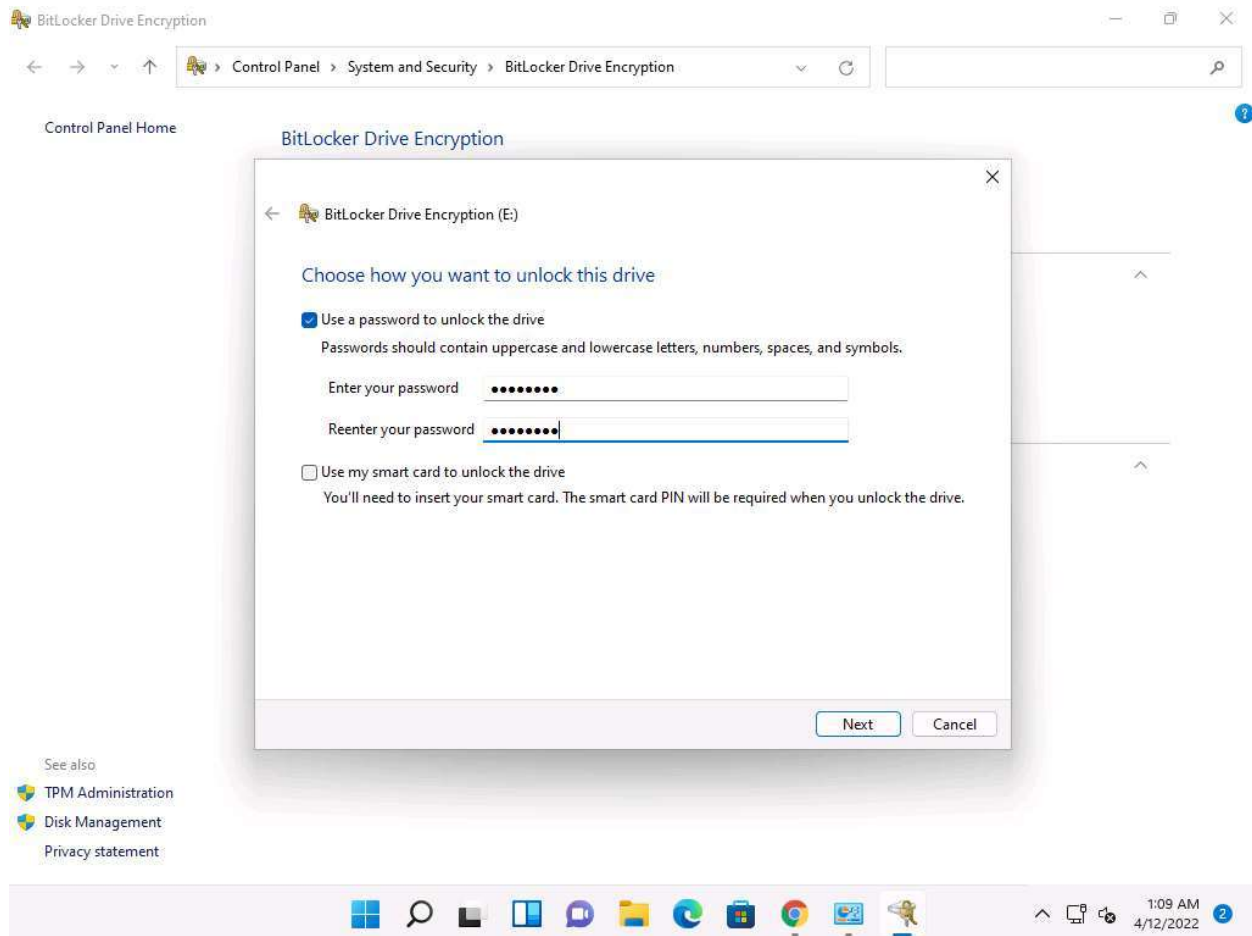




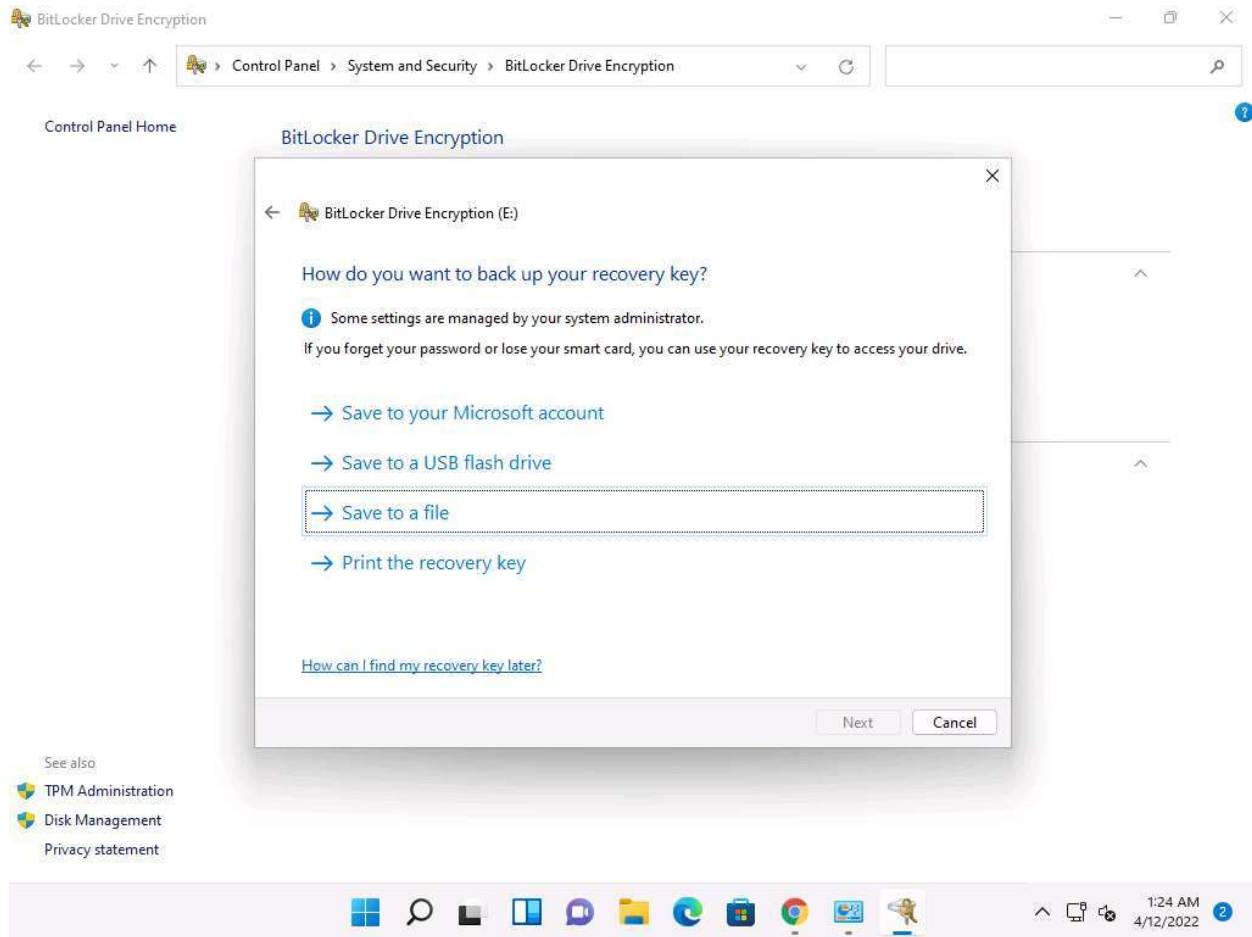
3. Click the **Turn on BitLocker** option under **New Volume (E:) BitLocker off**.



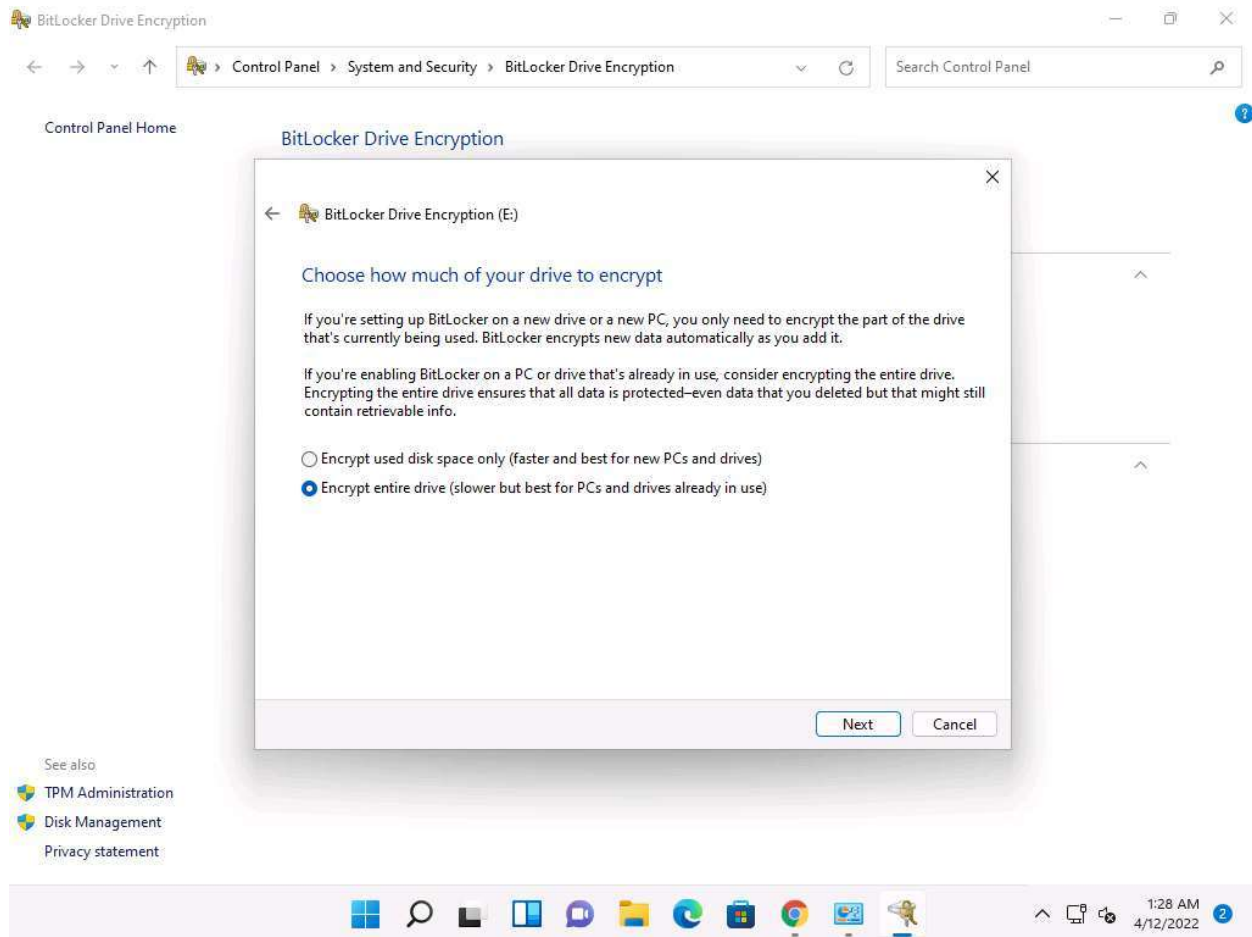
4. The **BitLocker Drive Encryption (E:)** wizard appears; check the **Use a password to unlock the drive** checkbox.
5. Type the password in the **Enter your password** field and re-type the password in the **Reenter your password** field; then, click **Next** (Here, the password entered is **test@123**).



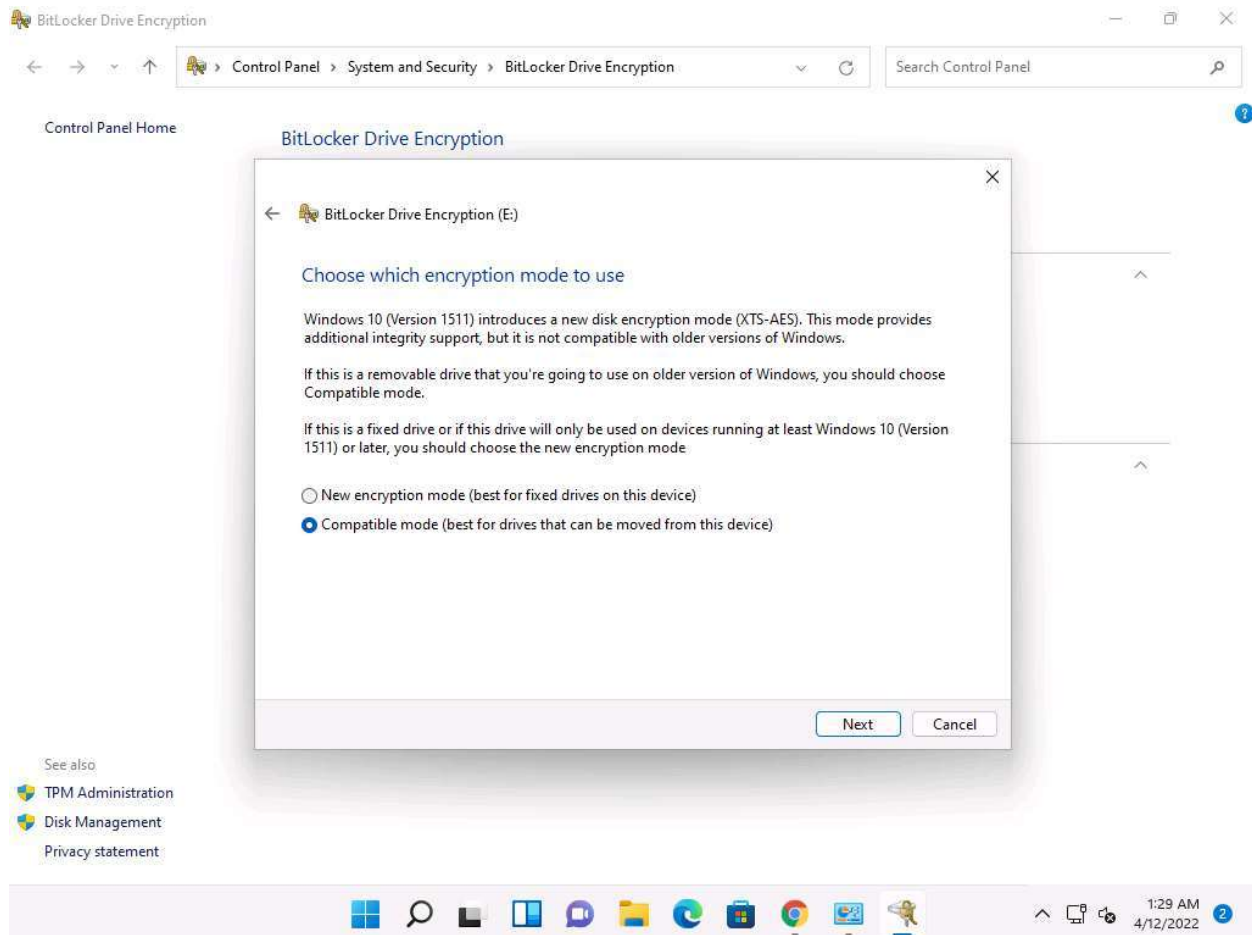
6. The **How do you want to back up your recovery key?** step appears; click **Save to a file** from the available options.



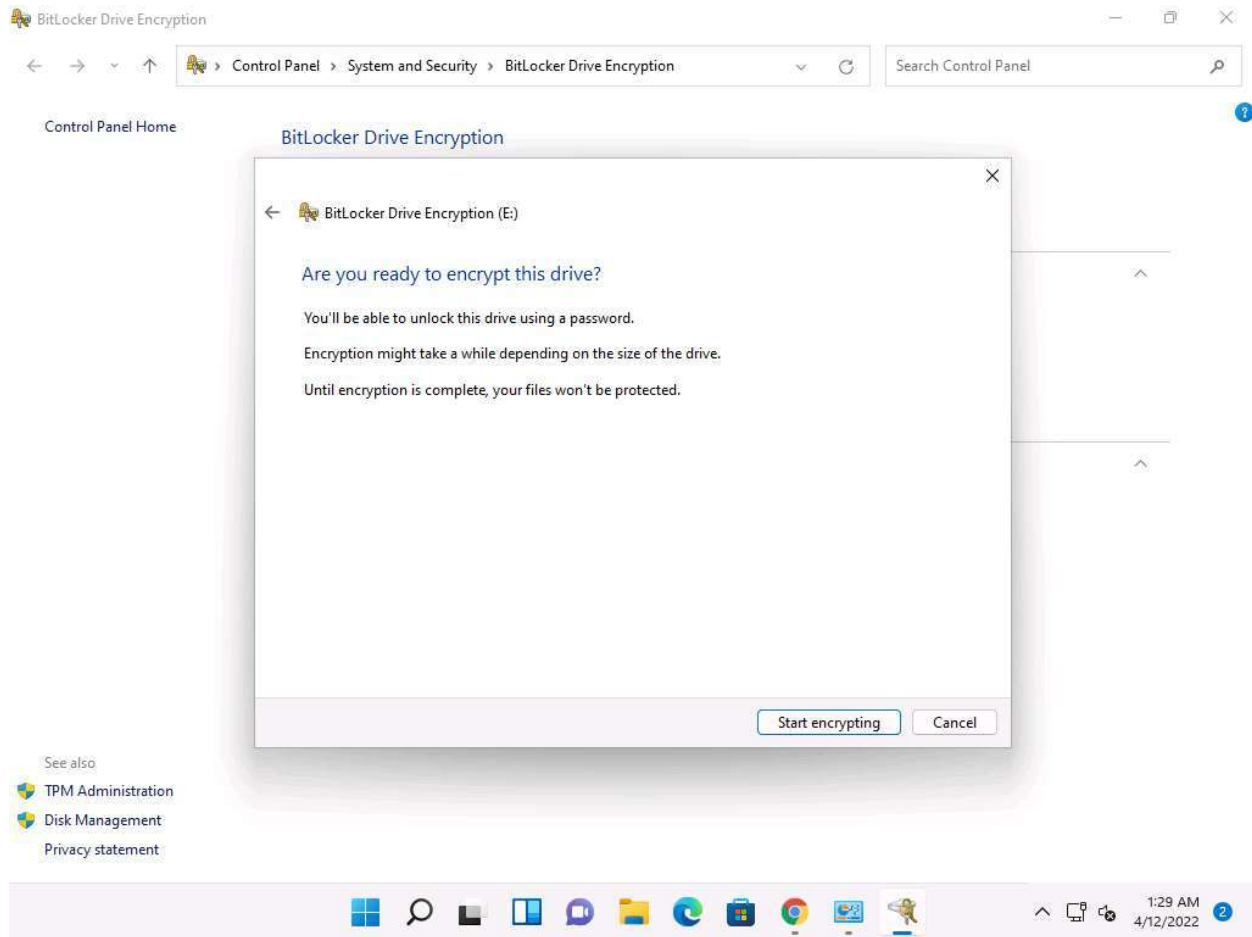
7. The **Save BitLocker recovery key as** window appears; keep the save location set to **This PC --> Documents** and click **Save**.
8. Click **Next** in the **How do you want to back up your recovery key?** step.
9. In the **Choose how much of your drive to encrypt** step, select the **Encrypt entire drive (slower but best for PCs and drives already in use)** button, and click **Next**.



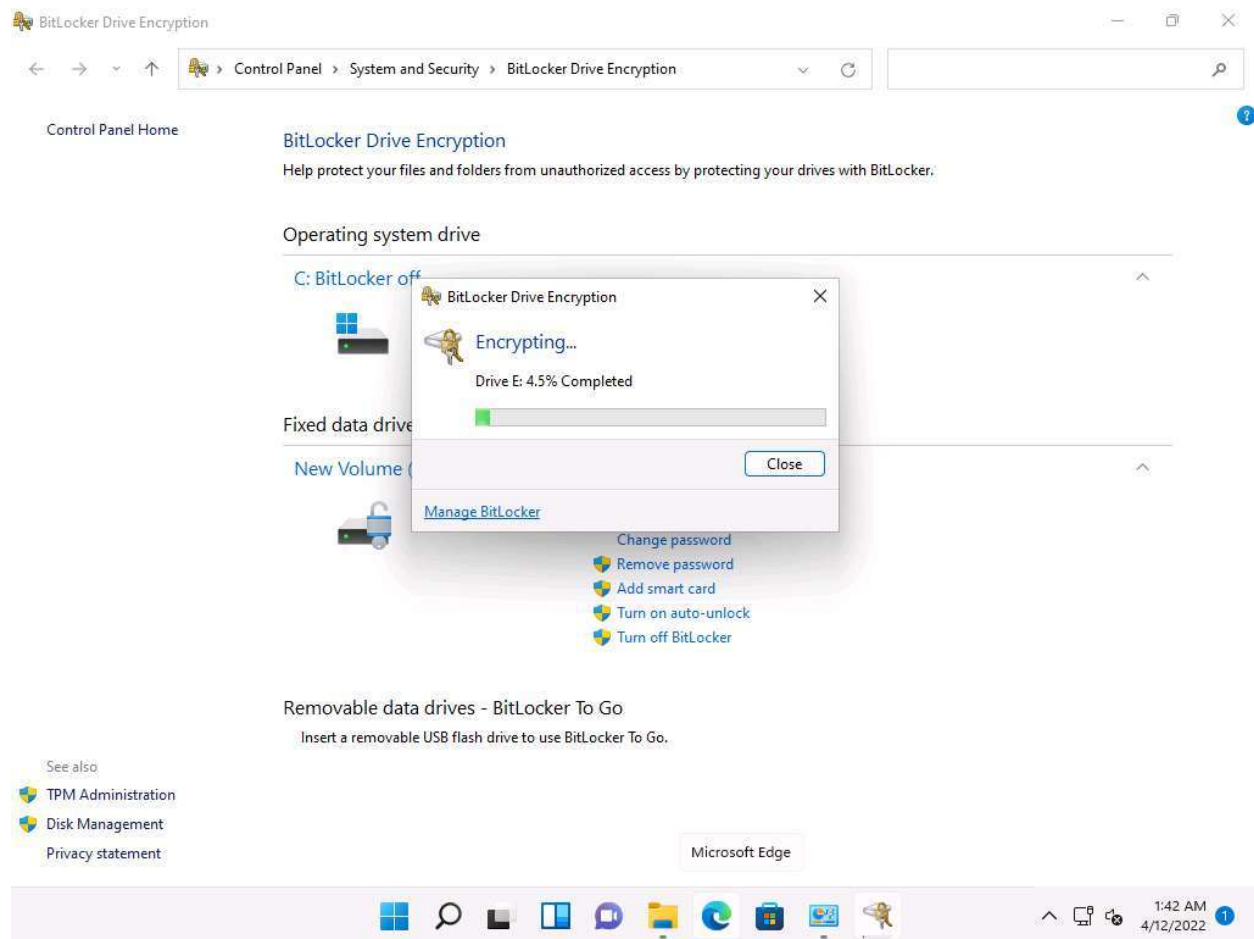
10. In the **Choose which encryption mode to use** step, ensure that the **Compatible mode (best for drives that can be moved from this device)** option is selected, and click **Next**.



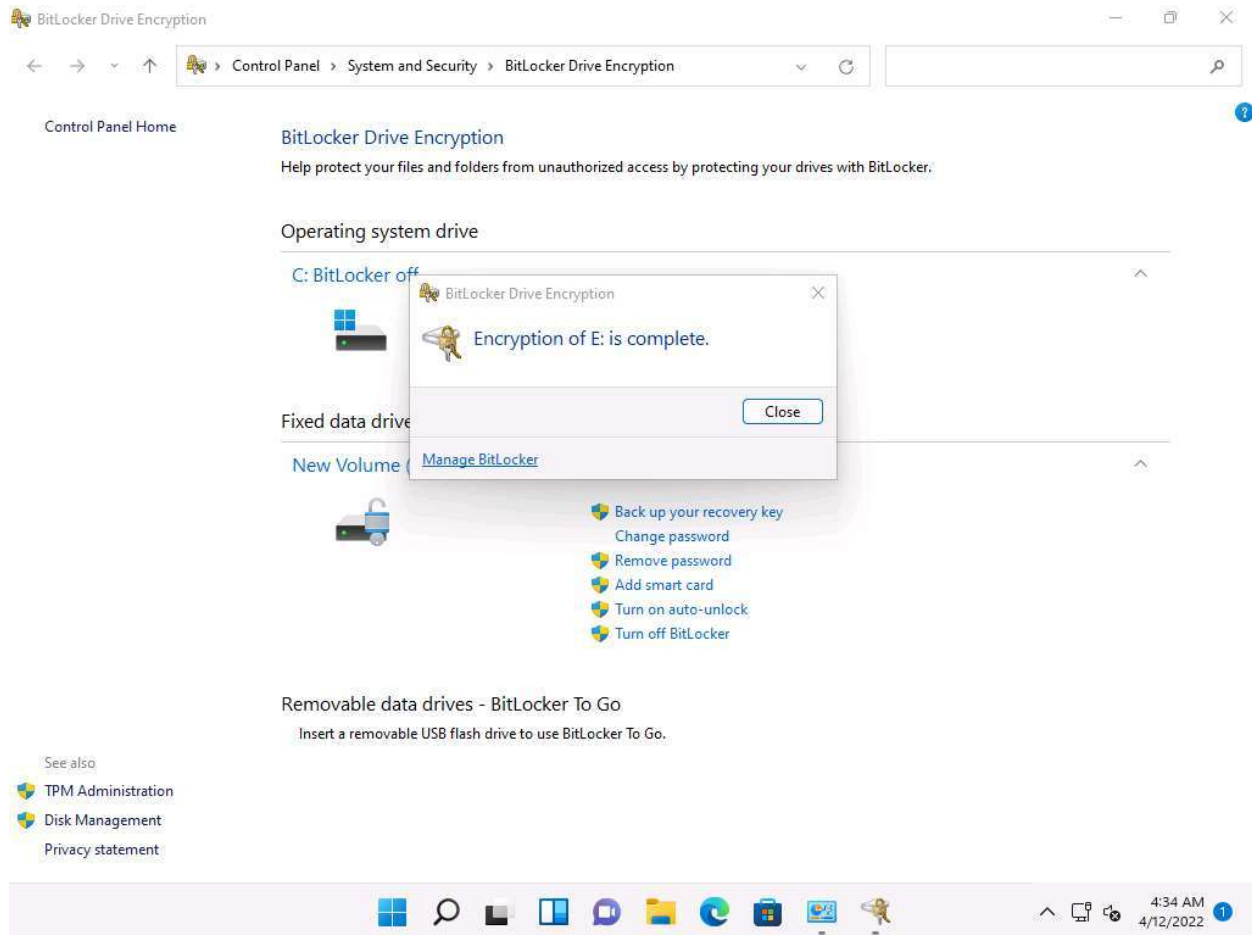
11. In the **Are you ready to encrypt this drive?** step, click **Start encrypting** to encrypt the selected drive.



## 12. The BitLocker Drive Encryption pop-up appears, showing the **Encrypting...** status.

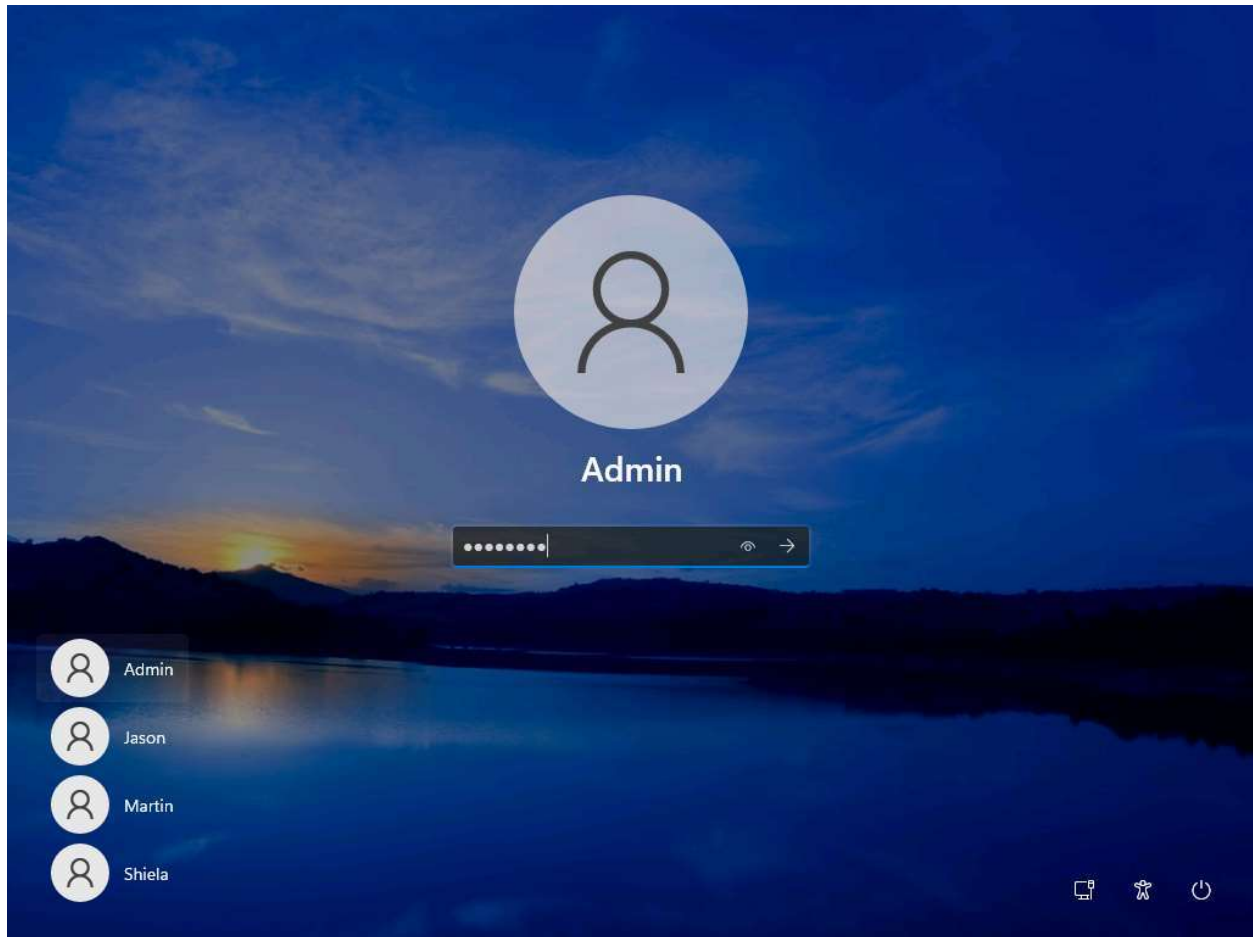


13. After the completion of the encryption process, the **Encryption of E: is complete** notification appears; click **Close** and **Restart** the machine.





14. After the system reboots, click [Ctrl+Alt+Delete](#) to activate it. By default, **Admin** user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login

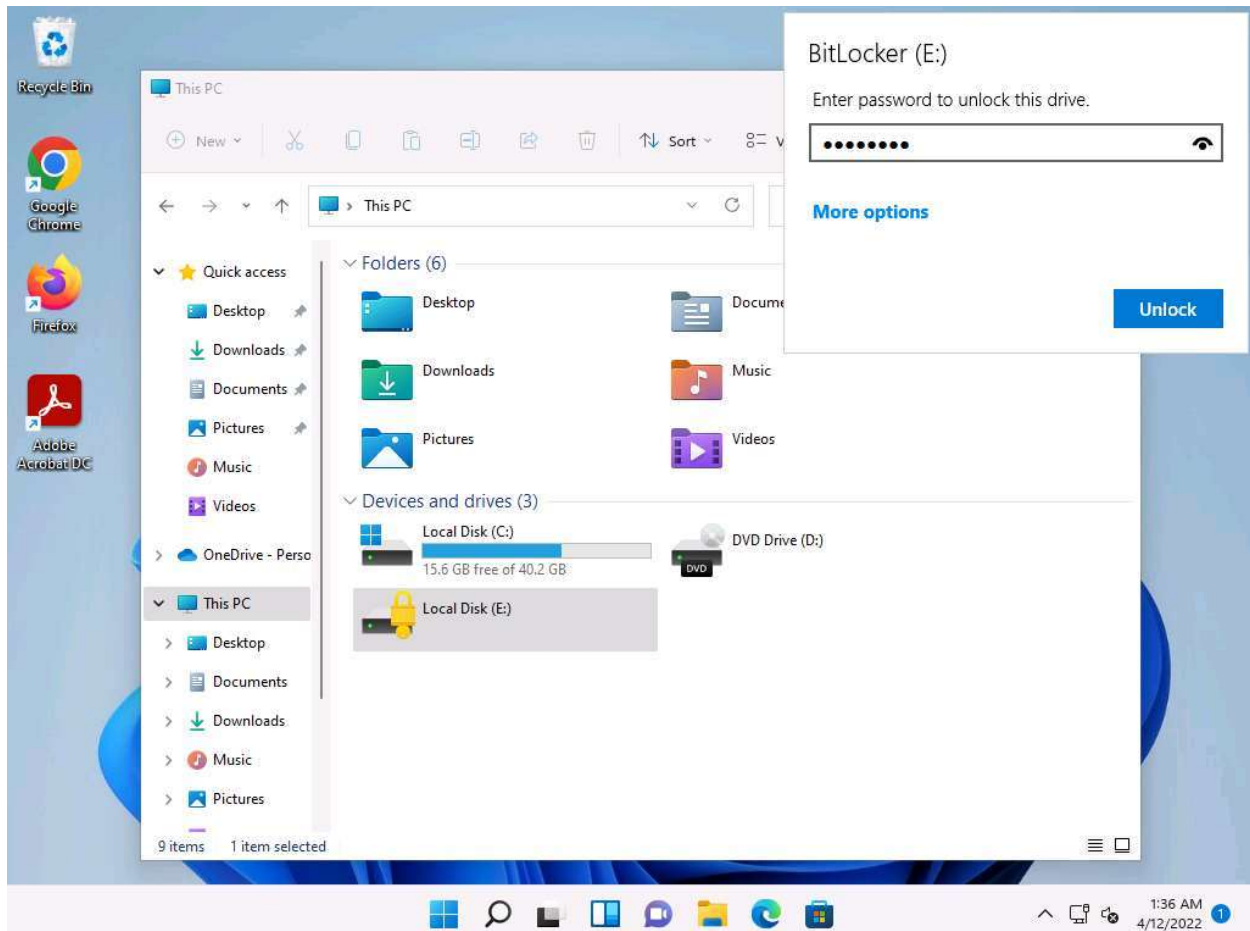


15. Open **File Explorer** and click **This PC** from the left pane.

16. You can observe that **Local Disk (E:)** is now encrypted; double-click and the **Local Disk (E:)** security pop-up appears at the top-right corner of **Desktop**

17. Type the password you provided in **Step#5** and click **Unlock**.

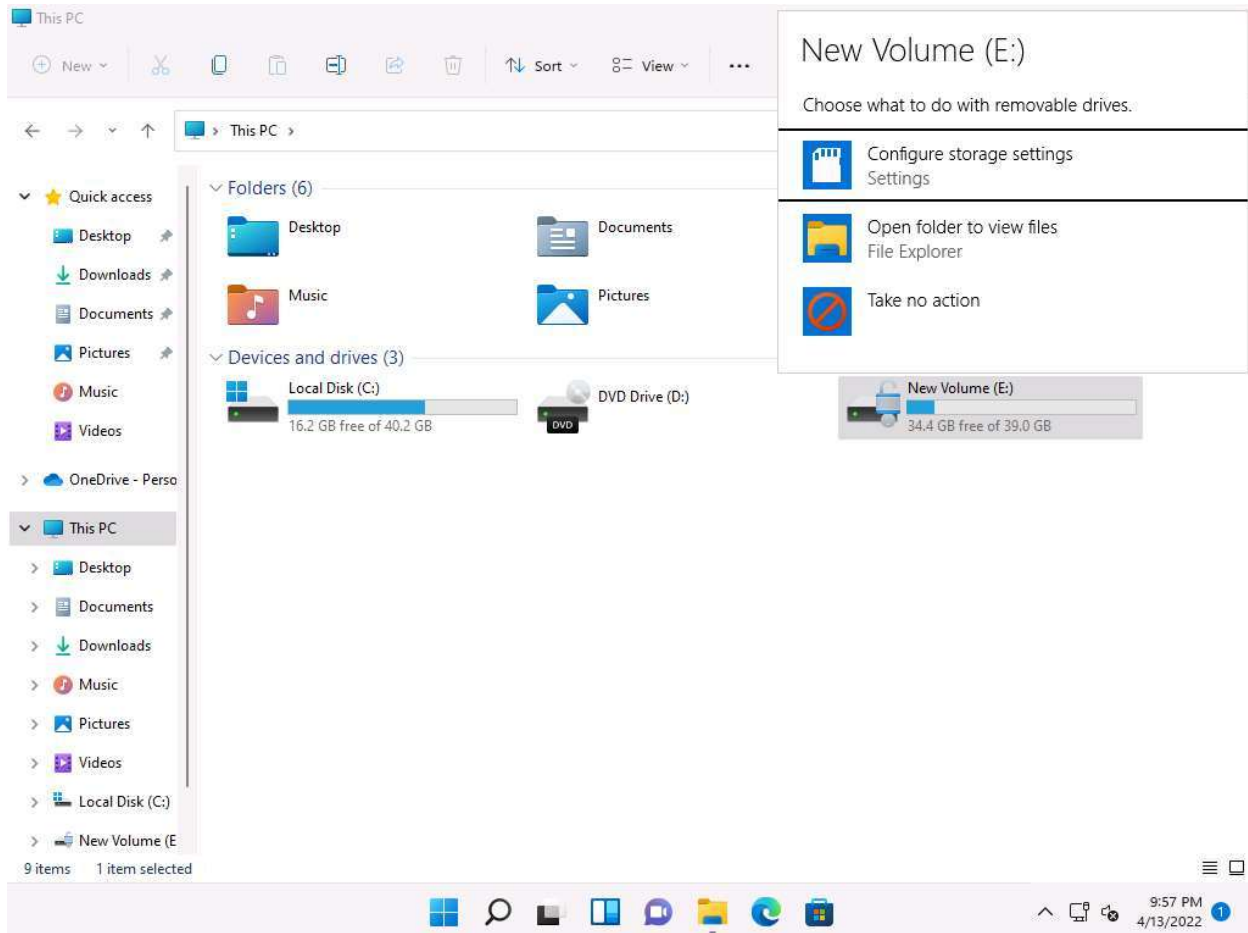
Here, the password is **test@123**.



If the **Local Disk (E:)** pop-up appears at the top-right corner of the window. Click the **Open folder to view files** option to view the disk content.

18. The **New Volume (E:)** window appears displaying the disk content, as shown in the screenshot.

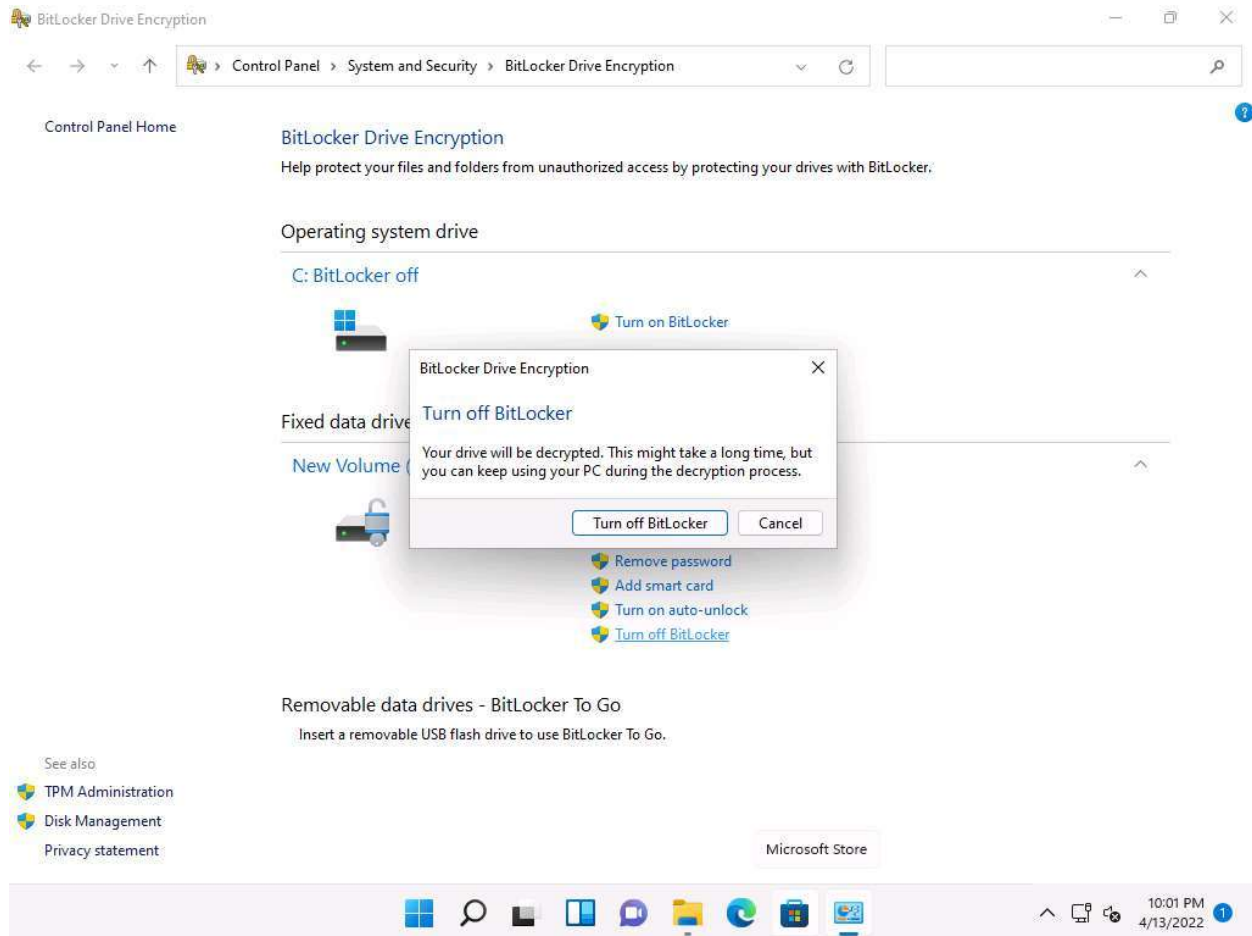
The disk will remain unlocked until the next time you restart the system.



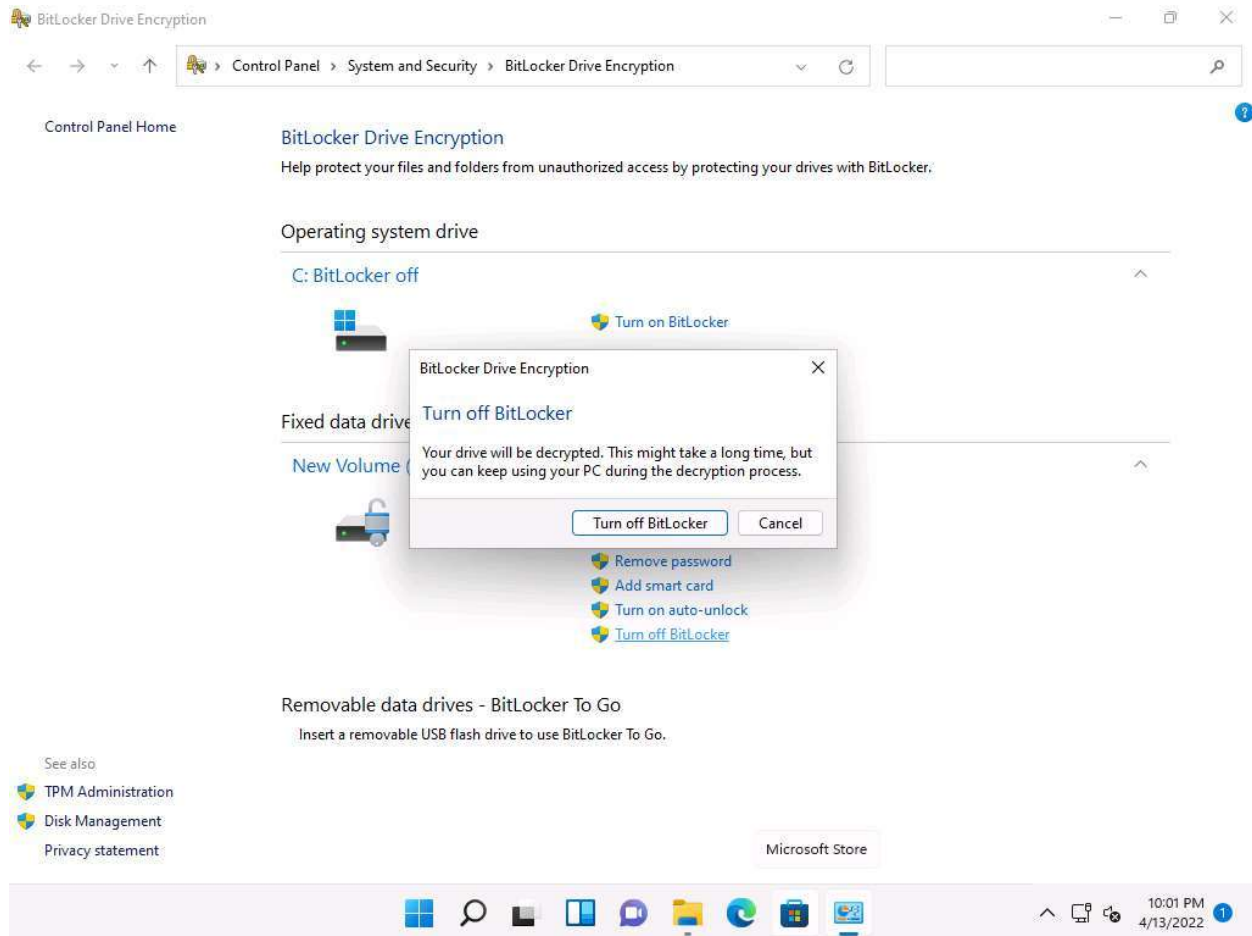
19. This concludes the demonstration of performing disk encryption using BitLocker Drive Encryption.

20. Once, you are done with this task; you must turn off BitLocker to decrypt the **New Volume (E:)** disk.

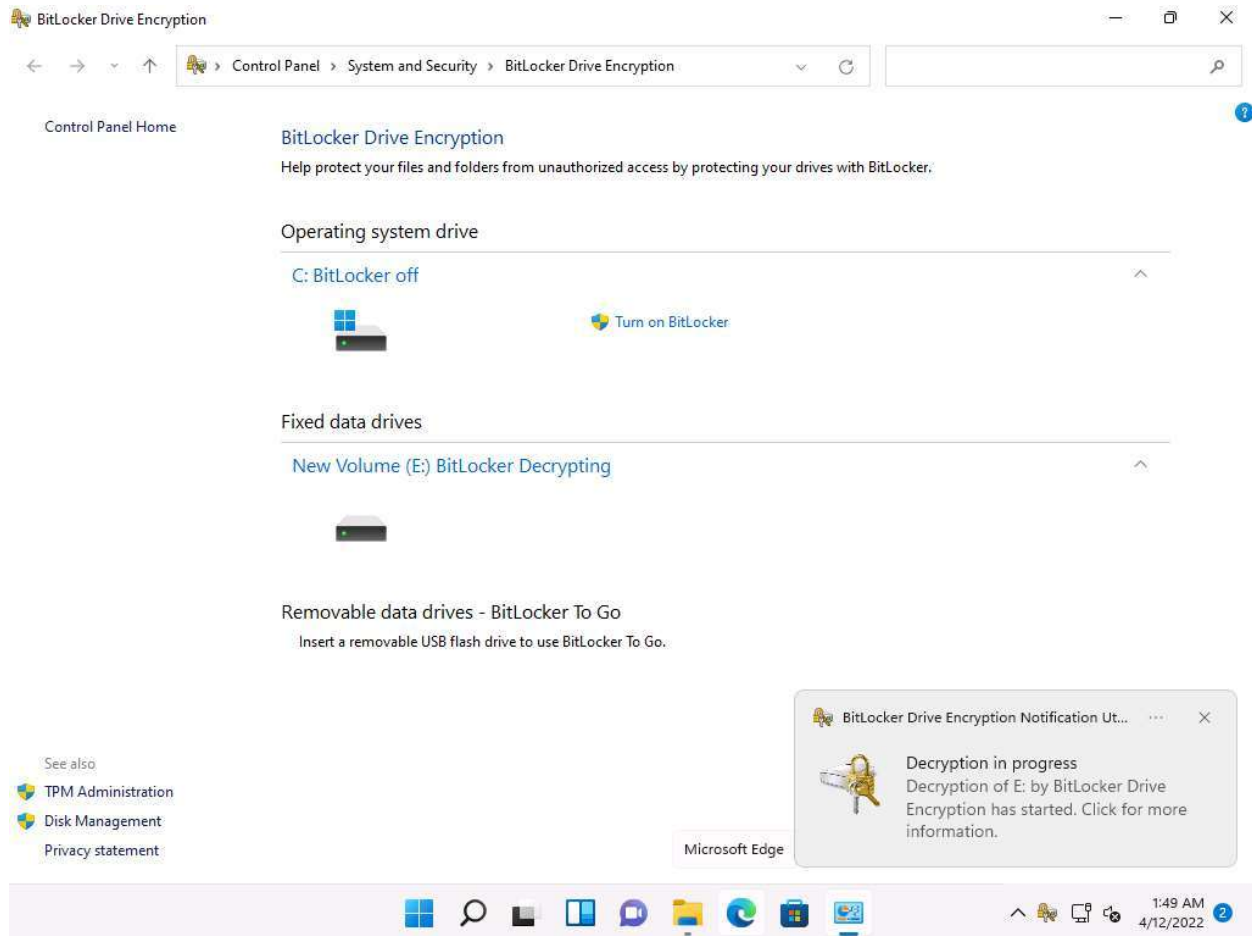
21. To do so, open the **BitLocker Drive Encryption** window, click **New Volume (E:) BitLocker on** and from the options click **Turn off BitLocker**.



## 22. The BitLocker Drive Encryption pop-up appears; click **Turn off BitLocker**.



### 23. BitLocker initiates the decryption process. Wait for it to complete.



If after the completion of decryption process, the **Decryption of E: is complete** pop-up appears; click **Close**.

24. The **New Volume (E:)** decrypts successfully.

25. Close all open windows and document all the acquired information.

#### **Question 20.4.2.1**

Use BitLocker to encrypt a disk volume. Which encryption mode is suitable for the drives that can be moved?

### Task 3: Perform Disk Encryption using Rohos Disk Encryption

Rohos Disk Encryption creates hidden and password-protected partitions on a computer or USB flash drive, and password protects/locks access to your Internet applications. It uses a NIST-approved AES encryption algorithm with a 256-bit encryption key length. Encryption is automatic and on-the-fly.

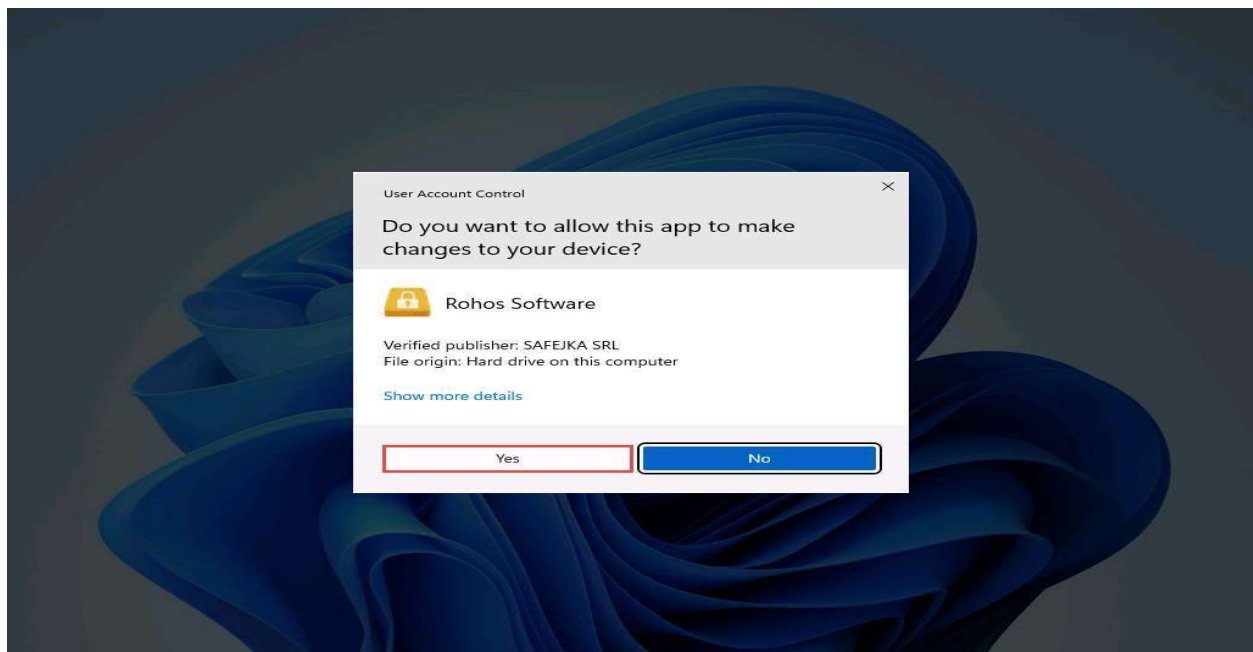
Here, we will use the Rohos Disk Encryption tool to perform disk encryption.

1. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Disk Encryption Tools\Rohos Disk Encryption** and double-click **rohos.exe**.

If a **User Account Control** pop-up appears, click **Yes**.

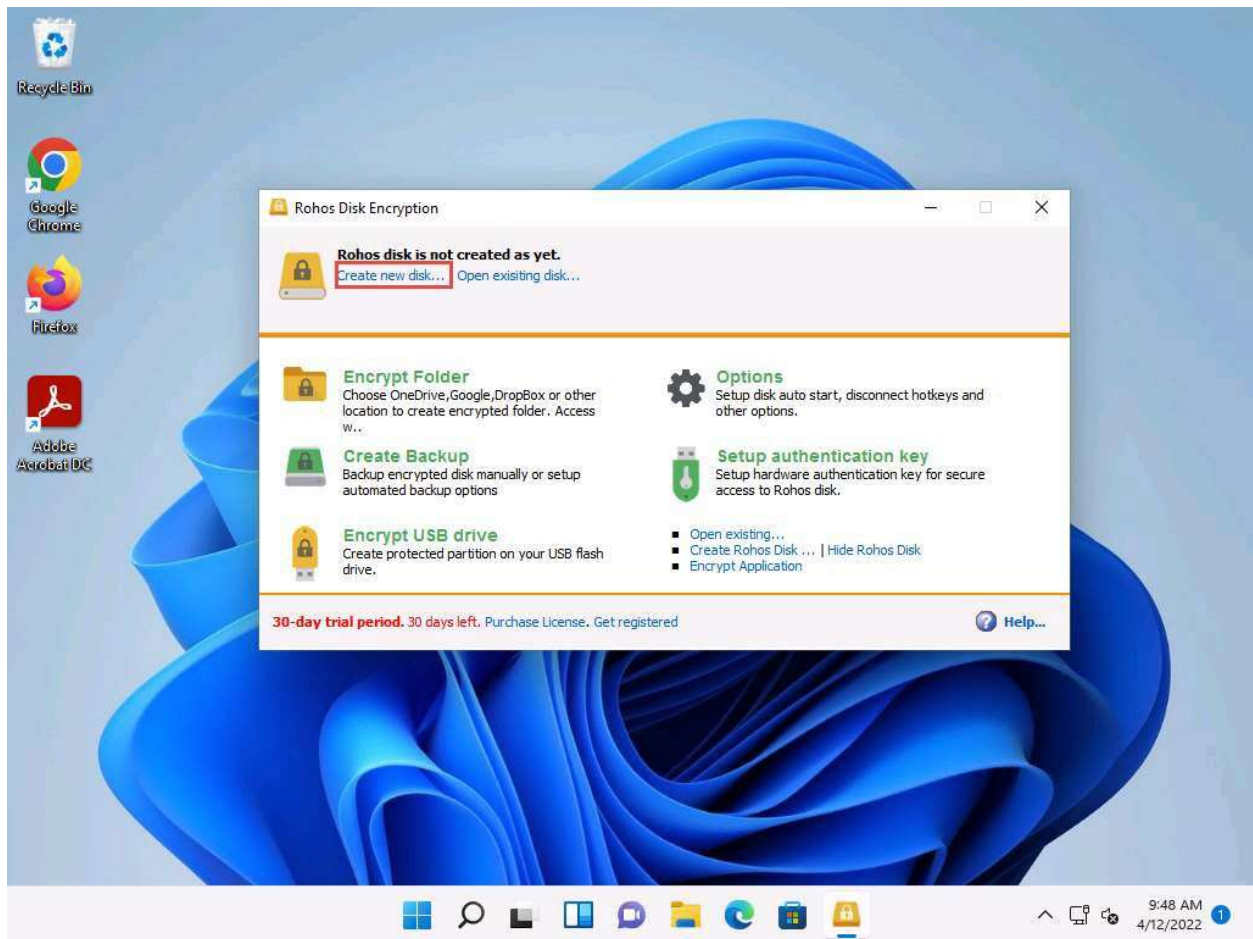
2. The **Select Setup Language** dialog box appears; click **OK**.
3. The **Setup - Rohos Disk Encryption** window appears; read the instruction and click **Next**.
4. Follow the steps and install the application using all default settings.
5. After the completion of the installation, **Completing the Rohos Disk Encryption Setup** wizard appears; ensure that the **Launch Rohos Disk** checkbox is checked and click **Finish**.

If **User Account Control** pop-up appears, click **Yes**.

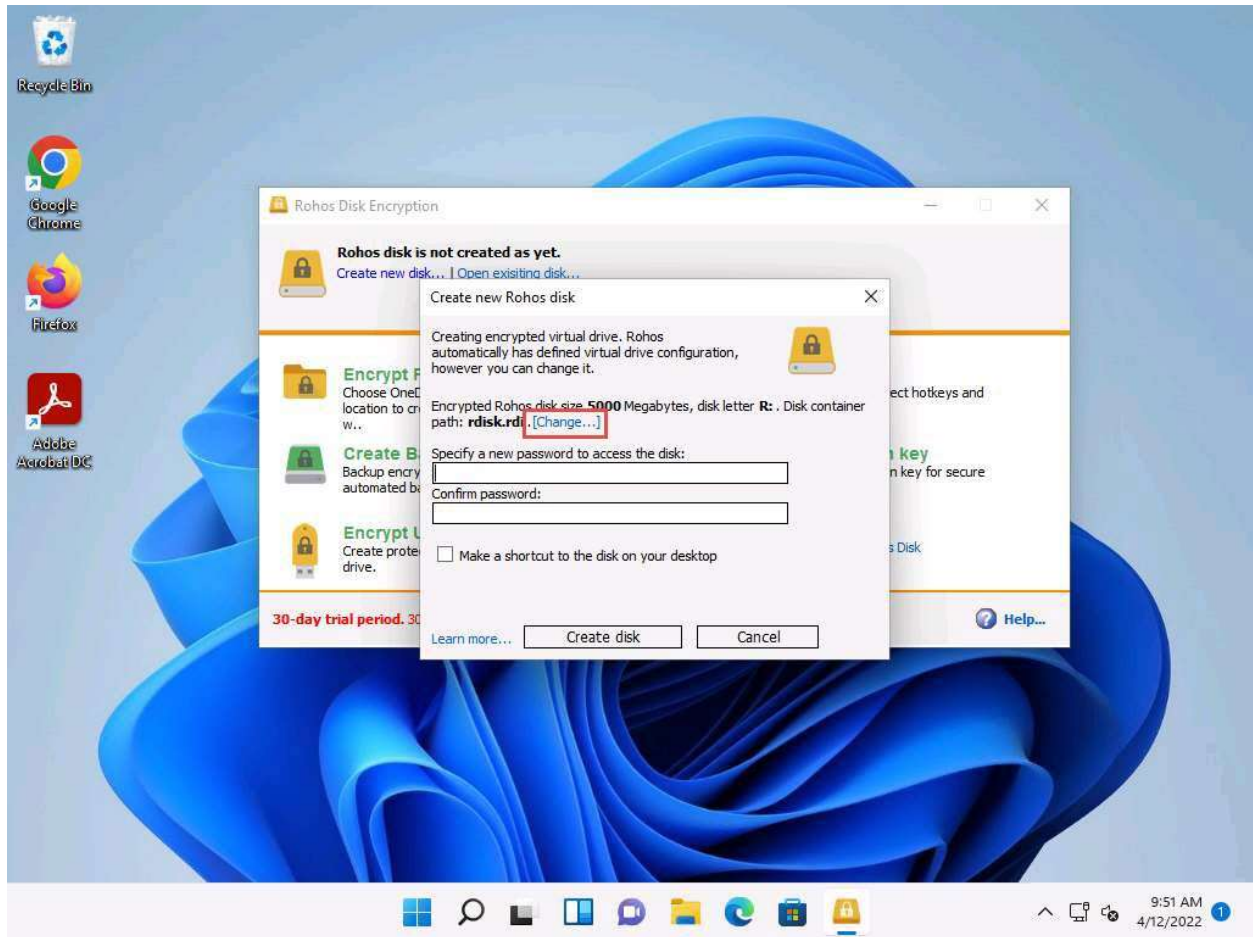




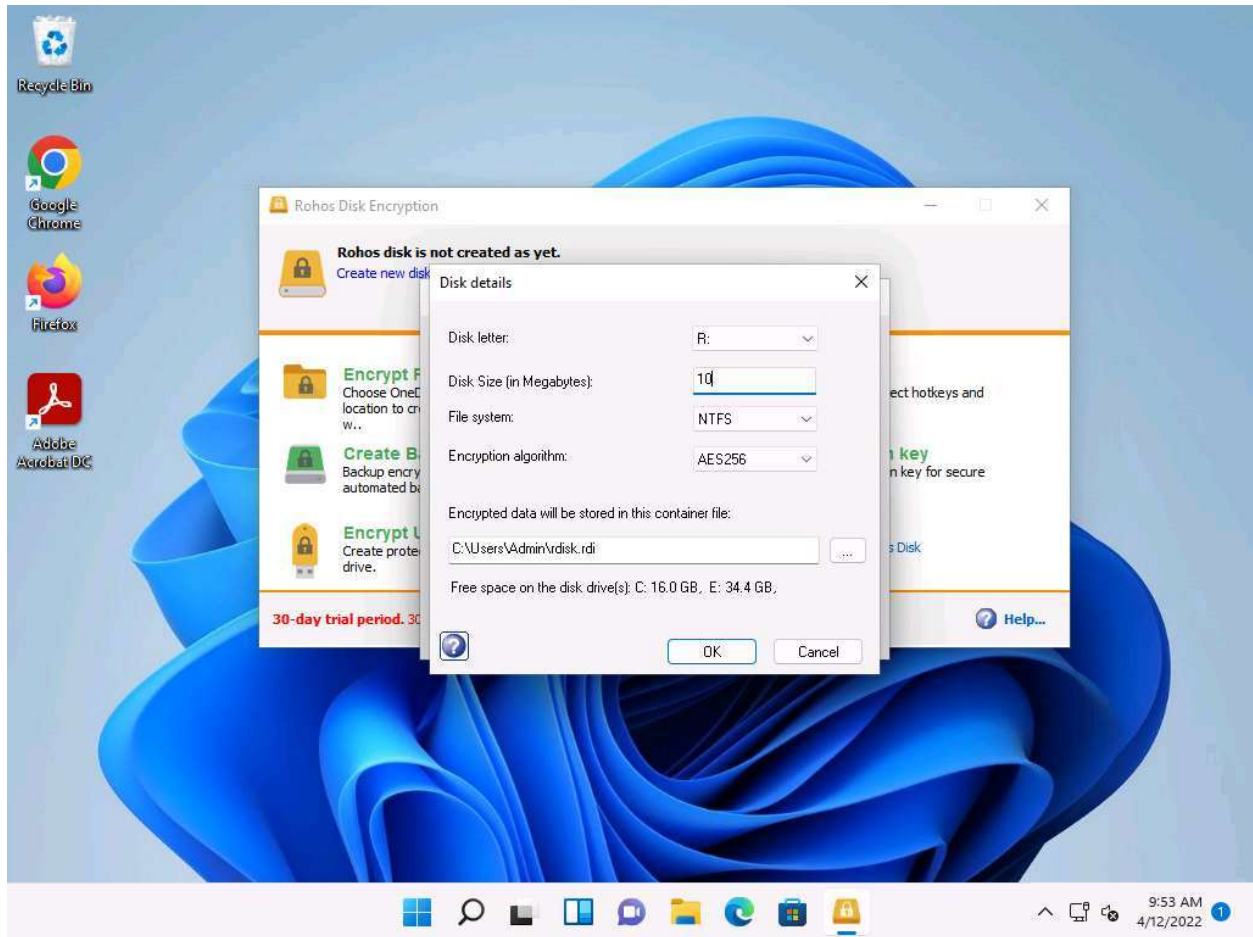
6. The **Rohos Disk Encryption** main window appears; click **Create new disk...**



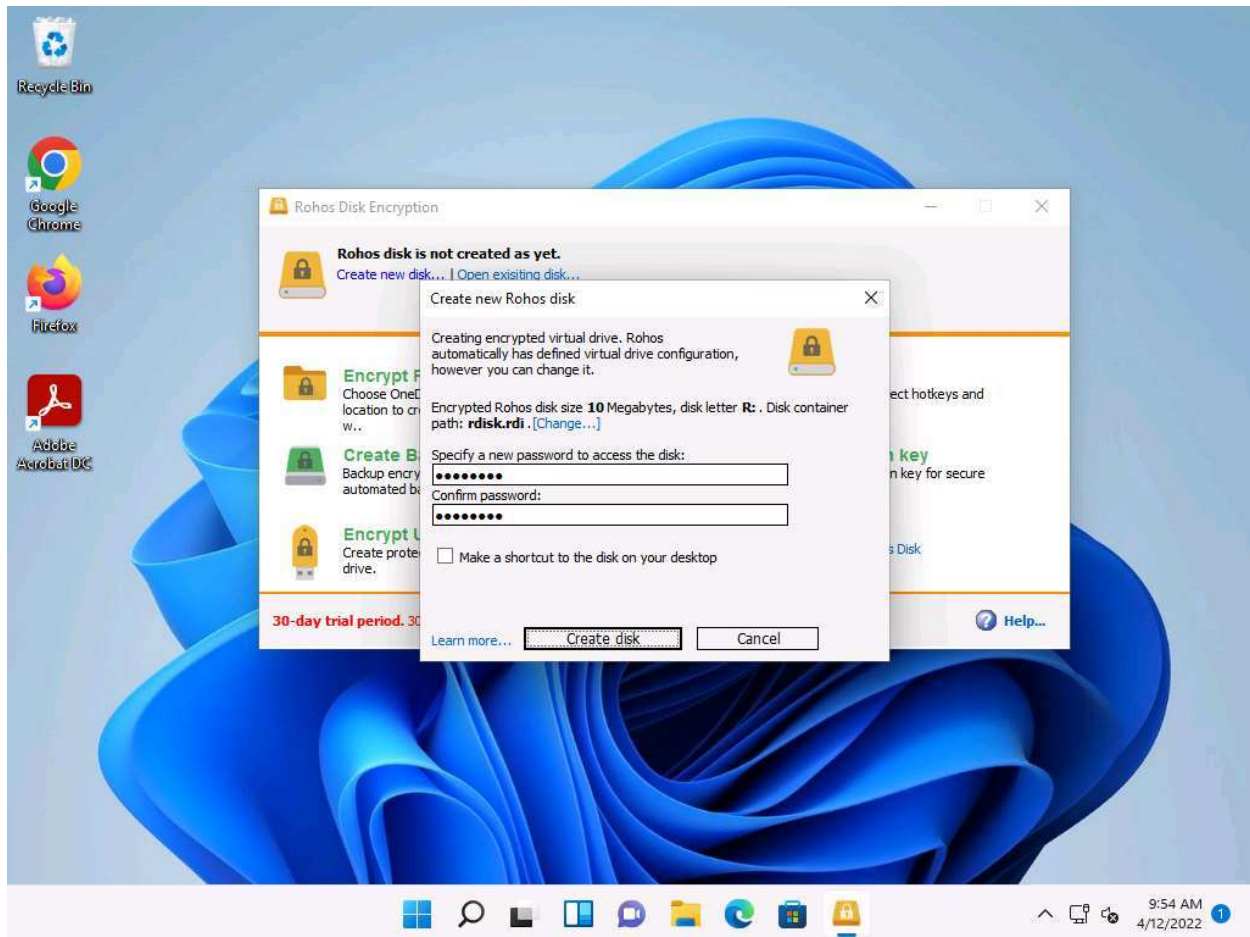
7. The **Create new Rohos disk** window appears; click **Change...** to modify the size of the encrypted disk.



8. The **Disk details** wizard appears; modify the disk size to **10** in the **Disk Size (in Megabytes)** field and leave all other settings to default; then, click **OK**.

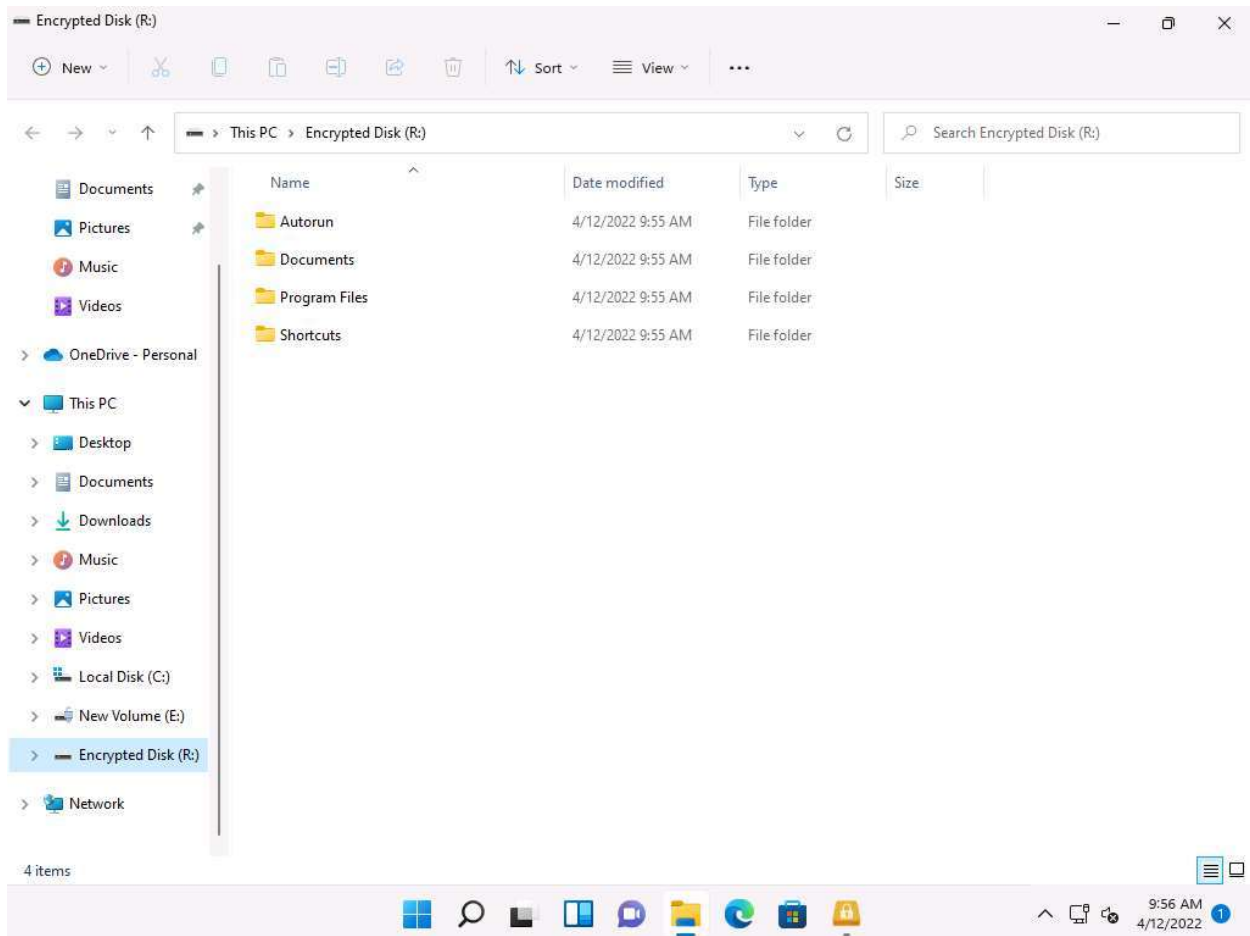


9. Provide a password in the **Specify a new password to access the disk** field and retype it into the **Confirm password** field; then, click **Create disk** button (Here, the password provided is **test@123**).



10. Wait until the encrypted volume is created. The time to create the encrypted volume depends upon the size you specified under the **Disk Size** option: if large, it will take a long time to create the volume.

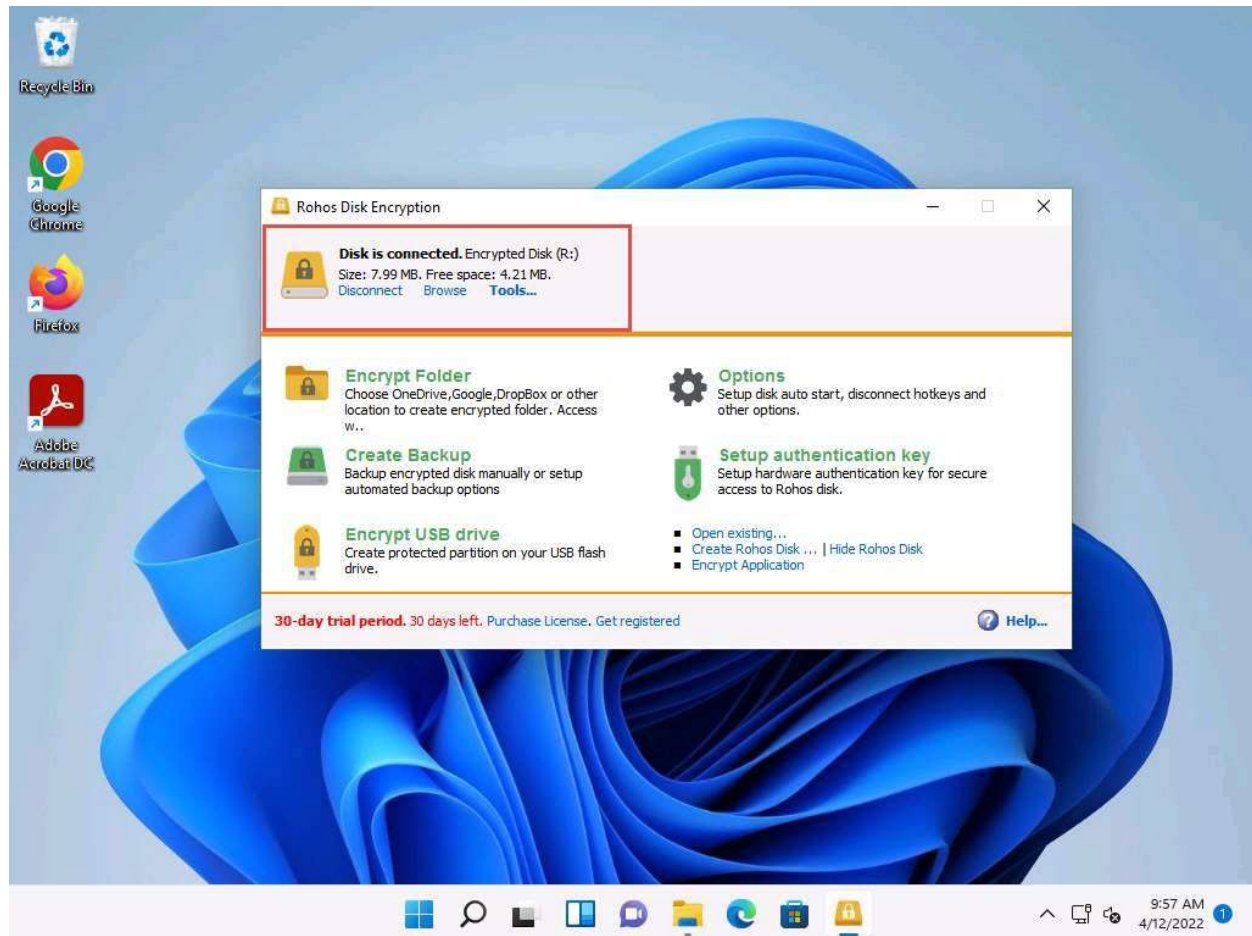
11. On creating the encrypted volume, the **Encrypted Disk (R:)** window appears, displaying the default disk content, as shown in the screenshot.





12. The **Disk is connected** notification appears at the top section of the **Rohos Disk Encryption** window.

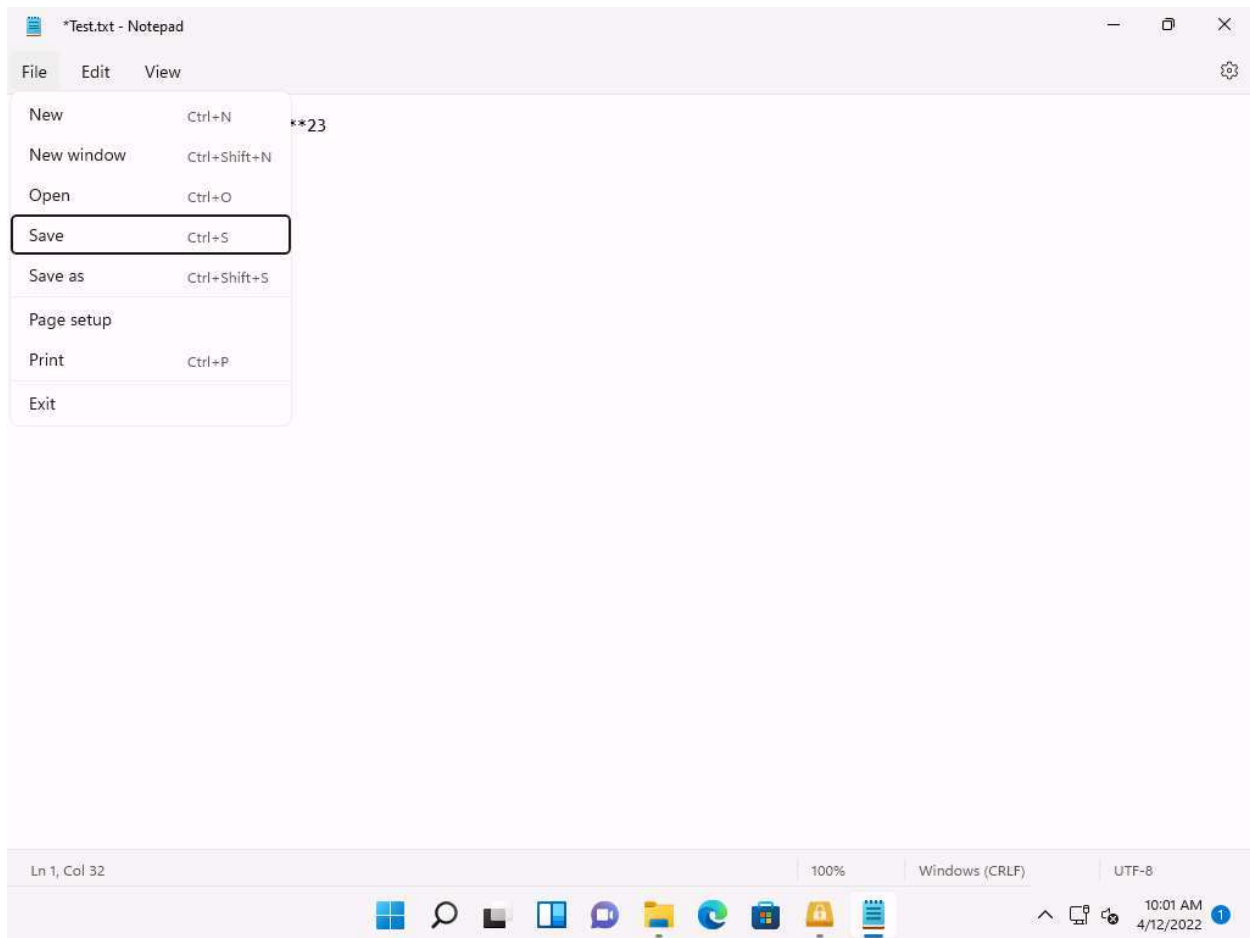
This drive appears only when you are connected to Rohos Disk Encryption, and disappears when you exit.



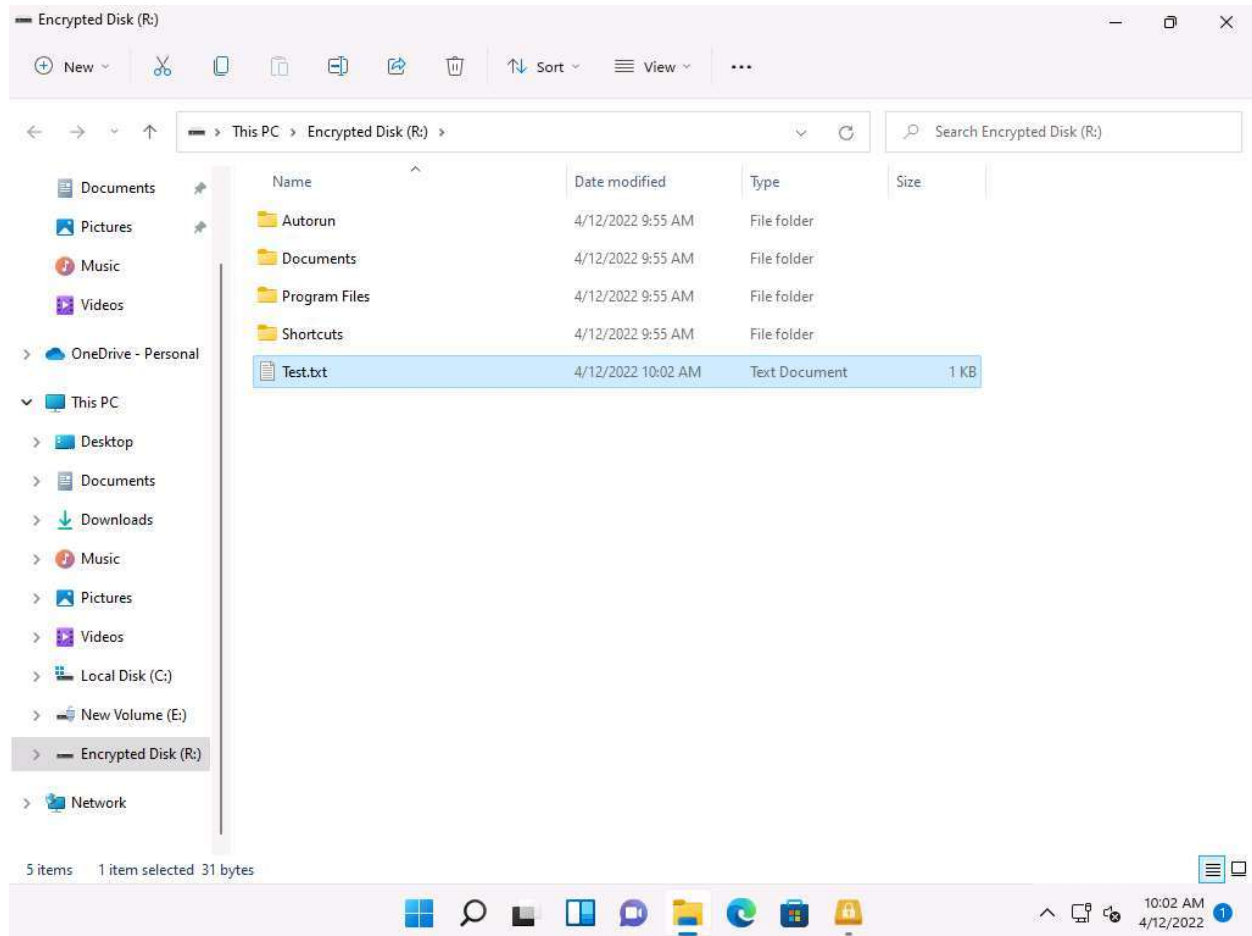
13. If you wish to conceal any important files/directories from anyone accessing your system, you can place them in this drive and access them whenever required (by launching Rohos and entering the password).

14. Now, we shall place a text file in **Encrypted disk (R:)**. To do so, create a text file on **Desktop** and name it **Test**. Open the file and insert text.

15. Click **File** in the menu bar and click **Save**.

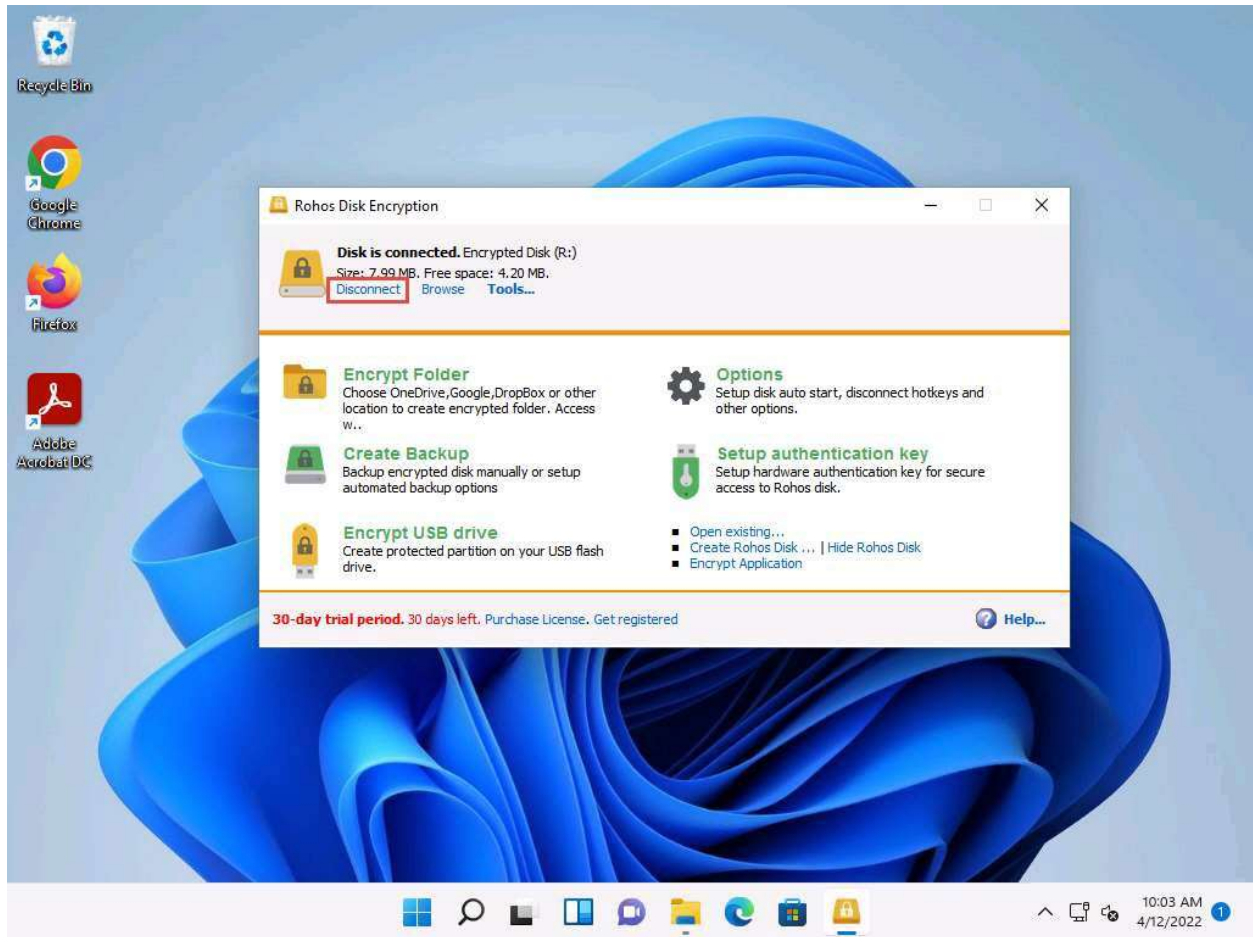


16. Copy the file from **Desktop** and paste into **Encrypted Disk (R:)**. Close the window.

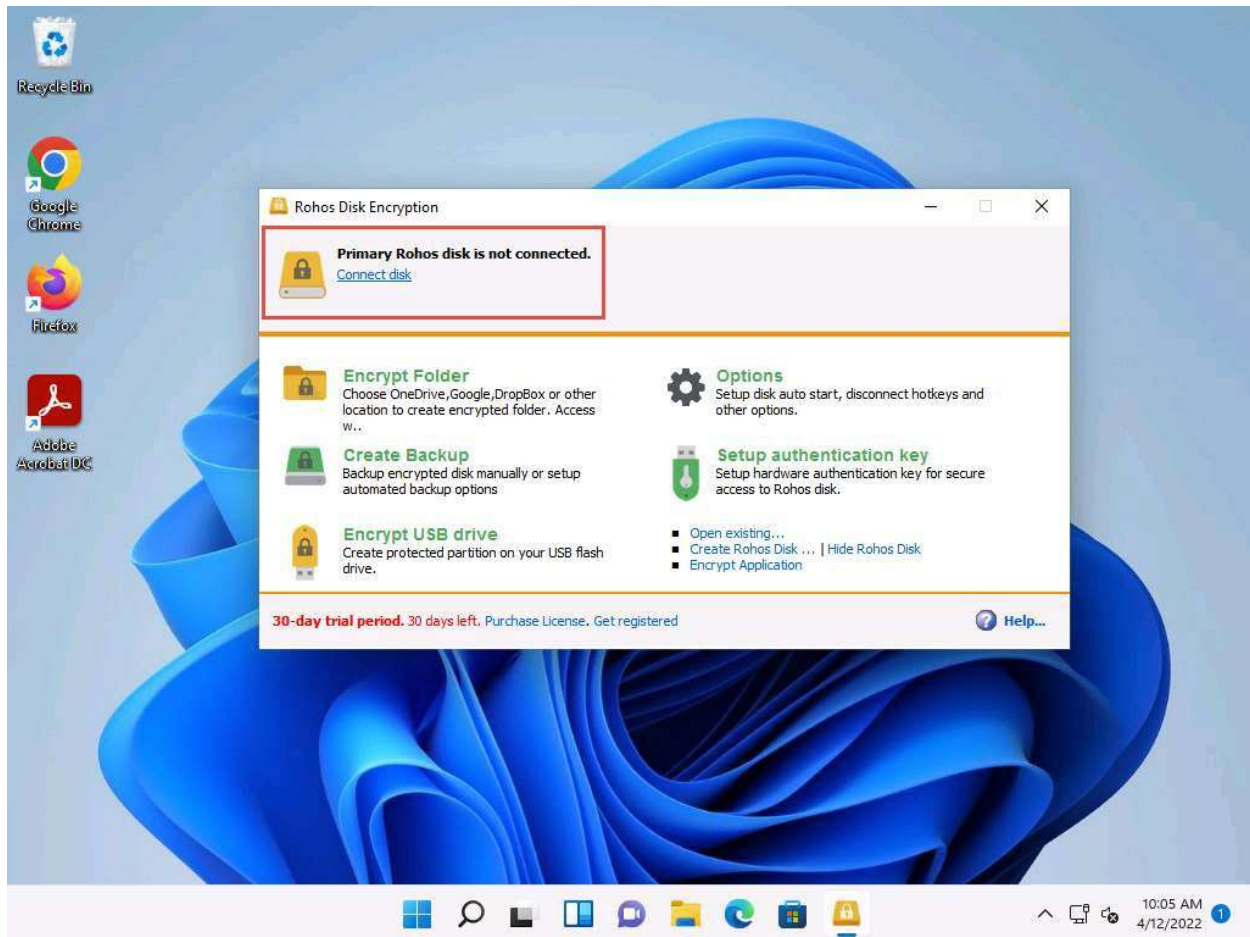




17. Switch to the **Rohos Disk Encryption** window and click **Disconnect** to dismount **Encrypted disk (R:)**.

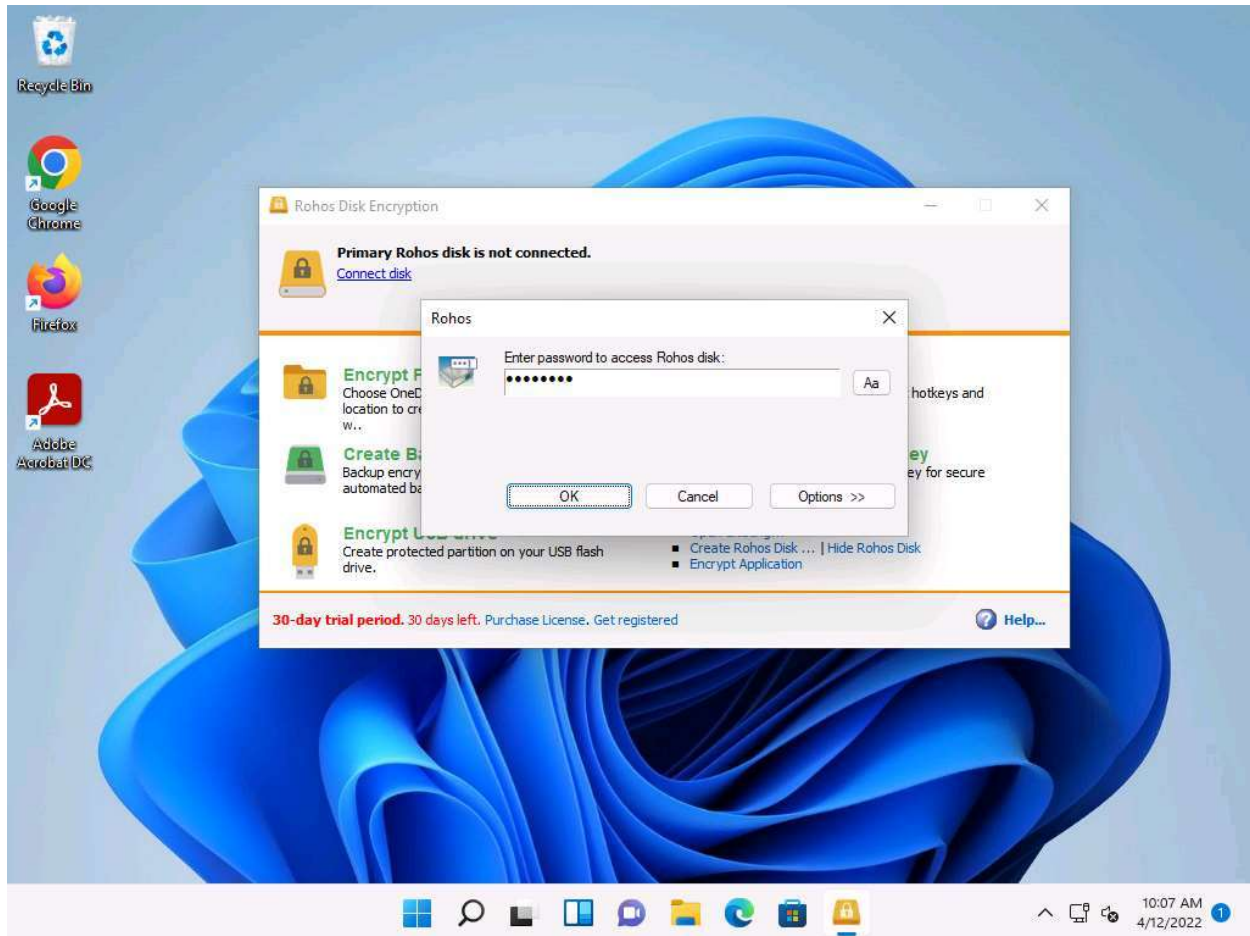


18. A notification appears stating **Primary Rohos disk is not connected** at the top of the **Rohos Disk Encryption** window. To mount the disk again, click the **Connect disk** option.

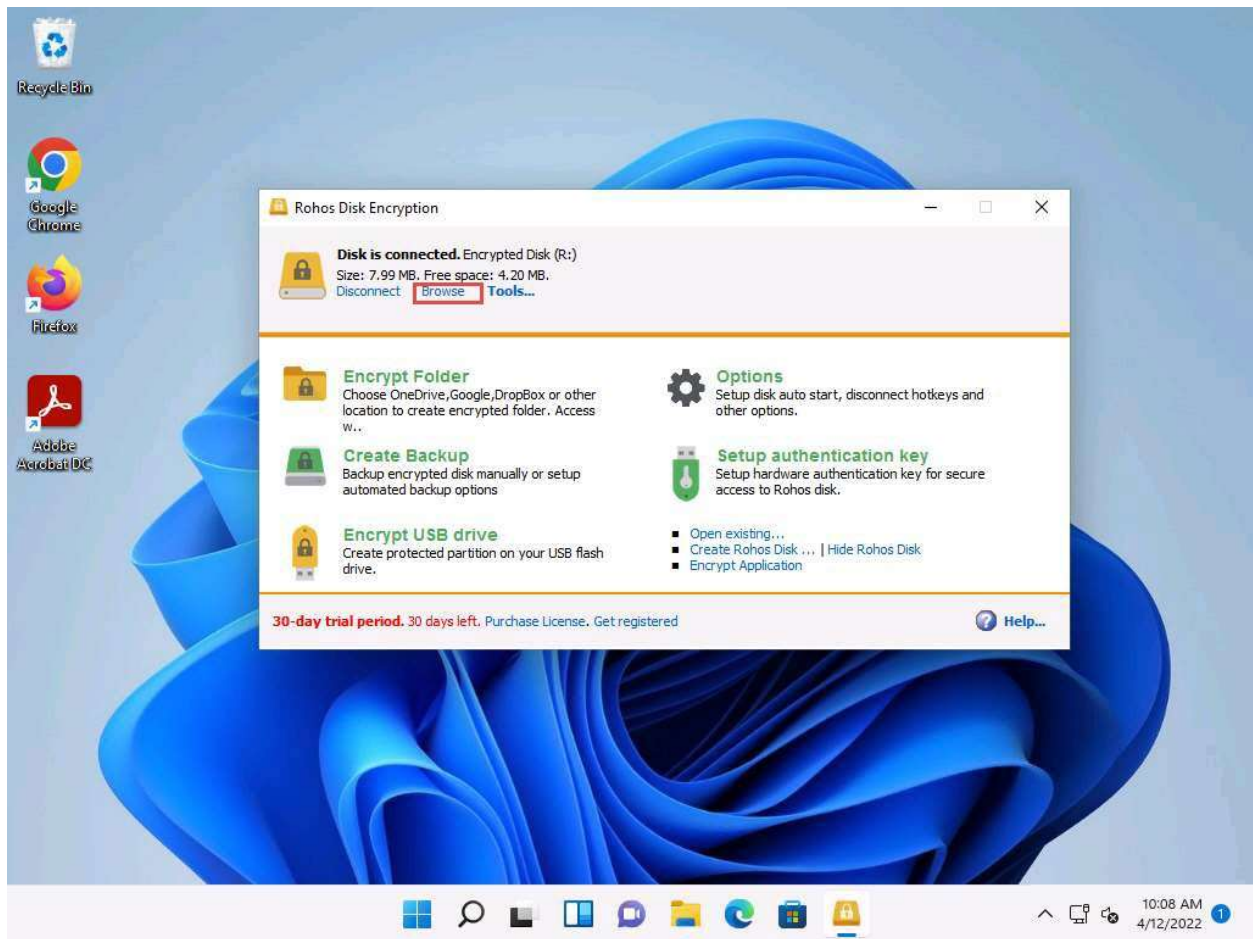


19. The **Rohos** pop-up appears; type the password you provided in **Step#6** into the **Enter password to access Rohos disk** field and click **OK**.

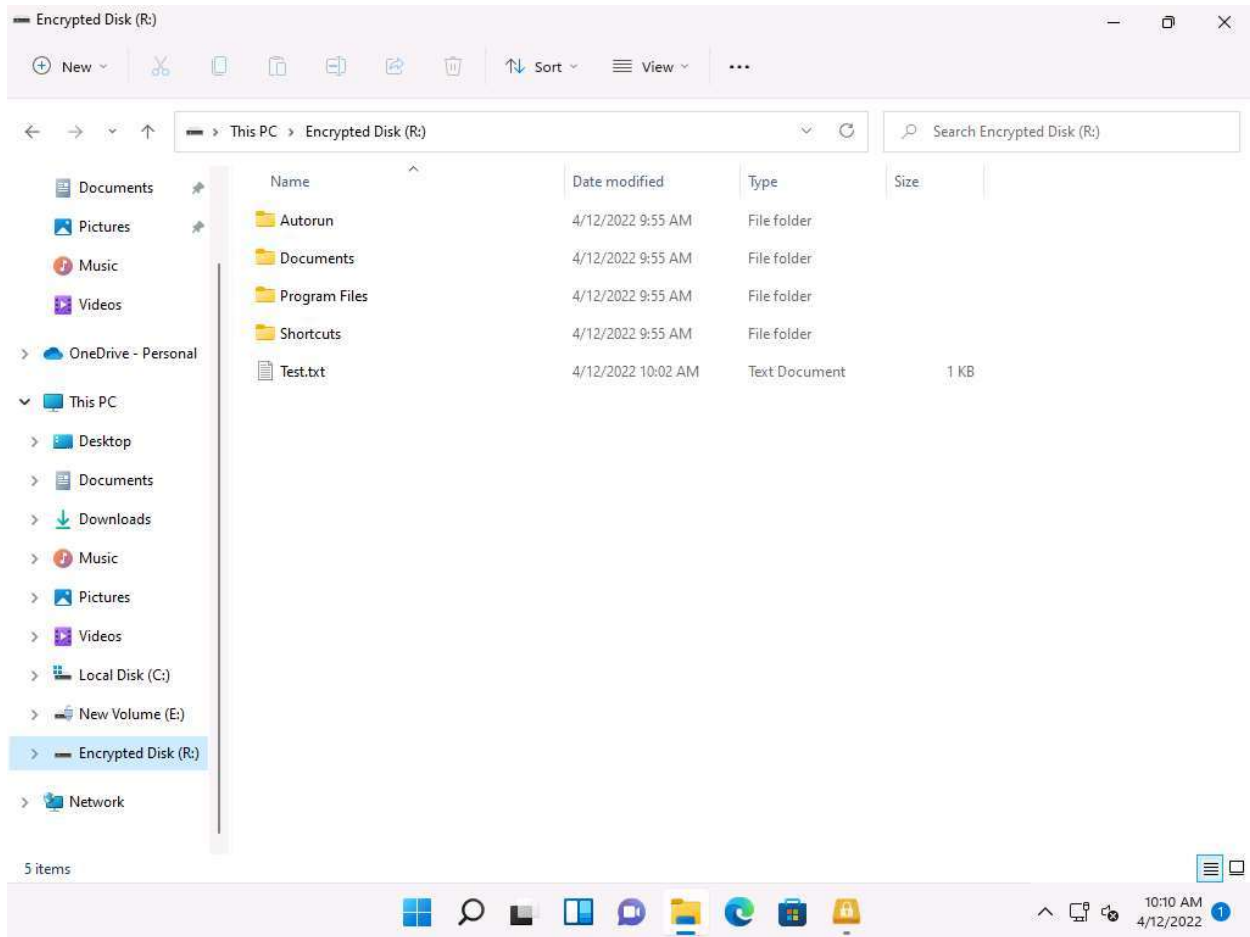
Here, the password is **test@123**.



20. The **Disk is connected** notification appears in the **Rohos Disk Encryption** window. Click **Browse** to explore the disk content.

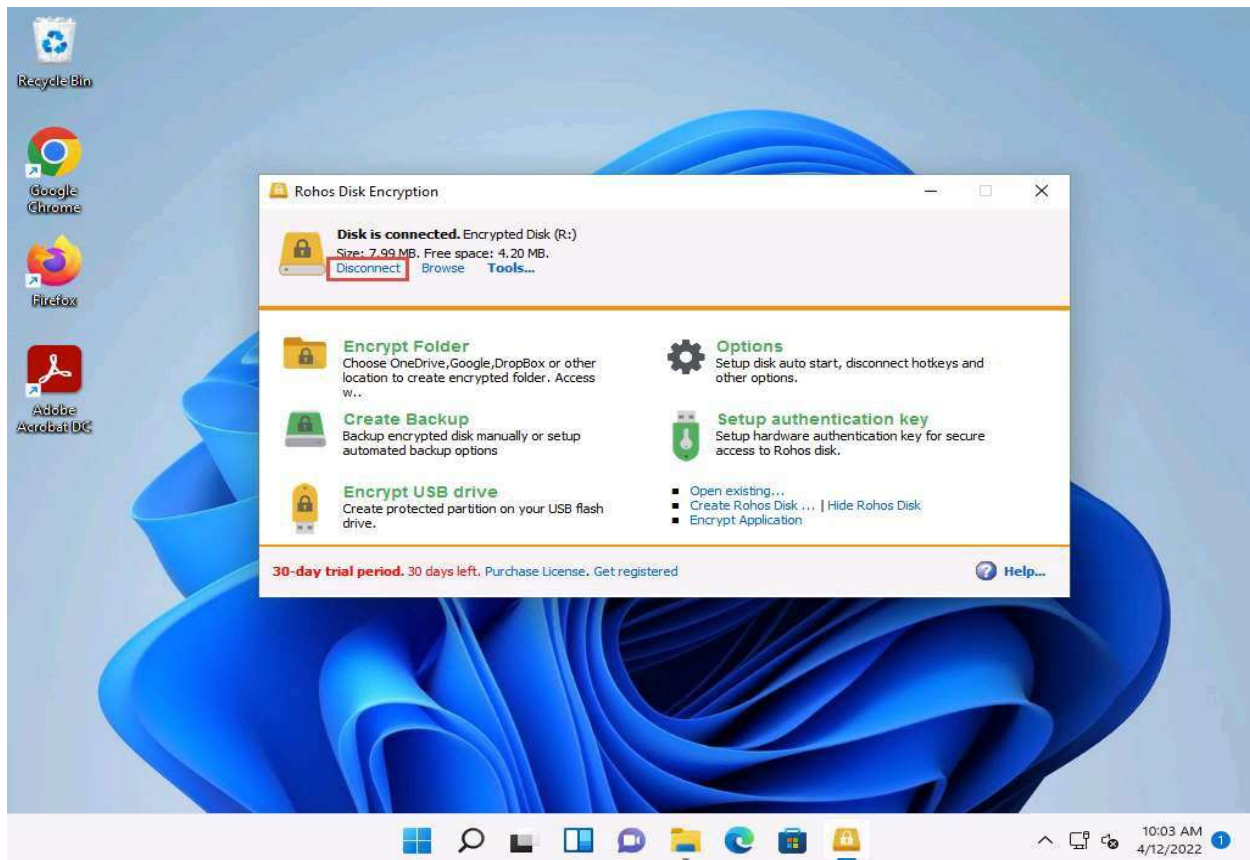


21. The **Encrypted Disk (R:)** window appears; you can see the **Test.txt** file that was pasted onto the disk earlier, as shown in the screenshot.



22. You can access the disk content and further add, delete, and modify the files. After making the intended changes, click **Disconnect** again in the **Rohos Disk Encryption** window to dismount the disk.





You can also use the Encrypt USB drive option to share sensible information with someone via USB. You can use this application to store the files in an encrypted disk and share the password with that person. The person with whom you want to share the files can access them only after entering the correct password. This way, you can protect the files from being viewed by a third person and thereby safeguard them.

23. This concludes the demonstration of performing disk encryption using Rohos Disk Encryption.

24. You can also use other disk encryption tools such as **FinalCrypt** (<http://www.finalcrypt.org>), **Seqrite Encryption Manager** (<https://www.seqrite.com>), **FileVault** (<https://support.apple.com>), and **Gillsoft Full Disk Encryption** (<http://www.gilisoft.com>) to perform disk encryption.

25. Close all open windows and document all the acquired information

### Question 20.4.3.1

Perform disk encryption using Rohos. Which encryption algorithm is used in Rohos?

## InstructionsResources

### Lab 5: Perform Cryptanalysis using Various Cryptanalysis Tools

#### Lab Scenario

Attackers tend to focus on easy to compromise targets. Therefore, in order to attain maximum network security, strong encryption is needed for all the traffic placed onto the transmission media, no matter the type and location: if an attacker wishes to break into an encrypted network, he/she faces decrypting a whole slew of encrypted packets, which is a difficult task. Therefore, the attacker is likely to try and find another target that is easy to compromise or will simply abort the attempt. Using the latest encryption algorithms provides a strong layer of security to an organization.

As a professional ethical hacker or pen tester, you should possess the required knowledge to investigate the security of cryptographic systems. In order to confirm the security of the cryptographic systems, you must implement various cryptography attacks to evade the system's security by exploiting vulnerabilities in codes, ciphers, cryptographic protocols, or key management schemes.

In this lab, you will learn how to compromise cryptographic systems using various cryptanalysis techniques and tools that help in breaching cryptographic security.

#### Lab Objectives

- Perform cryptanalysis using CrypTool
- Perform cryptanalysis using AlphaPeeler

#### Overview of Cryptanalysis

Cryptanalysis can be performed using various methods, including the following:

- **Linear Cryptanalysis:** A known plaintext attack that uses a linear approximation to describe the behavior of the block cipher
- **Differential Cryptanalysis:** The examination of differences in an input and how this affects the resultant difference in the output
- **Integral Cryptanalysis:** This attack is useful against block ciphers based on substitution-permutation networks and is an extension of differential cryptanalysis

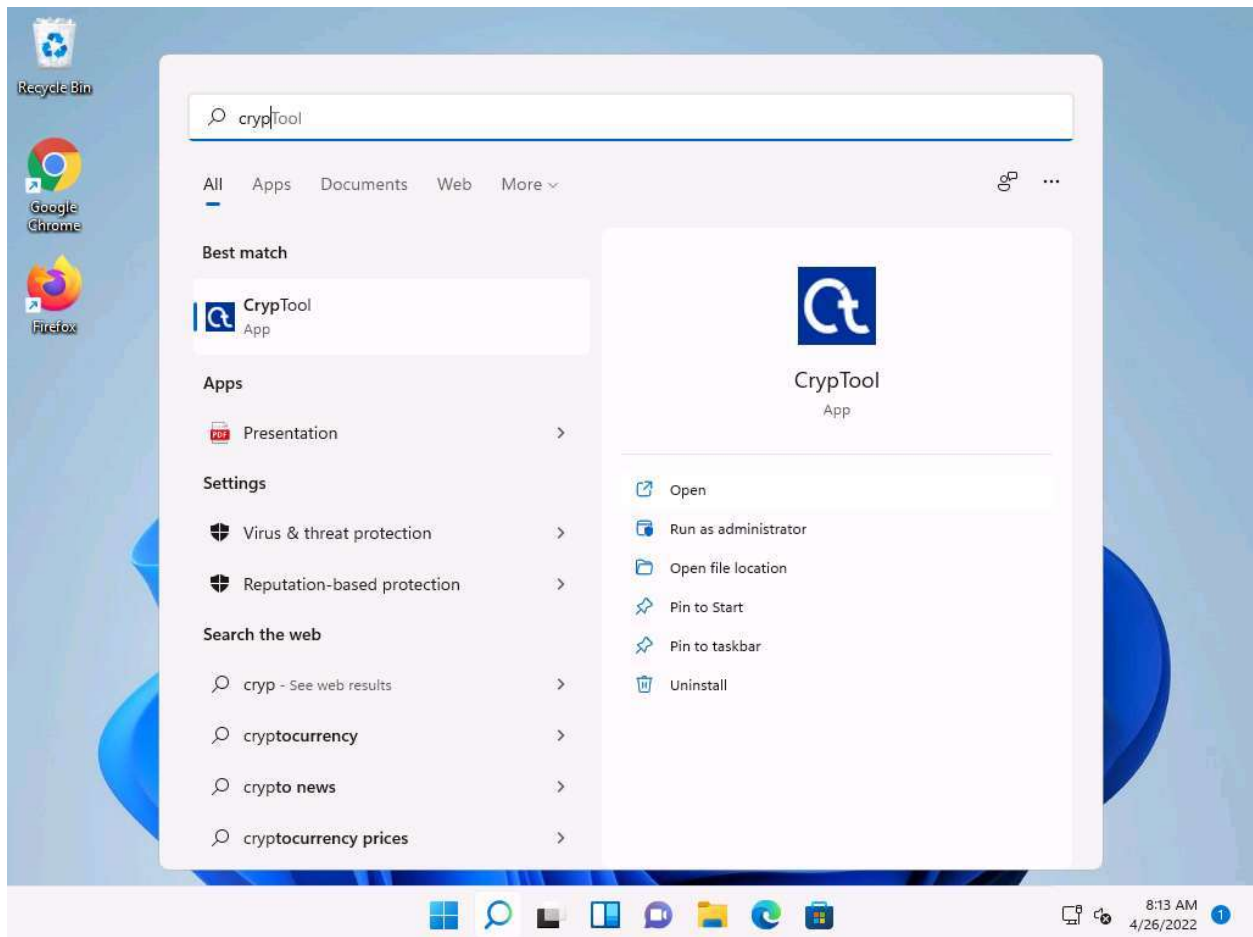
## Task 1: Perform Cryptanalysis using CrypTool

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms, and has the typical look and feel of a modern Windows application. CrypTool includes a multitude of state-of-the-art cryptographic functions and allows you to both learn and use cryptography within the same environment. CrypTool is a free, open-source e-learning application used in the implementation and analysis of cryptographic algorithms.

Here, we will use the CrypTool tool to perform cryptanalysis.

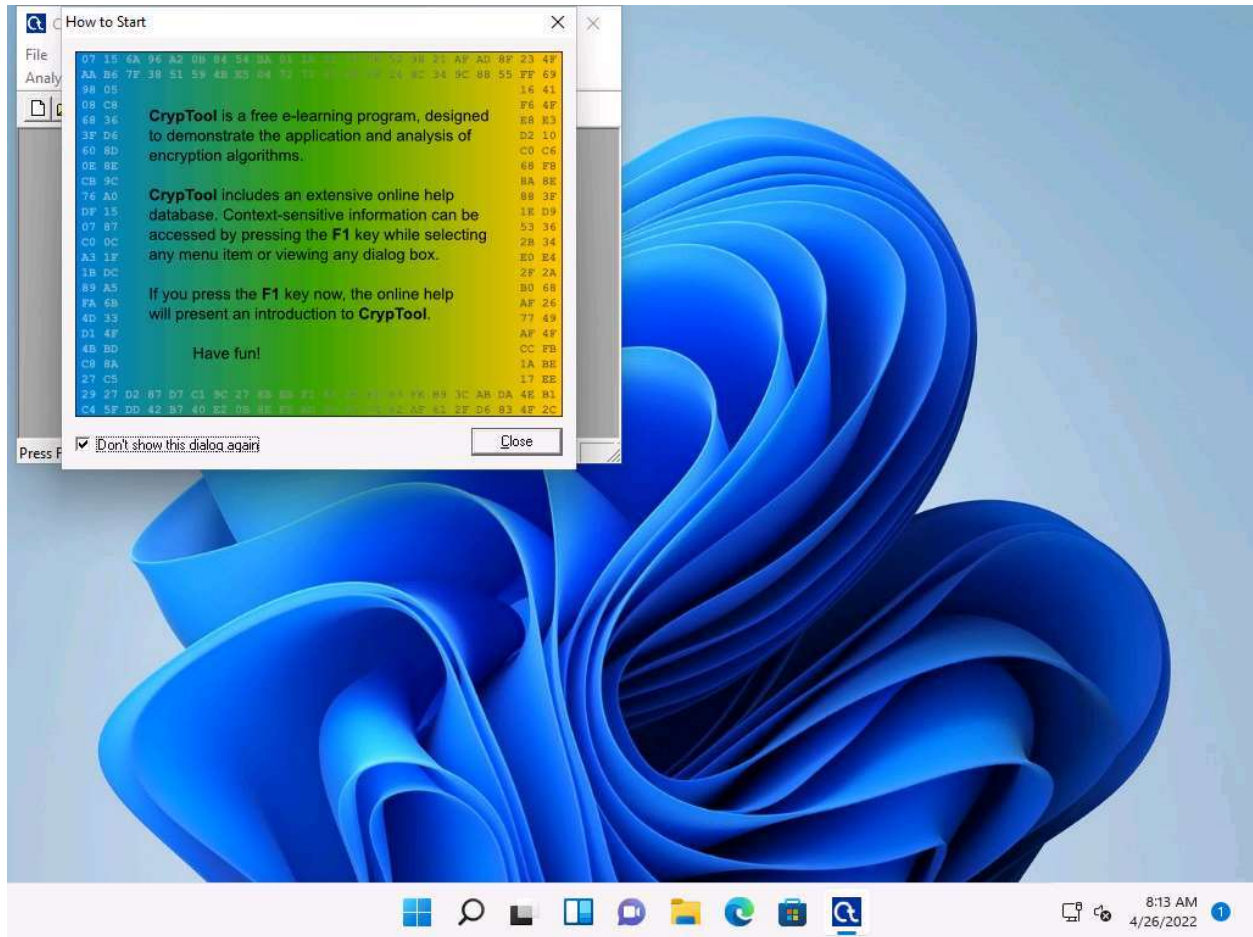
1. Click **Search** icon (  ) on the **Desktop**. Type **crypt** in the search field, the **CrypTool** appears in the results, click **Open** to launch it.

If a **User Account Control** pop-up appears, click **Yes**.

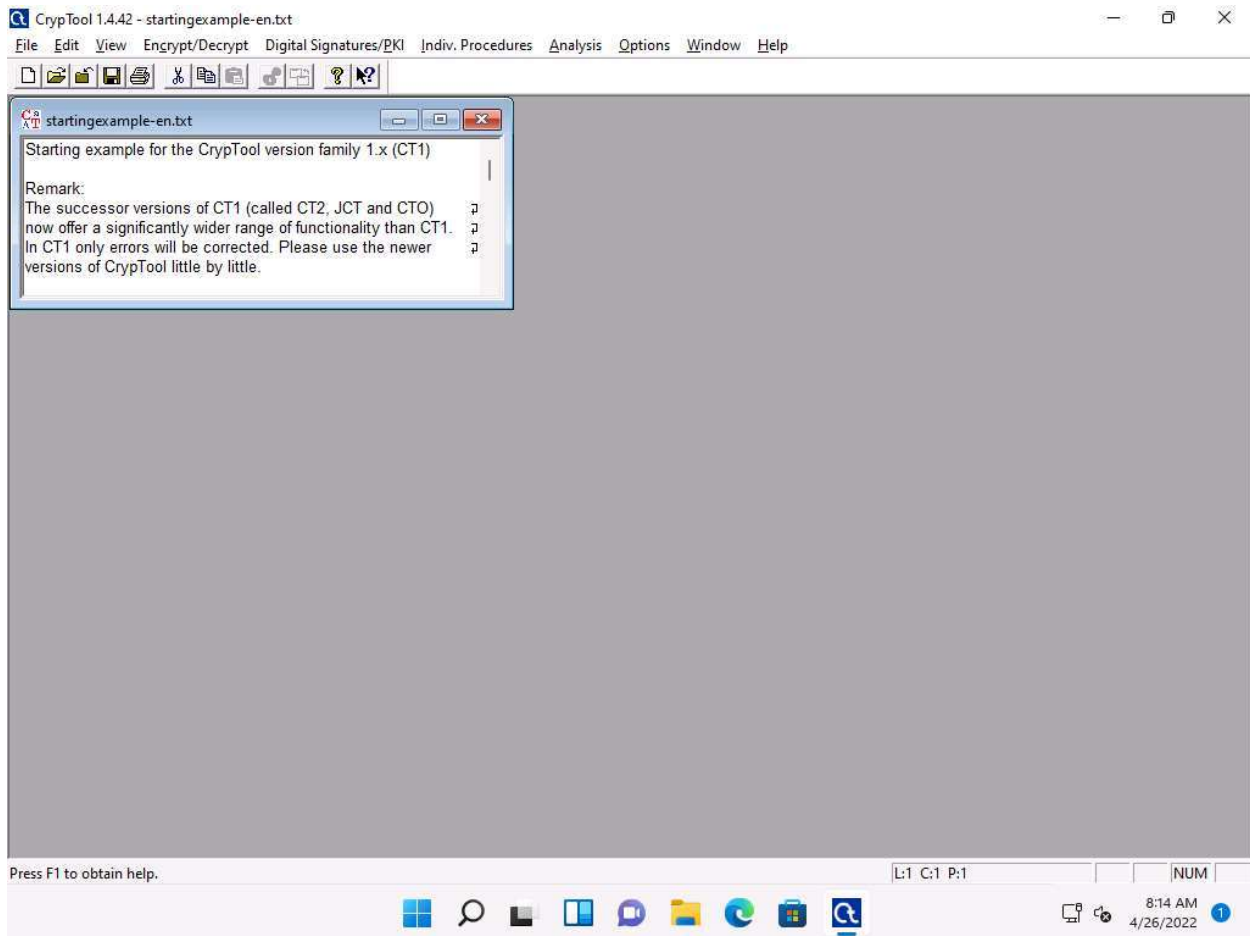




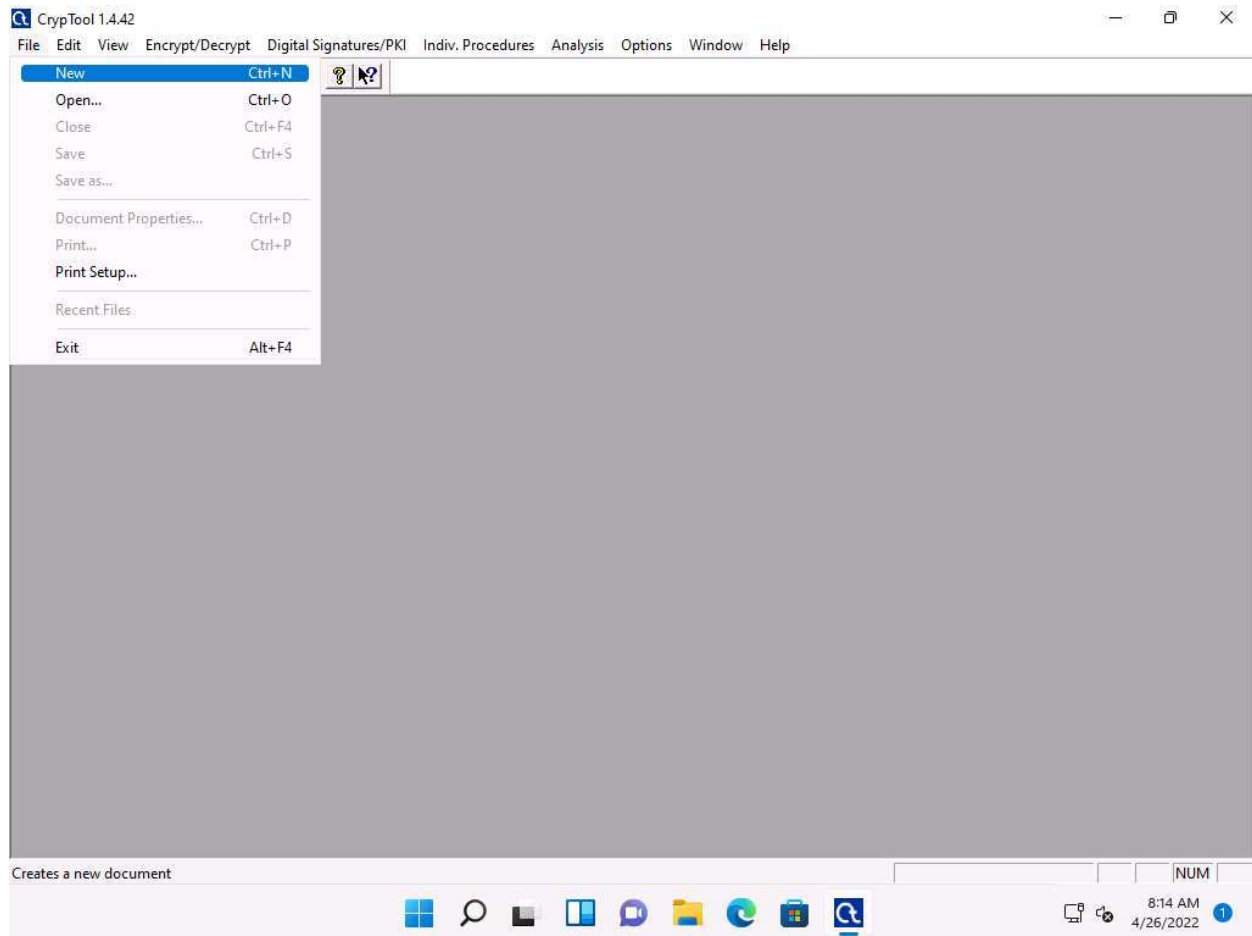
2. The **CrypTool** main window appears with a **How to Start** window. Check the **Don't show this dialog again** checkbox and click **Close**.



3. The **CrypTool** window appears; close the **startingexample-en.txt** window.

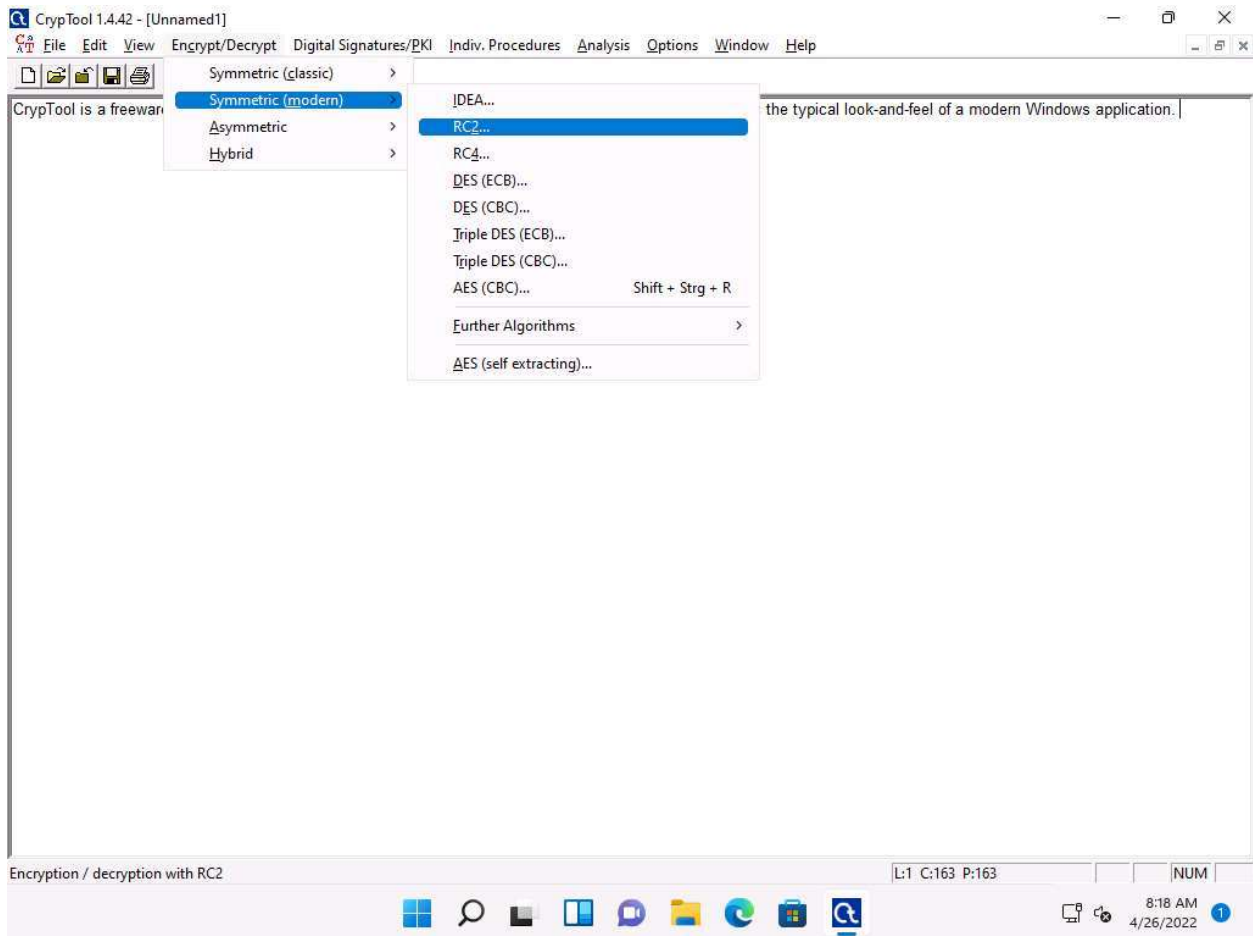


4. Click the **File** option from the menu bar and select **New** to create encrypted data.



5. The **Unnamed1** notepad appears; insert some text into the file. You will be encrypting this content.
6. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern)** --> **RC2....**

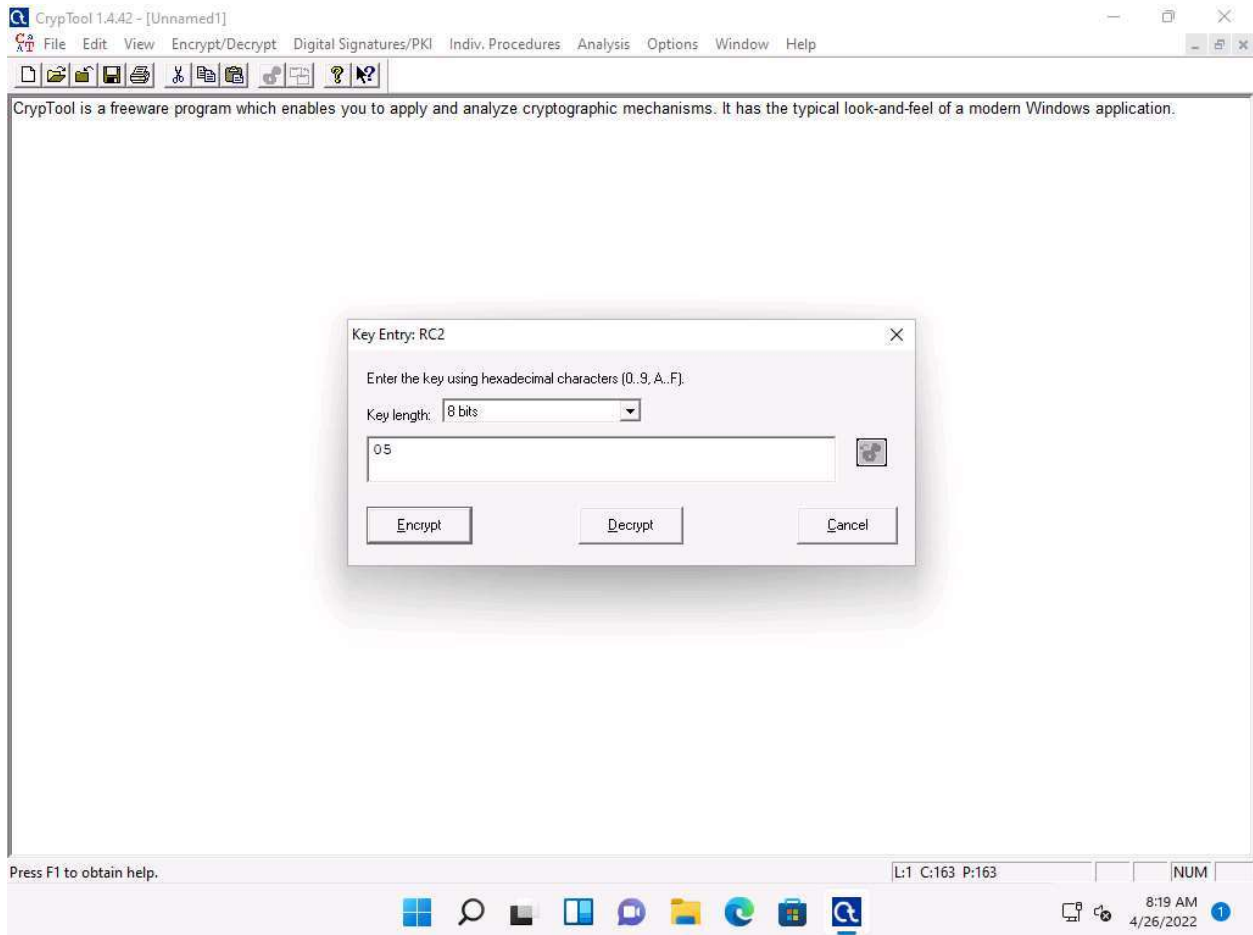
RC2 is a symmetric-key block cipher. It is a 64-bit block cipher with variable key size and uses 18 rounds.



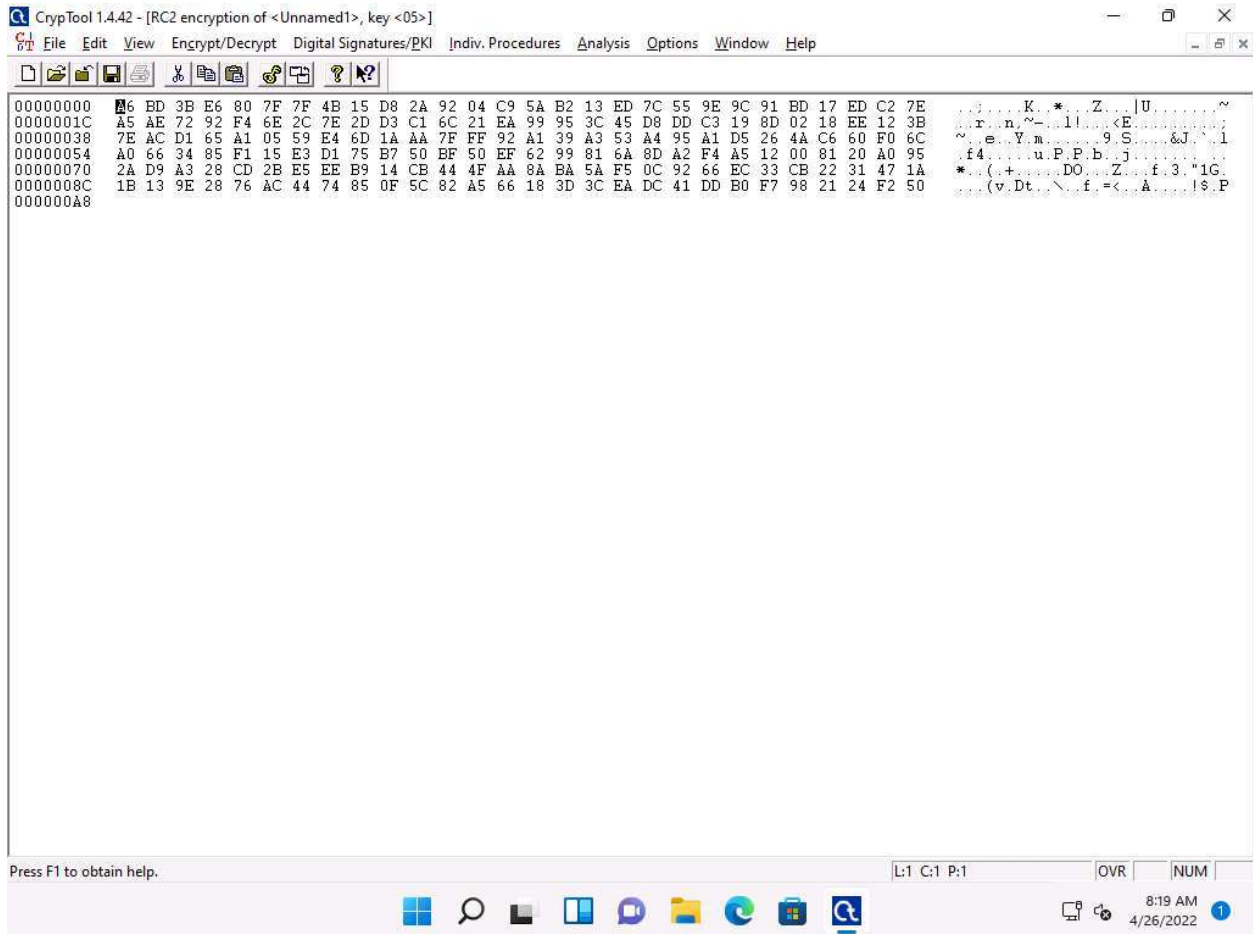
7. The **Key Entry: RC2** dialog box appears; keep the **Key length** set to default (**8 bits**).

8. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Encrypt**.

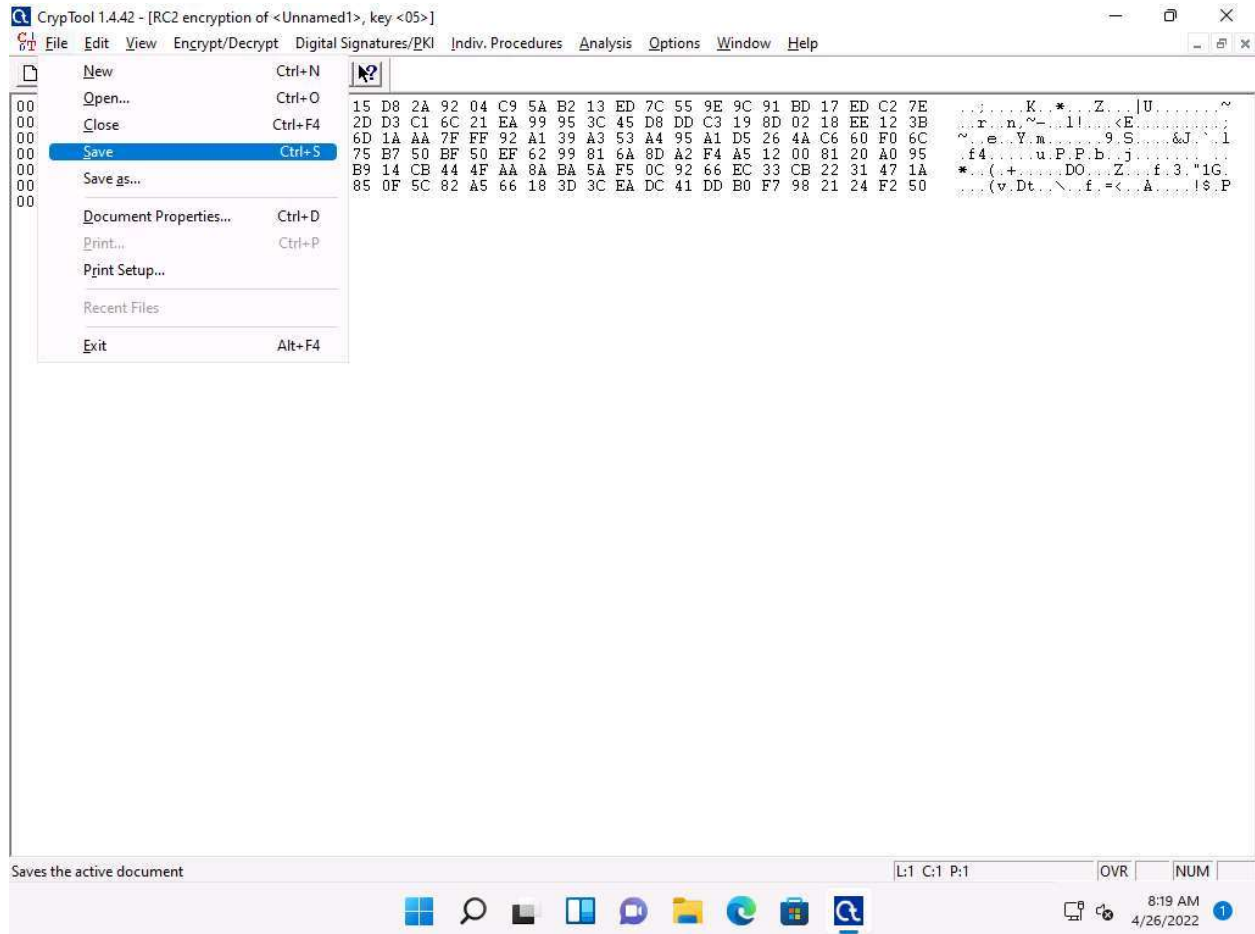
The chosen hexadecimal character acts as a key that you must send to the intended user along with the encrypted file.



9. The **RC encryption of Unnamed1** notepad file appears, as shown in the screenshot.

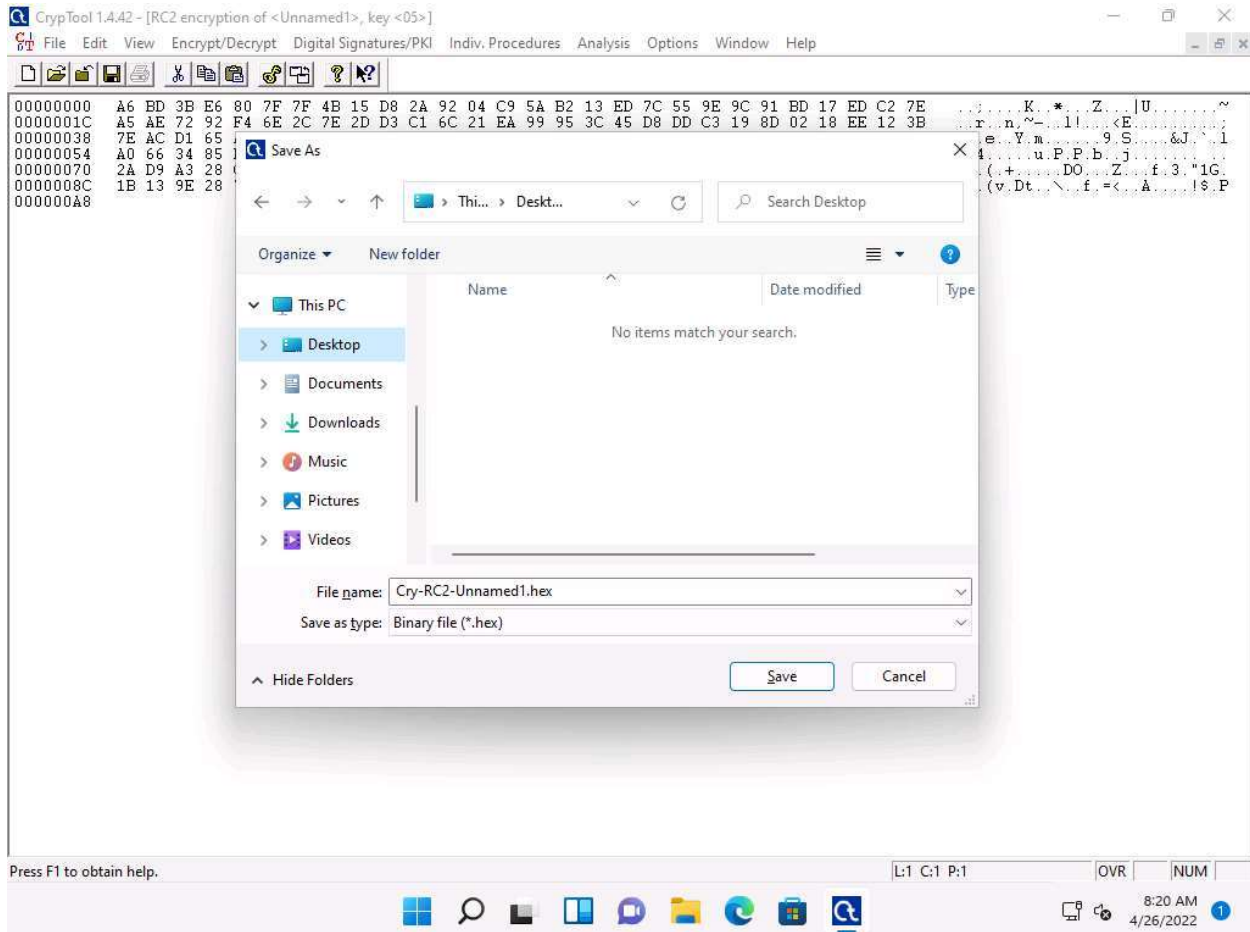


10. To save, click **File** in the menu bar and select **Save**.



11. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

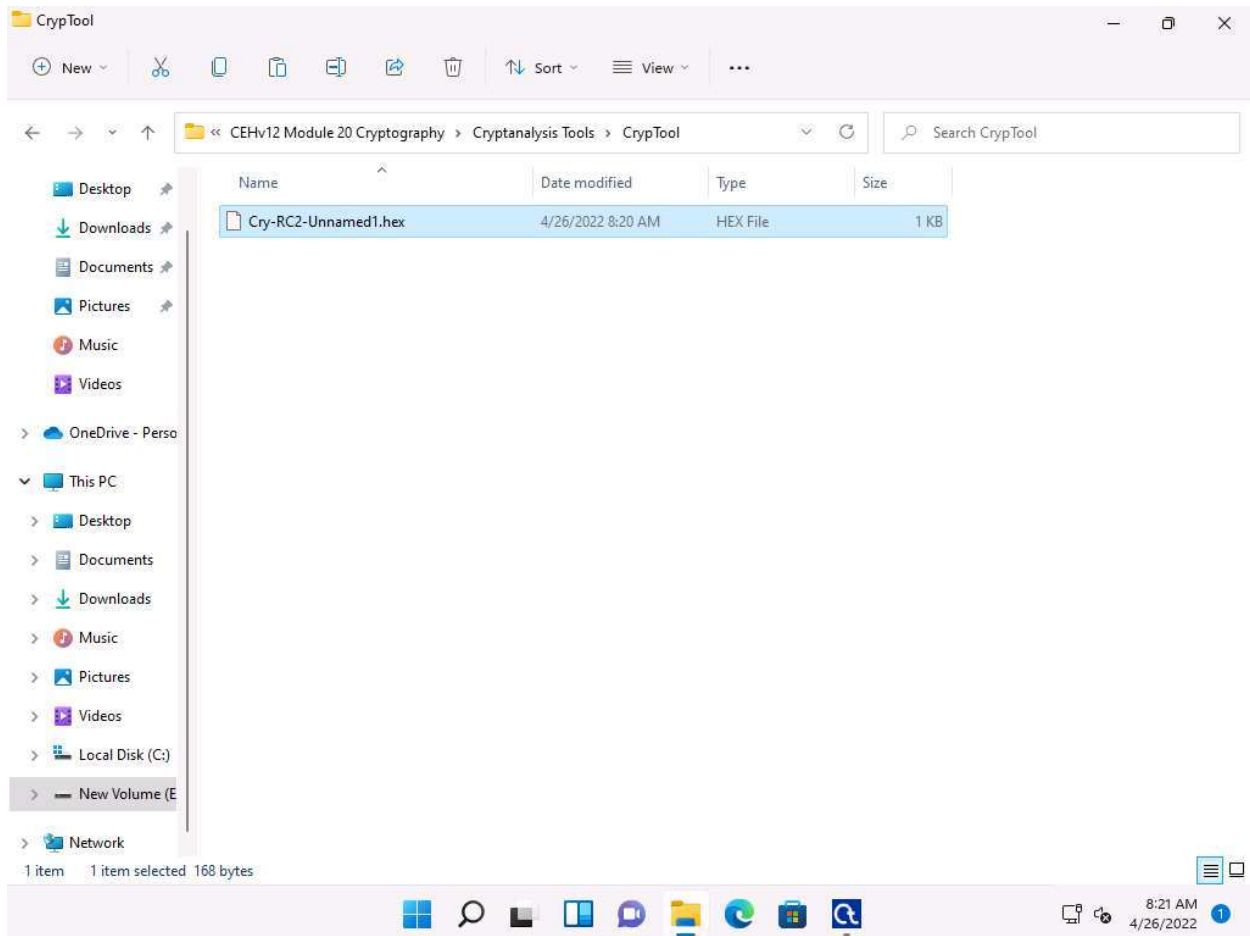
The file name may differ when you perform the task.



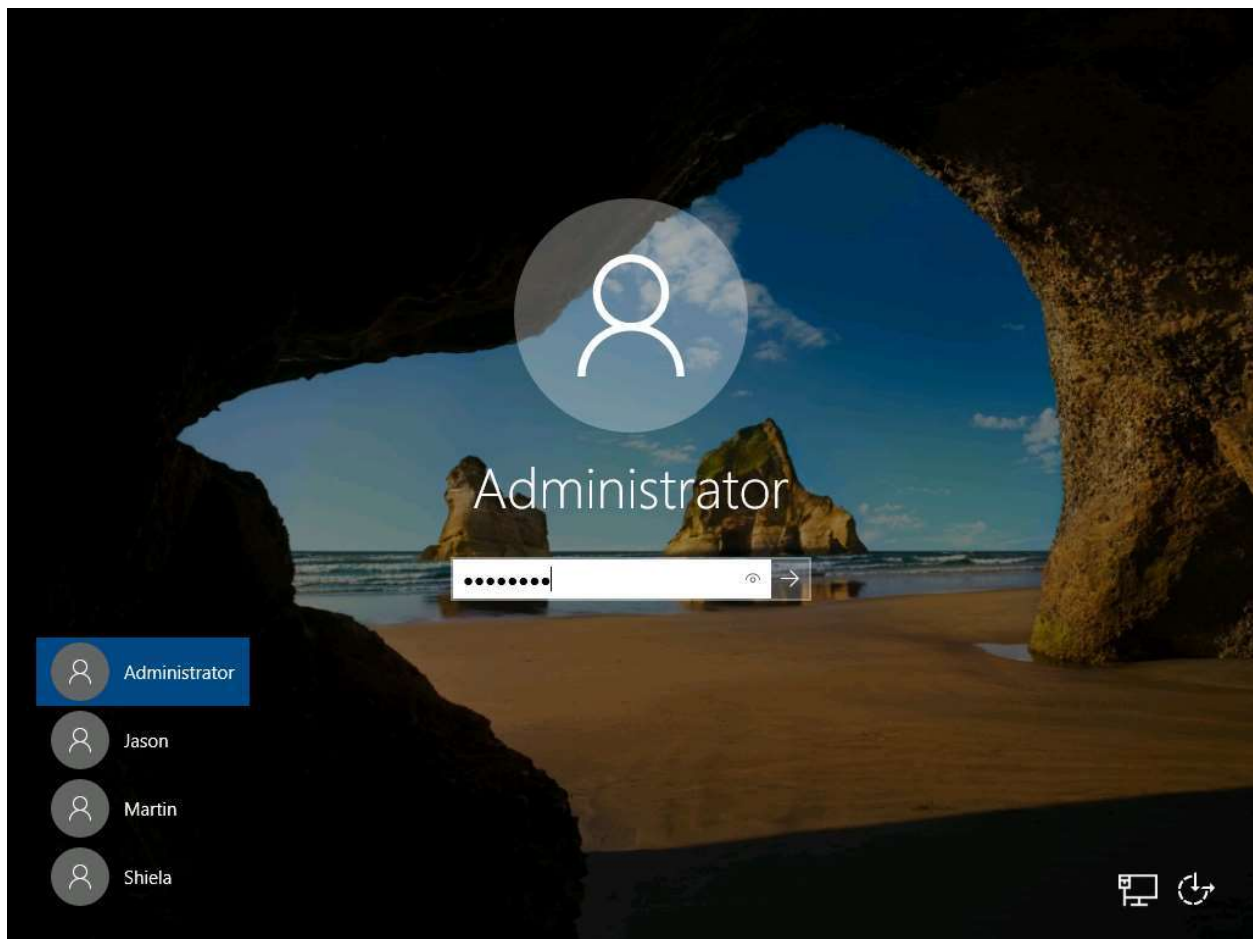


12. Now, you can send this file to the intended person by email or any other means and provide him/her with the hex value, which will be used to decrypt the file.

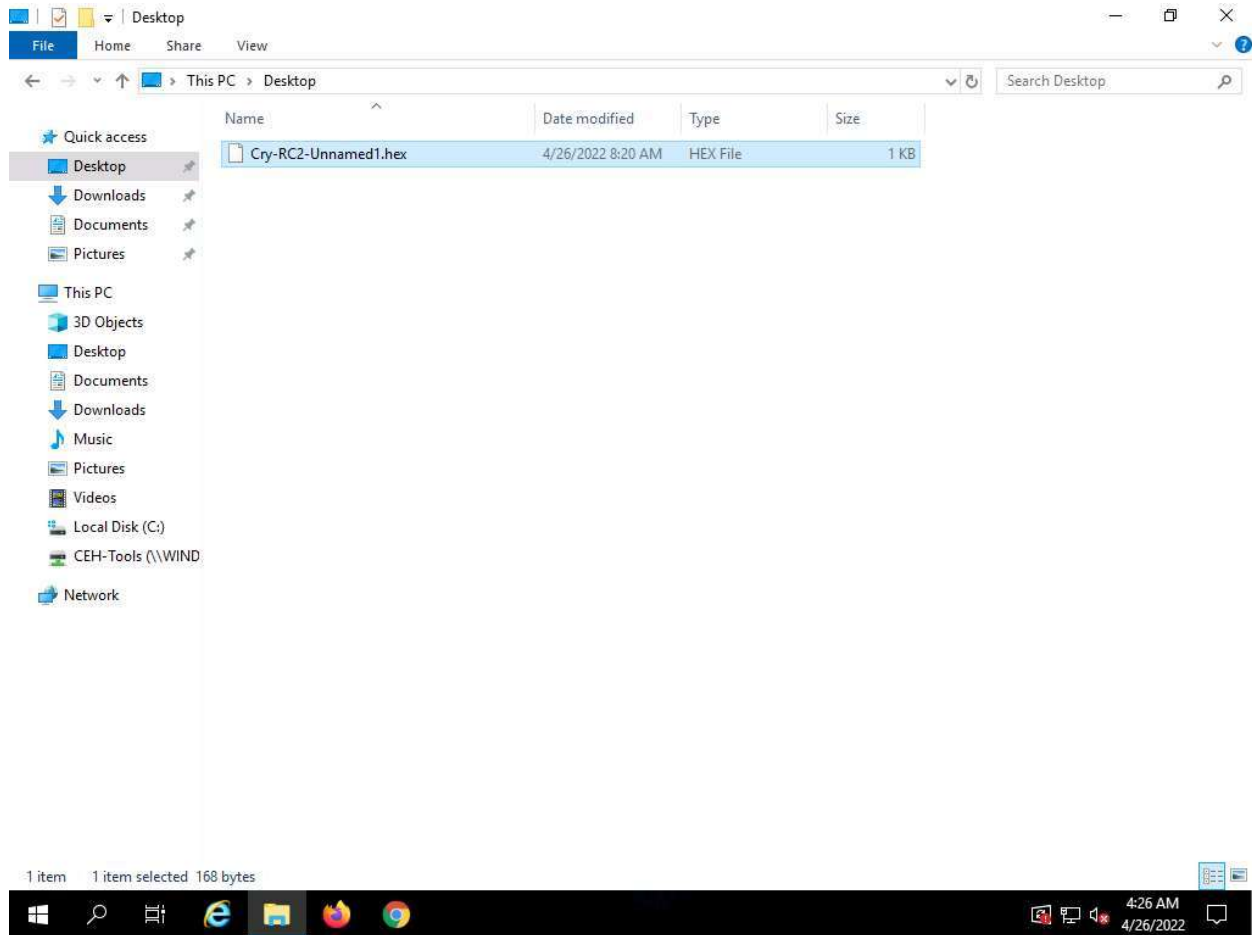
13. To share the file, you may copy the encrypted file (**Cry-RC2-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.



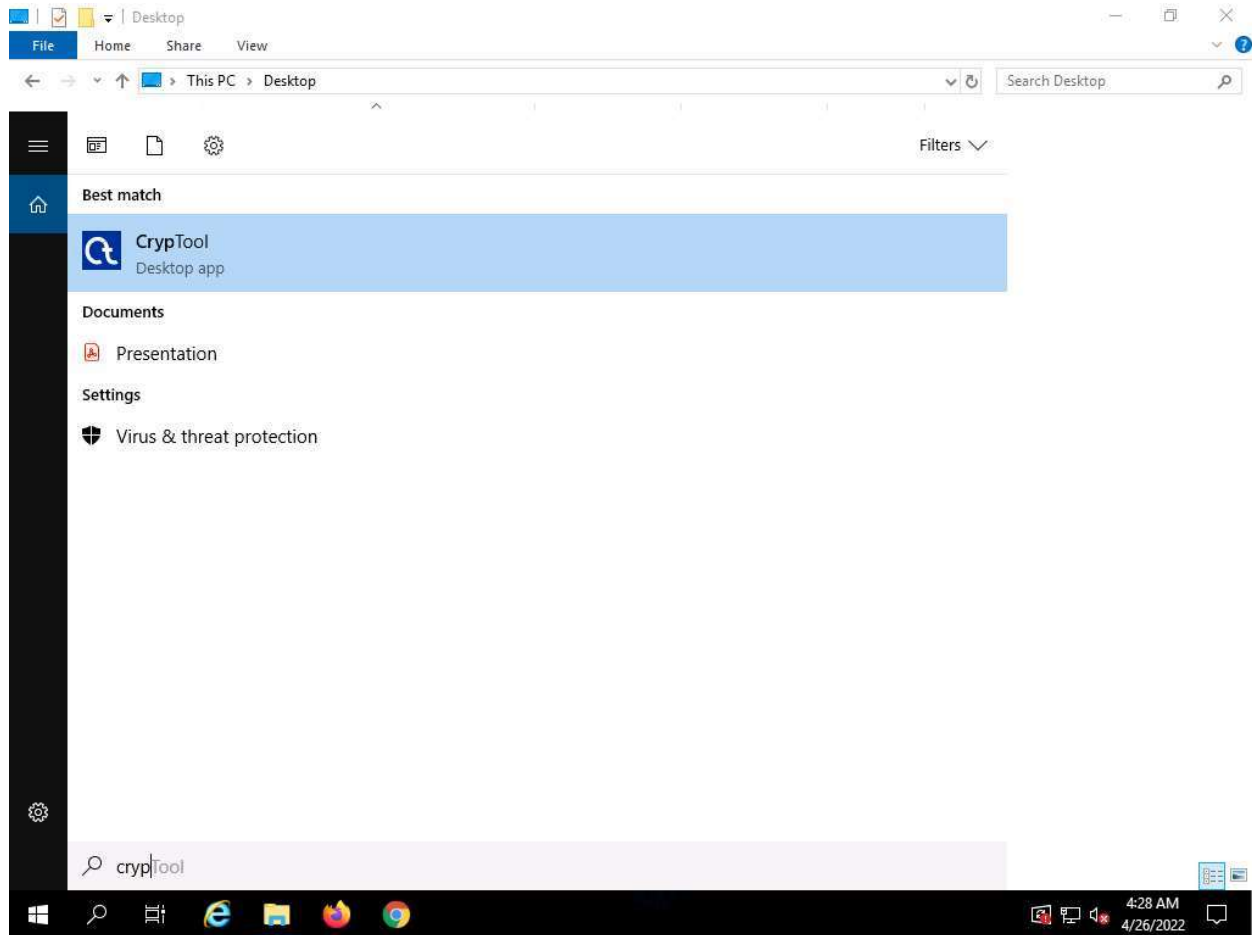
14. Assume that you are the intended recipient (working on Windows Server 2019) of the encrypted file through the shared network drive and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and see the data in plain-text.
15. Click on [Windows Server 2019](#) to switch to the **Windows Server 2019**, click [Ctrl+Alt+Delete](#) to activate the machine. By default, **Administrator** profile is selected, type \* *Pa\$\$w0rd*\* to enter password in the password field and press **Enter** to login.



16. Navigate to **Z:\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**, copy the **Cry-RC2-Unnamed1.hex** and paste it in the **Desktop**.



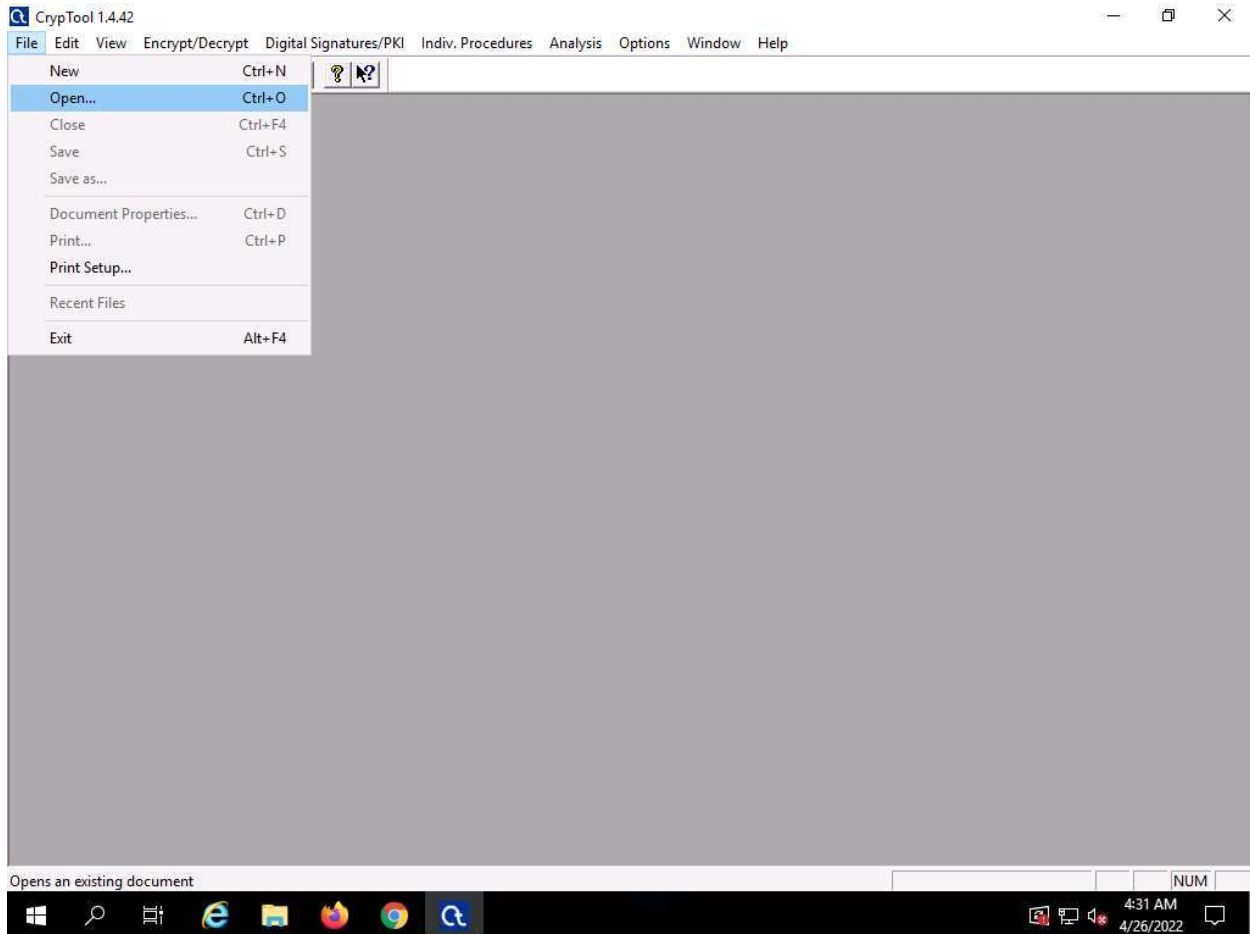
17. Click **Type here to search** icon on the Desktop. Type **crypt** in the search field, the **CrypTool** appears in the results, click on **CrypTool** to launch it.



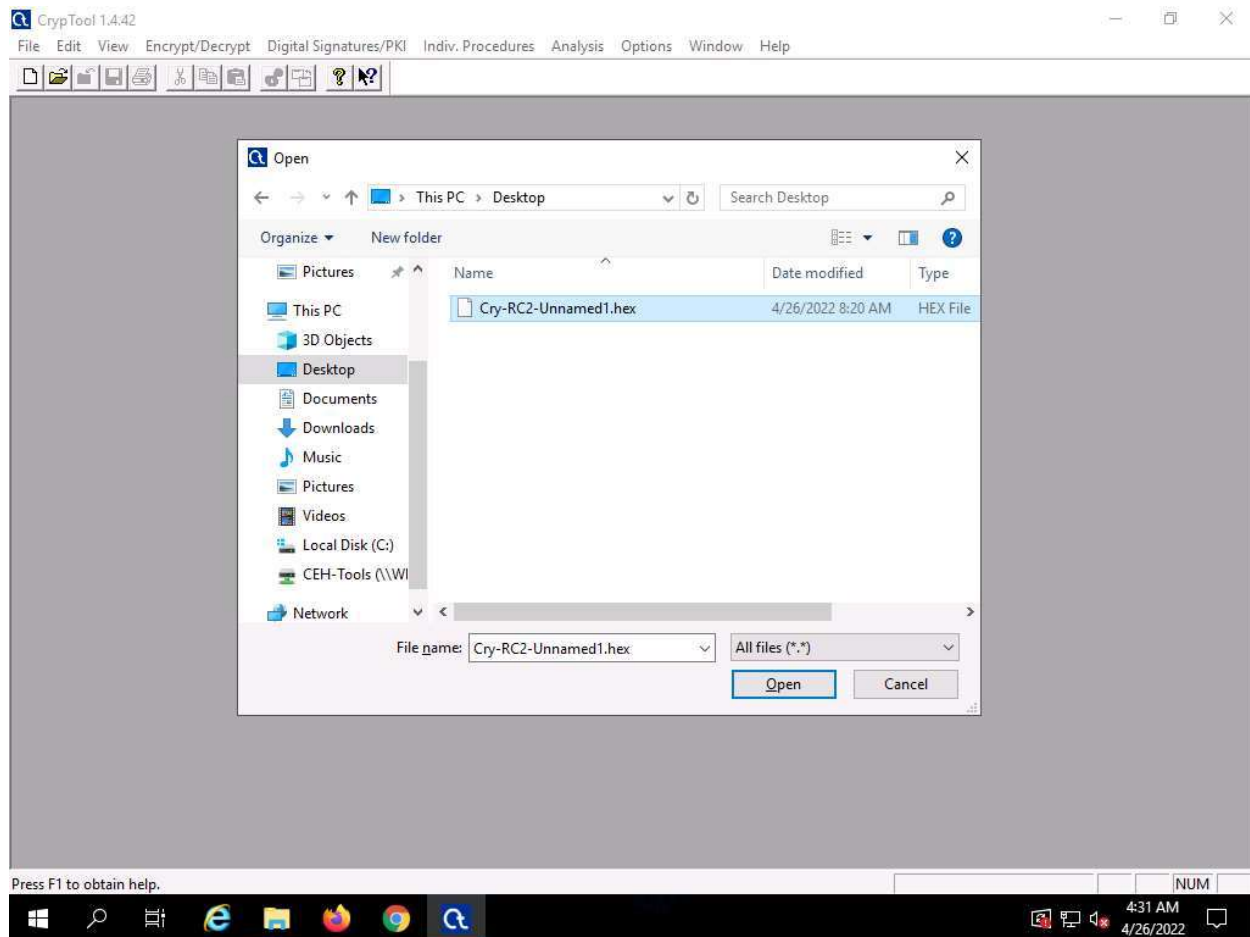
18. In the **CrypTool** window; click **File** in the menu bar and select **Open...**

If a **How to Start** window. Check the **Don't show this dialog again** checkbox and click **Close**.

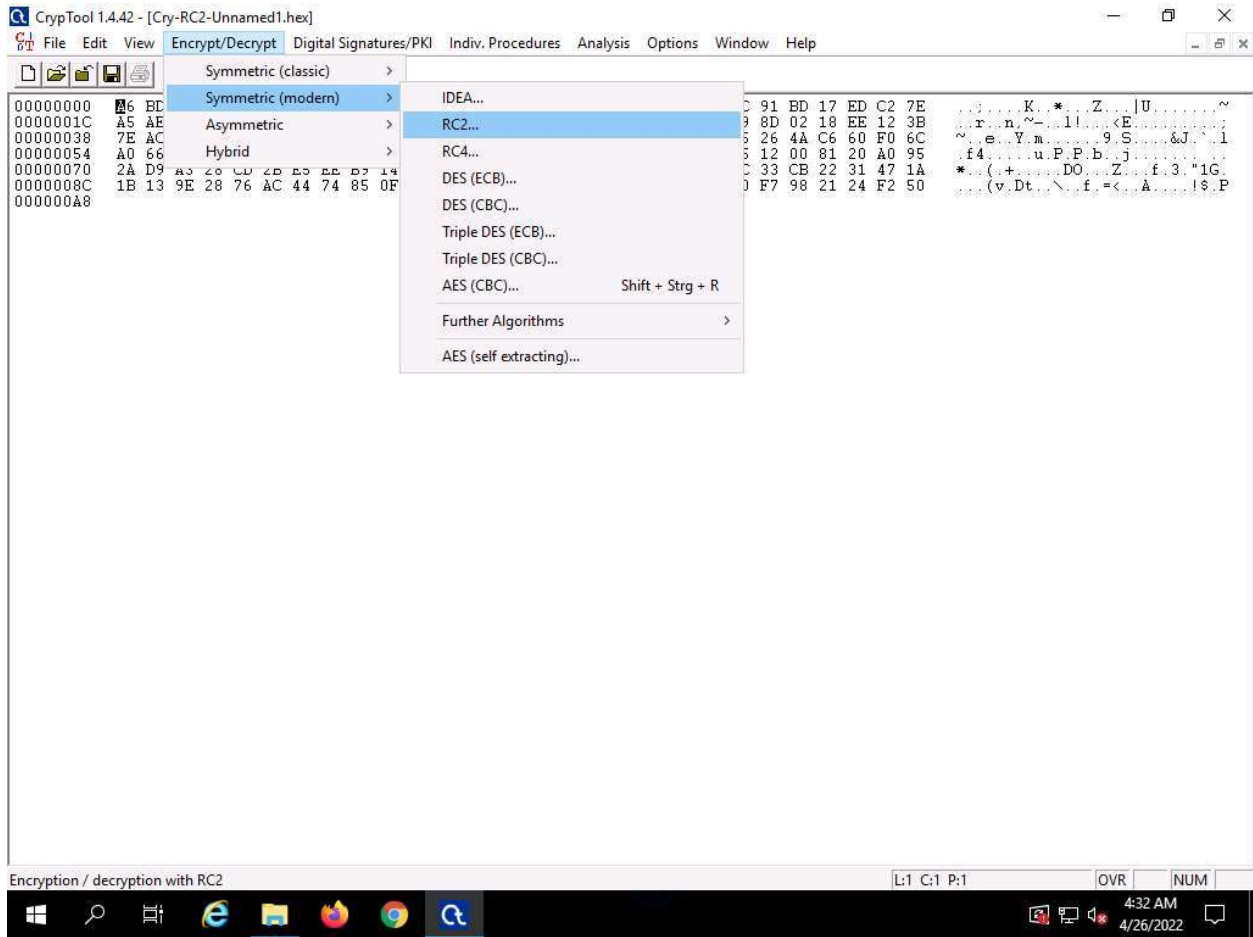
Close the **startingexample-en.txt** window.



19. The **Open** window appears; select **All files (\*.\*)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and then click **Open**.

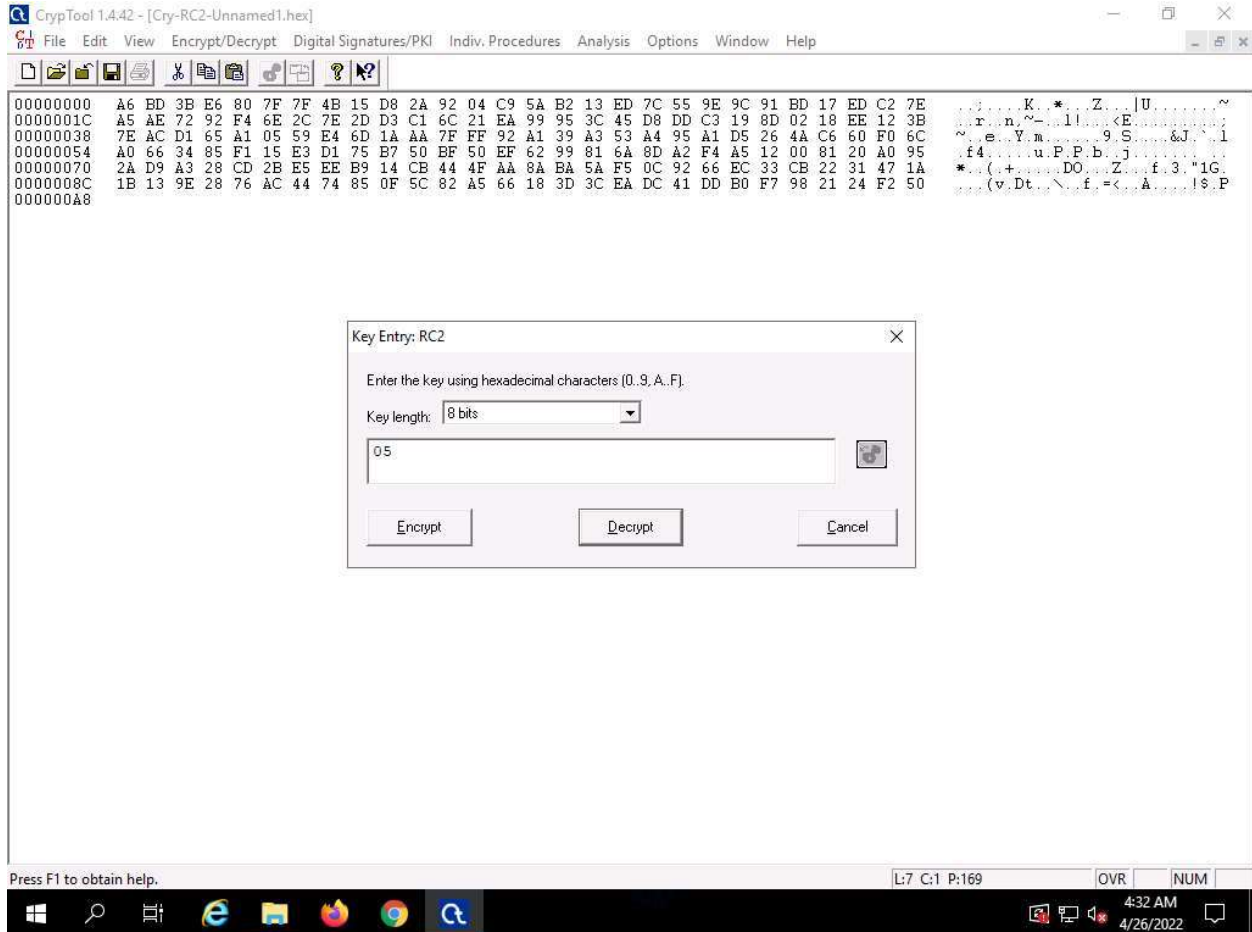


20. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) --> RC2...**



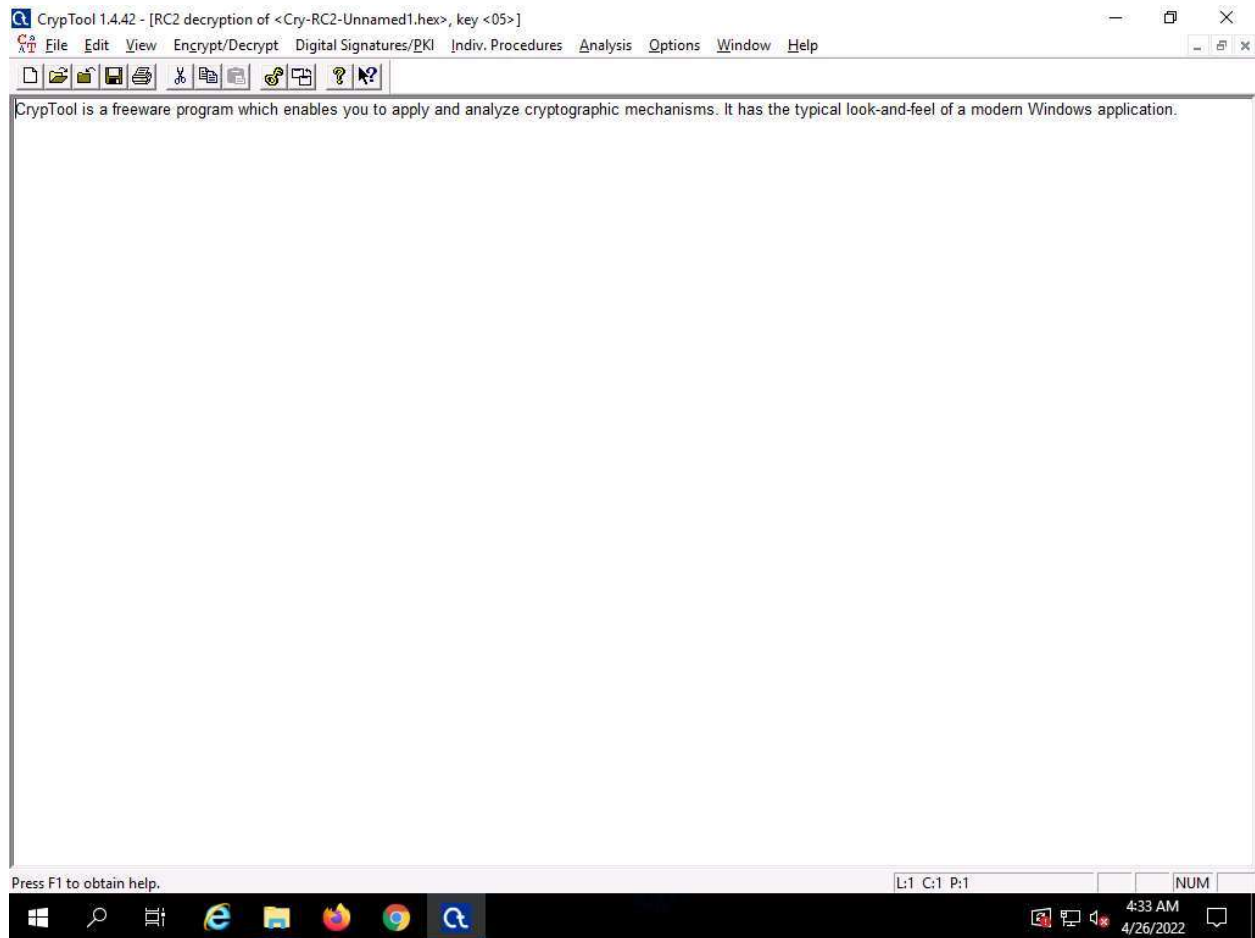
21. The **Key Entry: RC2** dialog box appears; leave the **Key length** set to default (**8 bits**).

22. In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Decrypt**.





23. The decrypted text appears, as shown in the screenshot:

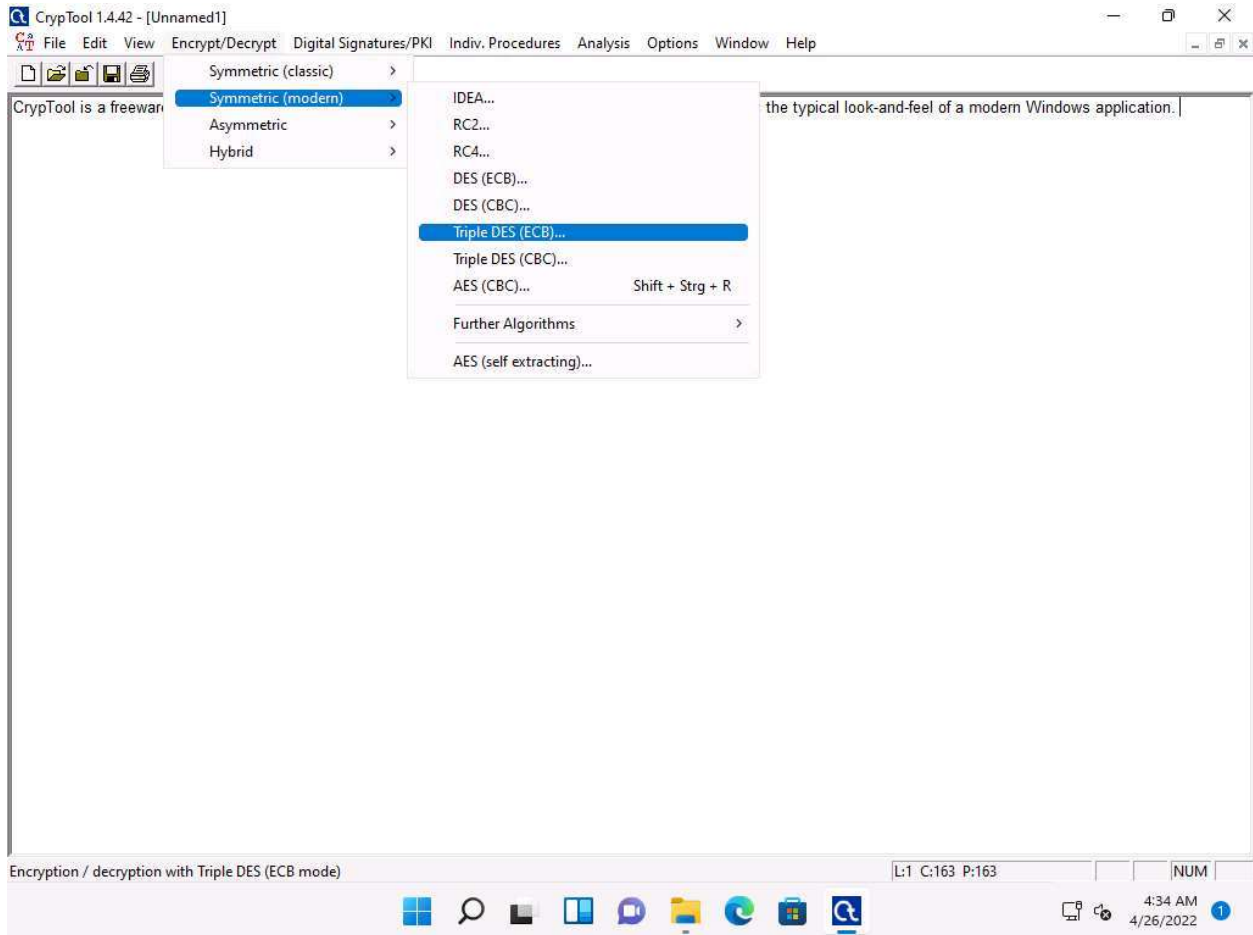


24. Now, we shall encrypt the data using Triple DES encryption.

25. Click [Windows 11](#) to switch back to the **Windows 11** machine.

26. In the **CrypTool** window, close **Cry-RC2-Unnamed1.hex** window. Leave the **Unnamed1** notepad window open.

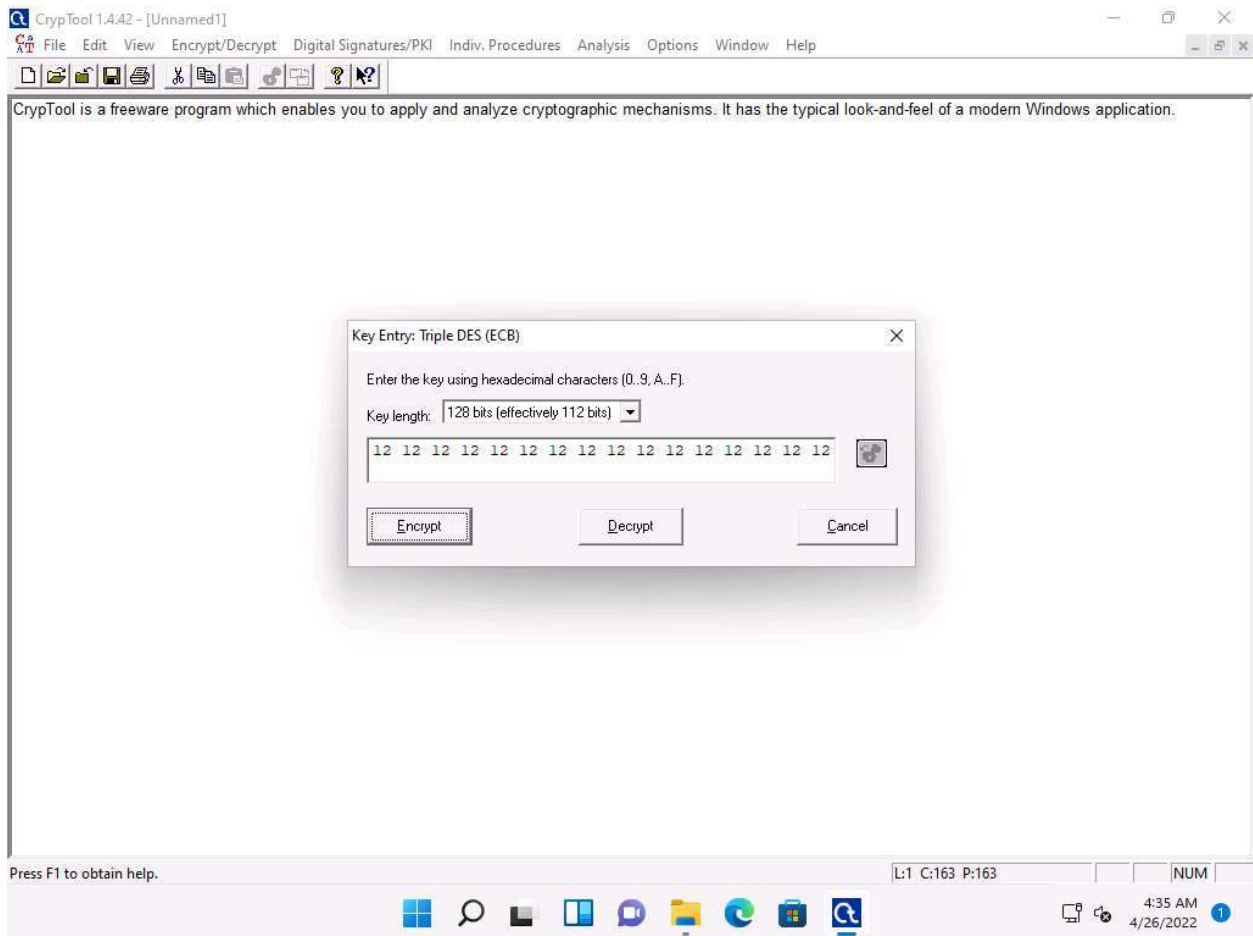
27. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) --> Triple DES (ECB)...**



28. The **Key Entry: Triple DES (ECB)** dialog-box appears; leave the **Key length** set to default (**128 bits (effectively 112 bits)**).

29. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters**, and click **Encrypt**.

The chosen hexadecimal characters act like a key that you must send to the intended user along with the encrypted file.



CrypTool 1.4.42 - [Triple DES (ECB) encryption of <Unnamed1>, key <12 12 12 12 12 12 12 12 12 12 12 12 12 12>]

File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help

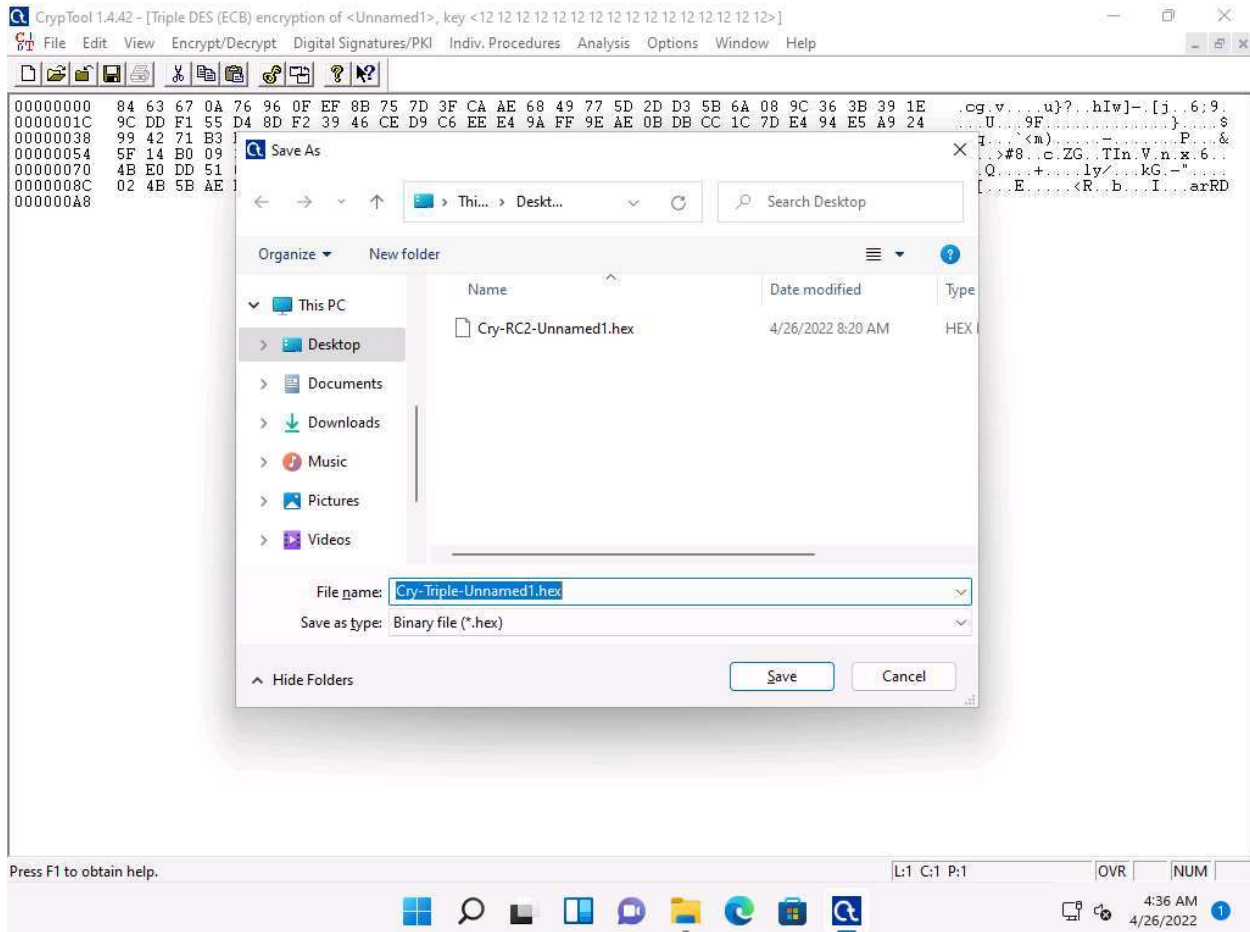
00000000 84 63 67 0A 76 96 0F EF 8B 75 7D 3F CA AE 68 49 77 5D 2D D3 5B 6A 08 9C 36 3B 39 1E .cg.v...u)?..hiw]-[j..6:9  
0000001C 9C DD F1 55 D4 8D F2 39 46 CE D9 C6 EE E4 9A FF 9E AE 0B DB CC 1C 7D E4 94 E5 A9 24 .U...9F...  
00000038 99 42 71 B3 F5 80 60 3C 6D 29 D6 C1 D9 E1 F5 2D 15 E0 01 01 DC 7F DF 50 D6 FB EB 26 .Bq...<m)...-...P...&  
00000054 5F 14 B0 09 3E 23 38 C5 F9 63 B4 5A 47 D7 DA 54 49 6E 98 56 B0 6E B0 78 D1 36 B7 14 .>#8..c.ZG..TIn.V.n.x.6..  
00000070 4B E0 DD 51 00 01 BE A7 2B C7 FB 87 B0 6C 79 2F 01 0E ED 6B 47 96 2D 22 1C AA 03 E8 .K.Q..E.+...ly/.kG.-"  
0000008C 02 4B 5B AE B1 1A 45 C7 F6 BE ED B6 3C 52 9A 84 62 FF 1B F0 49 83 9E 08 61 72 52 44 .Kl...E...<R..b...I...arRD  
000000A8

Press F1 to obtain help. L:1 C:1 P:1 OVR NUM 4:35 AM 4/26/2022

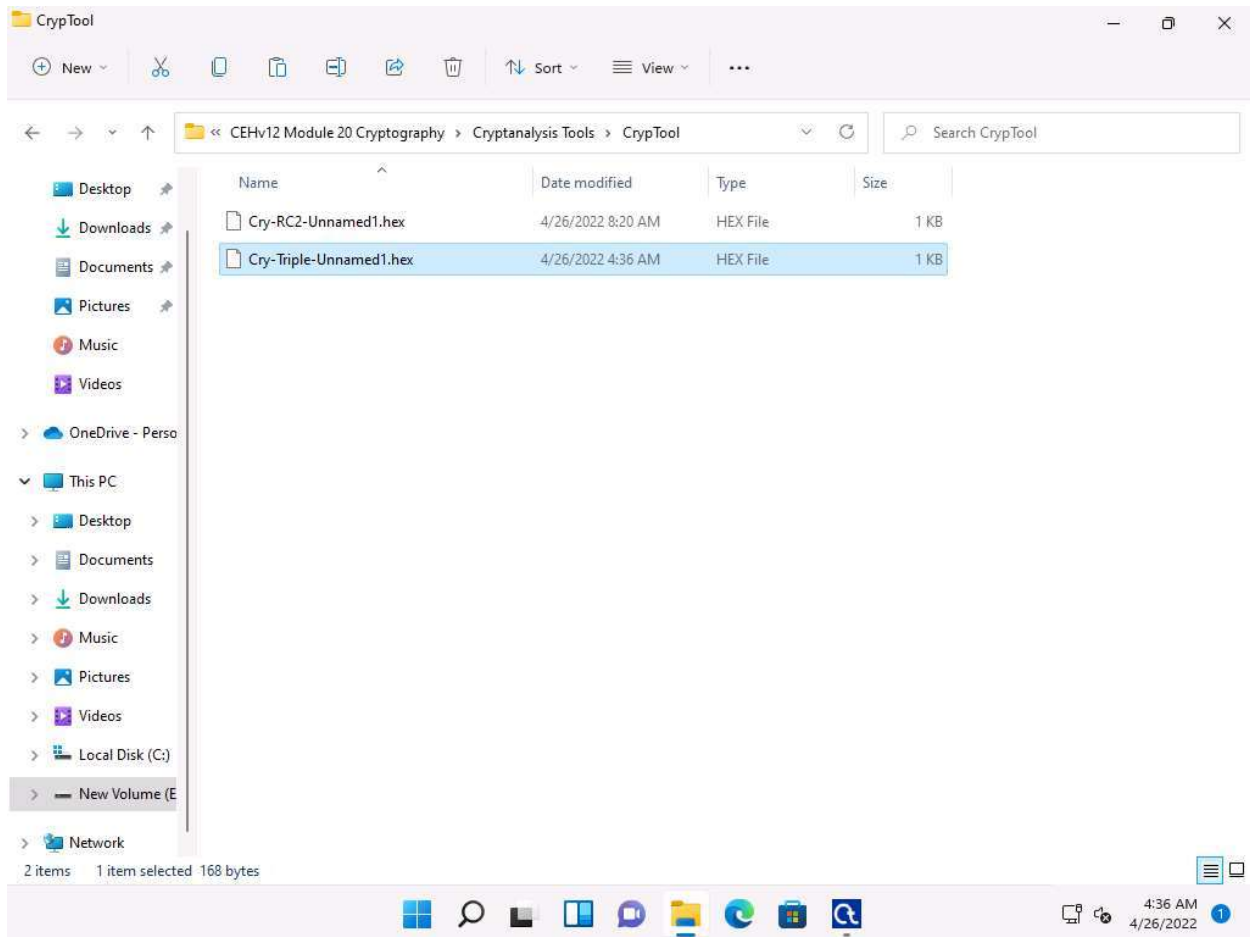
31. To save the file, click **File** in the menu bar and select **Save**.

32. The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

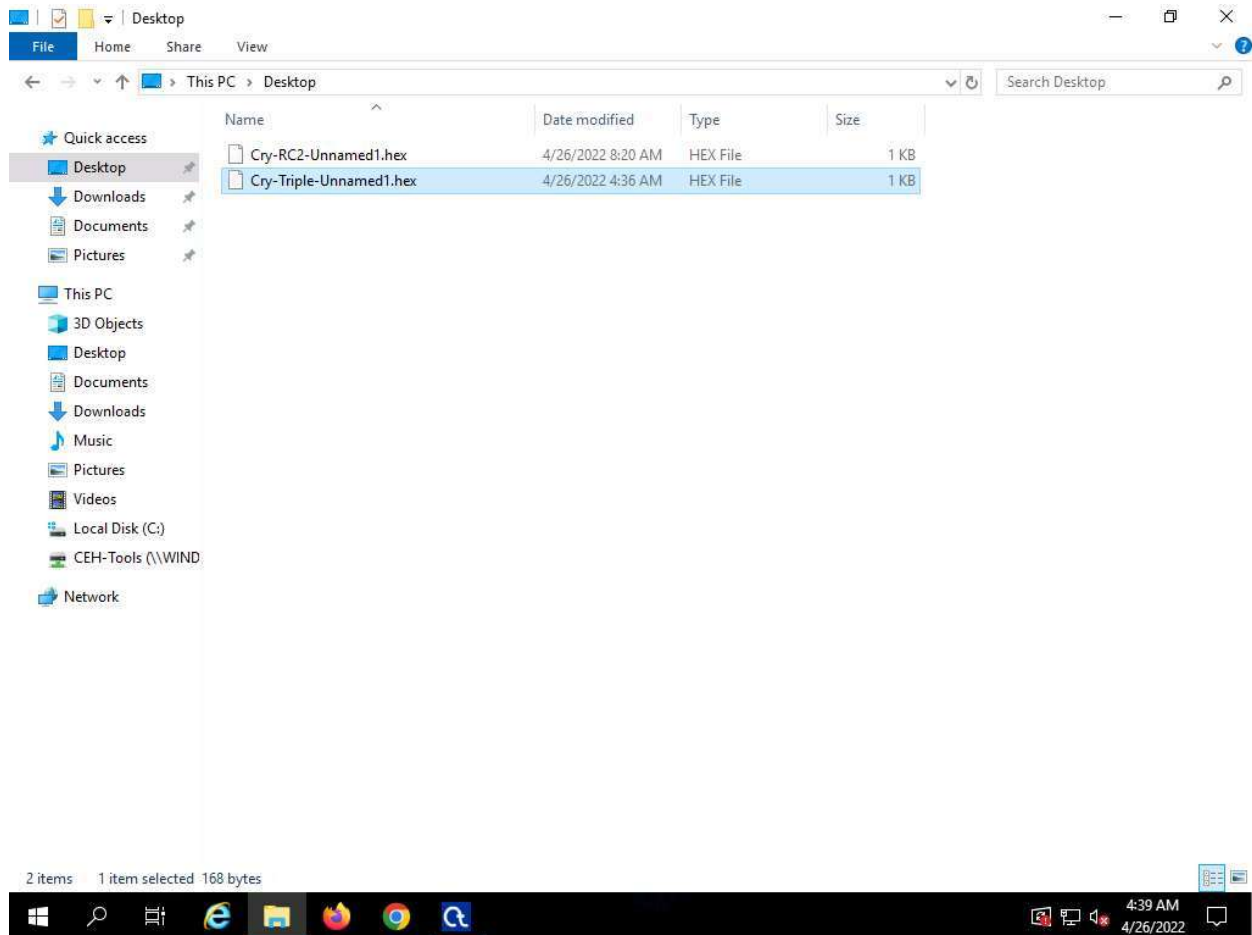
The file name may differ in your lab environment.



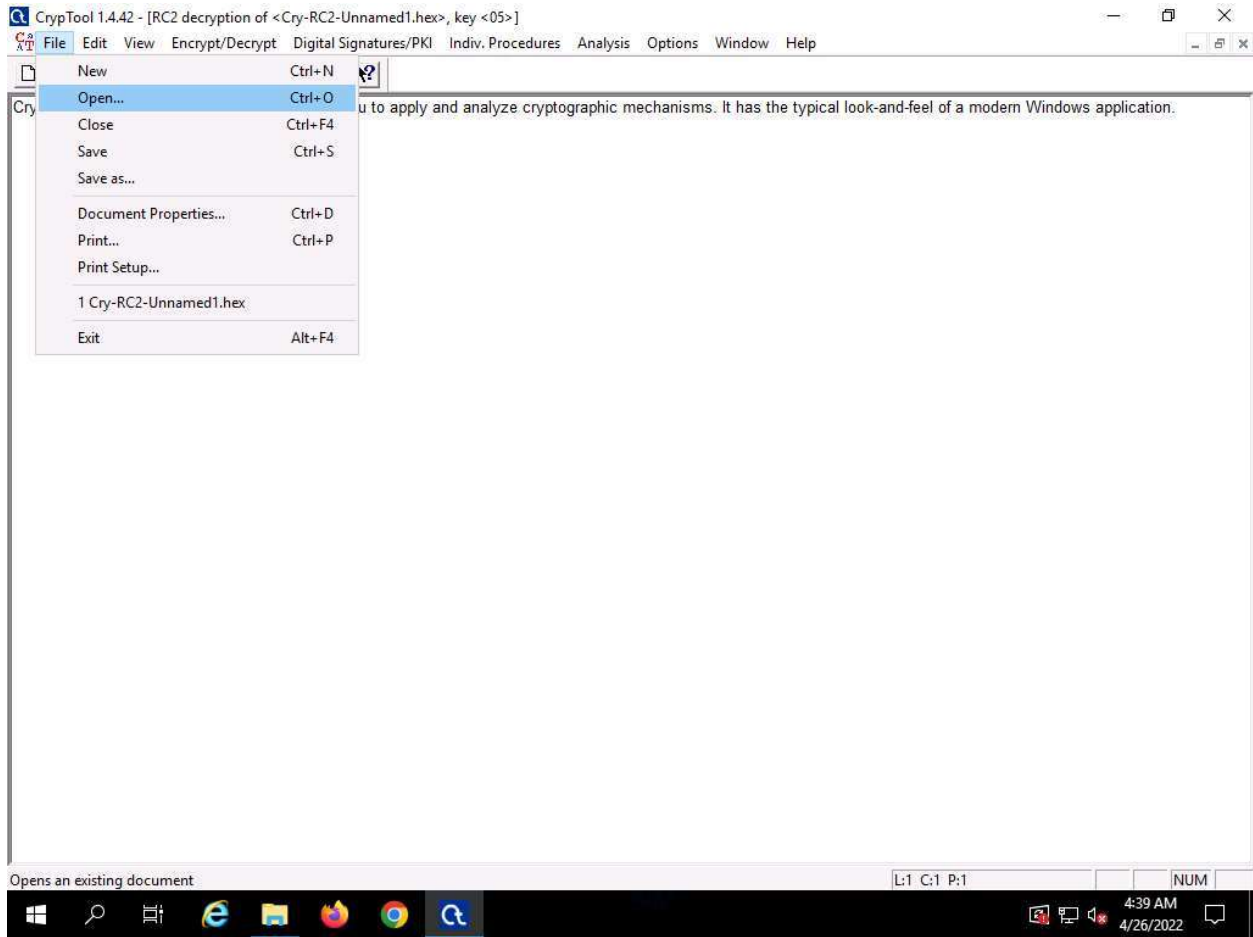
33. To share the file, you may copy the encrypted file (**Cry-Triple-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.



34. Click [Windows Server 2019](#) to switch to **Windows Server 2019**; copy the encrypted hex file (**Cry-Triple-Unnamed1.hex**) from **Z:\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and paste on **Desktop**.

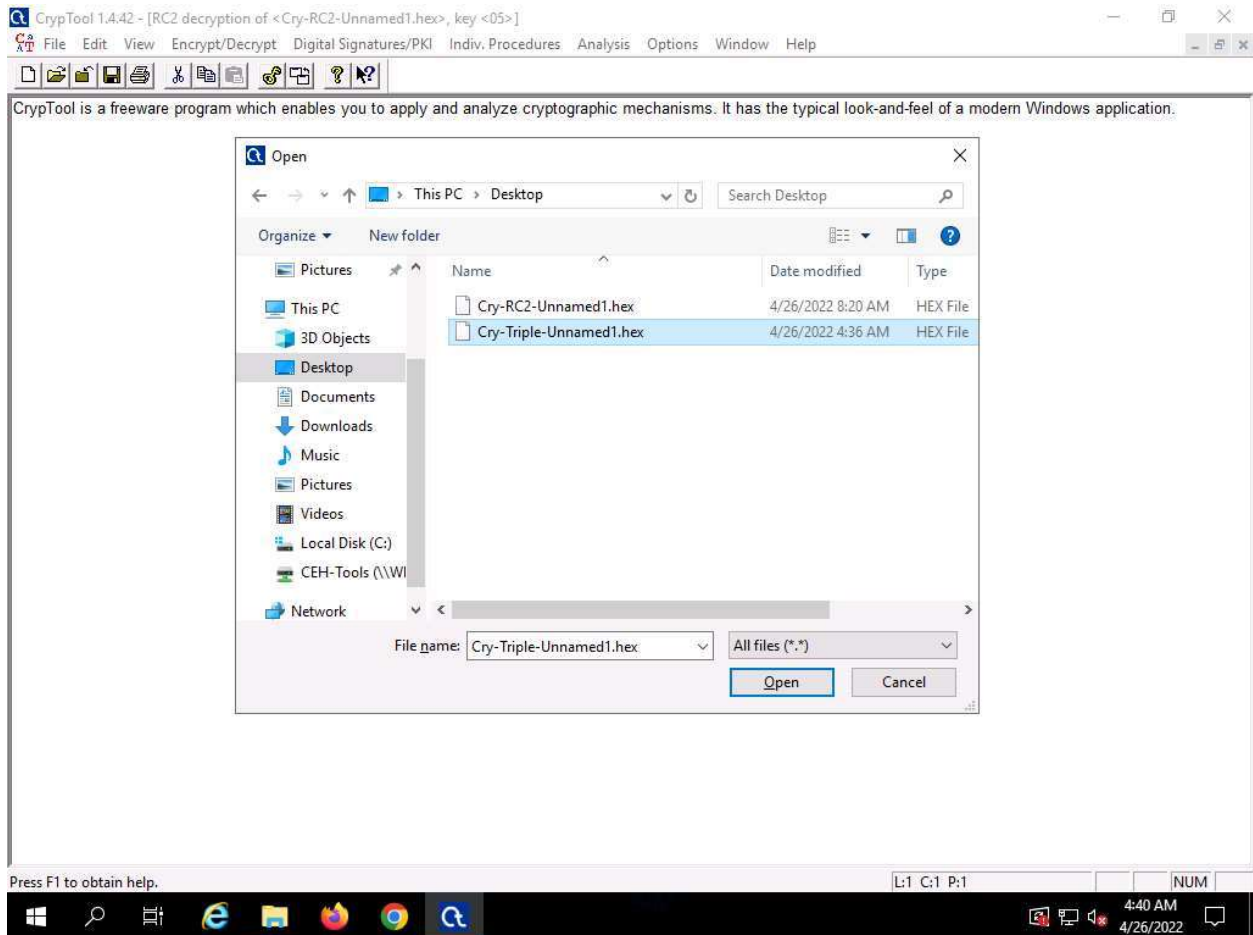


35. Switch to the **CrypTool** window to **decrypt** the data; click **File** in the menu bar and select **Open...**

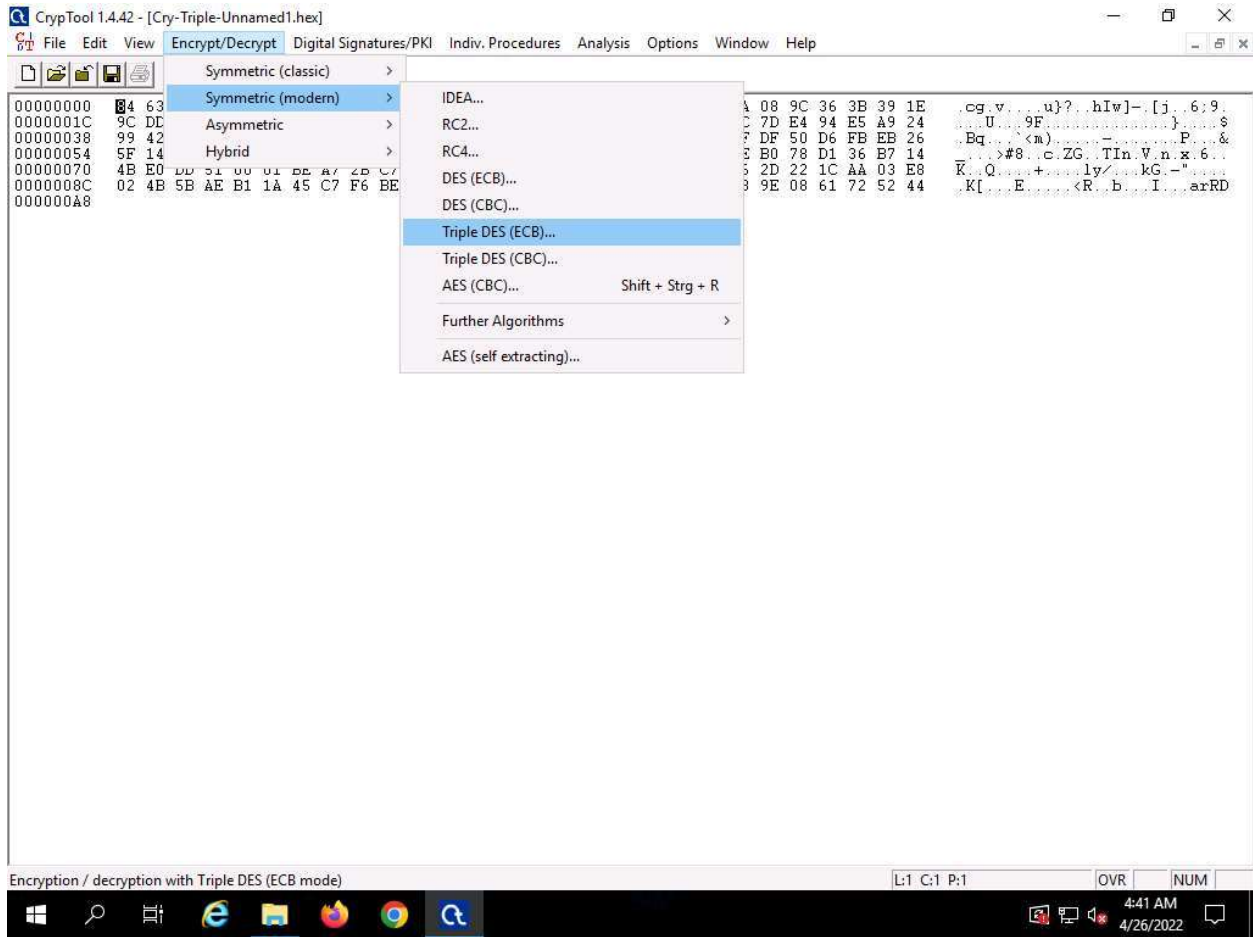




36. The **Open** window appears; select **All files (\*.\*)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and click **Open**.

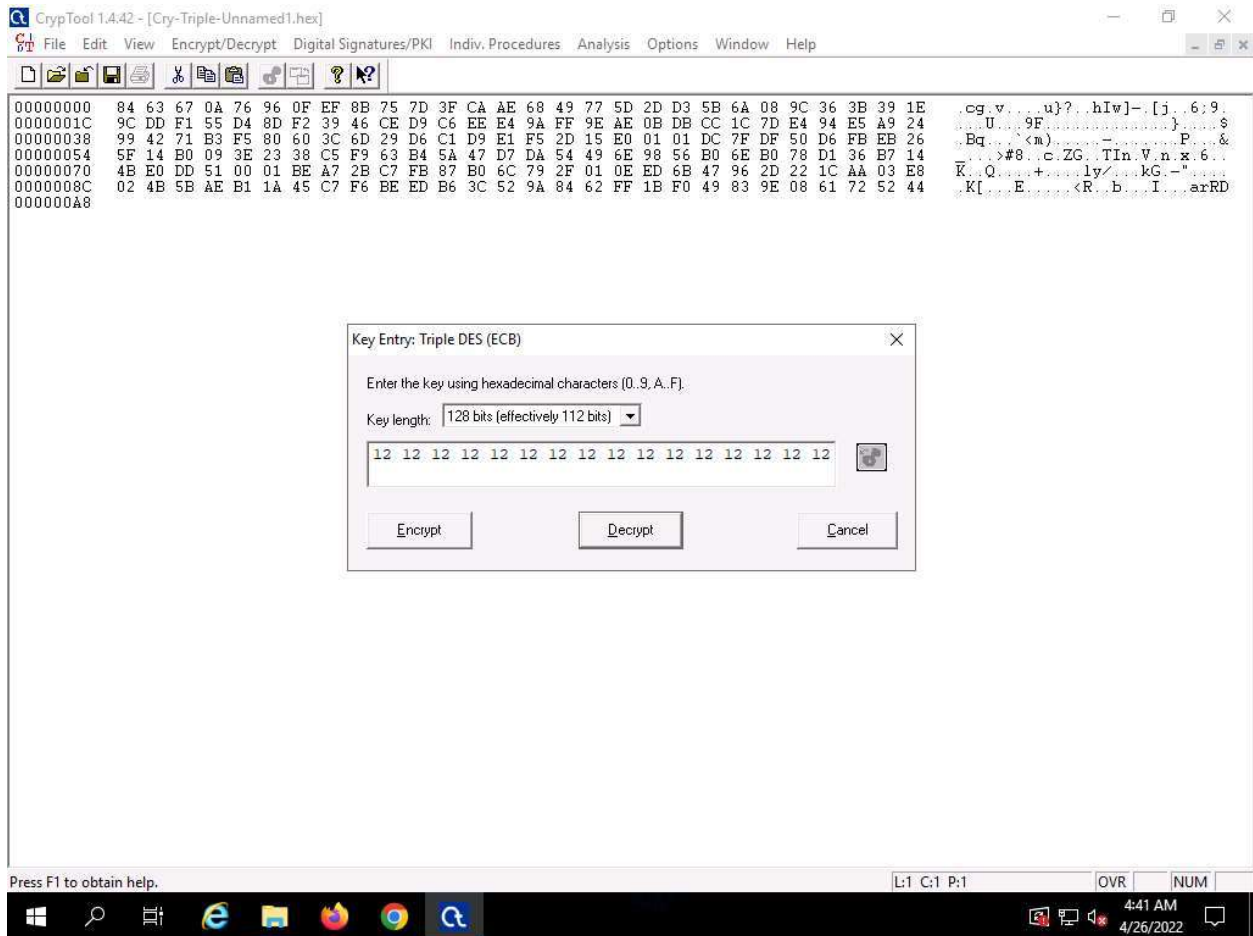


37. From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) --> Triple DES (ECB)...**

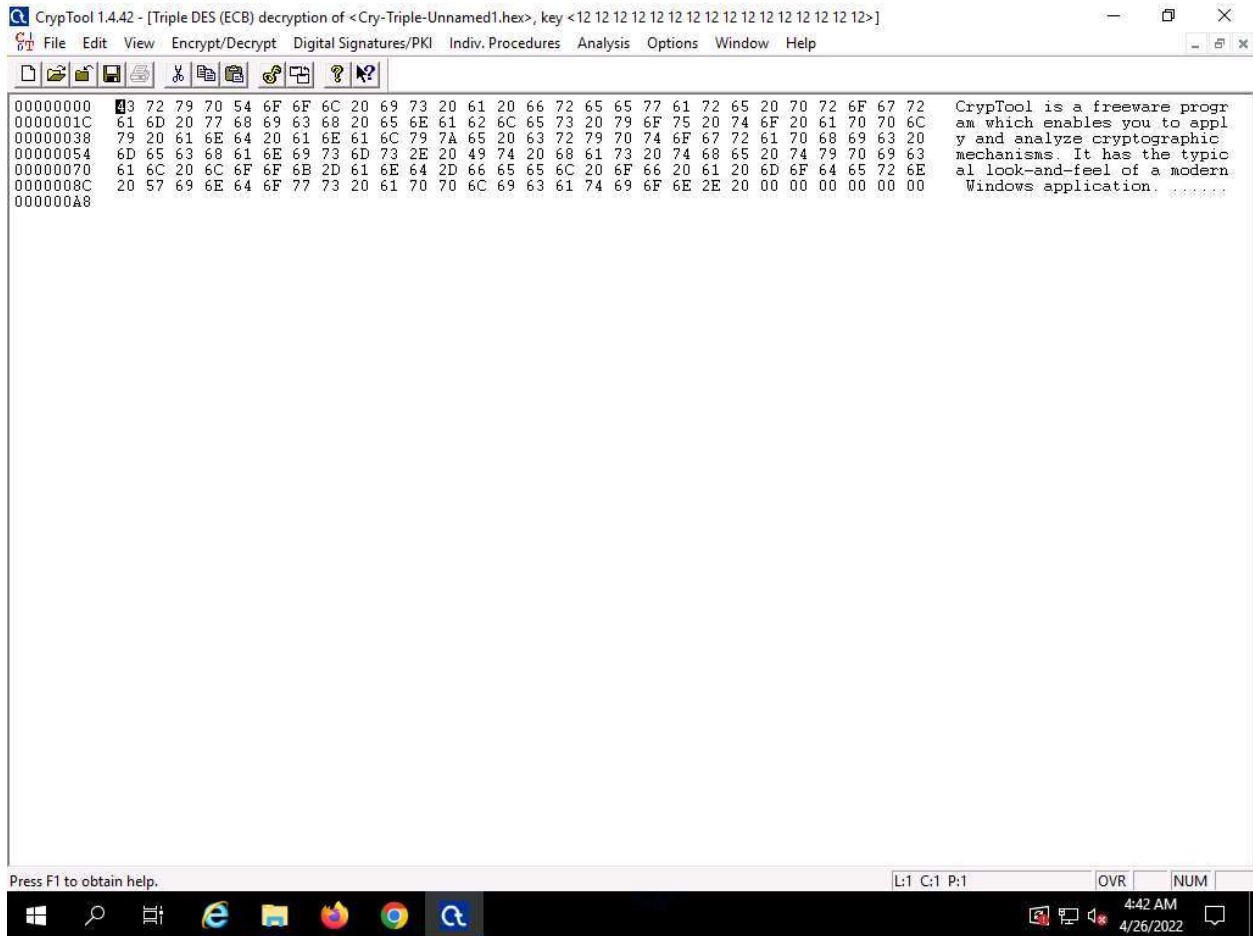


38. The **Key Entry: Triple DES (ECB)** dialog-box appears; keep the **Key length** set to default (**128 bits (effectively 112 bits)**).

39. In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters** and click **Decrypt**.



40. The decrypted text appears, as shown in the screenshot.




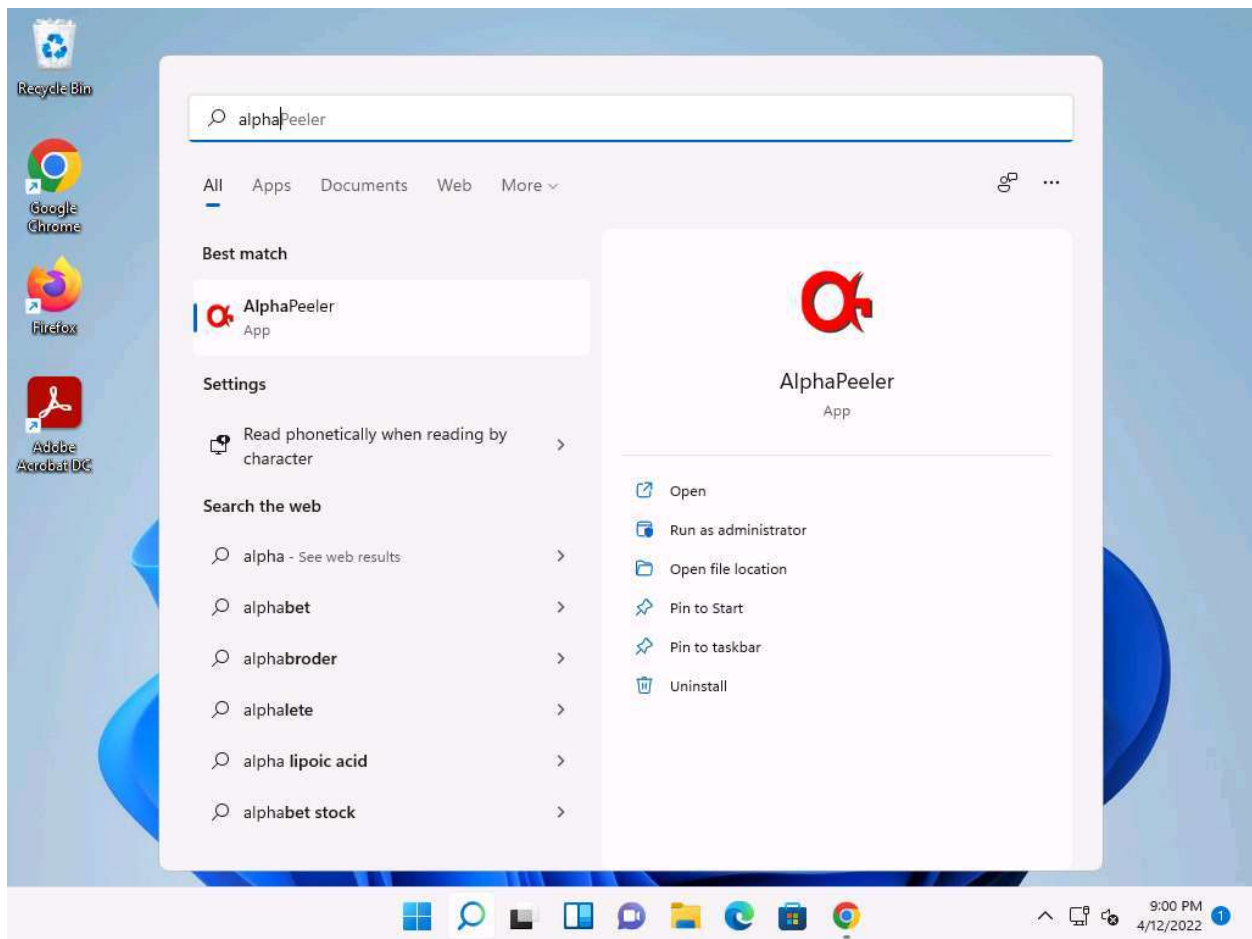
41. Using this method, files can be encrypted using CrypTool and shared with an individual in a secure manner, so that no one can intercept the data.
  42. This concludes the demonstration of performing cryptanalysis using CrypTool.
  43. Close all open windows and document all the acquired information.
-

## Task 2: Perform Cryptanalysis using AlphaPeeler

AlphaPeeler is a powerful tool for learning cryptology. It can be useful as an instructor's teaching aid and to create assignments for classical cryptography. You can easily learn classical techniques such as frequency analysis of alphabets, mono-alphabetic substitution, Caesar cipher, transposition cipher, Vigenere cipher, and Playfair cipher. AlphaPeeler Professional (powered by crypto++ library) also includes DES, Gzip/Gunzip, MD5, SHA-1, SHA-256, RIPEMD-16, RSA key generation, RSA crypto, RSA signature & validation, and generation of secret share files.

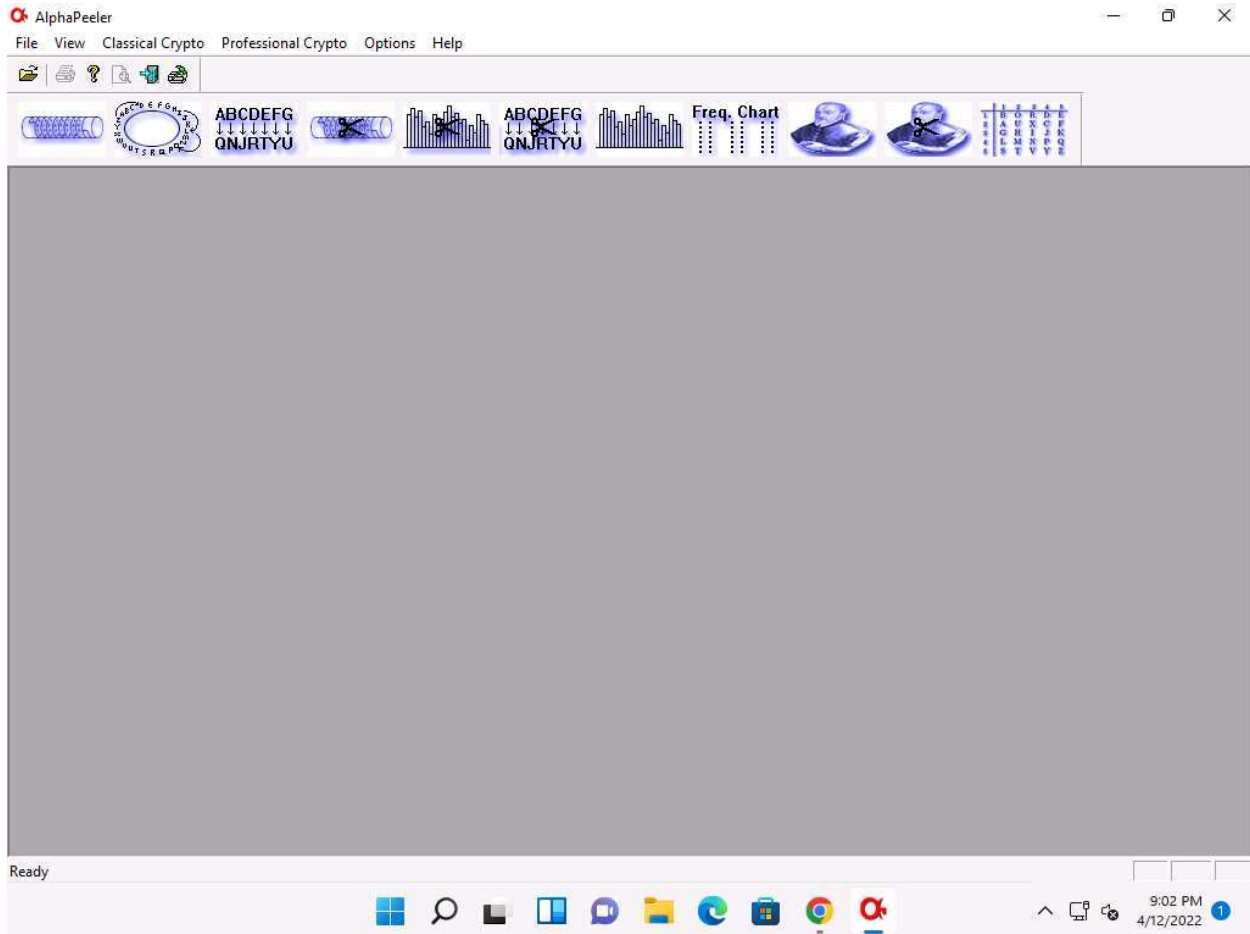
Here, we will use the AlphaPeeler tool to perform cryptanalysis.

1. Click on [Windows 11](#) to switch to the **Windows 11** machine, Click **Search** icon (  ) on the **Desktop**. Type **alpha** in the search field, the **AlphaPeeler** appears in the results, click **Open** to launch it.

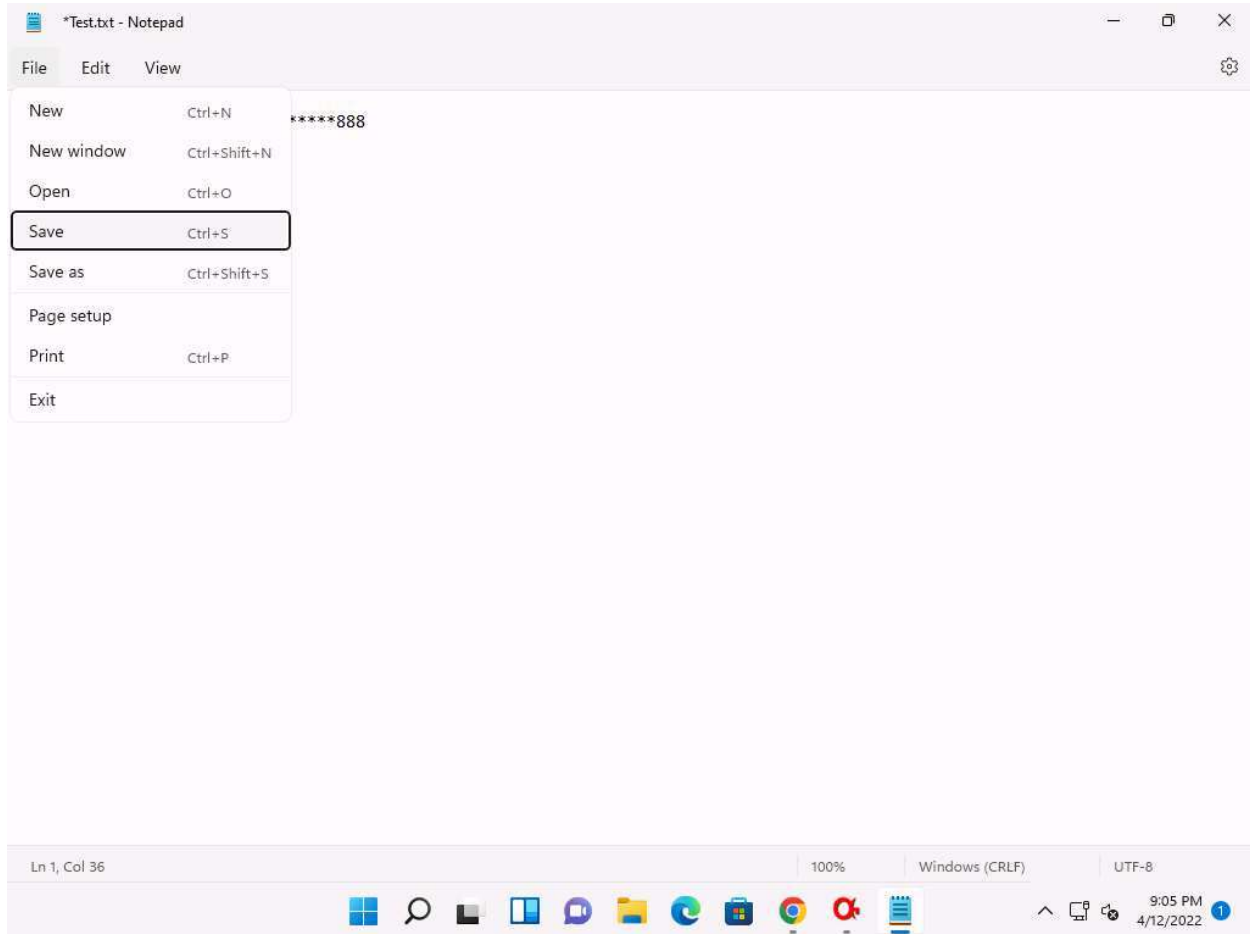


If an **Open File - Security Warning** pop-up appears, click **Run**.

2. **AlphaPeeler Professional** initializes and the **AlphaPeeler** main window appears, as shown in the screenshot.

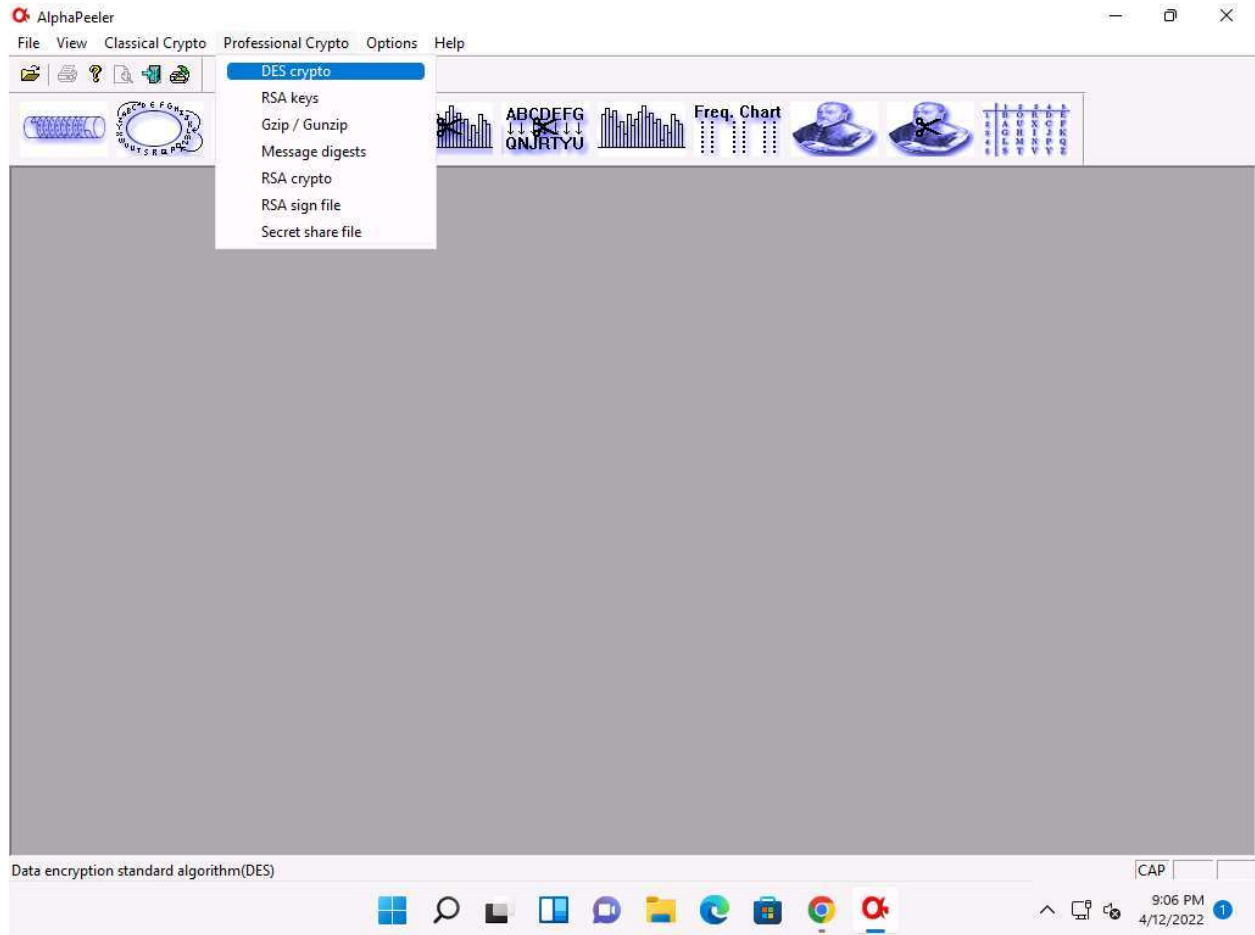


3. Now, minimize the AlphaPeeler window and create a text file on **Desktop**. Name it **Test**, open the file, and insert some text.
4. Click **File** in the menu bar and click **Save**.

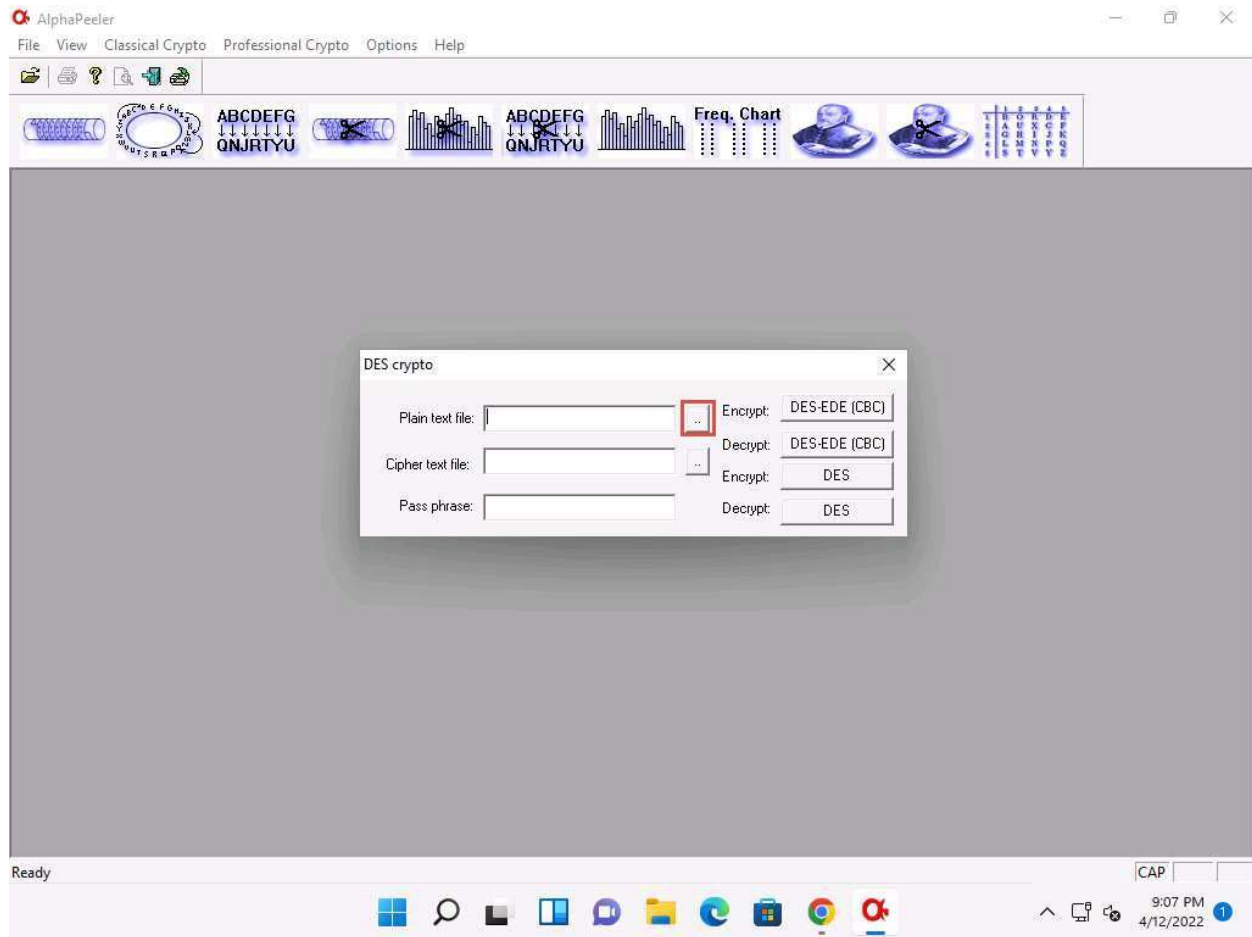




5. Switch back to the **AlphaPeeler** window; click **Professional Crypto** from the menu bar and select **DES crypto** from the options.

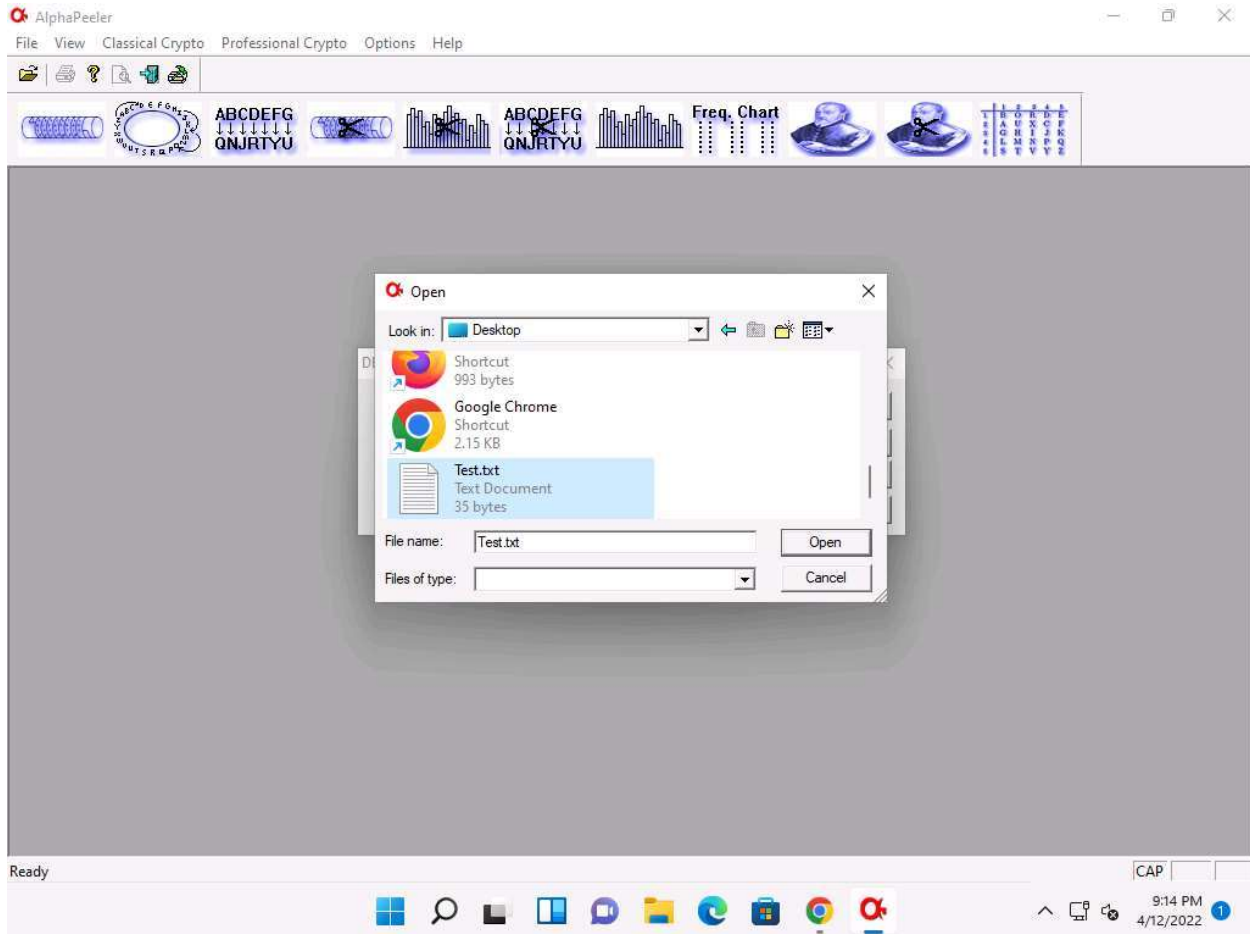


6. The **DES crypto** pop-up appears; click the ellipsis icon under the **Plain text file** option.

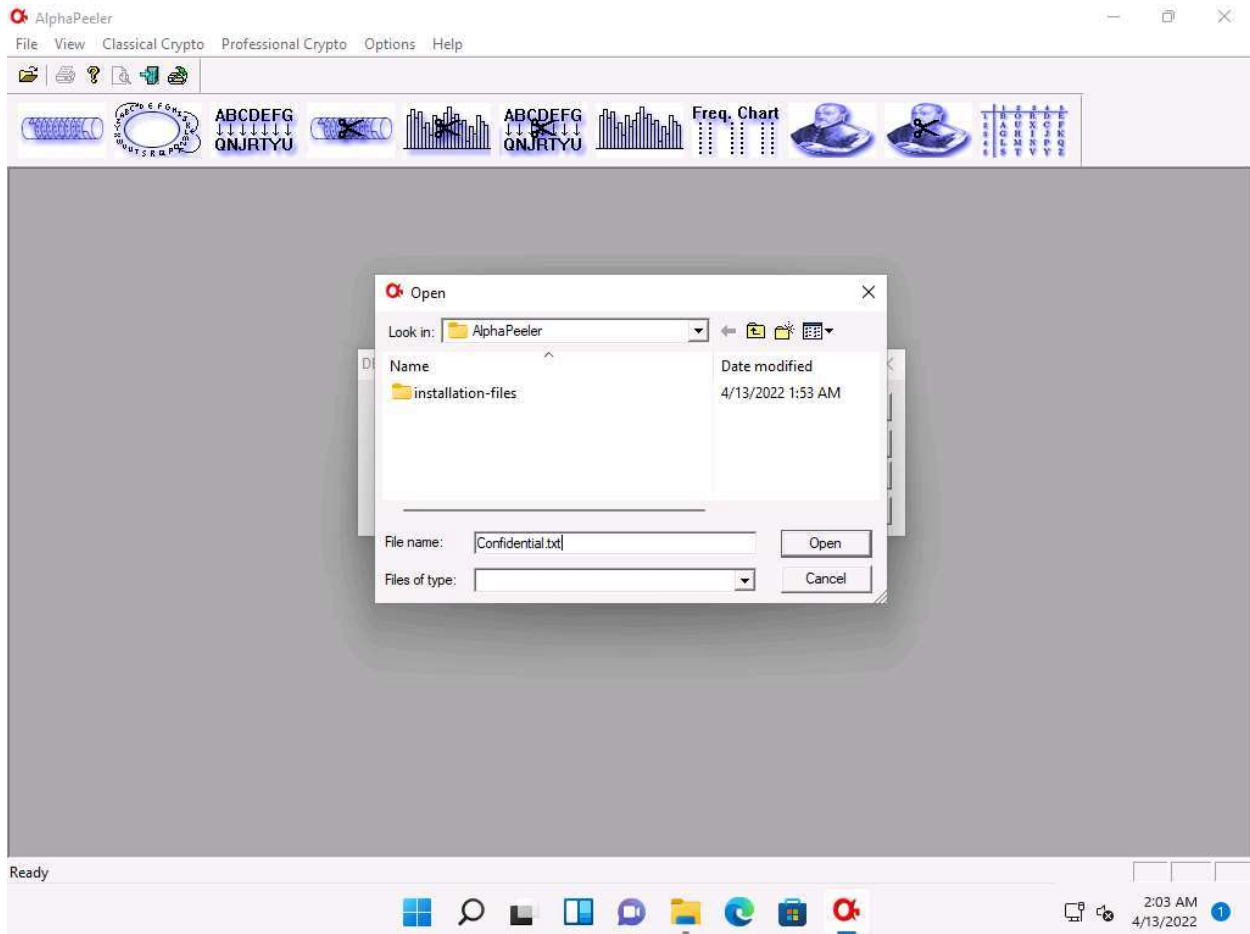


7. The **Open** window appears; navigate to **Desktop** and select **Test.txt** file; then, click **Open**.

Here, we are selecting the file that we will encrypt and this will act as an input file.

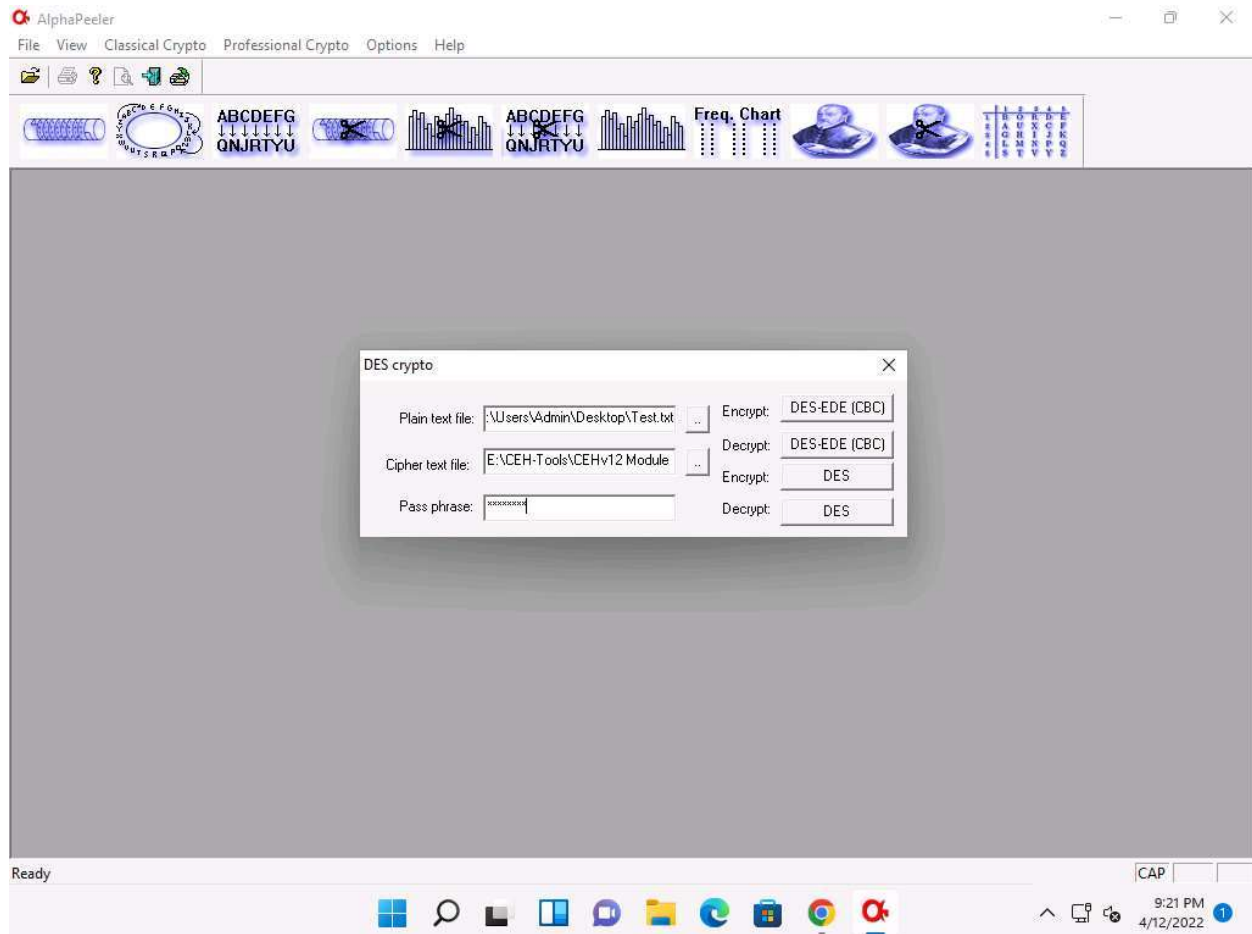


8. In the **DES crypto** pop-up; click the ellipsis icon under the **Cipher text file** option.
9. The **Open** window appears; select the save location (here, **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**) and name the file as **Confidential.txt**; then, click **Open**.

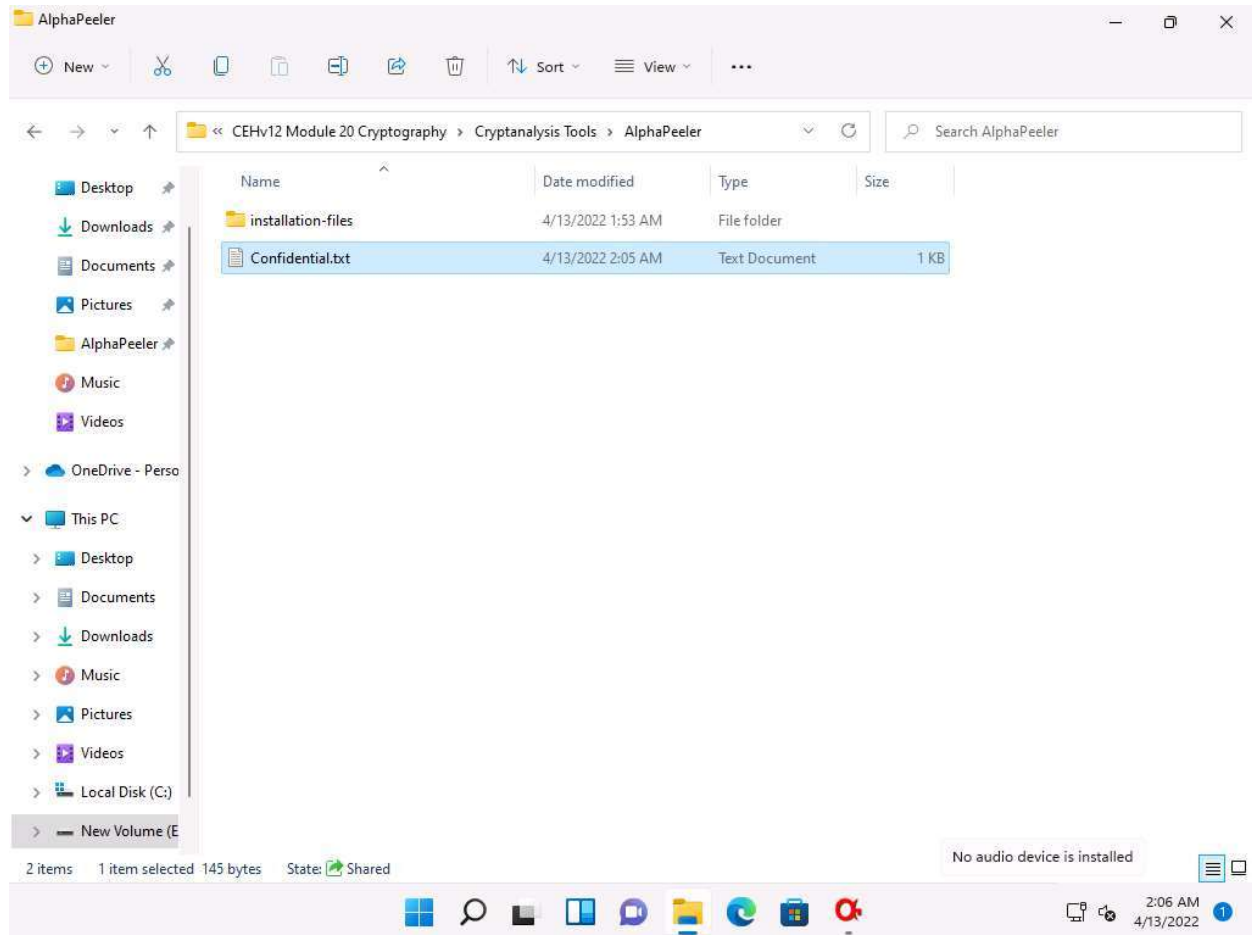


10. In the **DES crypto** pop-up; insert the password into the **Pass phrase** field and click **DES-EDE (CBC)** button under **Encrypt** option to encrypt the text file.

Here, the password provided is **test@123**.

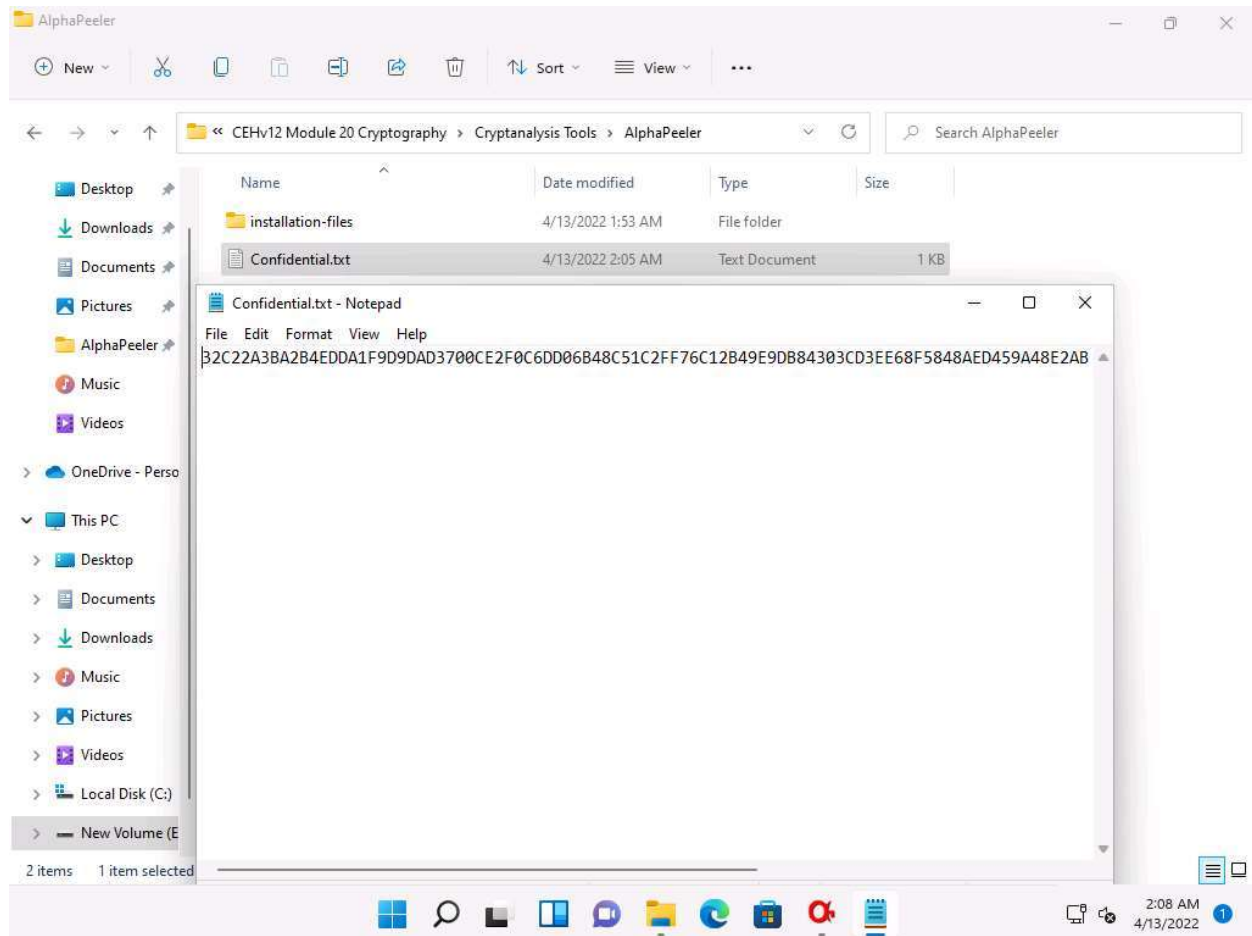


11. A new file **Confidential.txt** appears at location **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**, as shown in the screenshot.




12. Double-click **Confidential.txt** to open, and you can observe that the file's content is encrypted.

Here, the encrypted file is shared through shared network drive **E:\CEH-Tools\ CEHv12 Module 20 Cryptography** and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and view the data in plain-text.

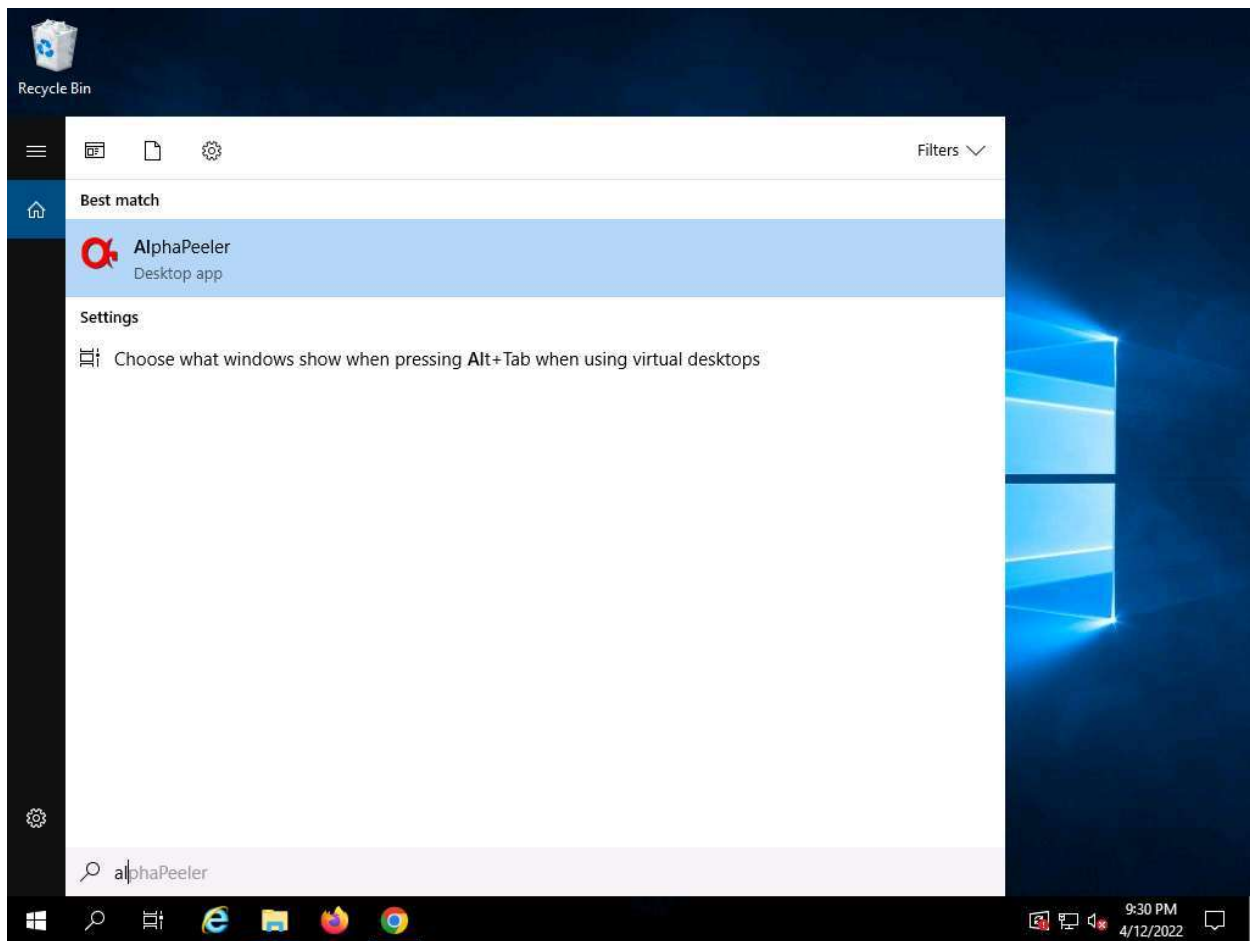


13. Close the **DES crypto** pop-up and the **AlphaPeeler** window.

14. Click on [Windows Server 2019](#) to switch to **Windows Server 2019**; Click **Search** icon

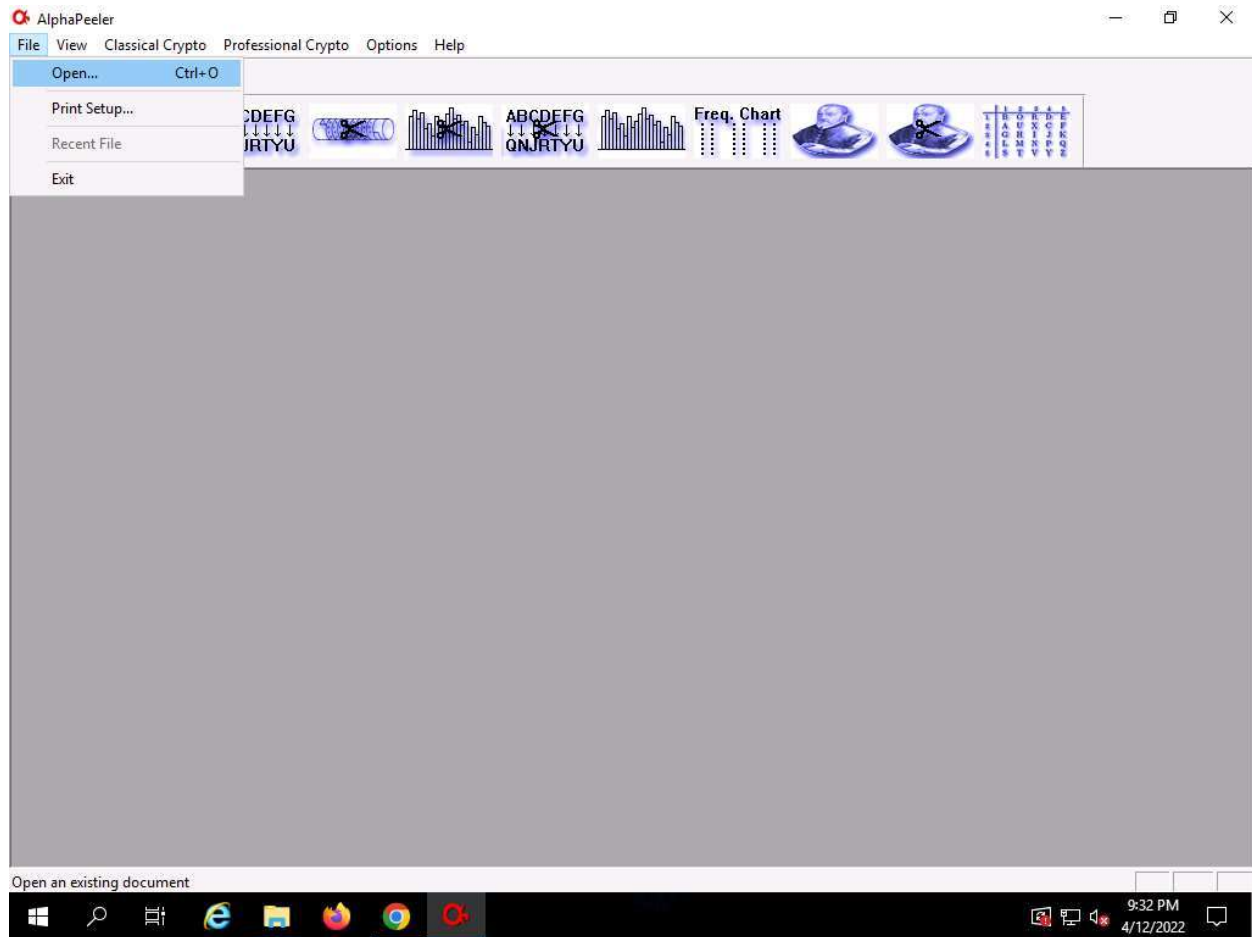
(  ) on the **Desktop**. Type **alpha** in the search field, the **AlphaPeeler** appears in the results, double click to launch it.

If an **Open File - Security Warning** pop-up appears, click **Run**.

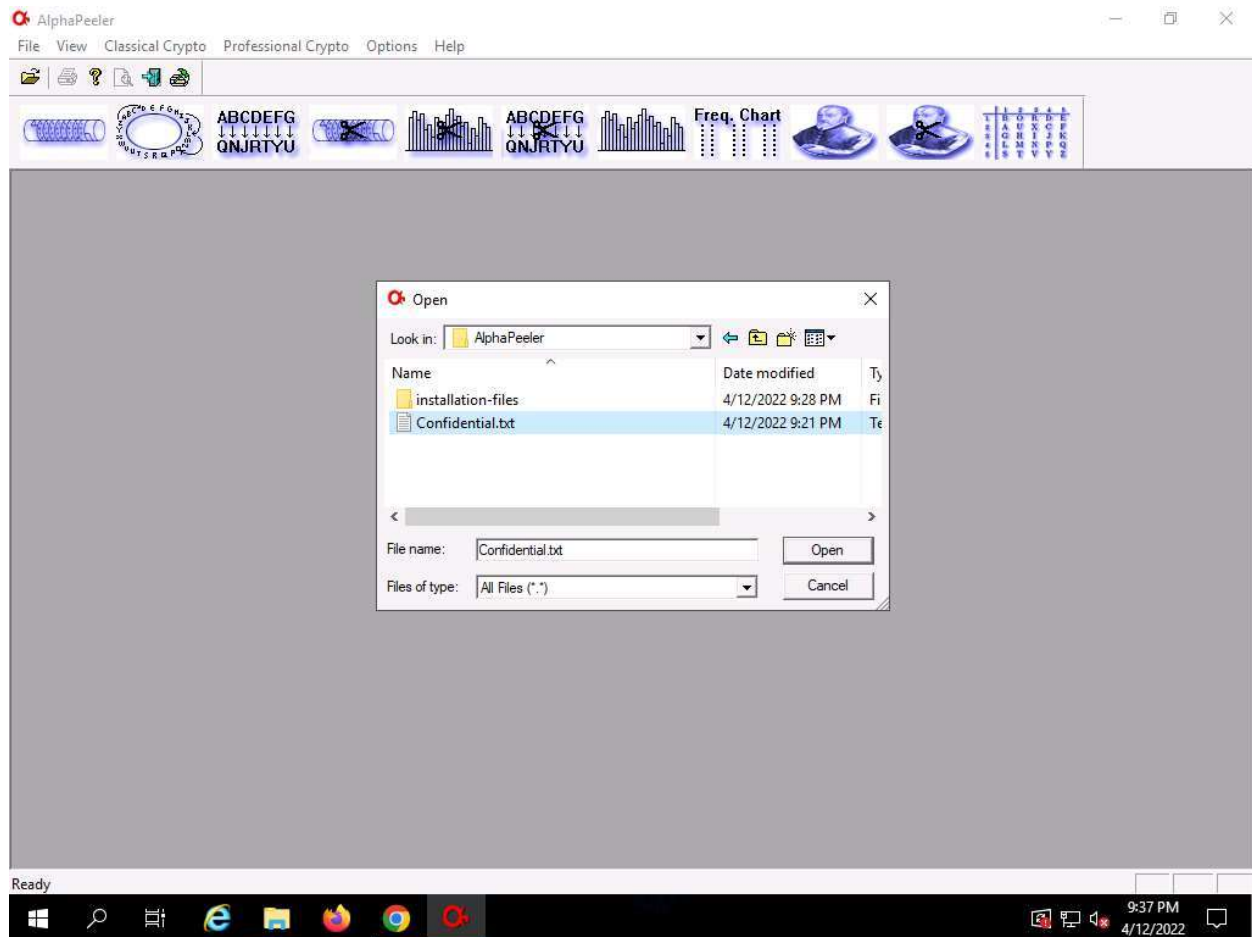




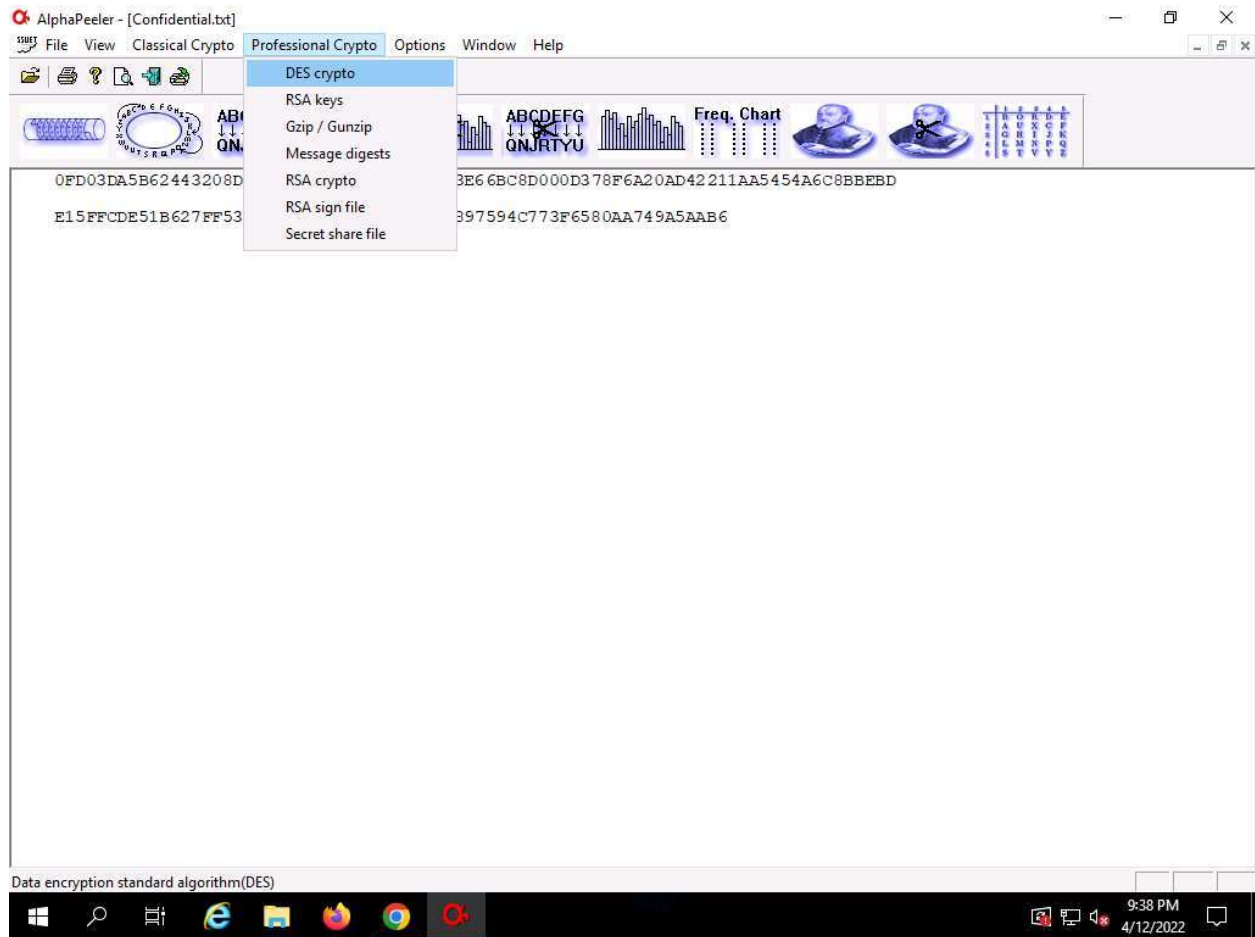
15. The **AlphaPeeler** main window appears; click **File** from the menu bar and click **Open...**



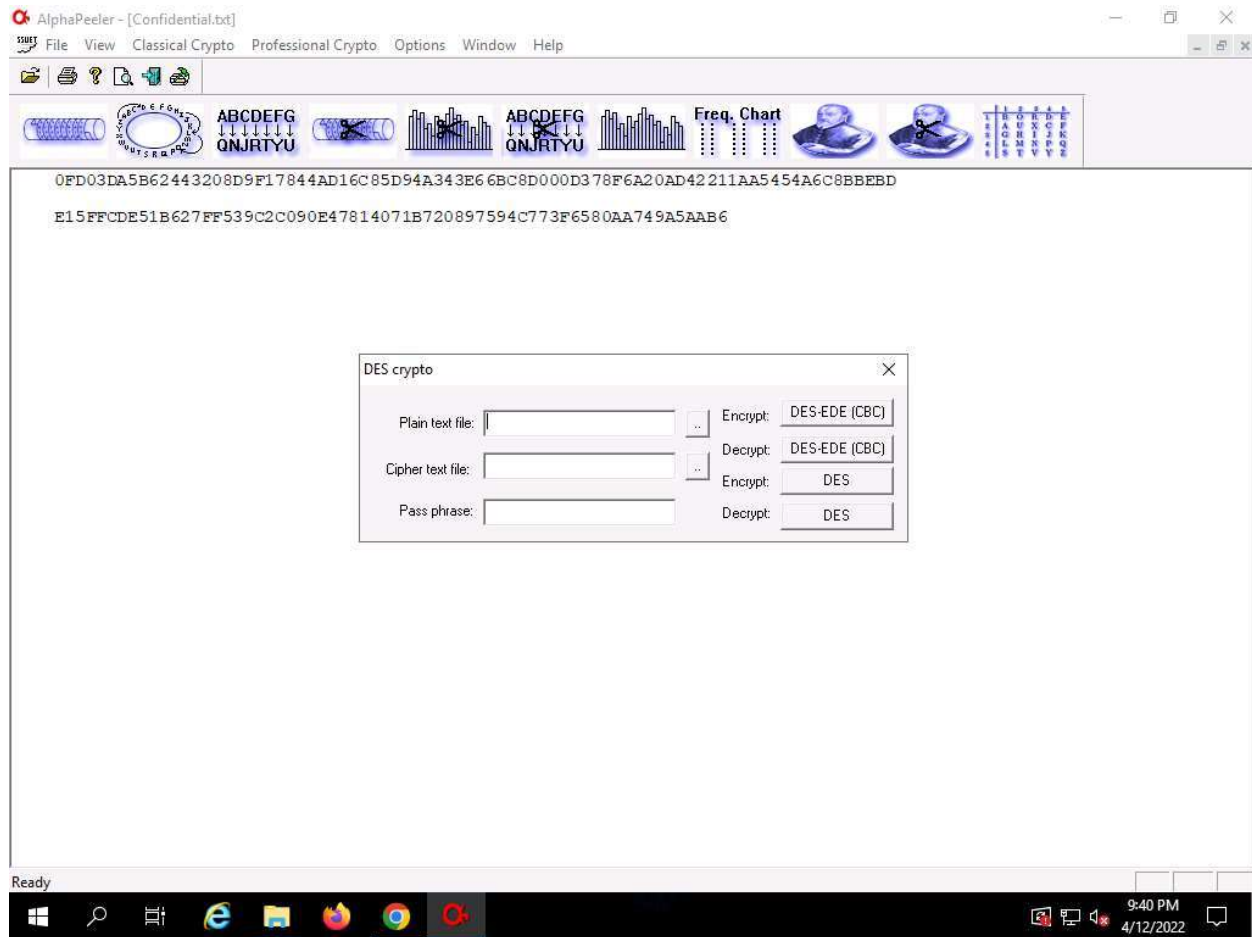
16. The **Open** window appears; in the **Look in** field, navigate to the location of **Z:\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and select **Confidential.txt** file; then, click **Open**.



17. The **Confidential.txt** file appears; click **Professional crypto** from the menu bar and select the **DES crypto** option.



18. The **DES crypto** pop-up appears; click the ellipsis icon next to the **Plain text file** option.

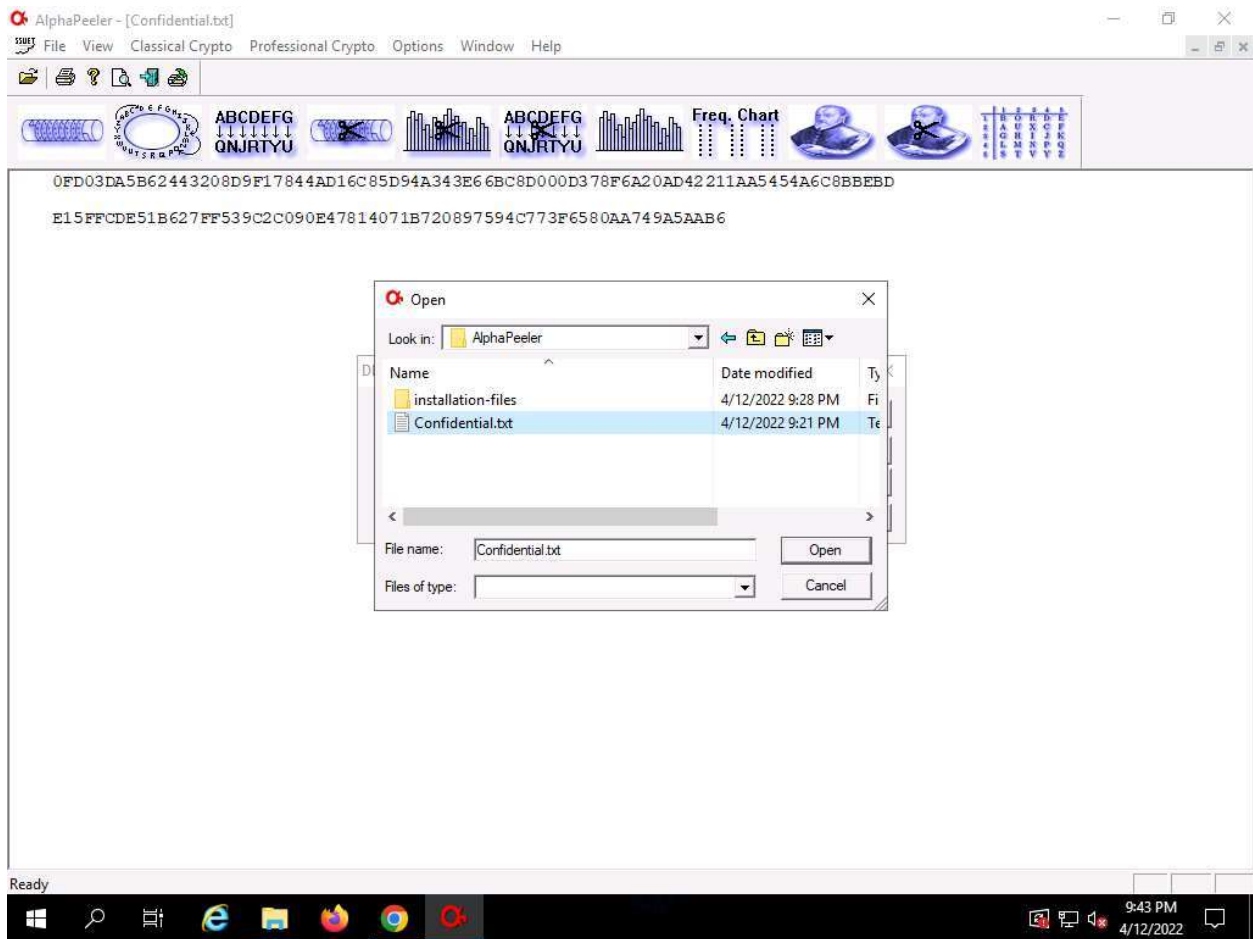


19. The **Open** window appears; navigate to **Desktop** and name the file **Result.txt**; then, click **Open**.

Here, we are creating an output file that will be in plain-text.

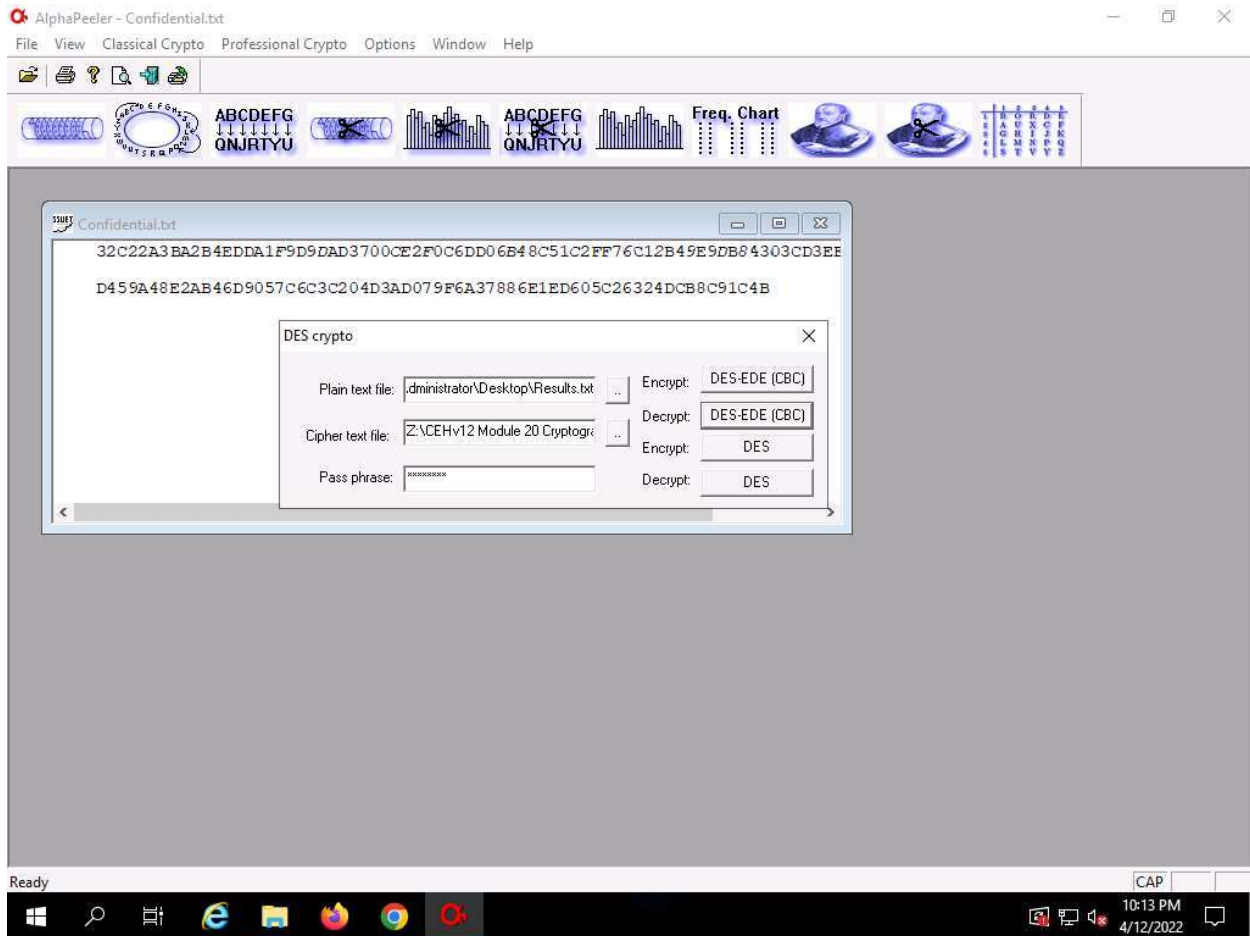
20. In the **DES crypto** pop-up; click the ellipsis icon under the **Cipher text file** option.

21. The **Open** window appears; select the encrypted file (**Confidential.txt**) located at **Z:\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and click **Open**.

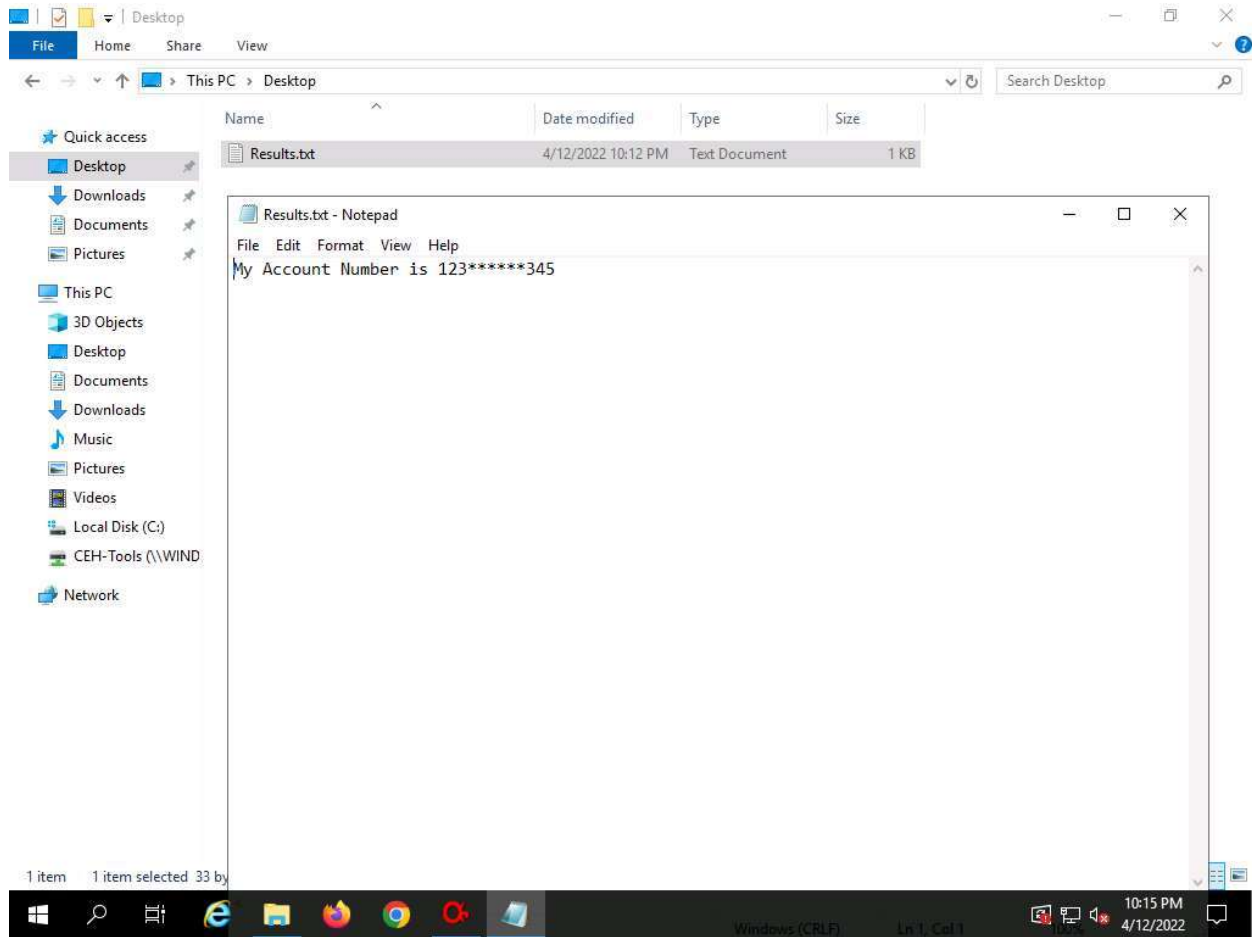


22. In the **DES crypto** pop-up, enter the password that you provided in **Step#10** into the **Pass phrase** field and click the **DES-EDE (CBC)** button next to **Decrypt** to decrypt the text file.

Here, the password provided is **test@123**.



23. Navigate to **Desktop** and double click the **Result.txt** file. You can observe the file content in plain-text, as shown in the screenshot.



24. This concludes the demonstration of performing cryptanalysis using AlphaPeeler.

25. You can also use other cryptanalysis tools such as **Cryptosense** (<https://cryptosense.com>), **RsaCtfTool** (<https://github.com>), **Msieve** (<https://sourceforge.net>), and **Cryptol** (<https://cryptol.net>) to perform cryptanalysis.

26. Close all open windows and document all the acquired information.