Module 20: Cryptography

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

- Perform multi-layer hashing using CyberChef
- Perform file and text message encryption using CryptoForge

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: Perform Multi-layer Hashing using CyberChef

CyberChef enables a wide array of "cyber" tasks directly in browser. It offers a wide range of operations and transformations, from basic text manipulation to complex cryptographic functions which include various hashing techniques such as MD5, SHA-1, SHA-256, SHA-512, etc., and encoding techniques such as text to hexadecimal, binary, Base64, or URL encoding.

A multi-layer hash typically refers to a hierarchical or nested structure of hash functions applied successively to data. Instead of just applying a single hash function to a piece of data, multiple hash functions are employed in layers or stages, with the output of one hash function serving as the input to the next one.

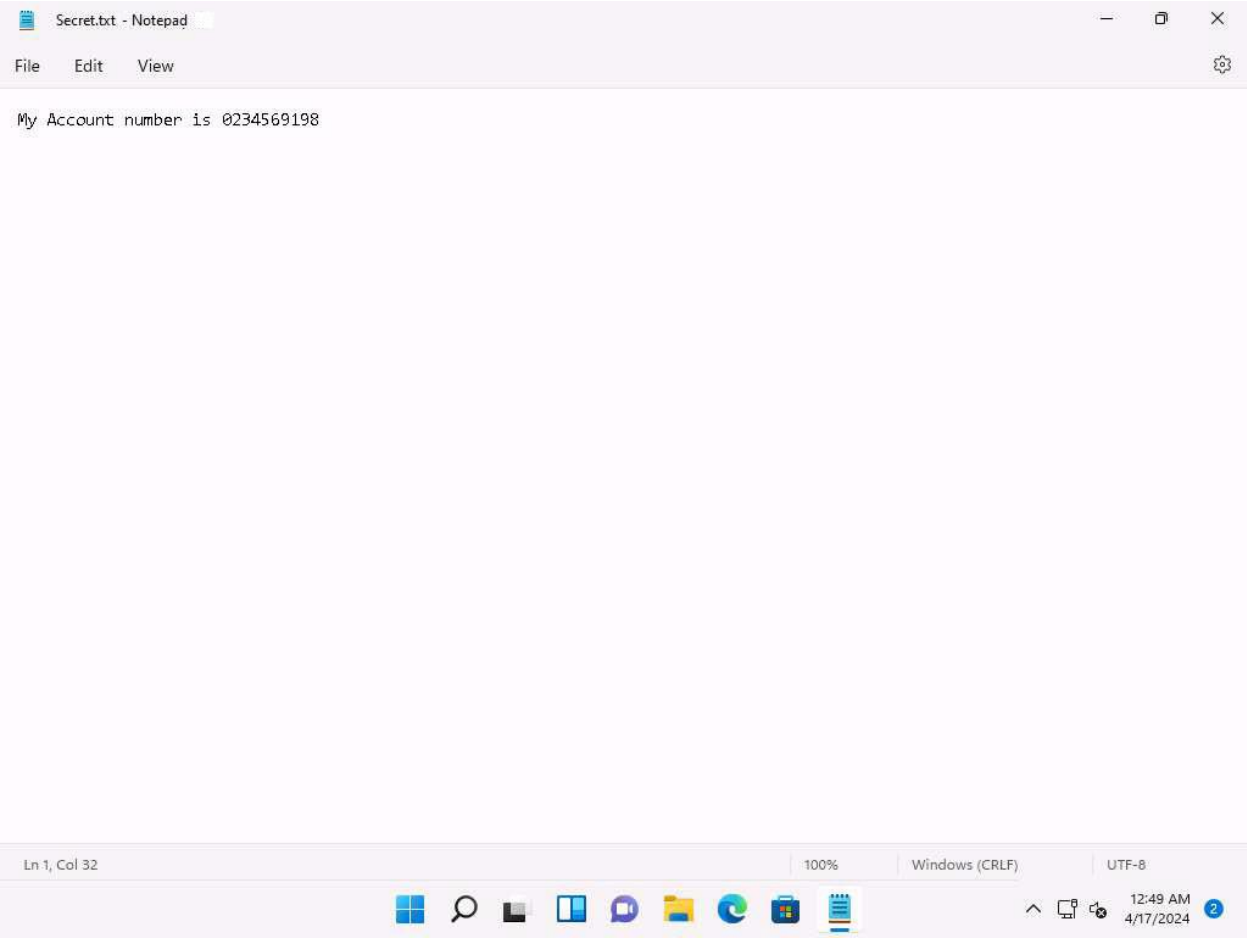
Here, we will perform multi-layer hashing using CyberChef.

1. Click Windows 11 to switch to the **Windows 11** machine. Click Ctrl+Alt+Delete to activate it and login with **Admin**/**Pa$$w0rd**.

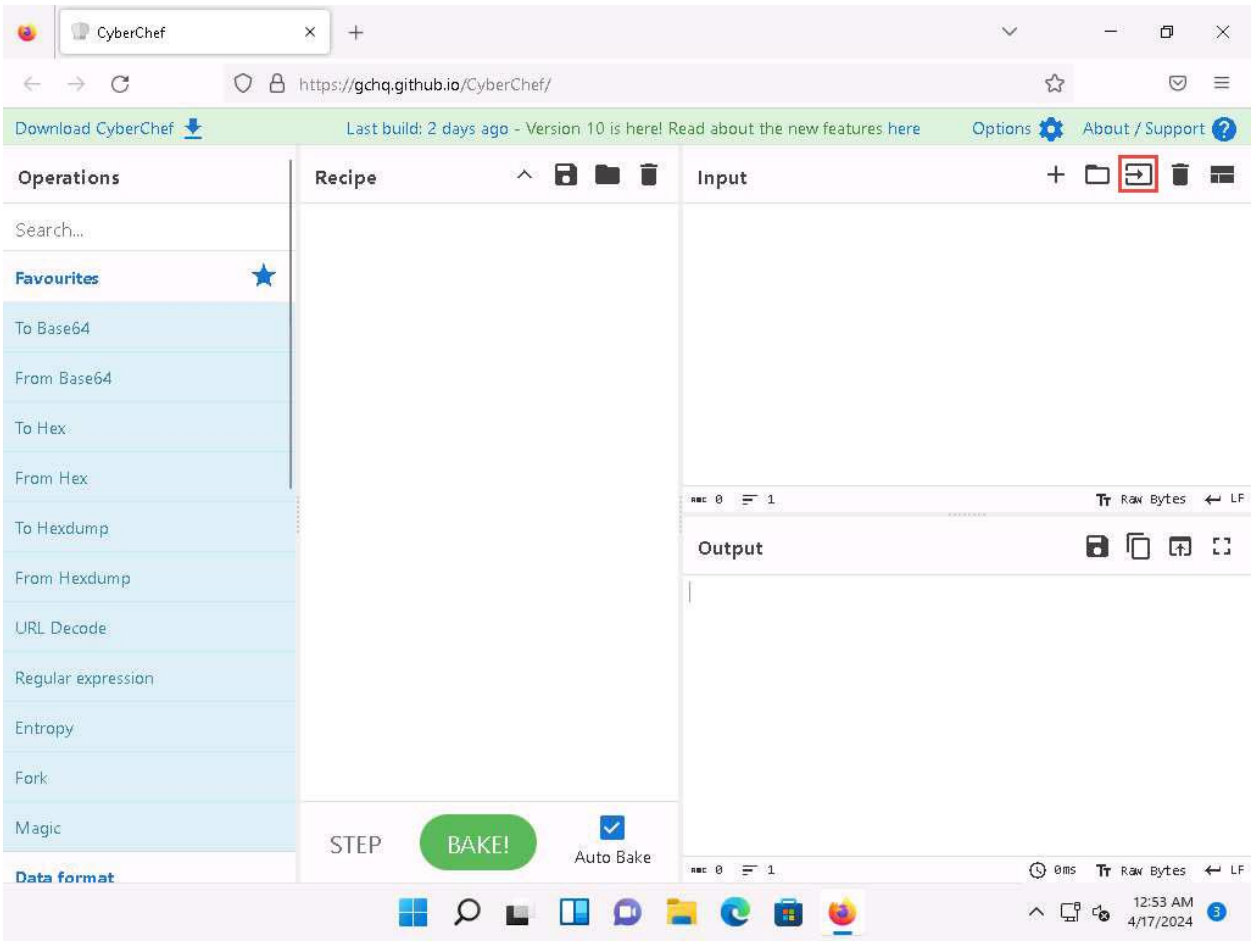
Alternatively, you can also click **Pa$$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane.

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

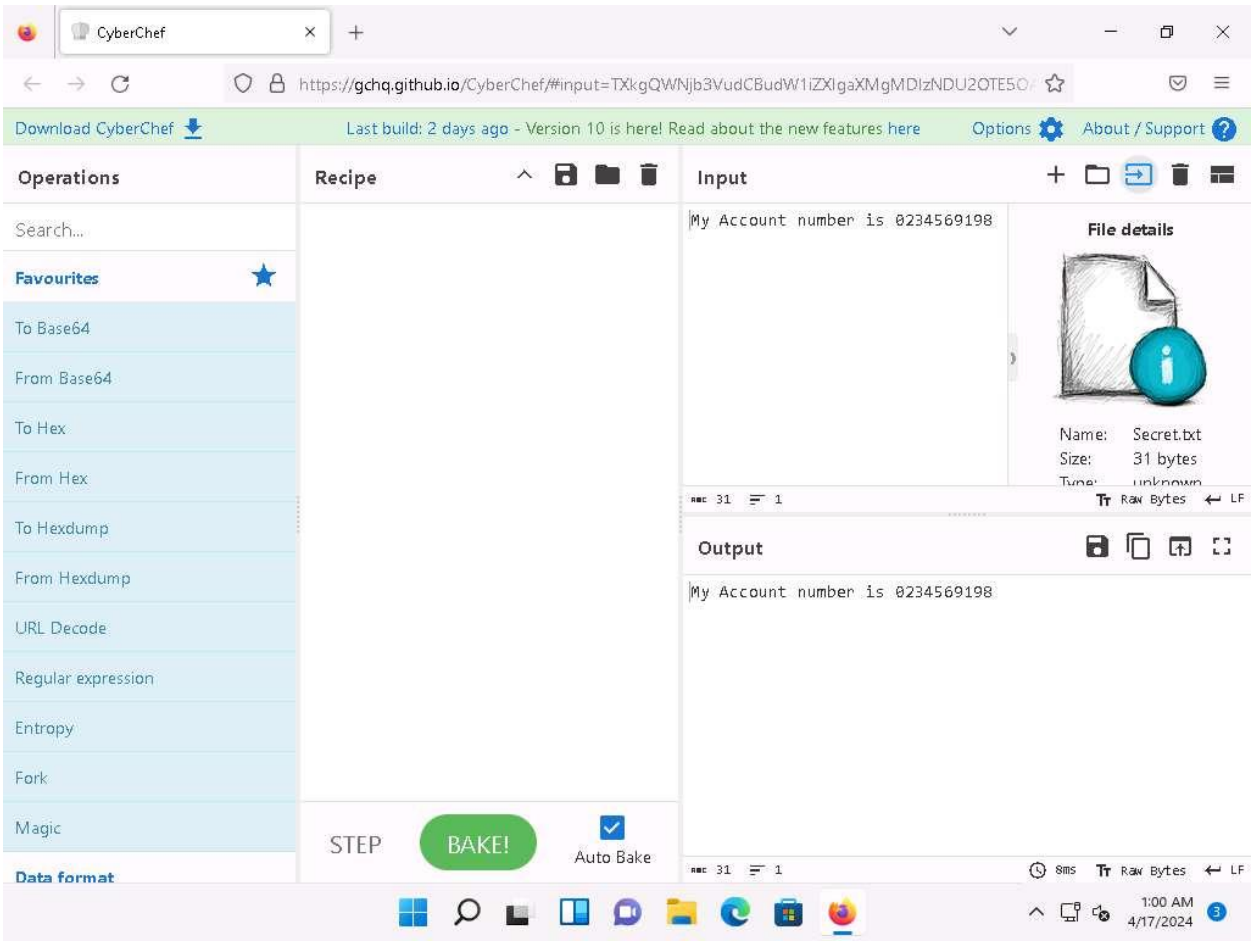
2. Navigate to **Desktop**, right-click on the **Desktop** window, and navigate to **New --> Text Document** to create a new text file. A newly created text file appears; rename it to **Secret.txt** and open it. Write some text in it (here, **My Account number is 0234569198**) and press **Ctrl+S** to save the file. Close the text file.



3. Launch any web browser, and go to **https://gchq.github.io/CyberChef/** (here, we are using **Mozilla Firefox**).
4. CyberChef website appears, click on **Open file as input** button present at the top of the **Input** section.



5. **File Upload** window appears, select **Secret.txt** file from **Desktop** and click **Open**.
6. The contents of the **Secret.txt** file will be displayed in the **Input** window.

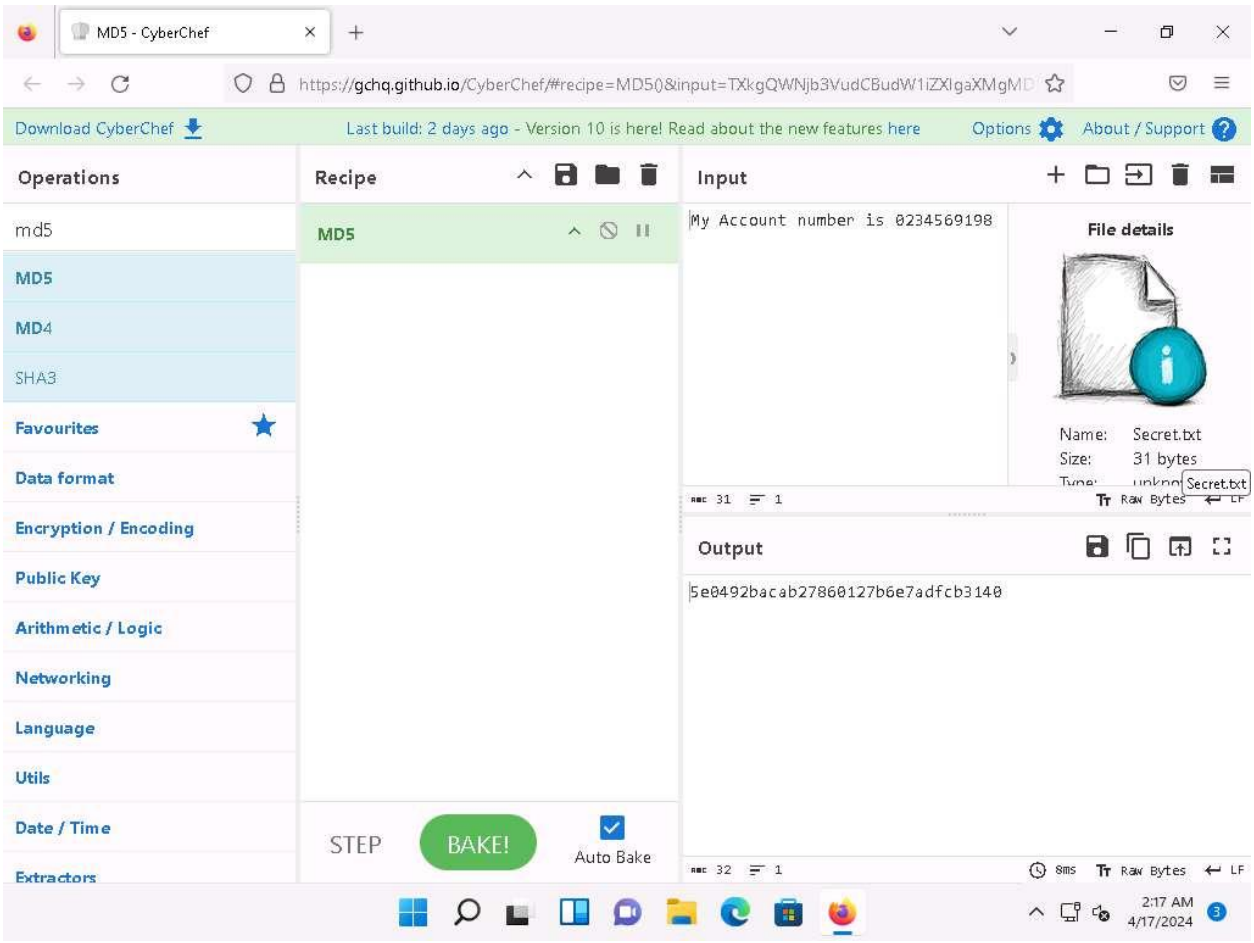


7. Now, we will calculate MD5 hash of the **Secret.txt** file, to do so, in the search field present under **Operations** section, type md5 and drag **MD5** from the results in the **Operations** section in to the **Recipe** section.

Alternatively, you can expand **Hashing** node in the **Operations** section and select **MD5** algorithm.

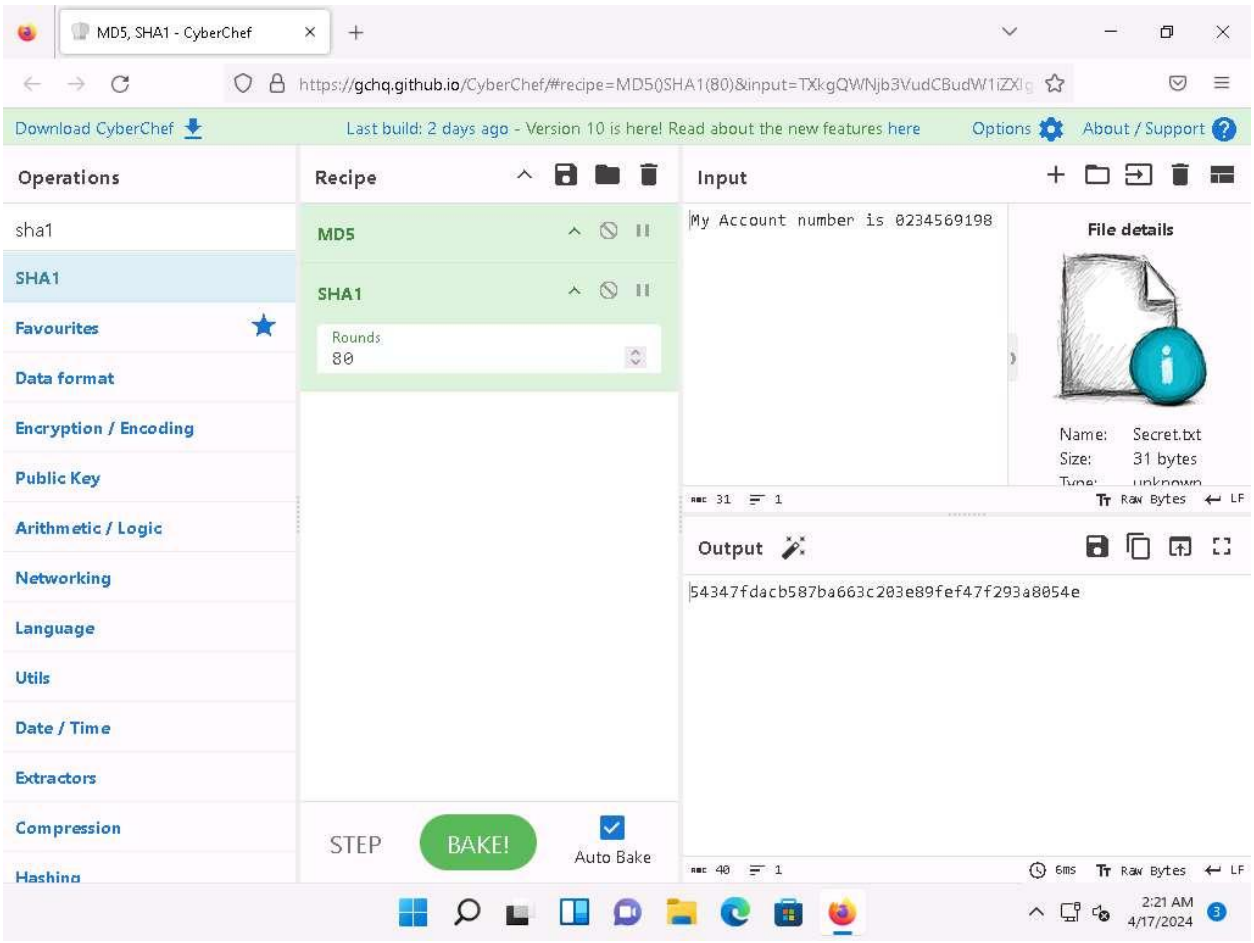
8. The tool calculates the **MD5** hash of the given input file and displays the output in the **Output** section.

Ensure that **Auto Bake** option is checked. If "Auto Bake" is enabled, CyberChef will promptly "bake" and generate the output as soon as either the input or the recipe is modified.

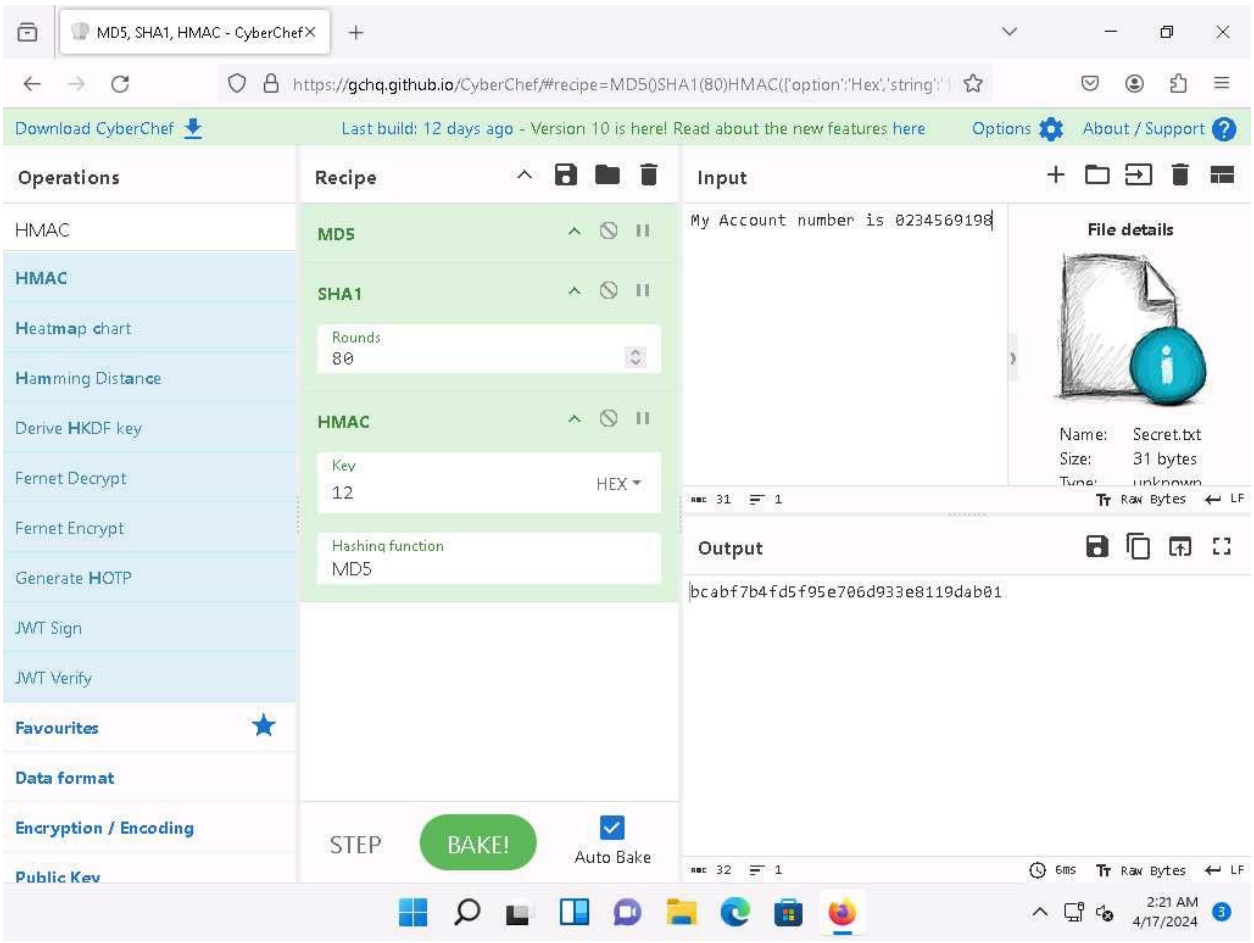


9. Now, we will compute **SHA1** hash of the output. To do so, search for **sha1** and drag **SHA1** from the **Operations** section to **Recipe** section ensure the number of rounds is **80**.

10. The **Output** section displays the computed **SHA1** hash of the **MD5** value.



11. Now, we will add **HMAC** as another layer of hash, search for hmac and drag **HMAC** from **Operations** section to **Recipe** section.
12. In **HMAC** Recipe, enter the key as **12** and select the **Hashing function** as **MD5** from the drop-down.
13. The **Output** section displays the **HMAC** hash of the **SHA1** hash.



14. In addition, we can set break point to the hash operation by clicking on the **Set breakpoint** button present in the Recipe.

Breakpoints on an operation in the recipe will pause execution before running it.

15. We can also disable a hash operation by clicking the **Disable Operation** button present in the Recipie.
16. This concludes the demonstration of performing multi-layer hashing using CyberChef.
17. Close all open windows and document all the acquired information.

Question 20.1.1.1

In Windows 11 machine create a Secret.txt file with My Account number is 0234569198 and use CyberChef (https://gchq.github.io/CyberChef/) and perform multi-layer hashing. Which button in the recipe will pause execution before running it.

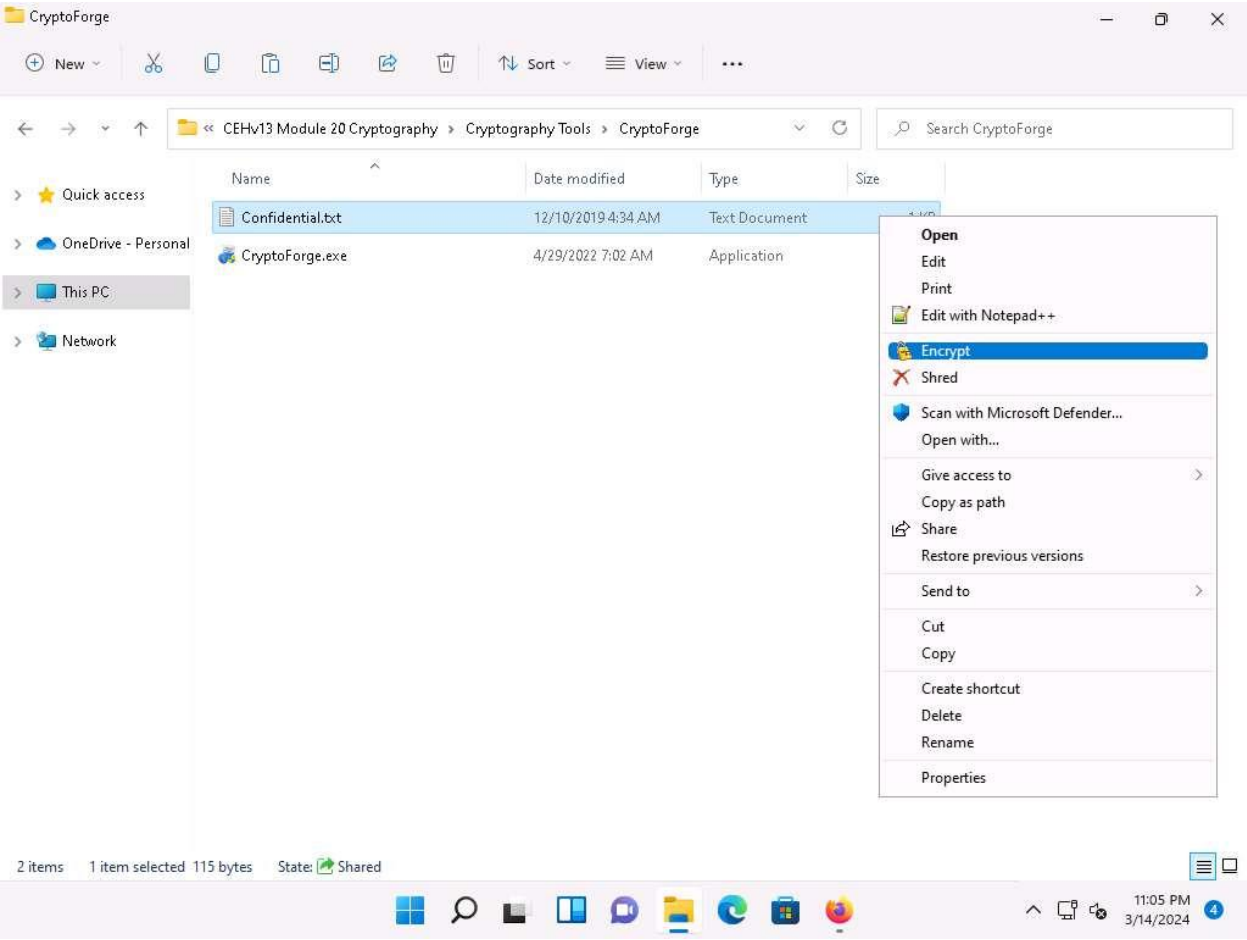
Task 2: Perform File and Text Message Encryption using CryptoForge

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.

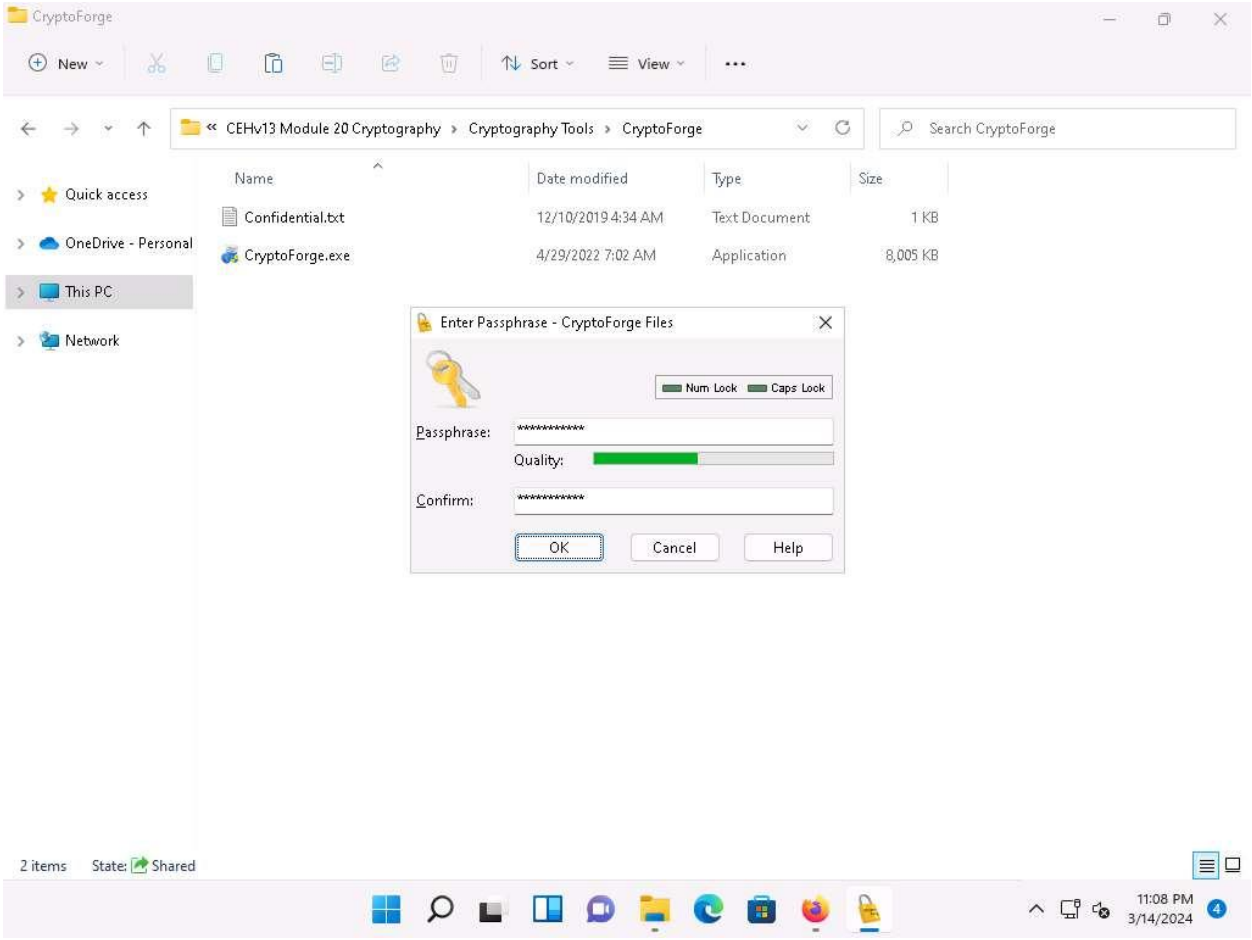
Here, we will use the CryptoForge tool to encrypt a file and text message.

1. Click on Windows 11 to switch to the **Windows 11** machine. Navigate to **E:\CEH-Tools\CEHv13 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.

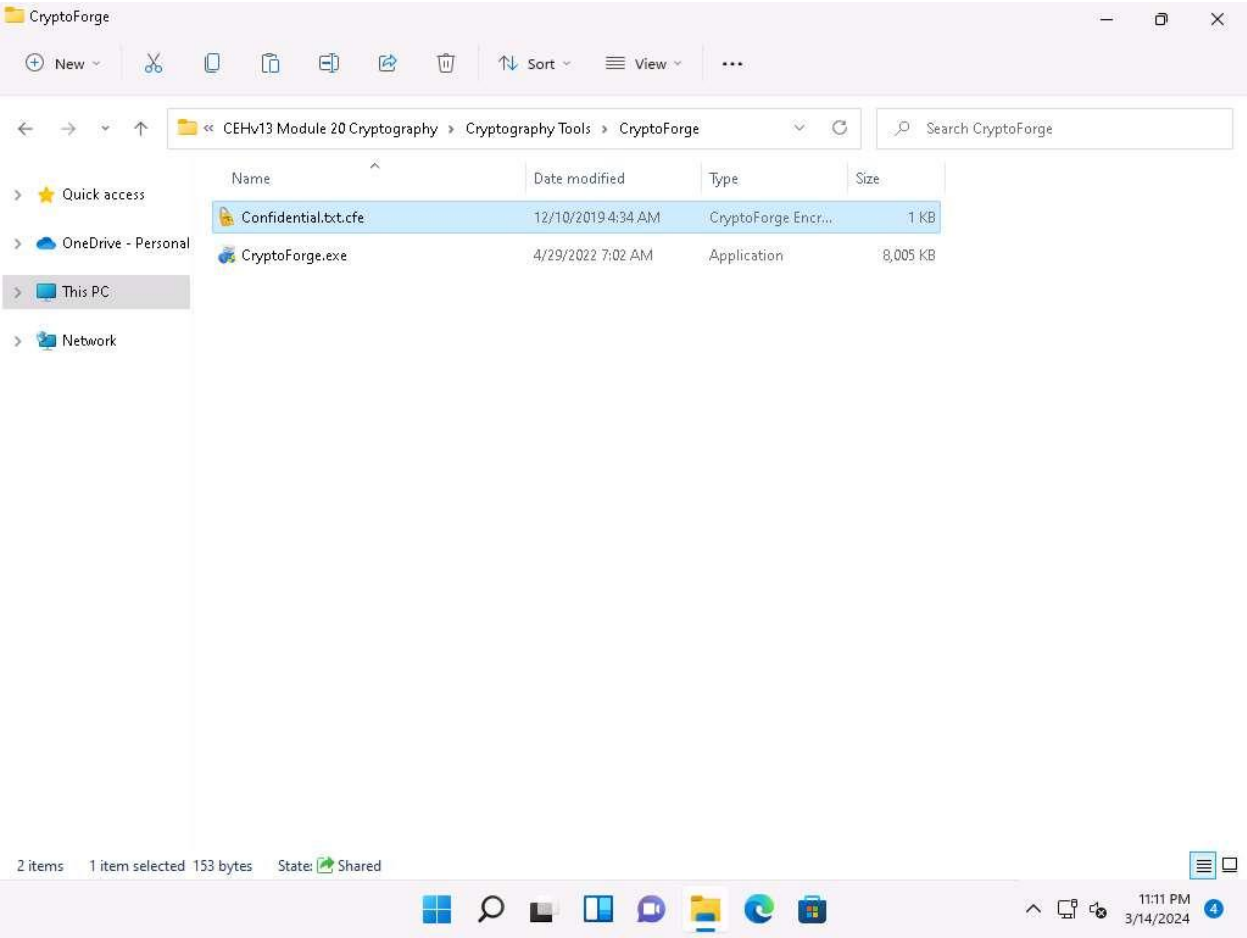


2. The **Enter Passphrase - CryptoForge Files** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **qwerty@1234**.

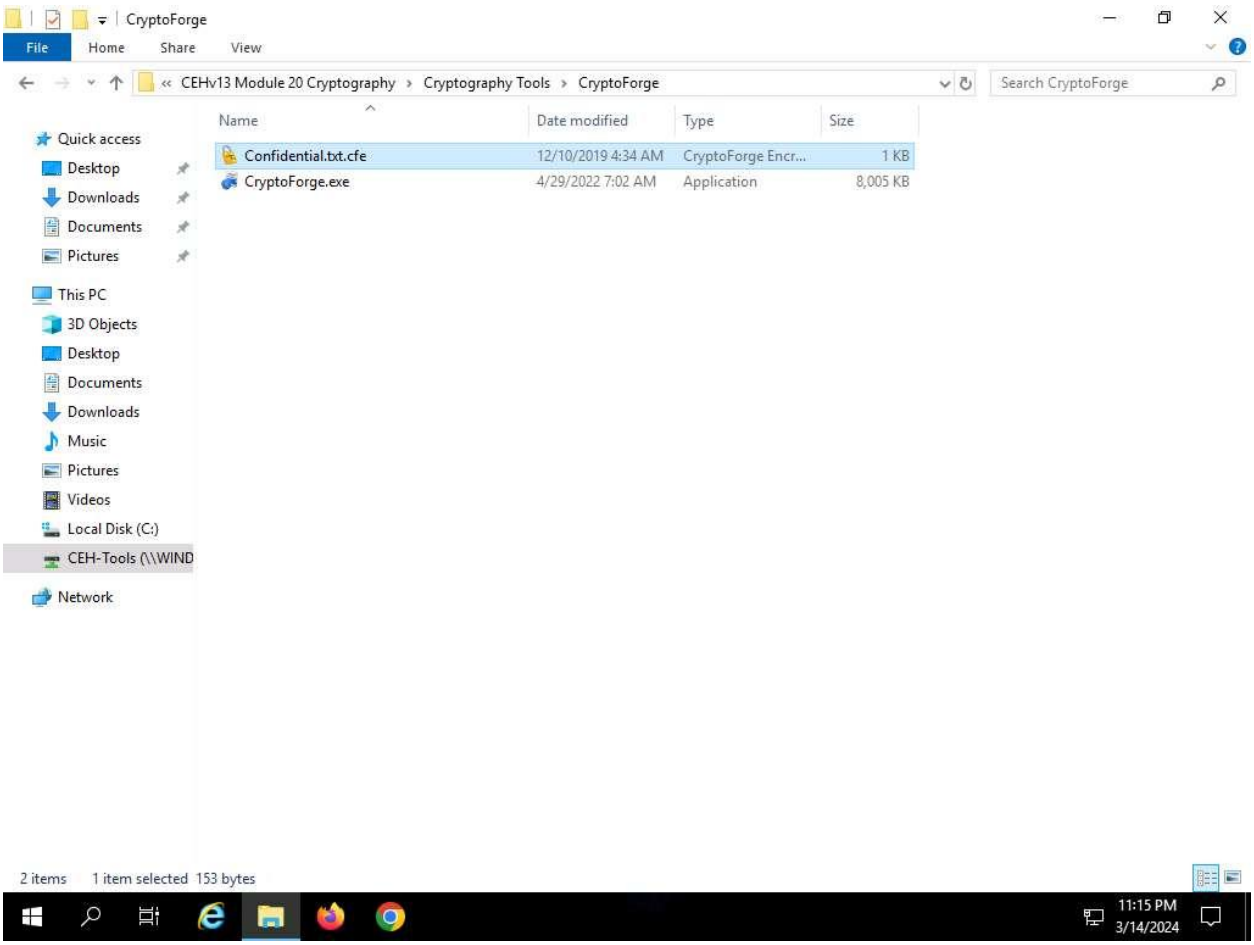


3. Now, the file will be encrypted in the same location, and the old file will be deleted automatically, as shown in the screenshot.

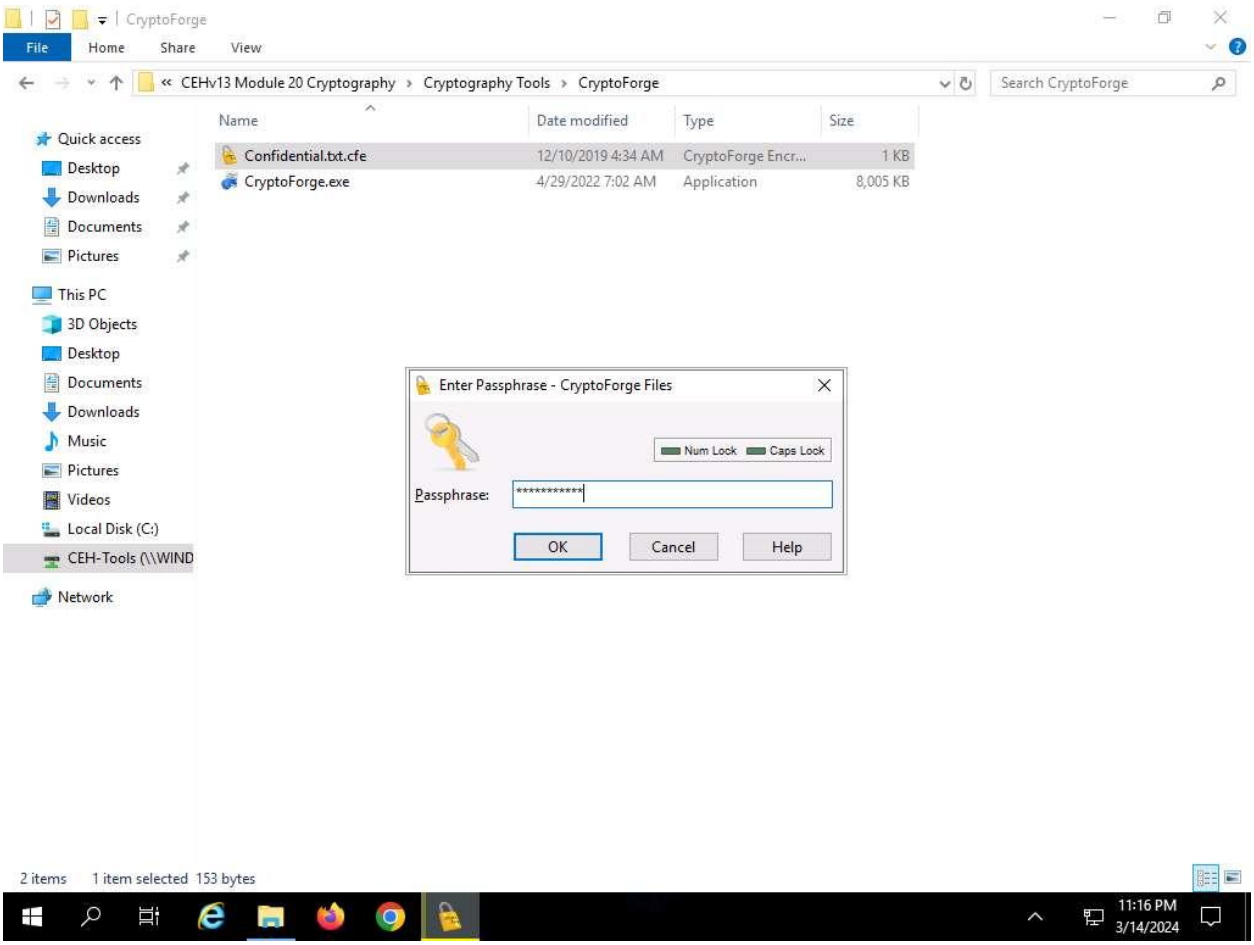
No one can access this file unless the user provides the password for the encrypted file. You will have to share the password with the user through message, email, or any other means.



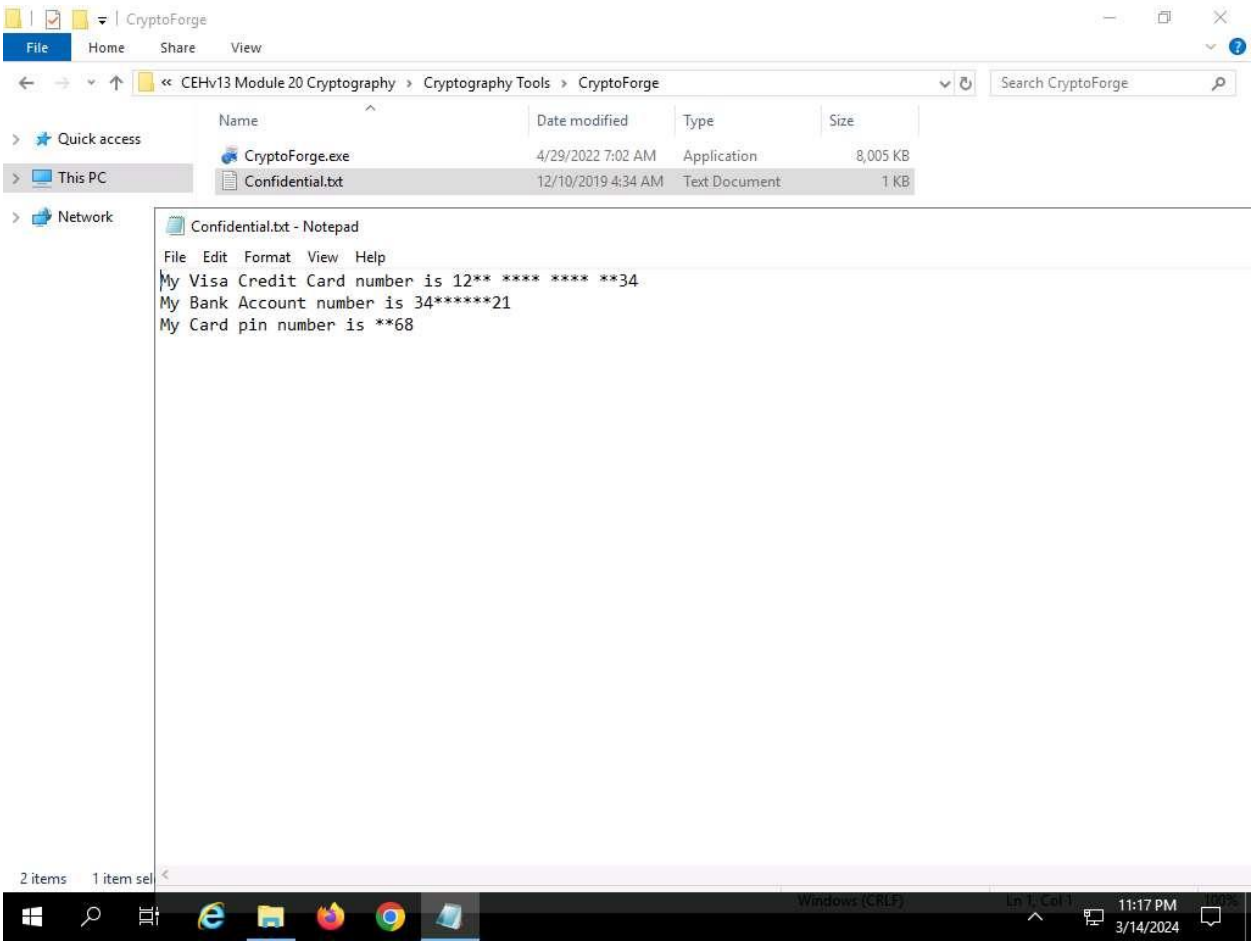
4. Let us assume that you shared this file through a shared network drive.
5. Now, click on Windows Server 2019 to switch to the **Windows Server 2019**, click Ctrl+Alt+Delete to activate the machine and login with **Administrator/Pa$$w0rd**.
6. Navigate to **Z:\CEHv13 Module 20 Cryptography\Cryptography Tools\CryptoForge**. You will observe the encrypted file in this location.
7. Double-click the encrypted file to decrypt it and view its contents.



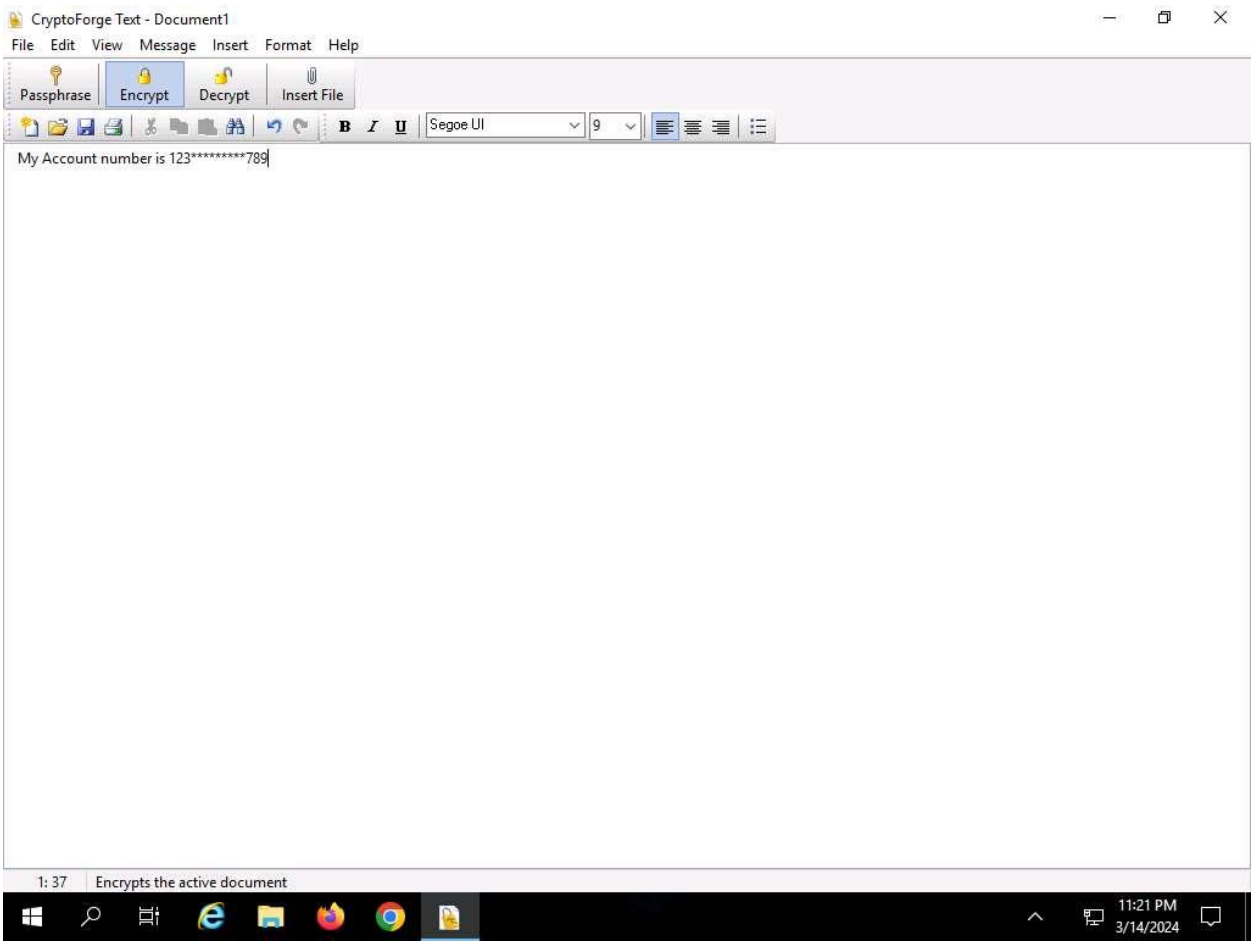
8. The **Enter Passphrase - CryptoForge Files** dialog-box appears; enter the password that you have provided in **Step#2** to encrypt the file and click **OK**.



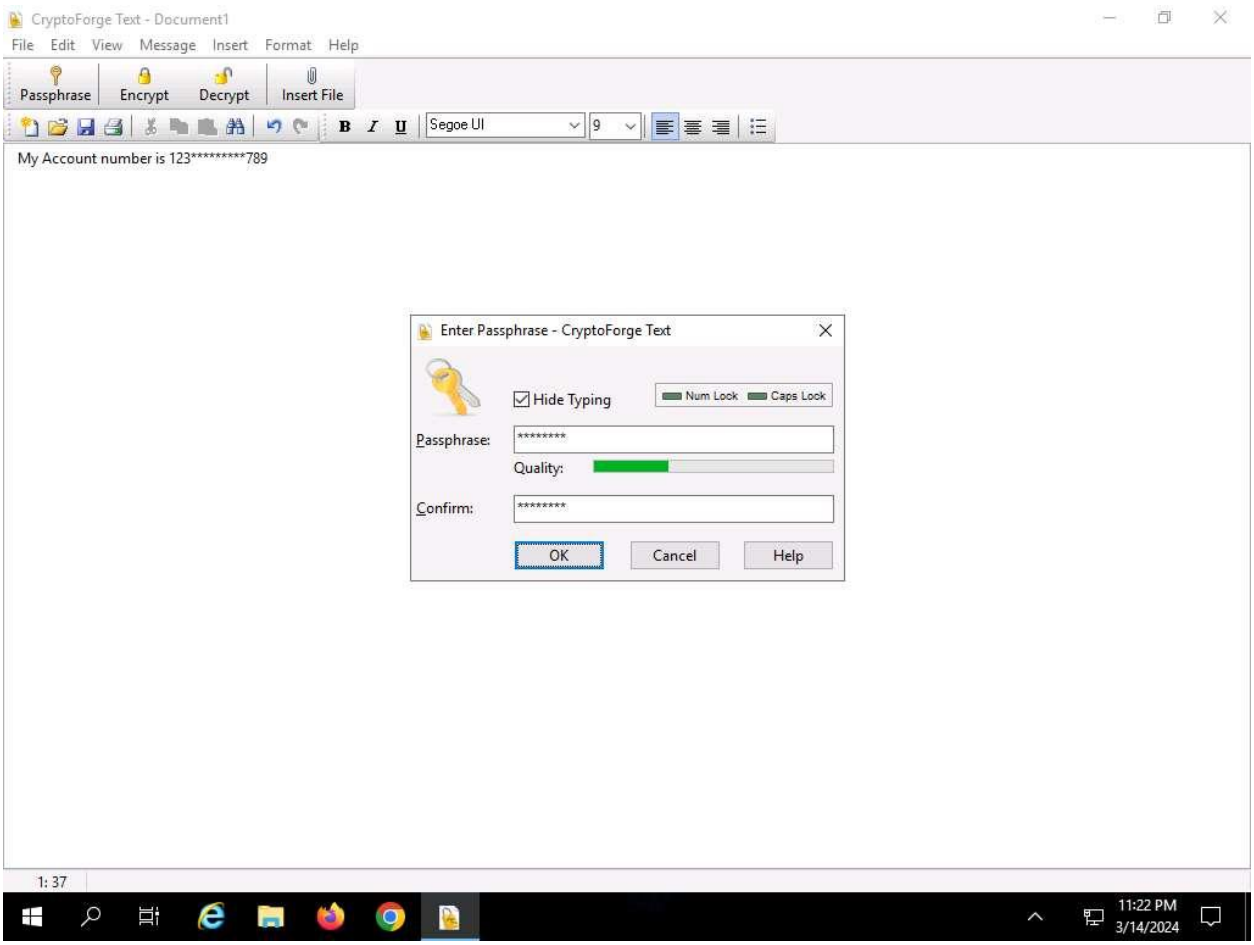
9. Upon entering the password, the file will be successfully decrypted. You may now double-click the text file to view its contents.



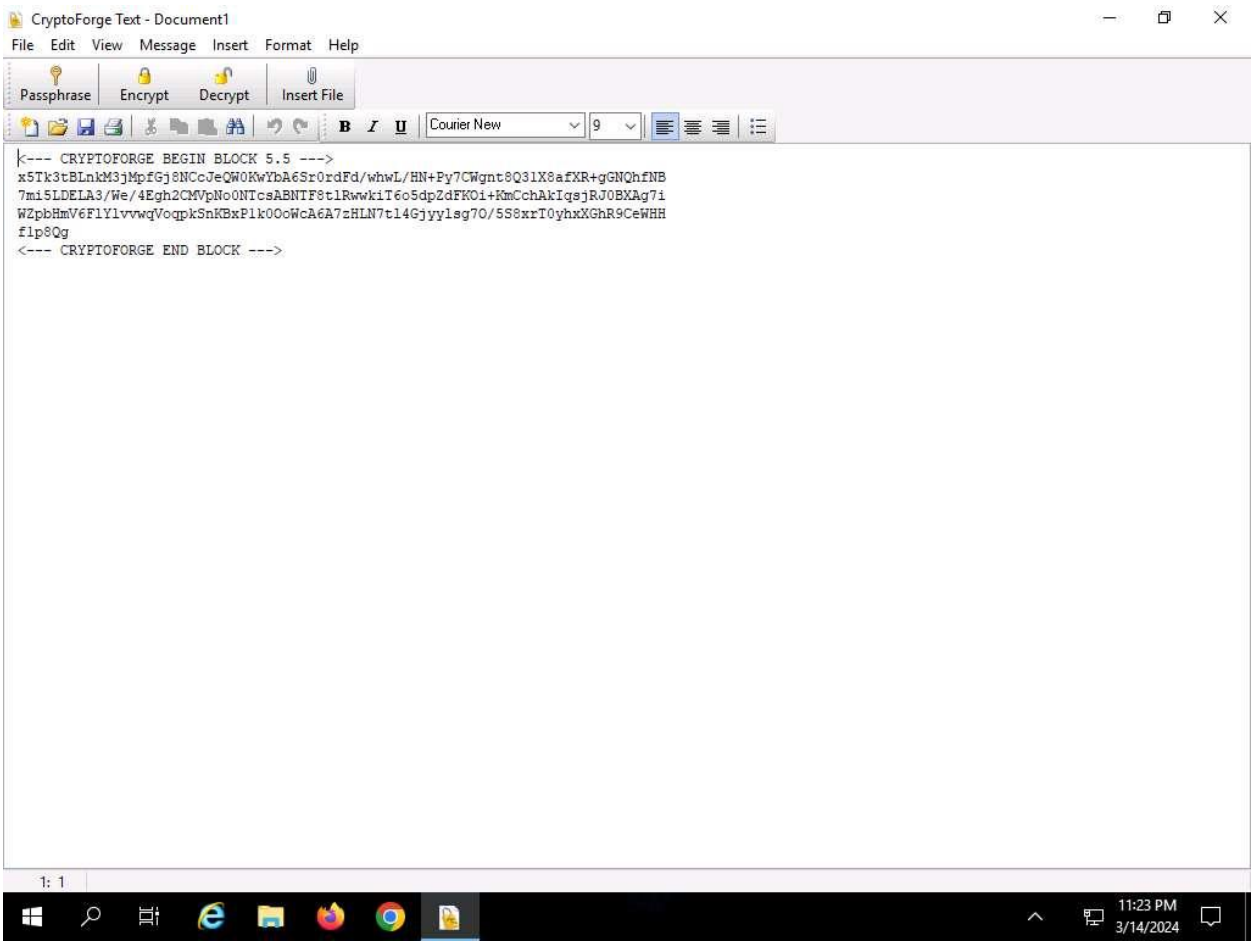
10. So far, you have seen how to encrypt a file and share it with the intended user. Now, we shall share an encrypted message with a user.
11. In the **Windows Server 2019** machine, click the **Type here to search** icon in the **Desktop**, type **crypto** in the search field and click **CryptoForge Text** from the apps to launch the application.
12. The **CryptoForge Text** window appears; type a message and click **Encrypt** from the toolbar.



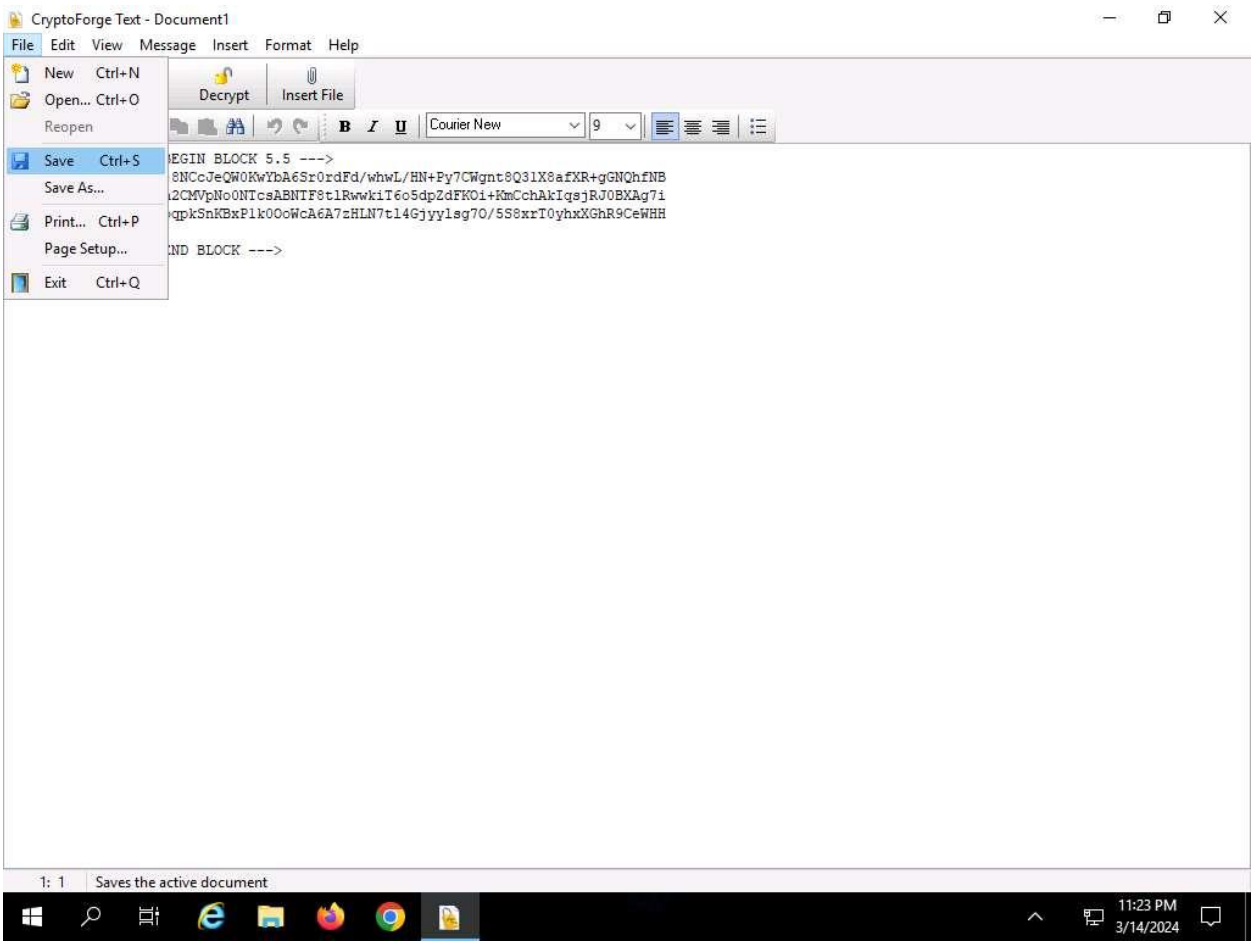
13. The **Enter Passphrase - CryptoForge Text** dialog-box appears; type a password in the **Passphrase** field, retype it in the **Confirm** field, and click **OK**. The password used in this lab is **test@123**.



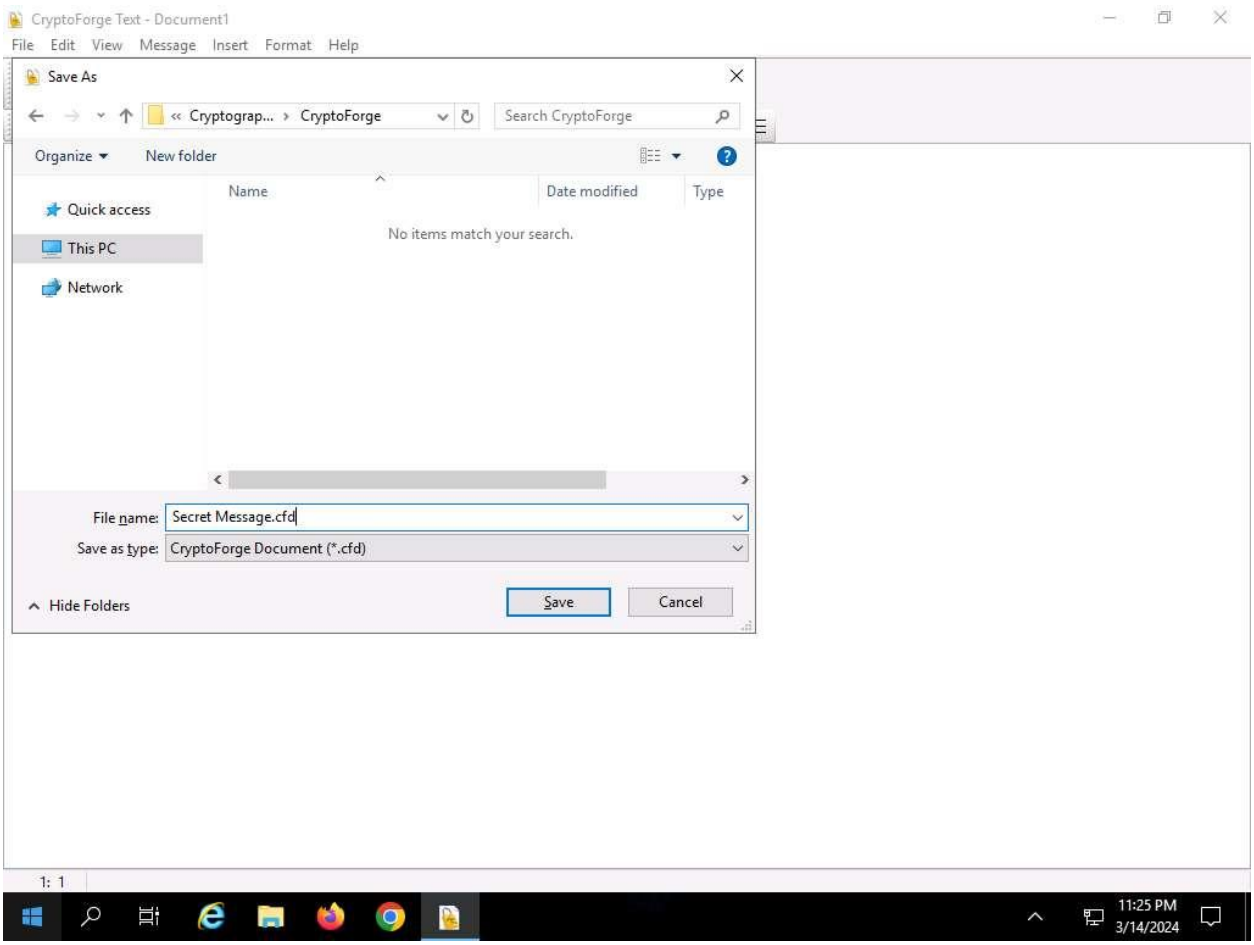
14. The message that you have typed will be encrypted, as shown in the screenshot.



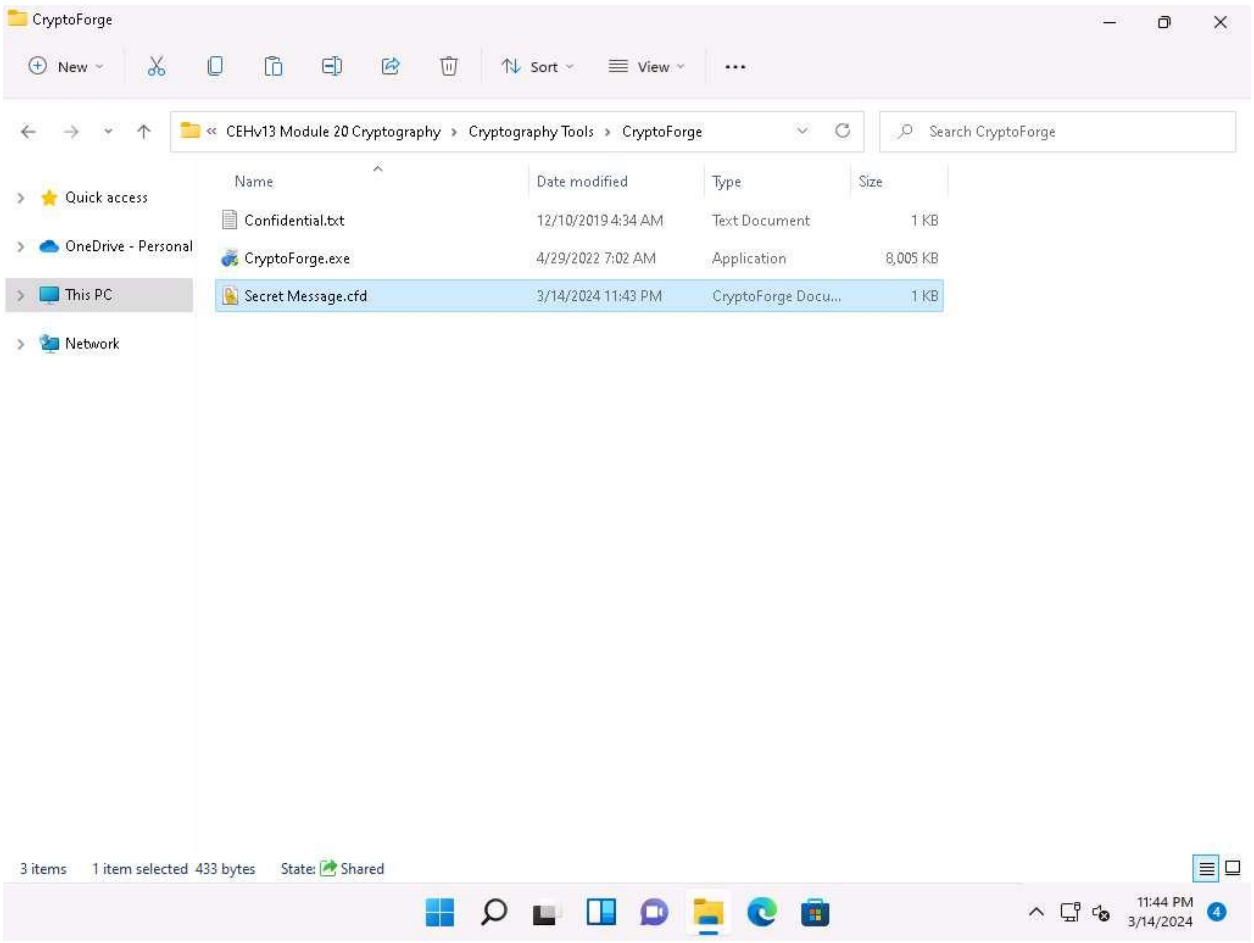
15. Now, you need to save the file. Click **File** in the menu bar and click **Save**.



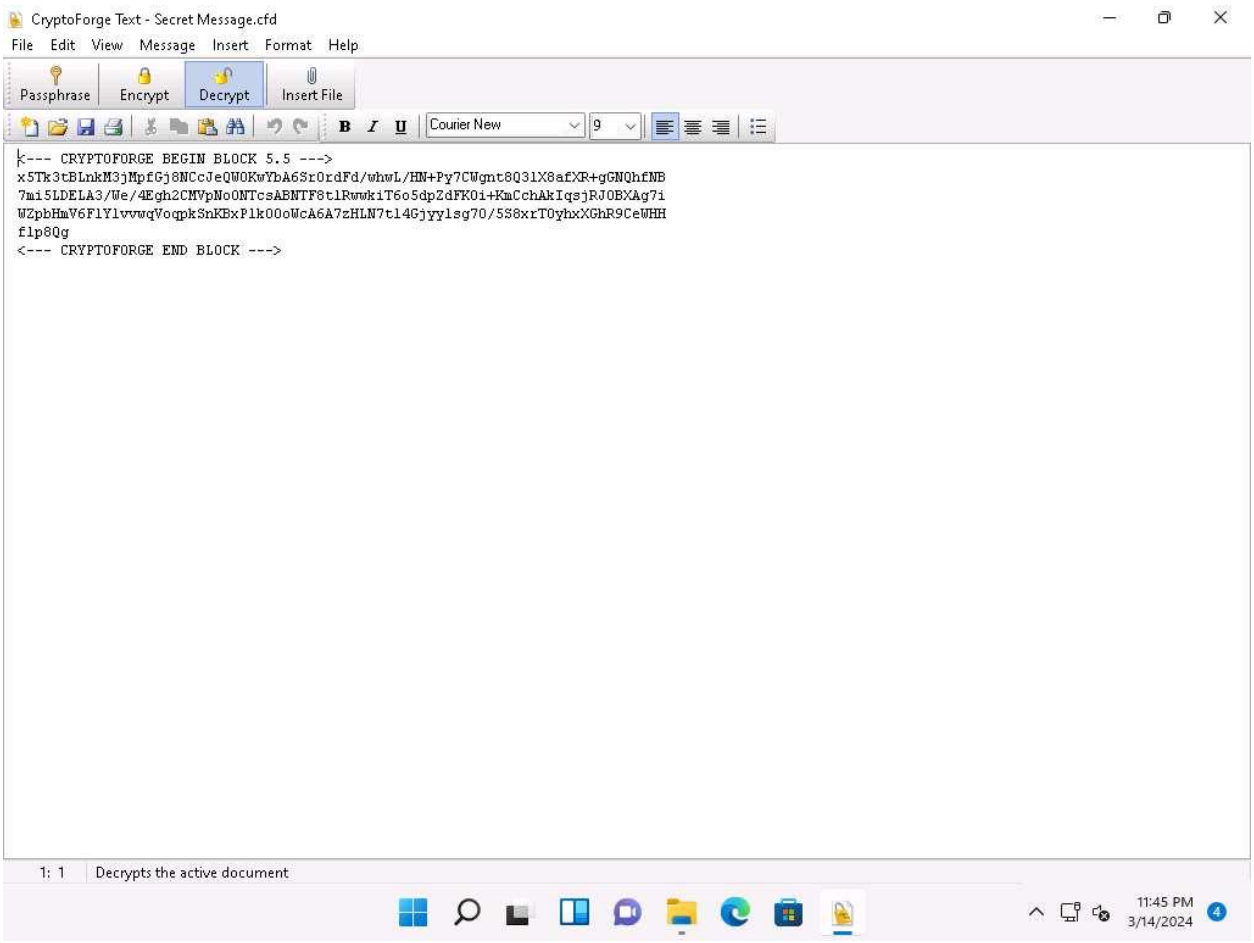
16. The **Save As** window appears; navigate to **Z:\CEHv13 Module 20 Cryptography\Cryptography Tools\CryptoForge**, specify the file name as **Secret Message.cfd**, and click **Save**.



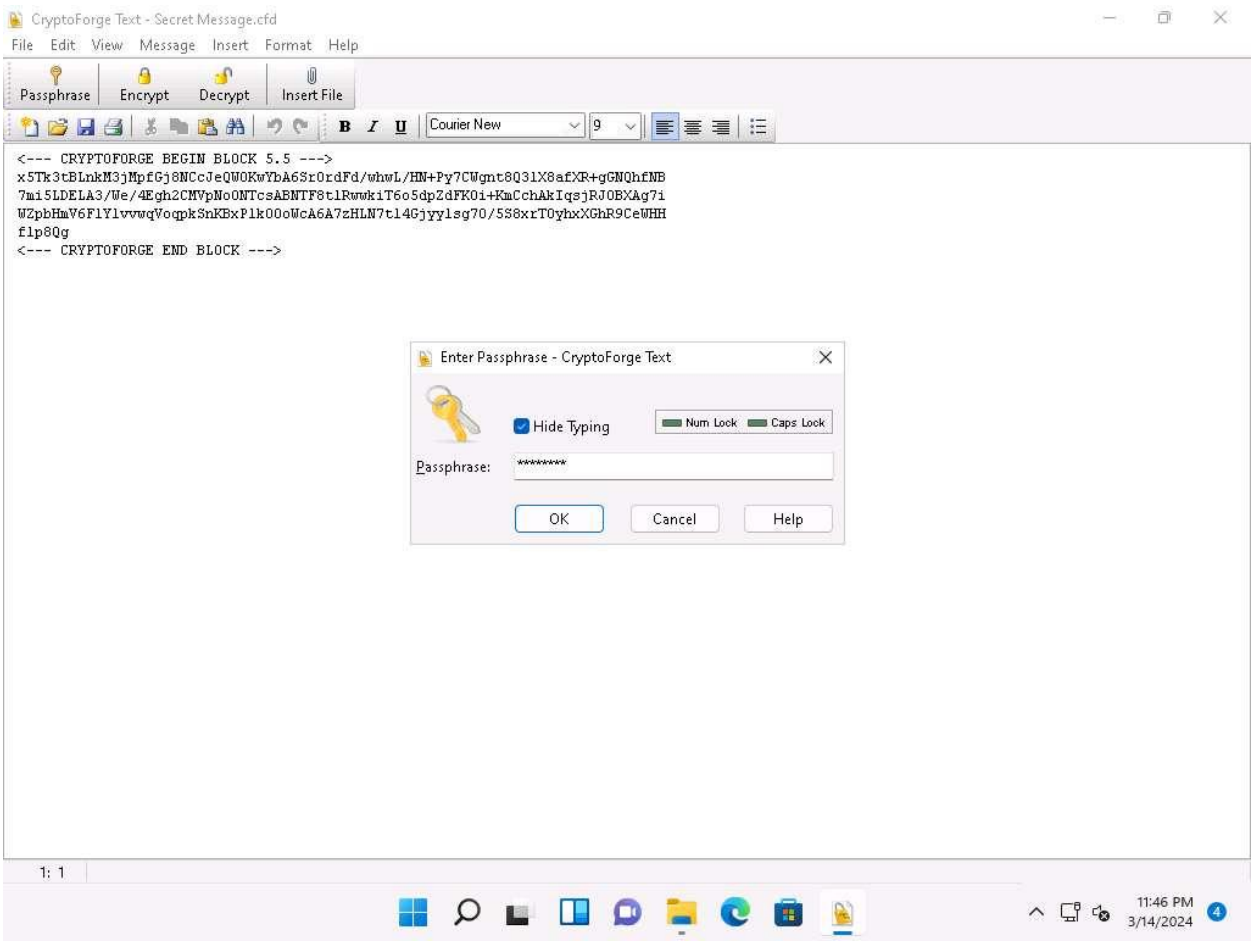
17. Close the **CryptoForge Text** window.
18. Now, let us assume that you shared the file through the mapped network drive and shared the password to decrypt the file in an email message or through some other means.
19. Click on Windows 11 to switch to the **Windows 11** machine and navigate to **E:\CEH-Tools\CEHv13 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.

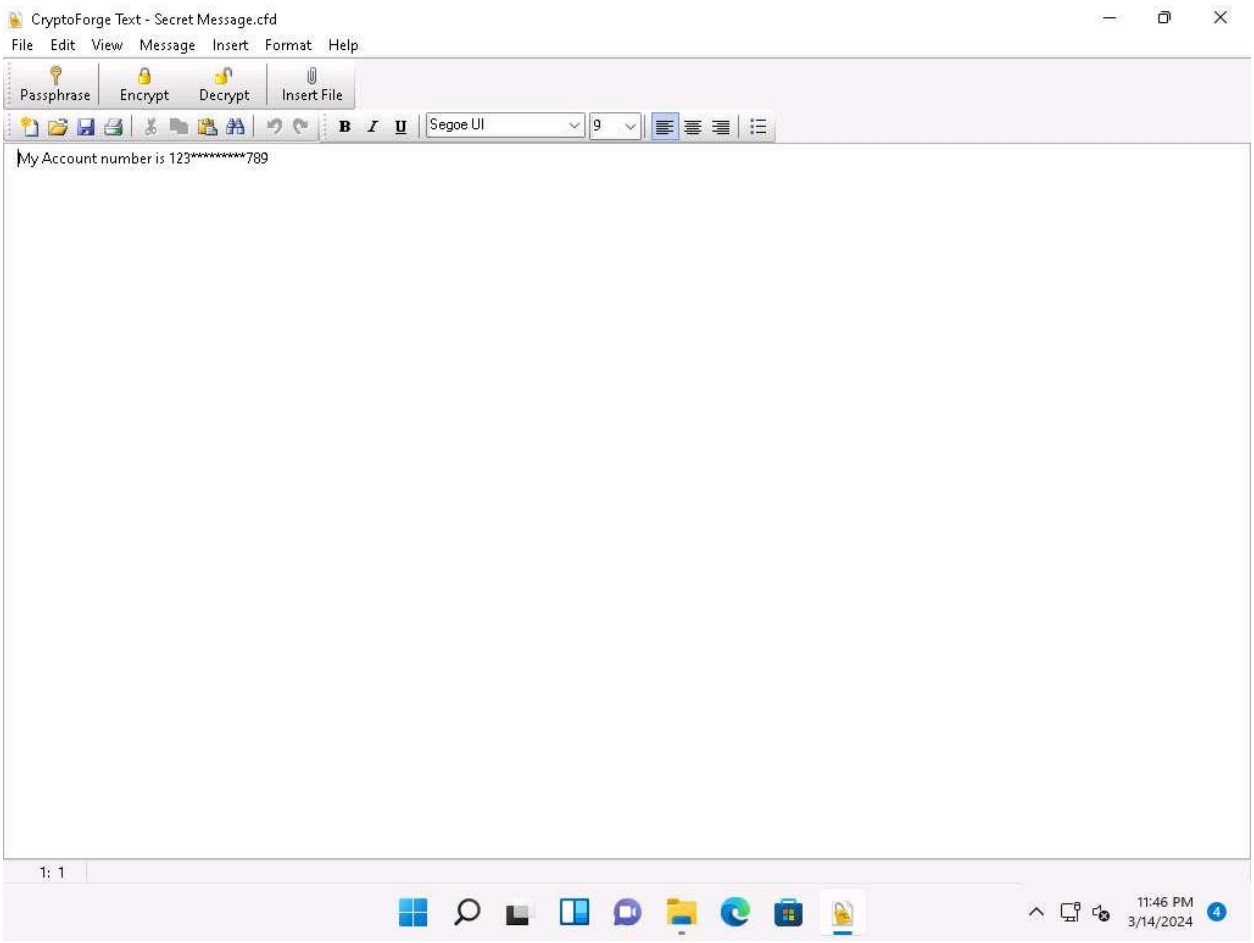


22. The **Enter Passphrase - CryptoForge Text** dialog-box appears; enter the password you provided in **Step#13** to decrypt the message in the **Passphrase** field and click **OK**.



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 20.1.2.1

Use CryptoForge to encrypt the file E:\CEH-Tools\CEHv13 Module 20 Cryptography\Cryptography Tools\CryptoForge\Confidential.txt on the Windows 11 machine. What is the extension of the encrypted file?