

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

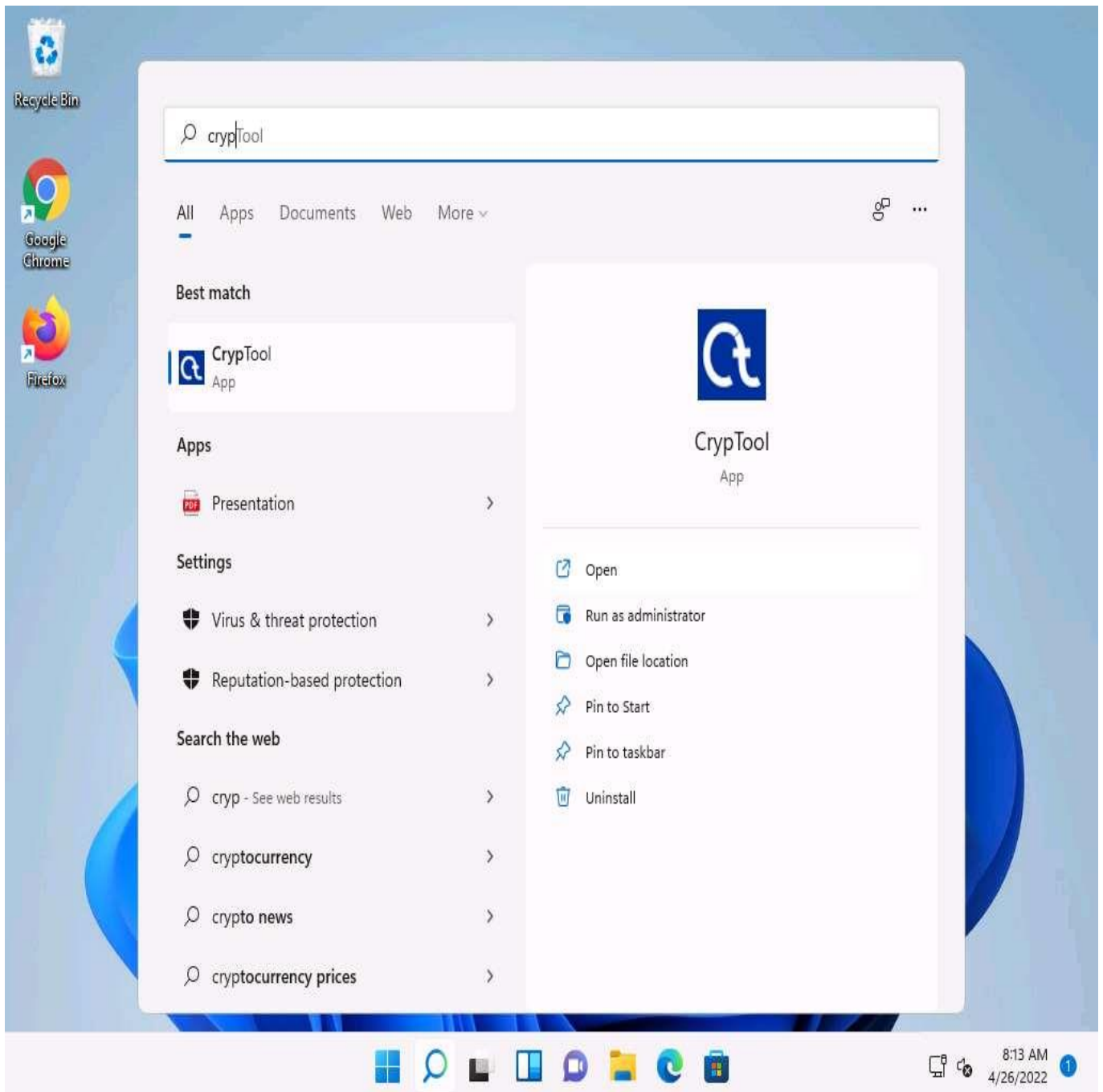
Task 1: Perform Cryptanalysis using CrypTool

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.

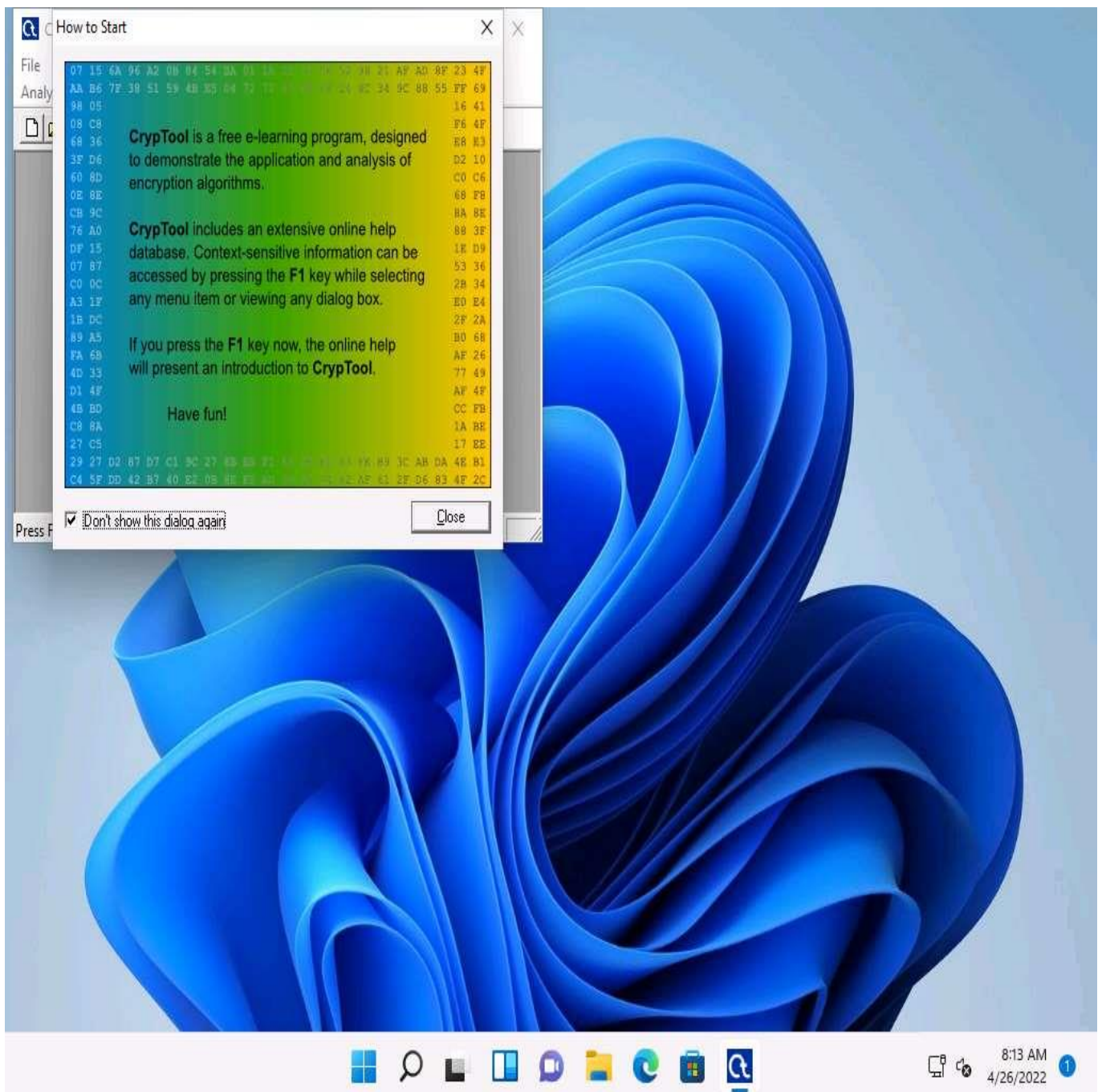
Here, we will use the CrypTool tool to perform cryptanalysis.

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

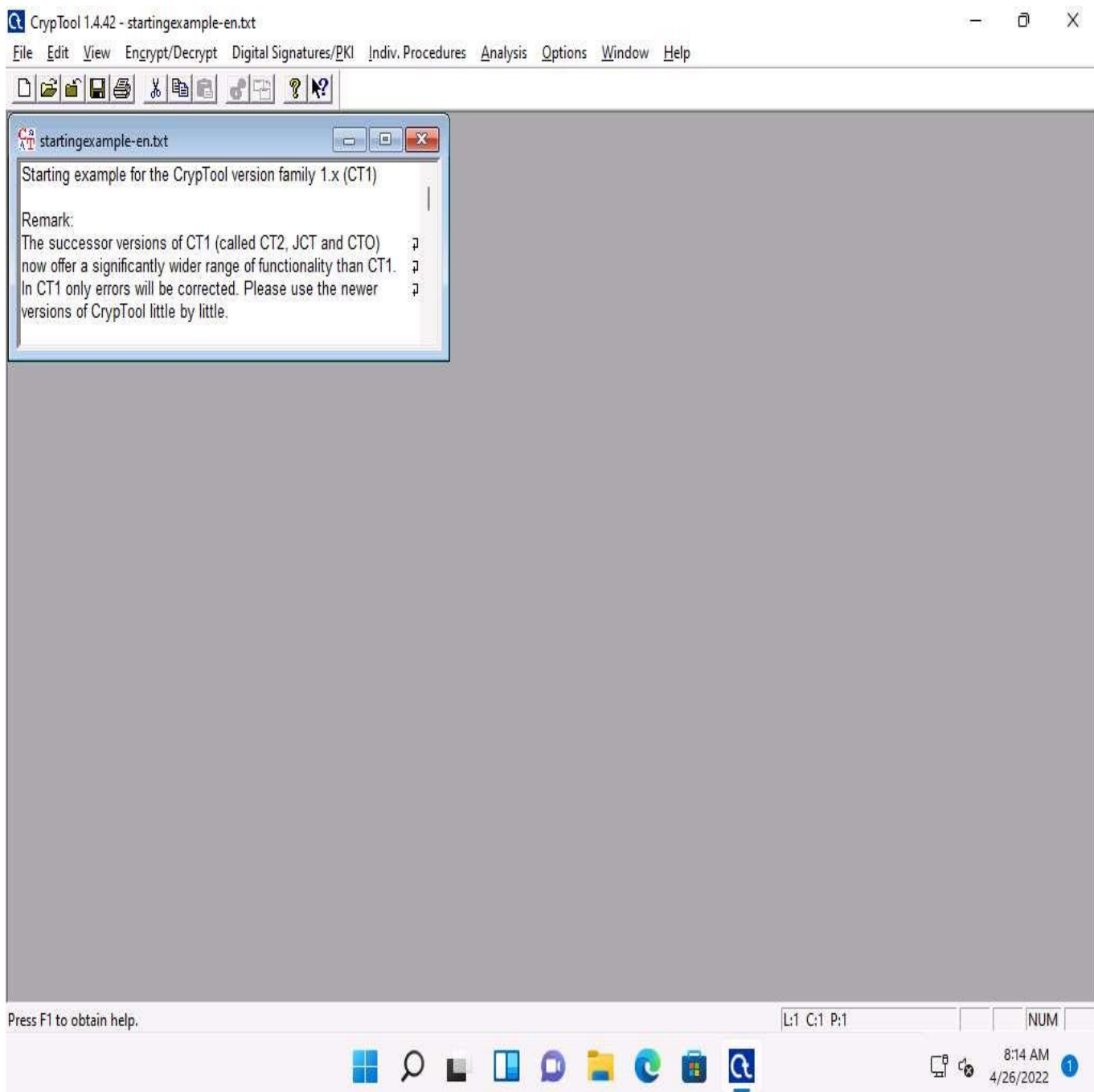
If a **User Account Control** pop-up appears, click **Yes**.



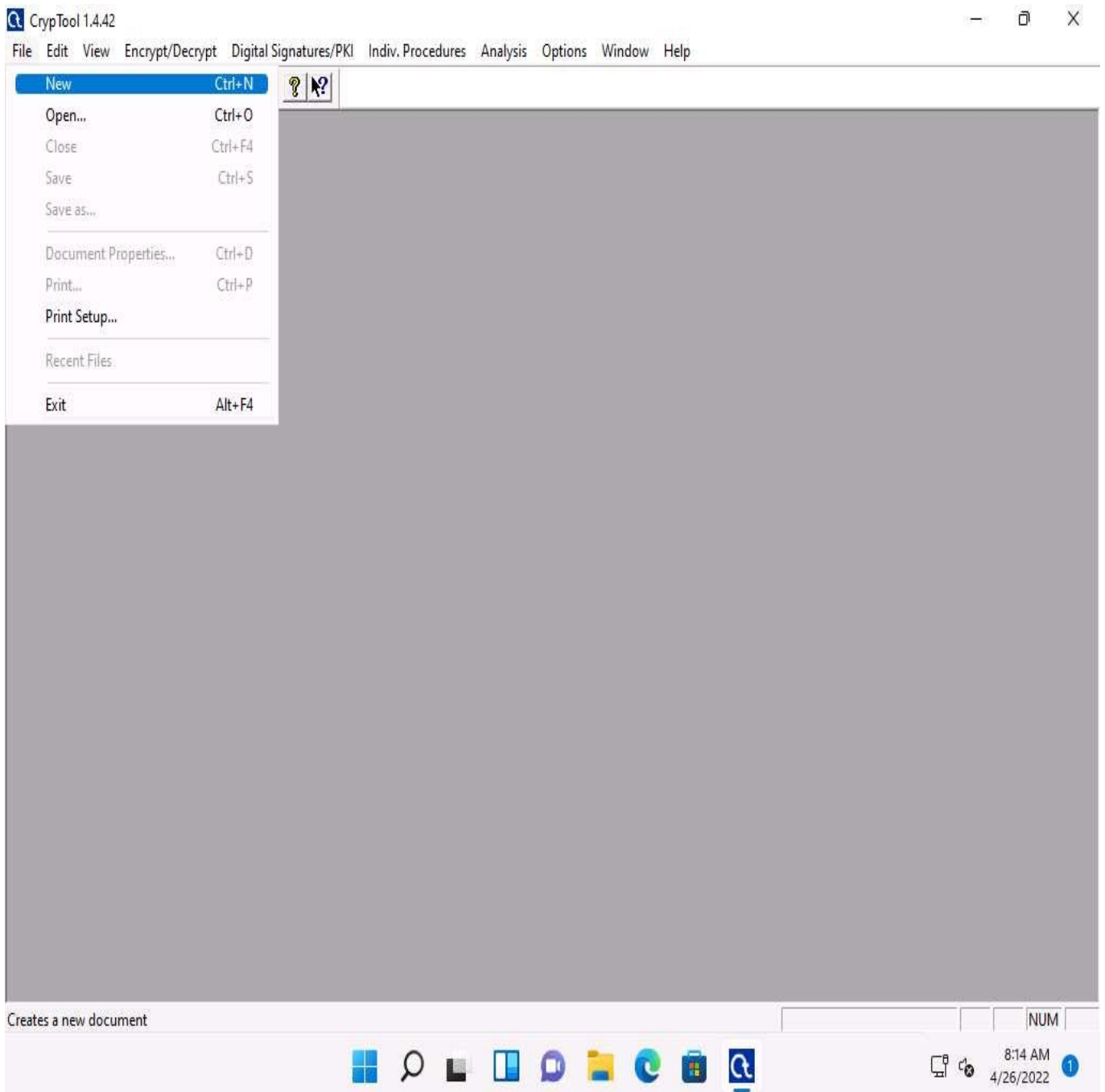
2. ☐ The **CrypTool** main window appears with a **How to Start** window. Check the **Don't show this dialog again** checkbox and click **Close**.



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

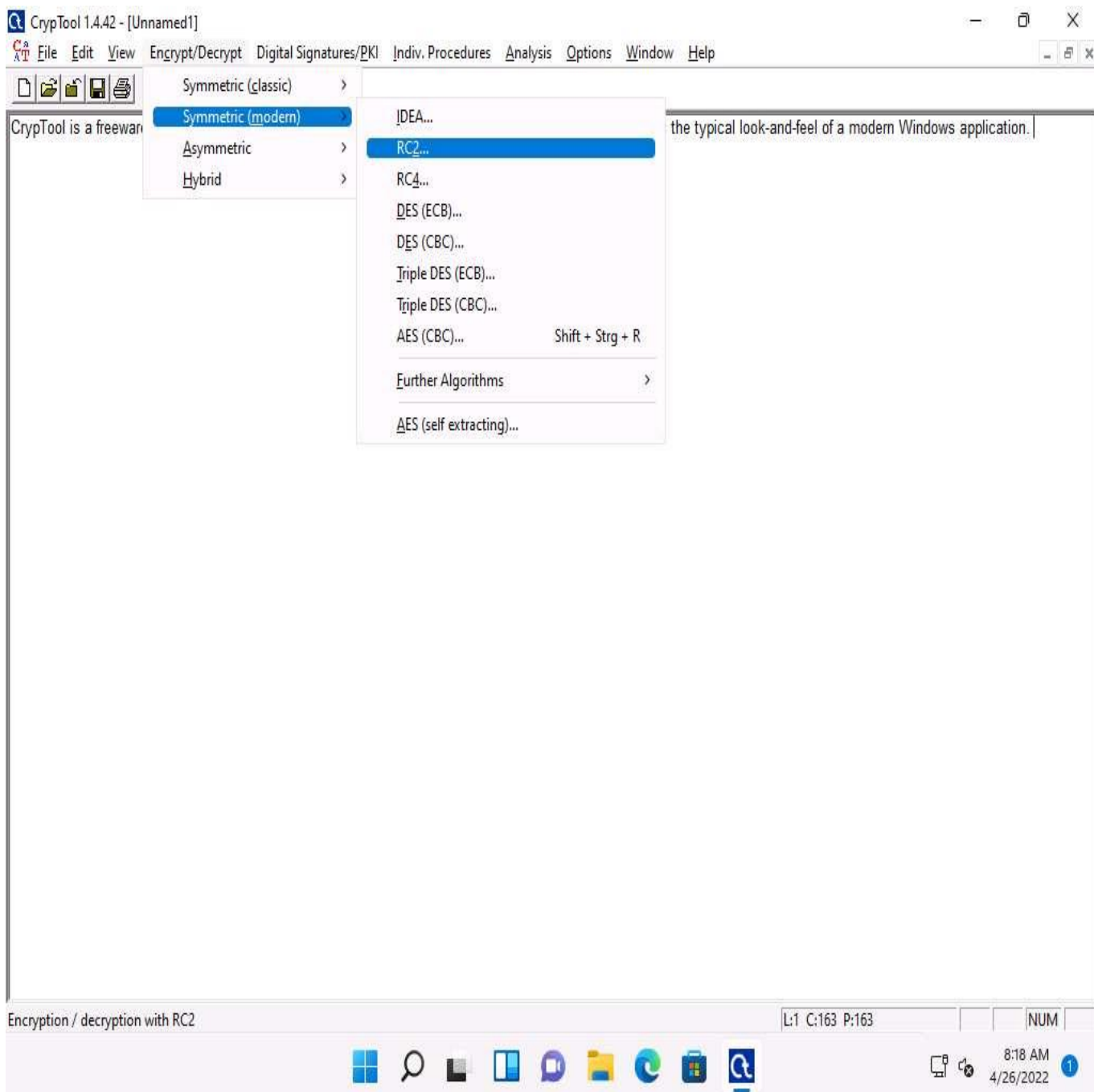


4. ☐ Click the **File** option from the menu bar and select **New** to create encrypted data.



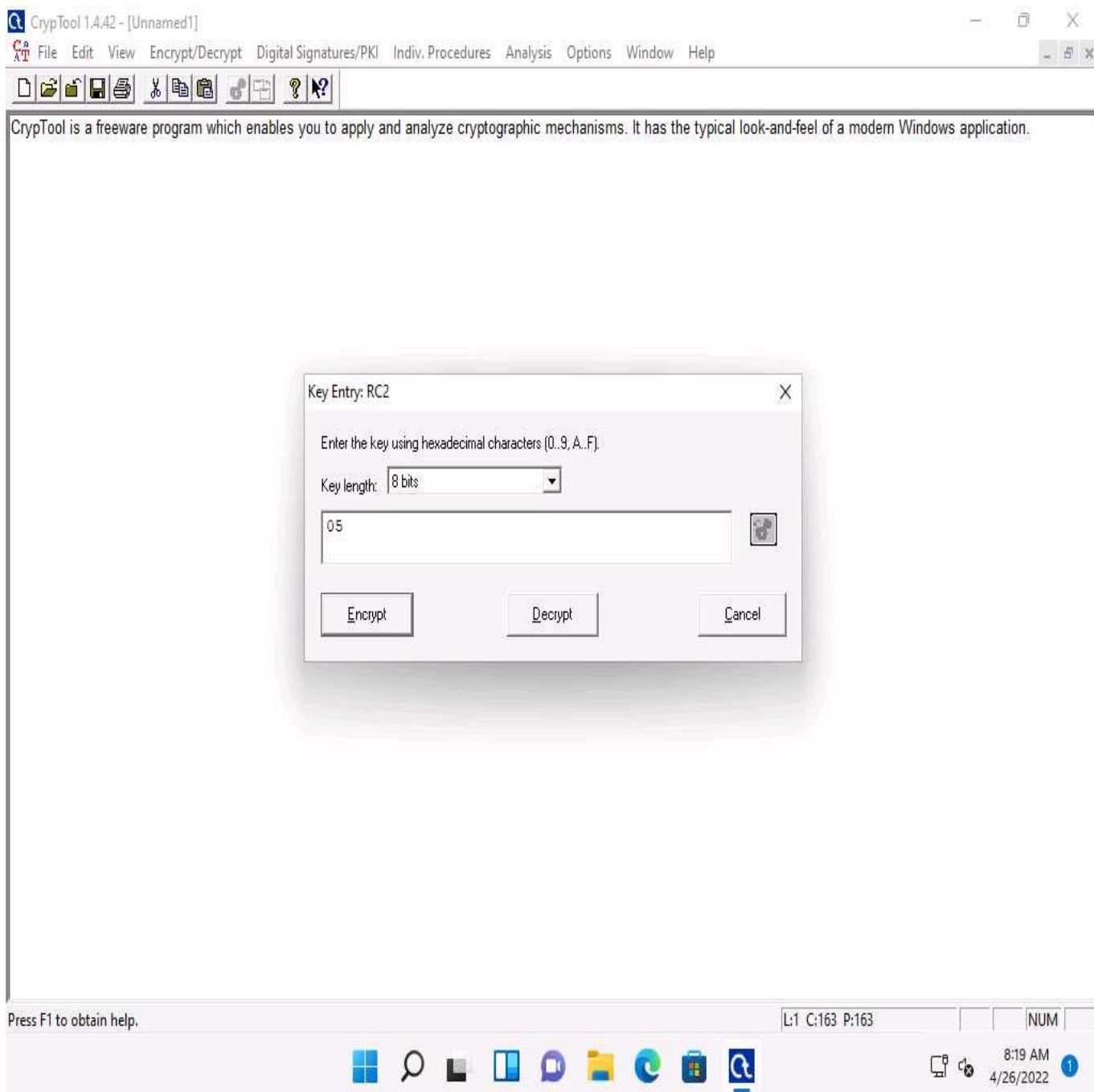
5. ☐ The **Unnamed1** notepad appears; insert some text into the file. You will be encrypting this content.
6. ☐ From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern)** --> **RC2....**

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

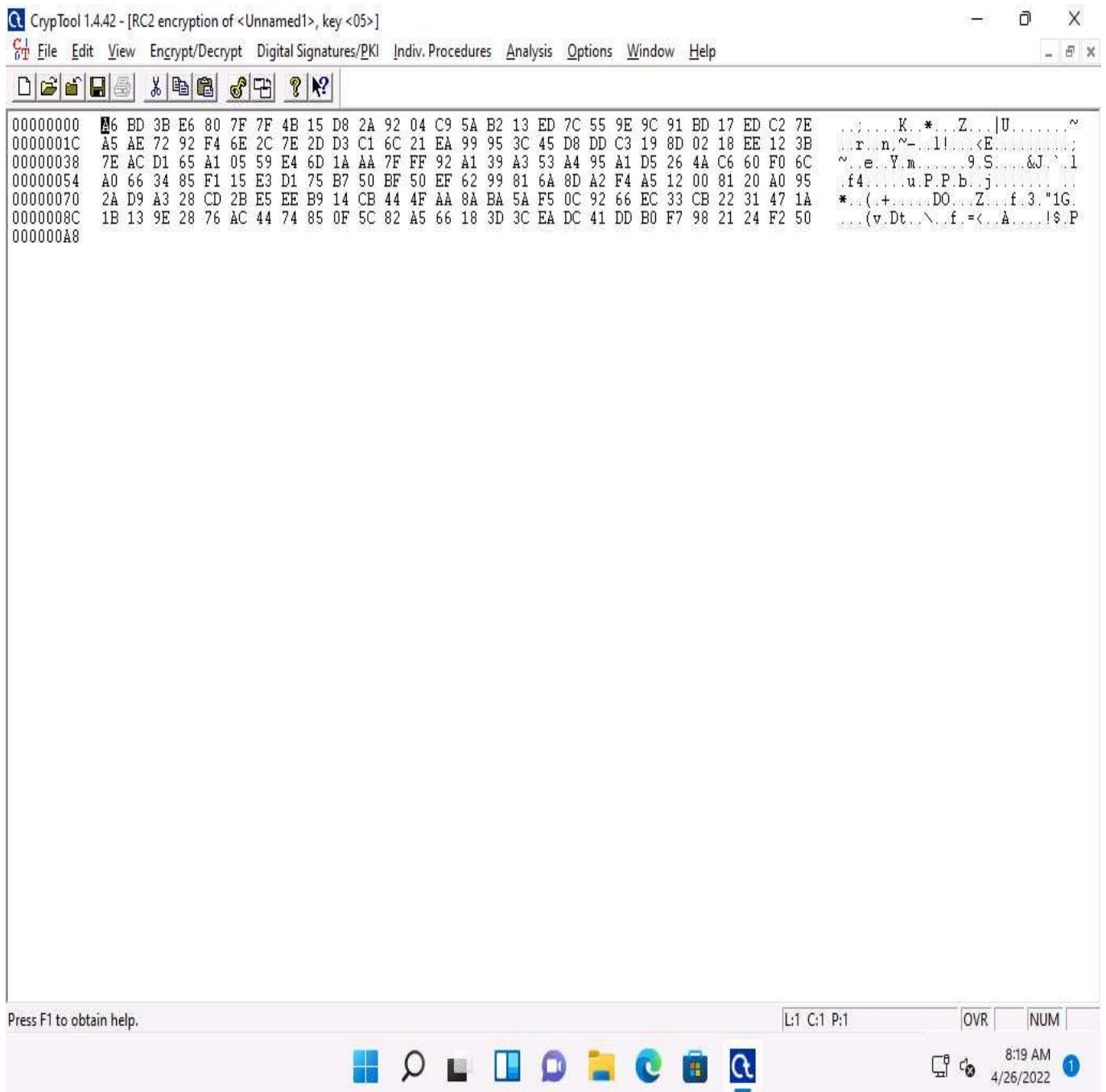


7. ☐ The **Key Entry: RC2** dialog box appears; keep the **Key length** set to default (**8 bits**).
8. ☐ In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Encrypt**.

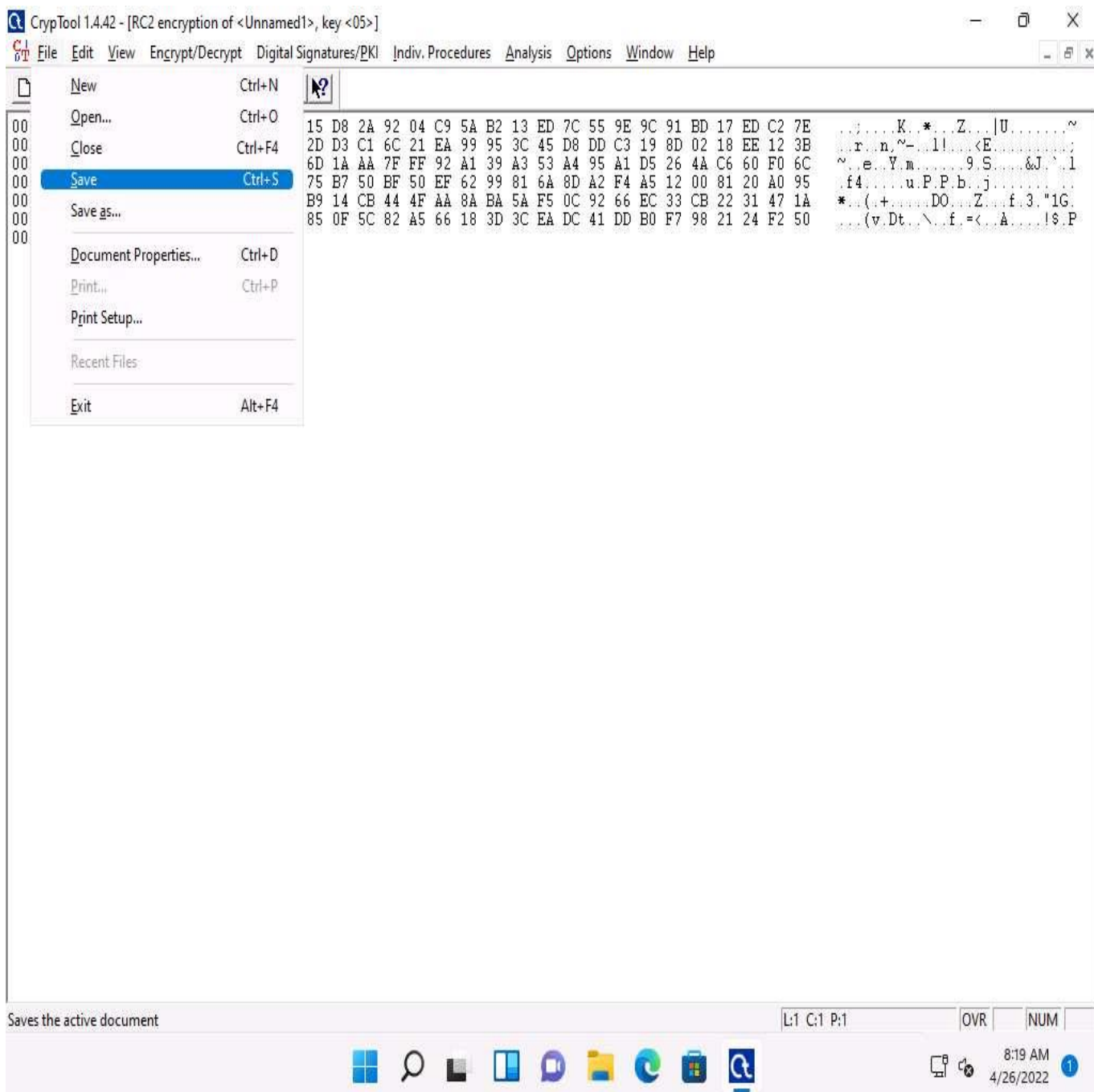
The chosen hexadecimal character acts as a key that you must send to the intended user along with the encrypted file.



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

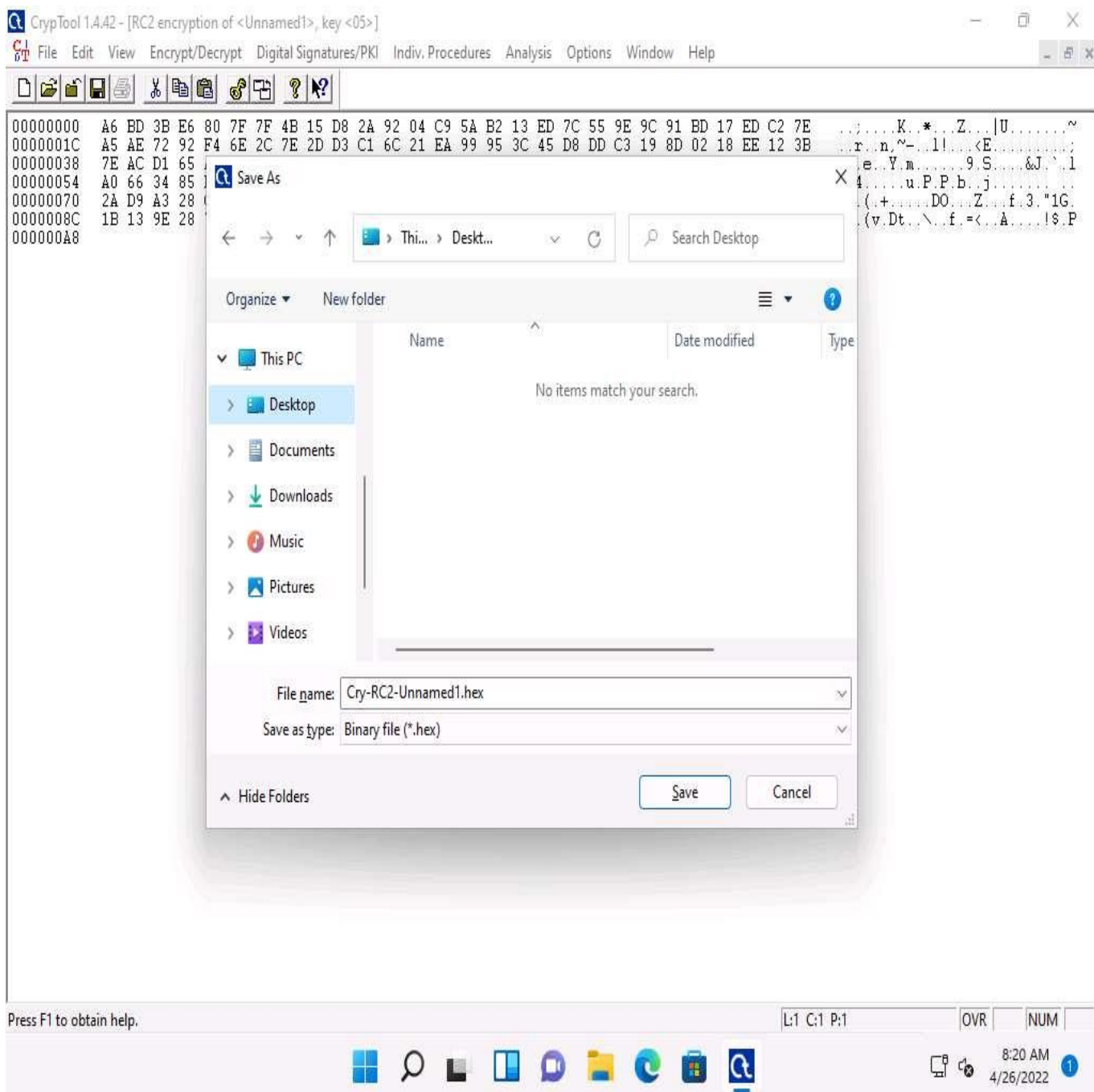


10. ☐ To save, click **File** in the menu bar and select **Save**.

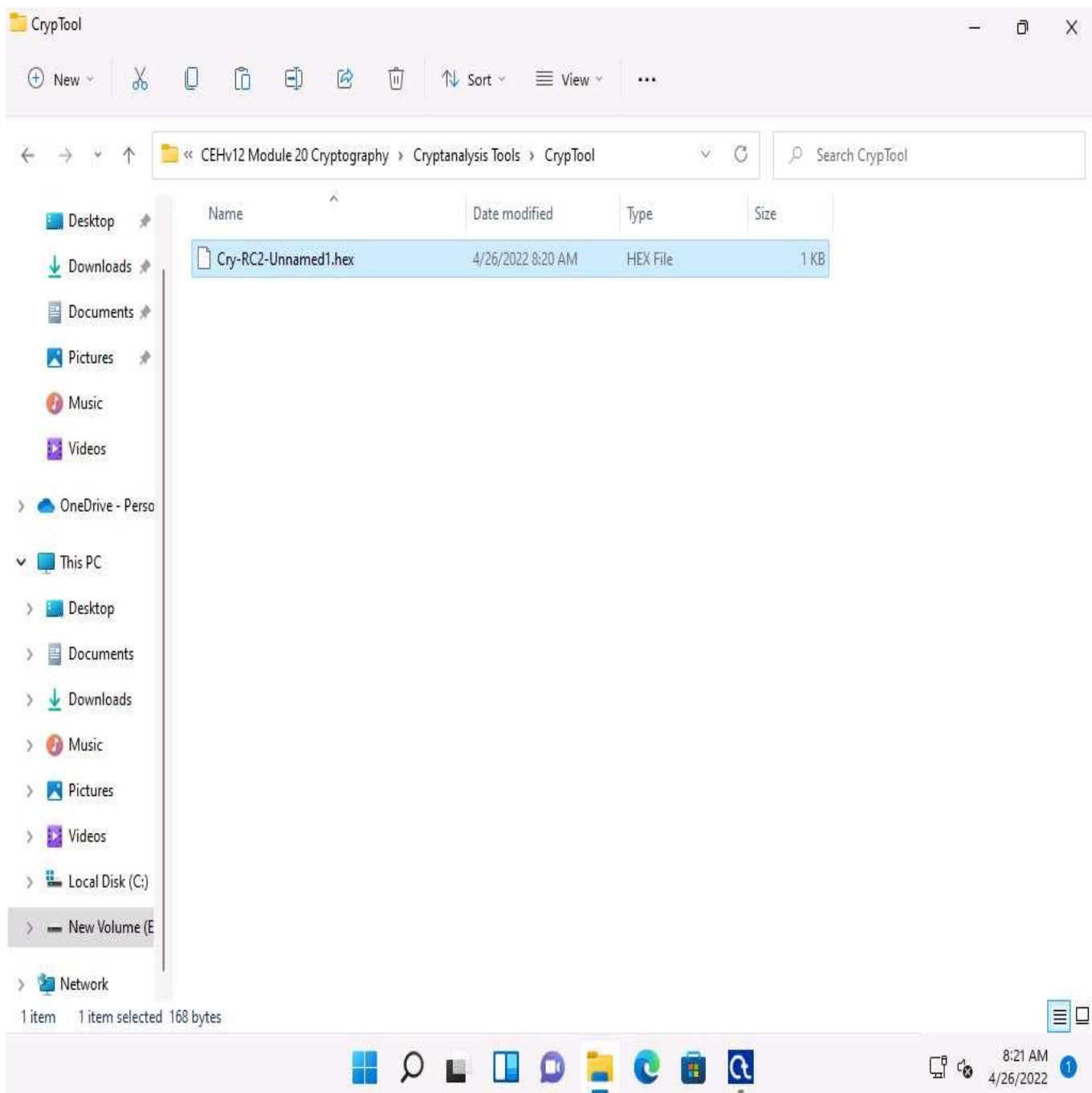


11. ☐ The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

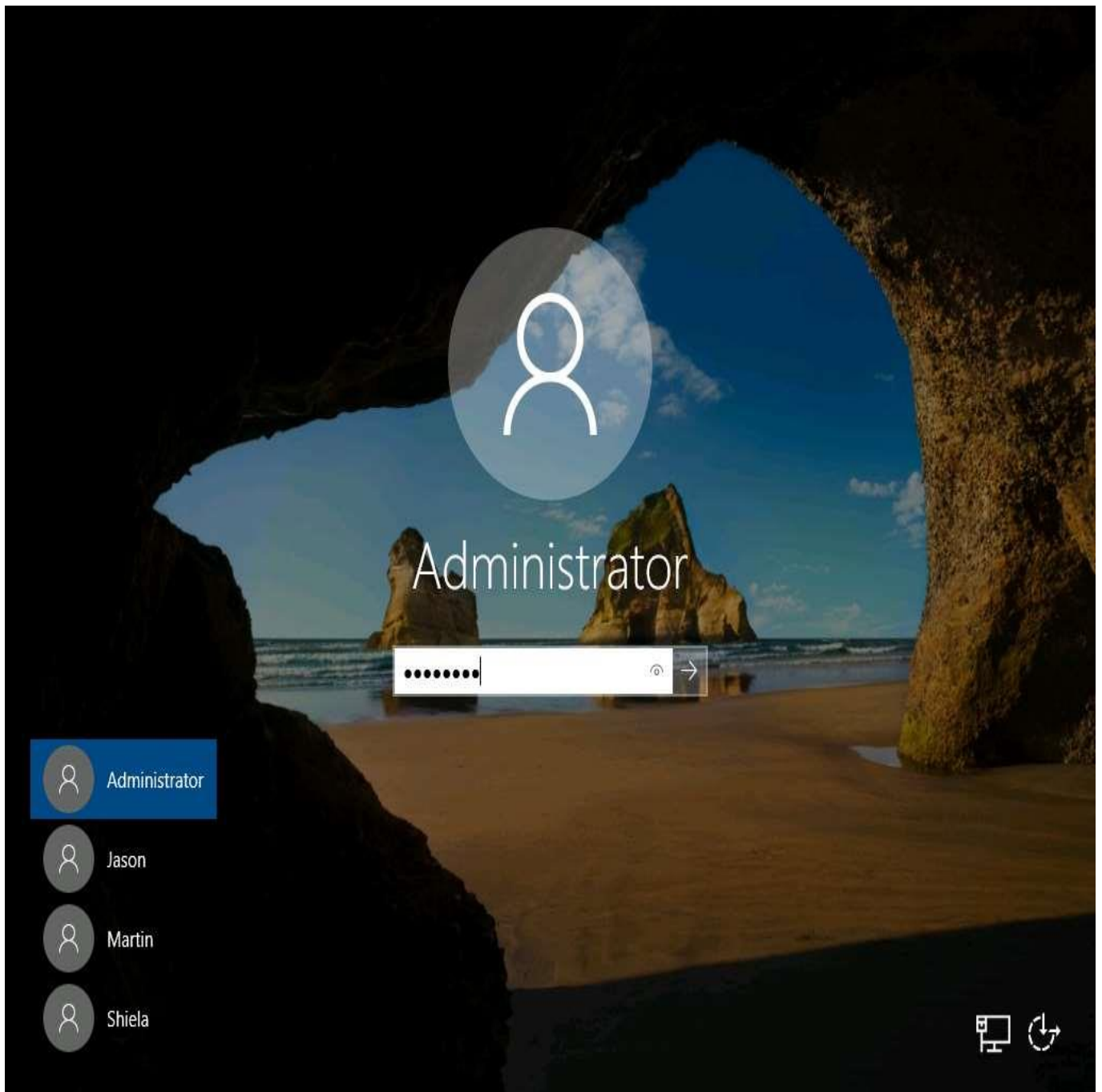
The file name may differ when you perform the task.



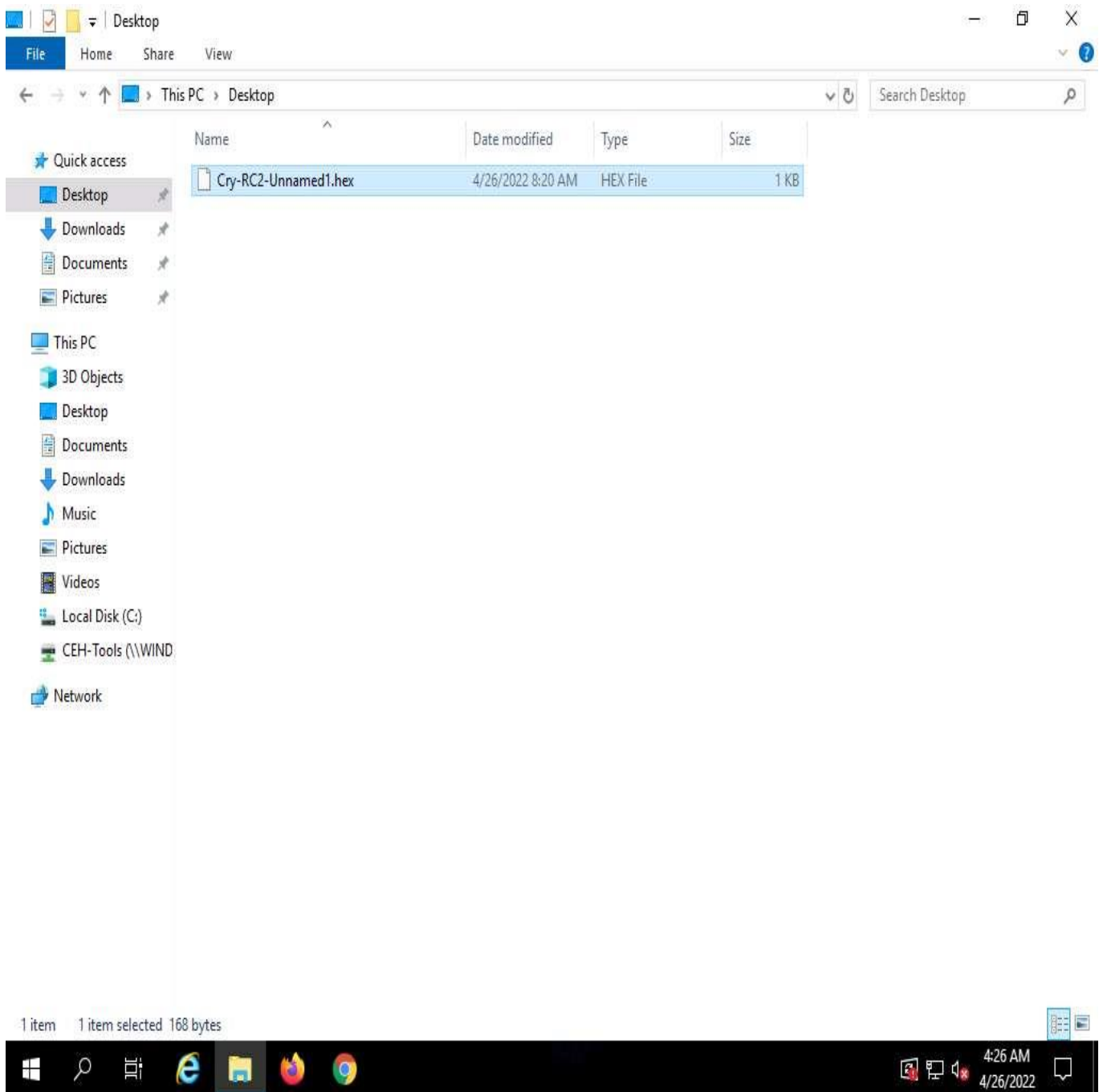
12. ☐ Now, you can send this file to the intended person by email or any other means and provide him/her with the hex value, which will be used to decrypt the file.
13. ☐ To share the file, you may copy the encrypted file (**Cry-RC2-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.



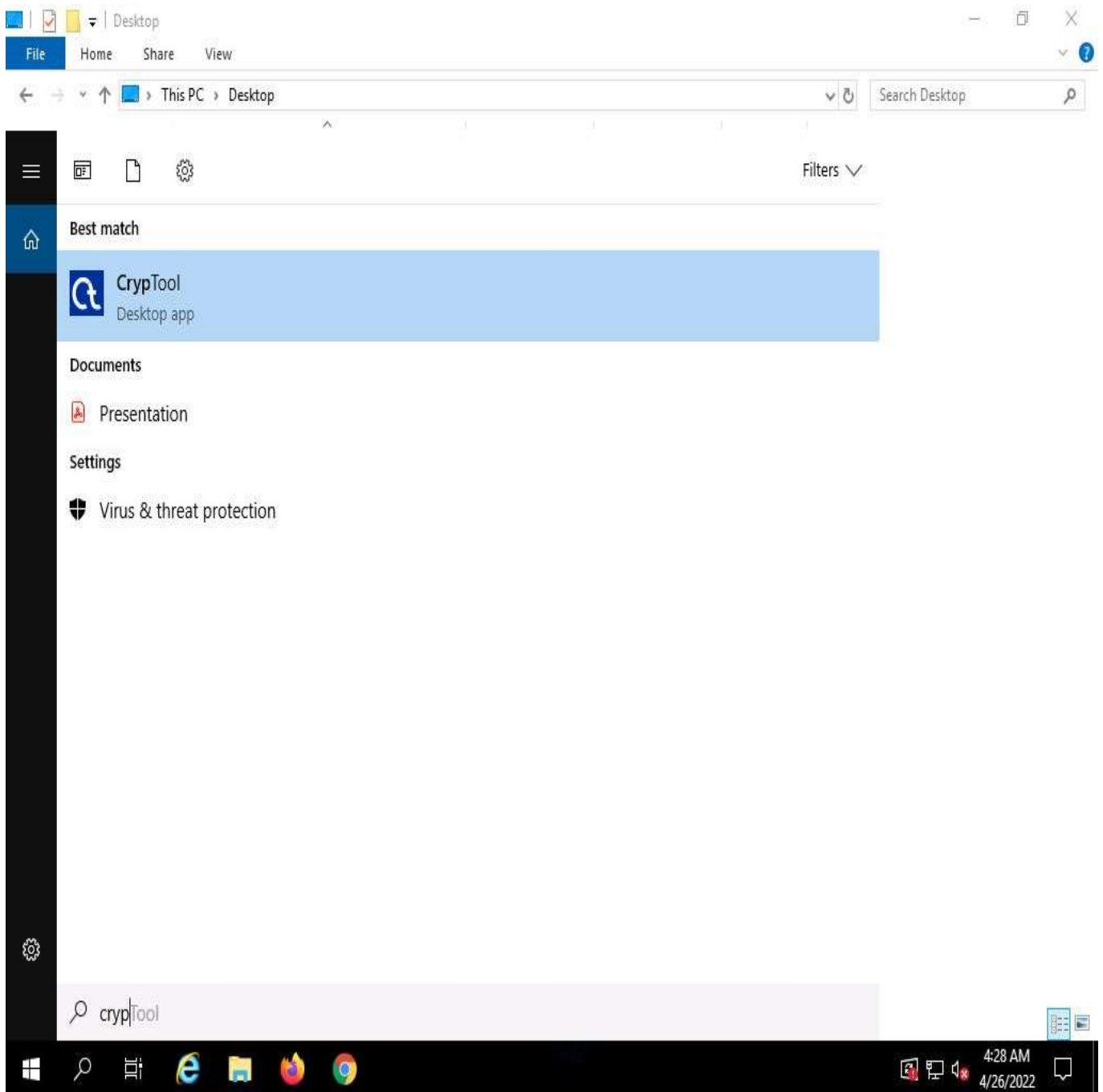
14. ☐ Assume that you are the intended recipient (working on Windows Server 2019) of the encrypted file through the shared network drive and the key to open the encrypted data was sent to you via an email. Using this, you can decrypt the encrypted data and see the data in plain-text.
15. ☐ Click on [Windows 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**.



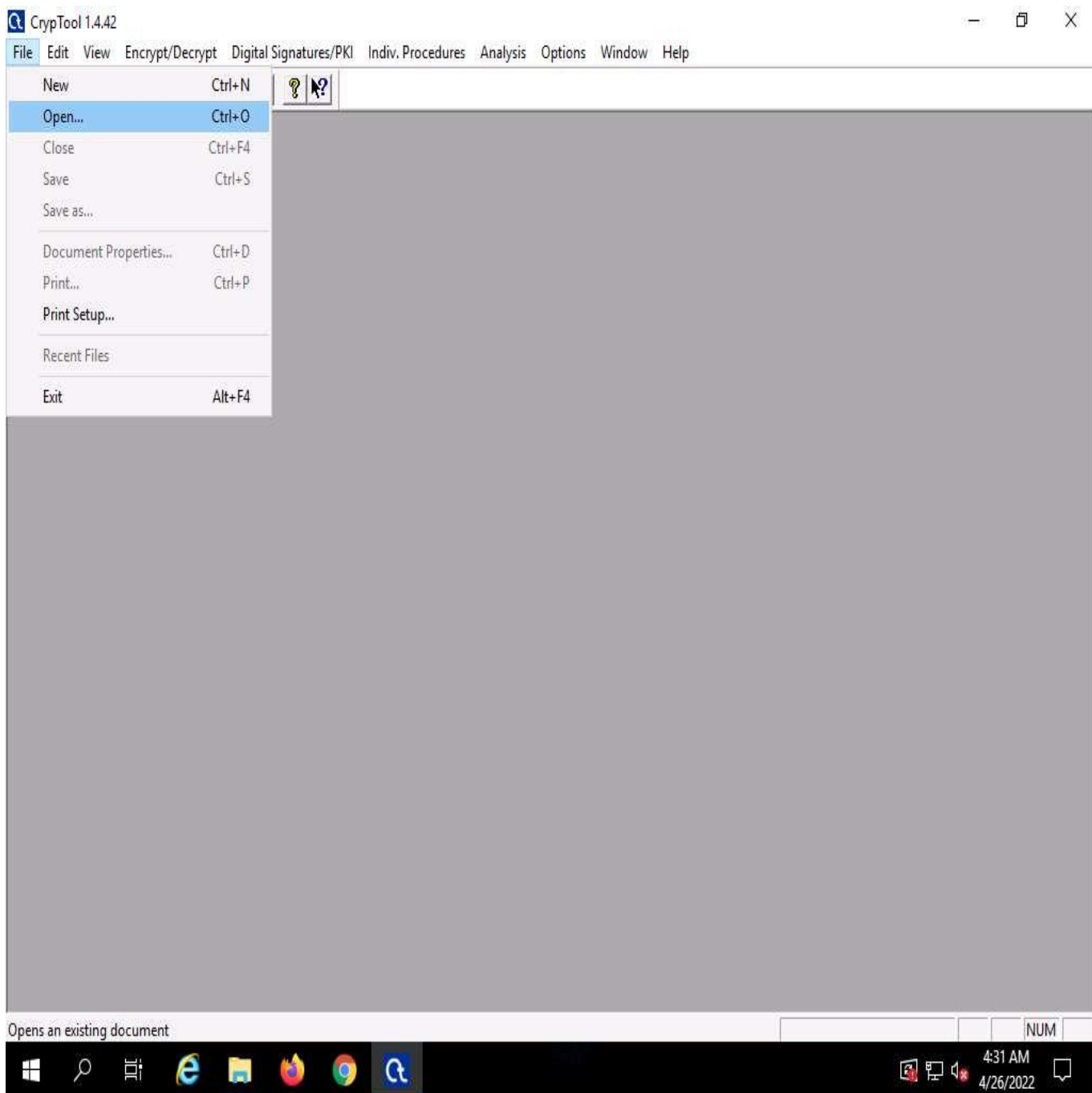
17. ☐ Click **Type here to search** icon on the Desktop. Type **cryp** in the search field, the **CrypTool** appears in the results, click on **CrypTool** to launch it.



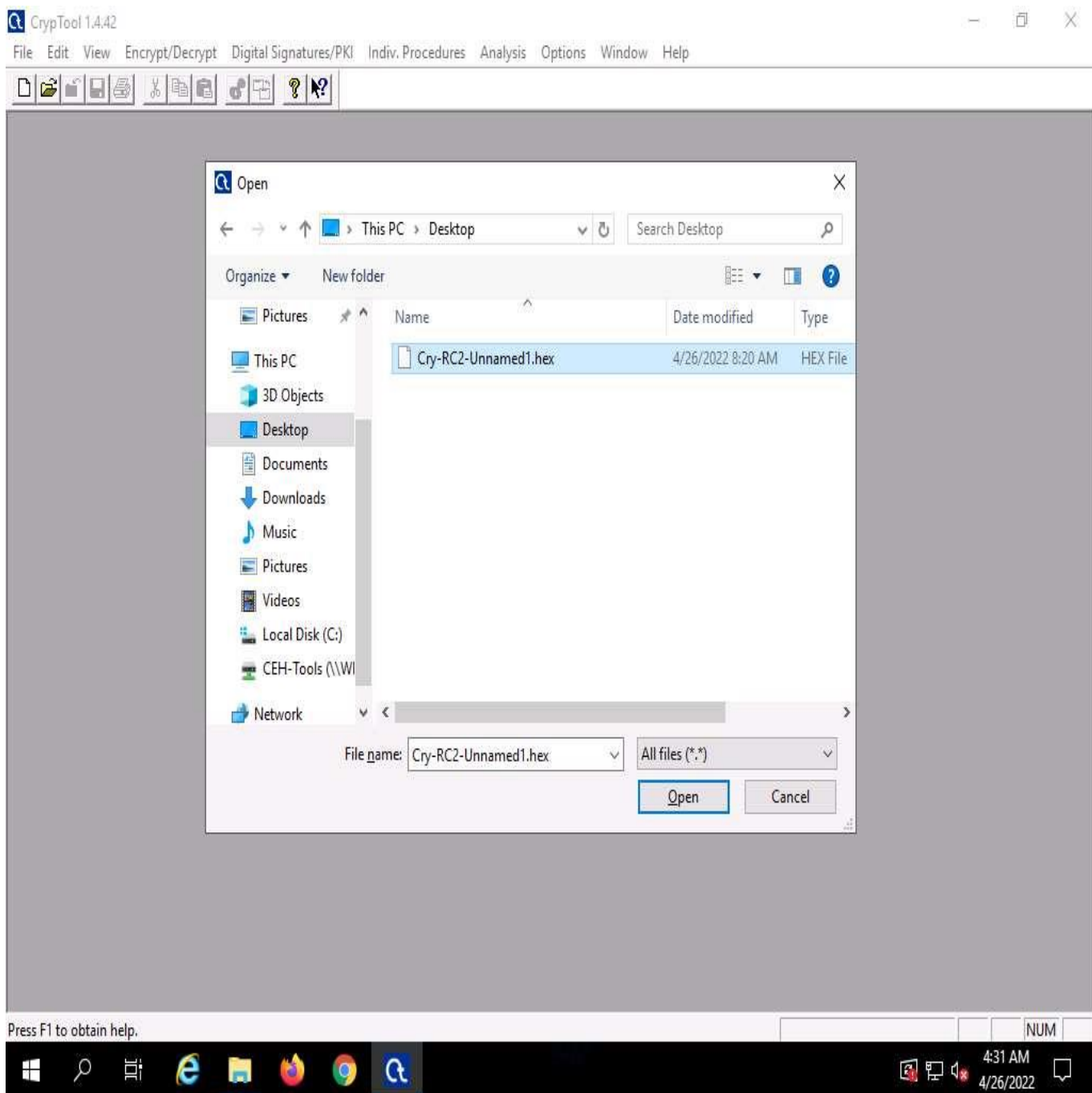
18. ☐ In the **CrypTool** window; click **File** in the menu bar and select **Open...**

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

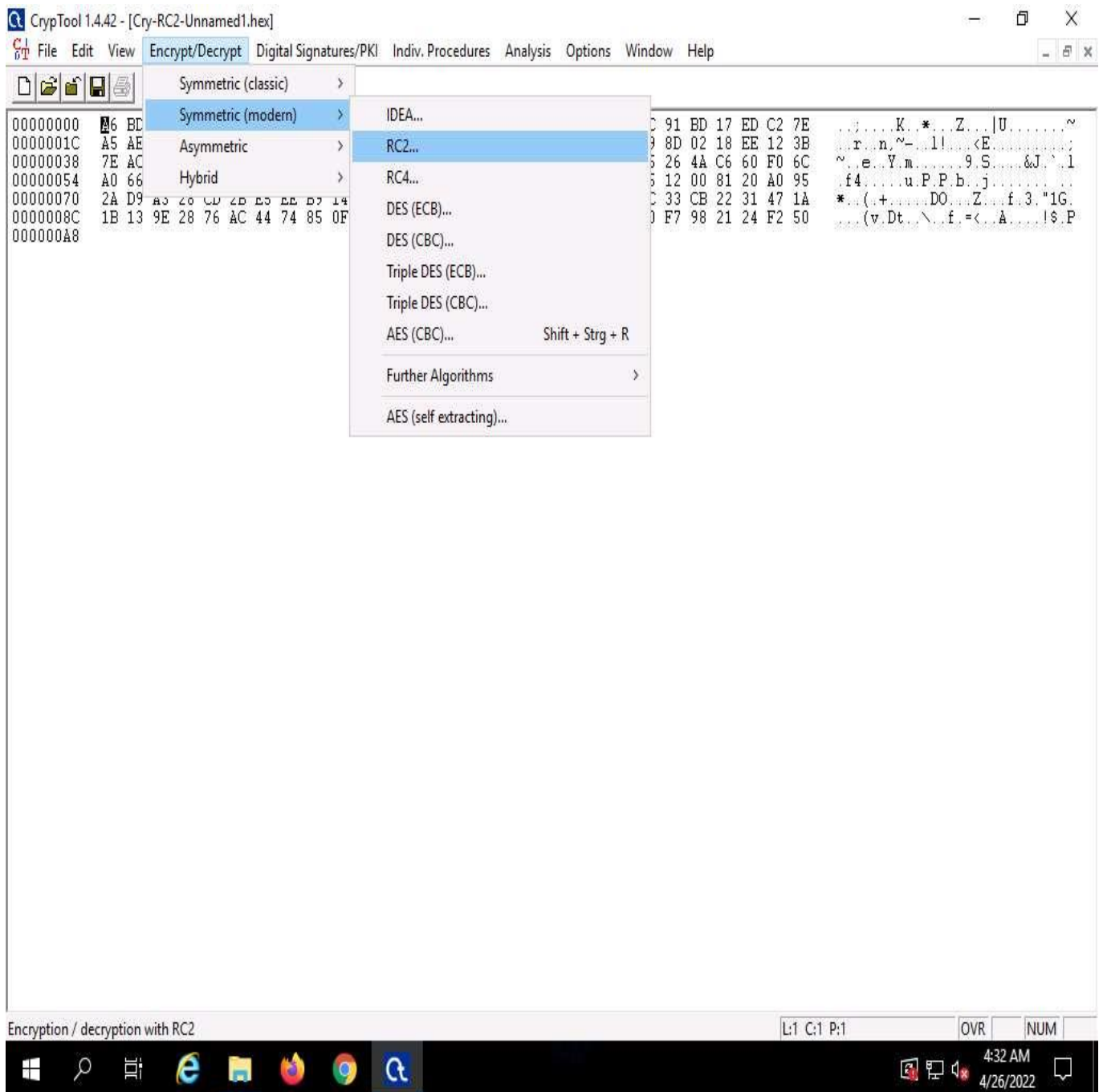
Close the **startingexample-en.txt** window.



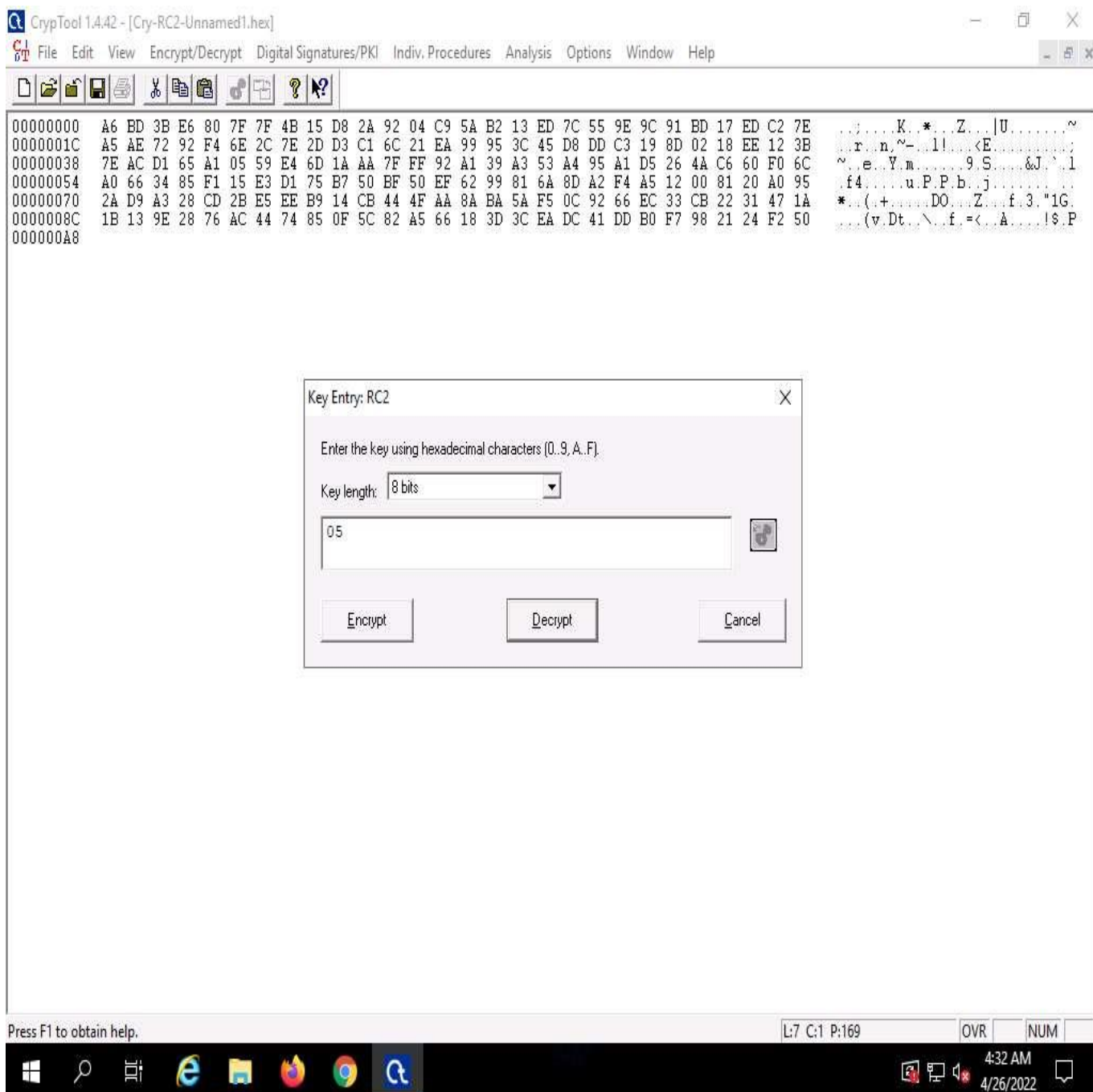
19. ☐ The **Open** window appears; select **All files(*.*)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and then click **Open**.



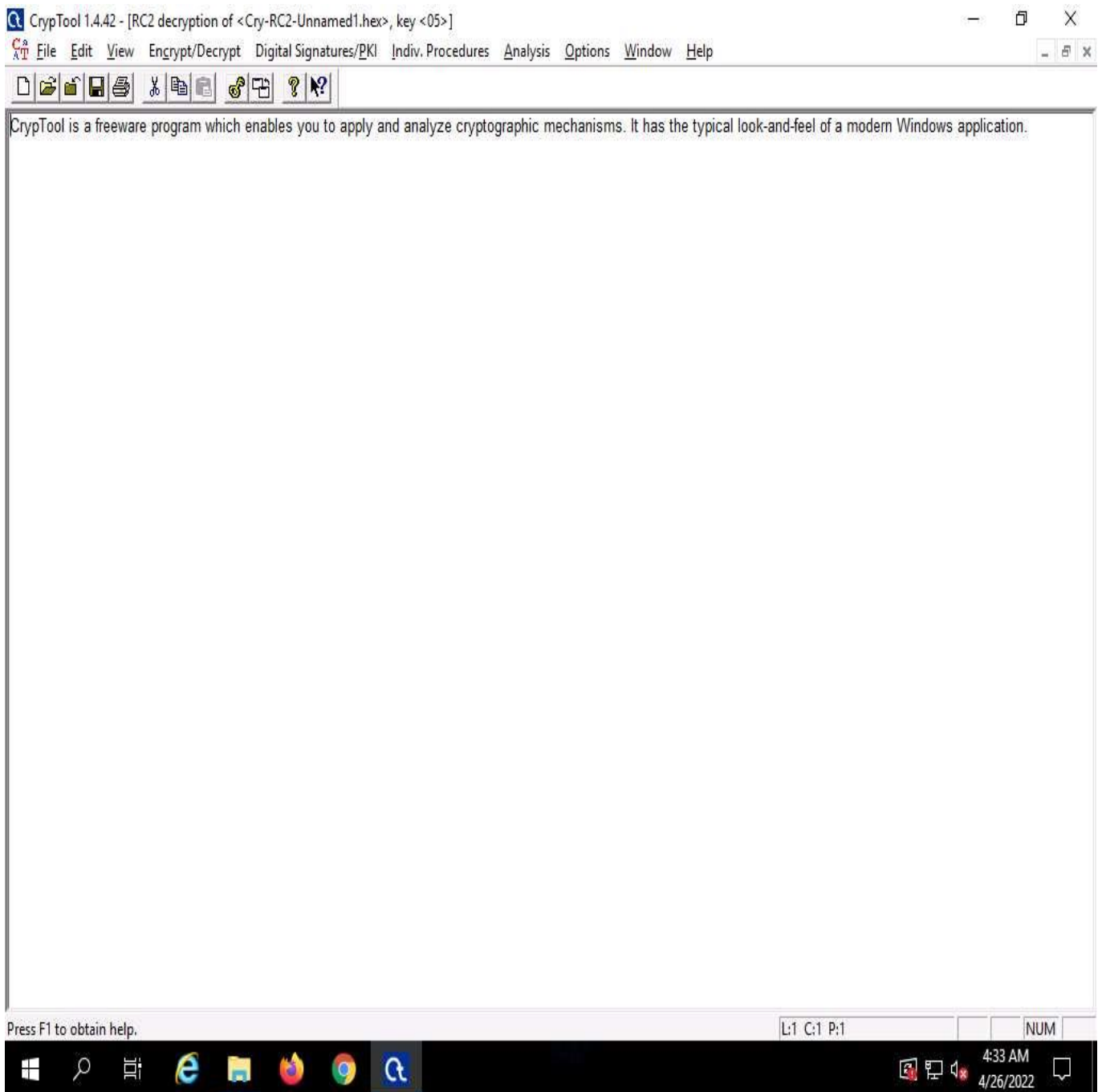
20. ☐ From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern)** --> **RC2...**



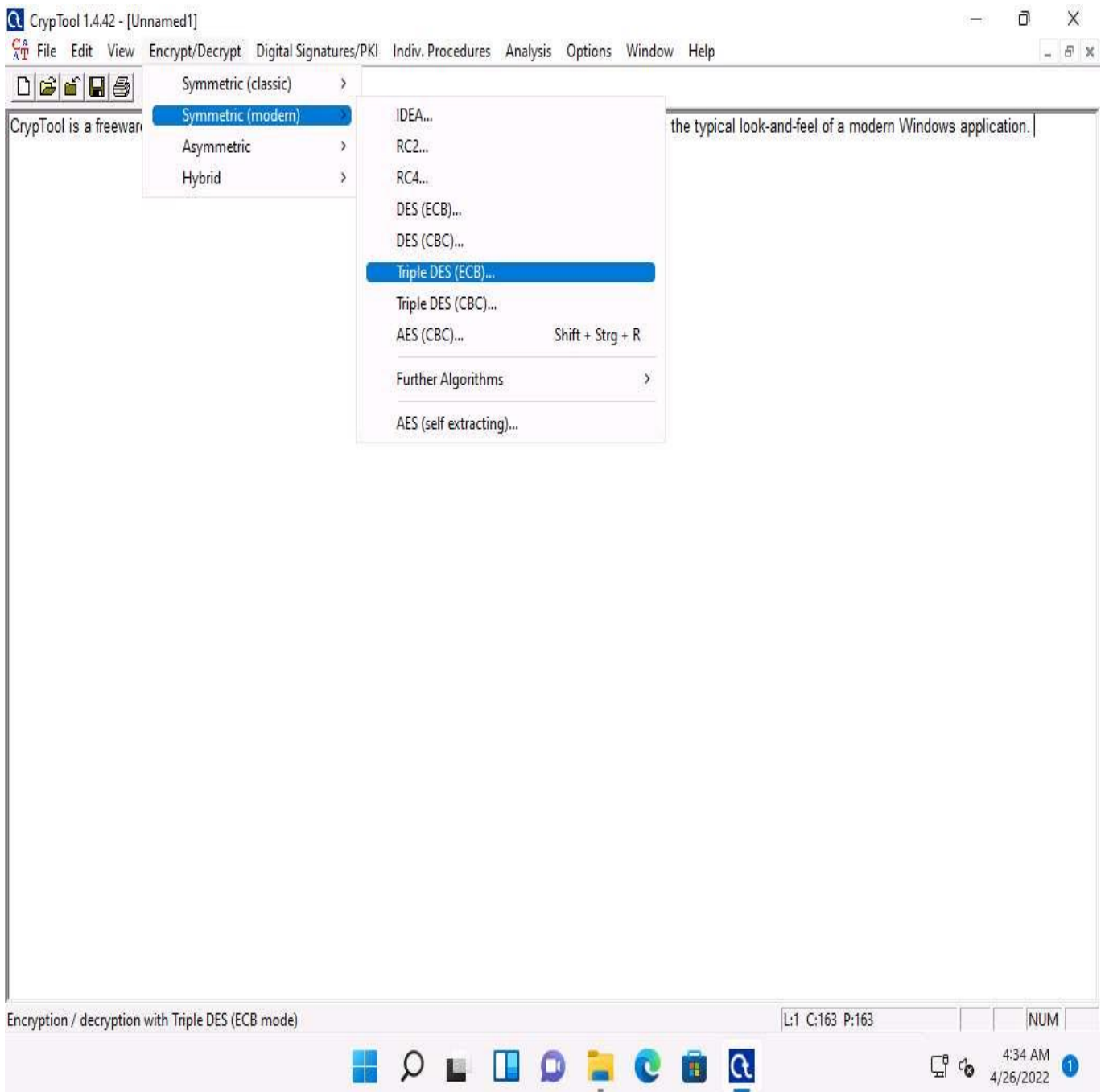
21. ☐ The **Key Entry: RC2** dialog box appears; leave the **Key length** set to default (**8 bits**).
22. ☐ In the text field below **Key length**, enter **05** as **hexadecimal characters**, and click **Decrypt**.



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

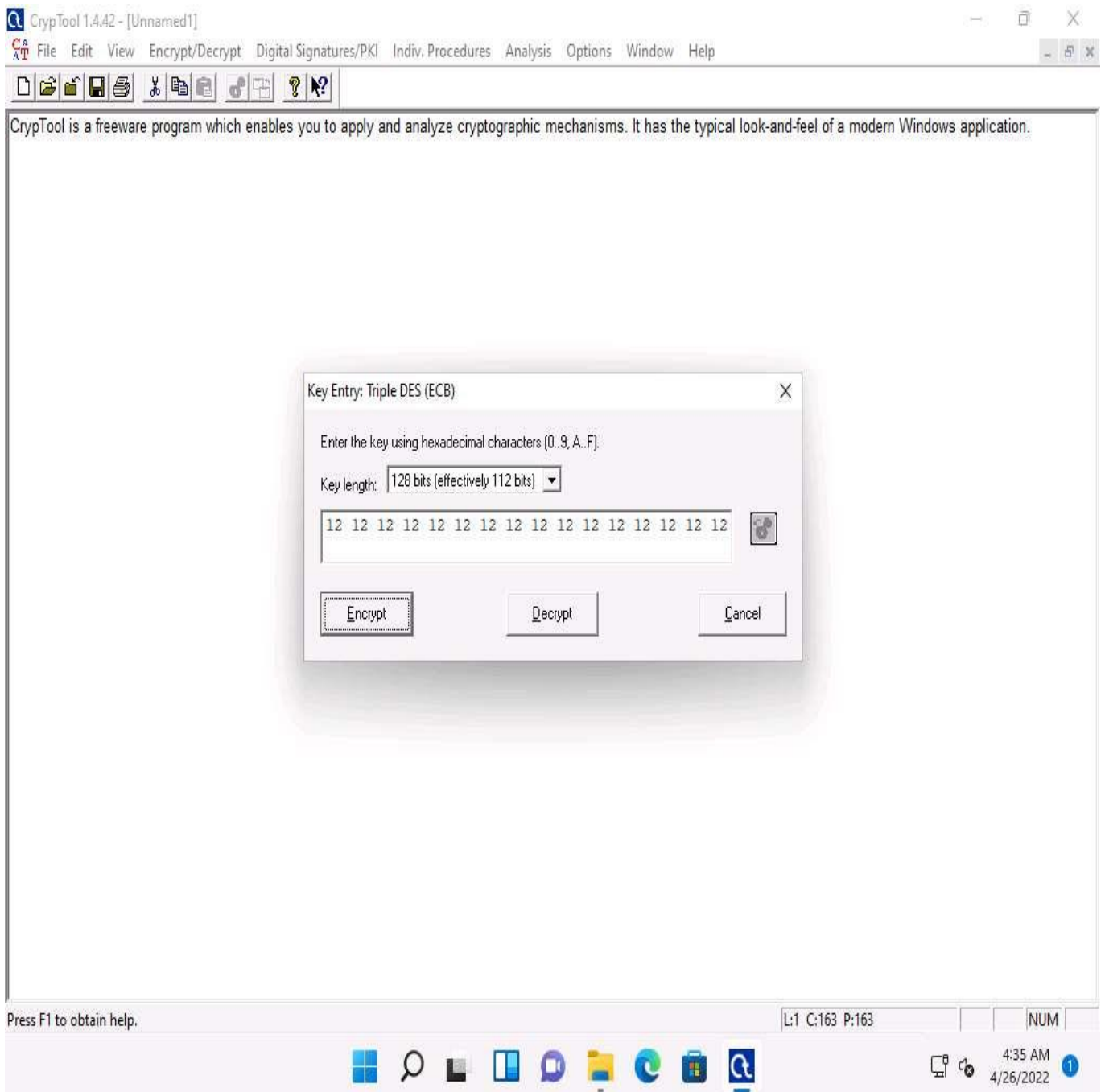


24. ☐ Now, we shall encrypt the data using Triple DES encryption.
25. ☐ Click [Windows 11](#) to switch back to the **Windows 11** machine.
26. ☐ In the **CrypTool** window, close **Cry-RC2-Unnamed1.hex** window. Leave the **Unnamed1** notepad window open.
27. ☐ From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern) --> Triple DES (ECB)...**

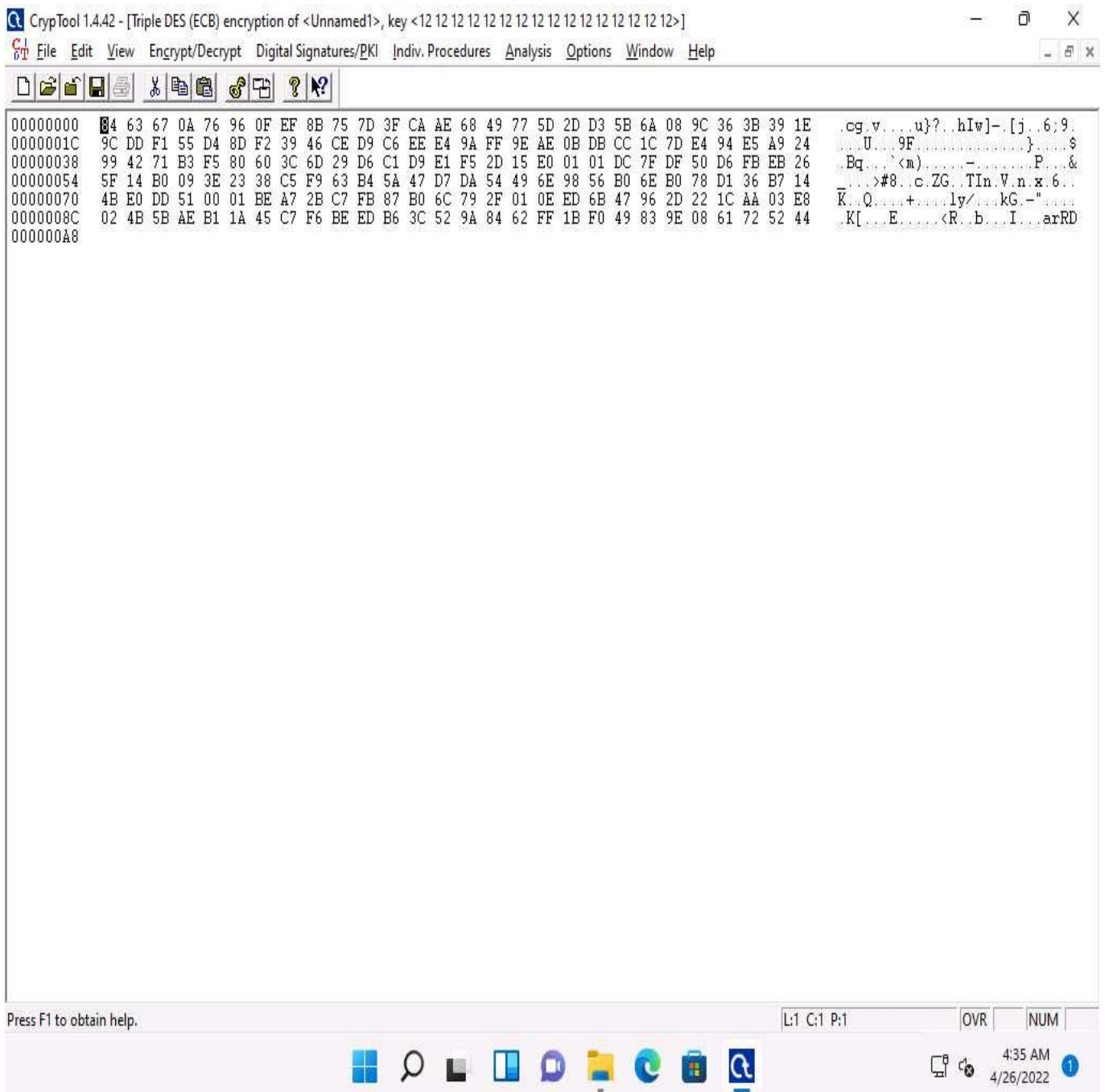


28. ☐ The **Key Entry: Triple DES (ECB)** dialog-box appears; leave the **Key length** set to default (**128 bits (effectively 112 bits)**).
29. ☐ In the text field below **Key length**, enter the combinations of **12** as **hexadecimal characters**, and click **Encrypt**.

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

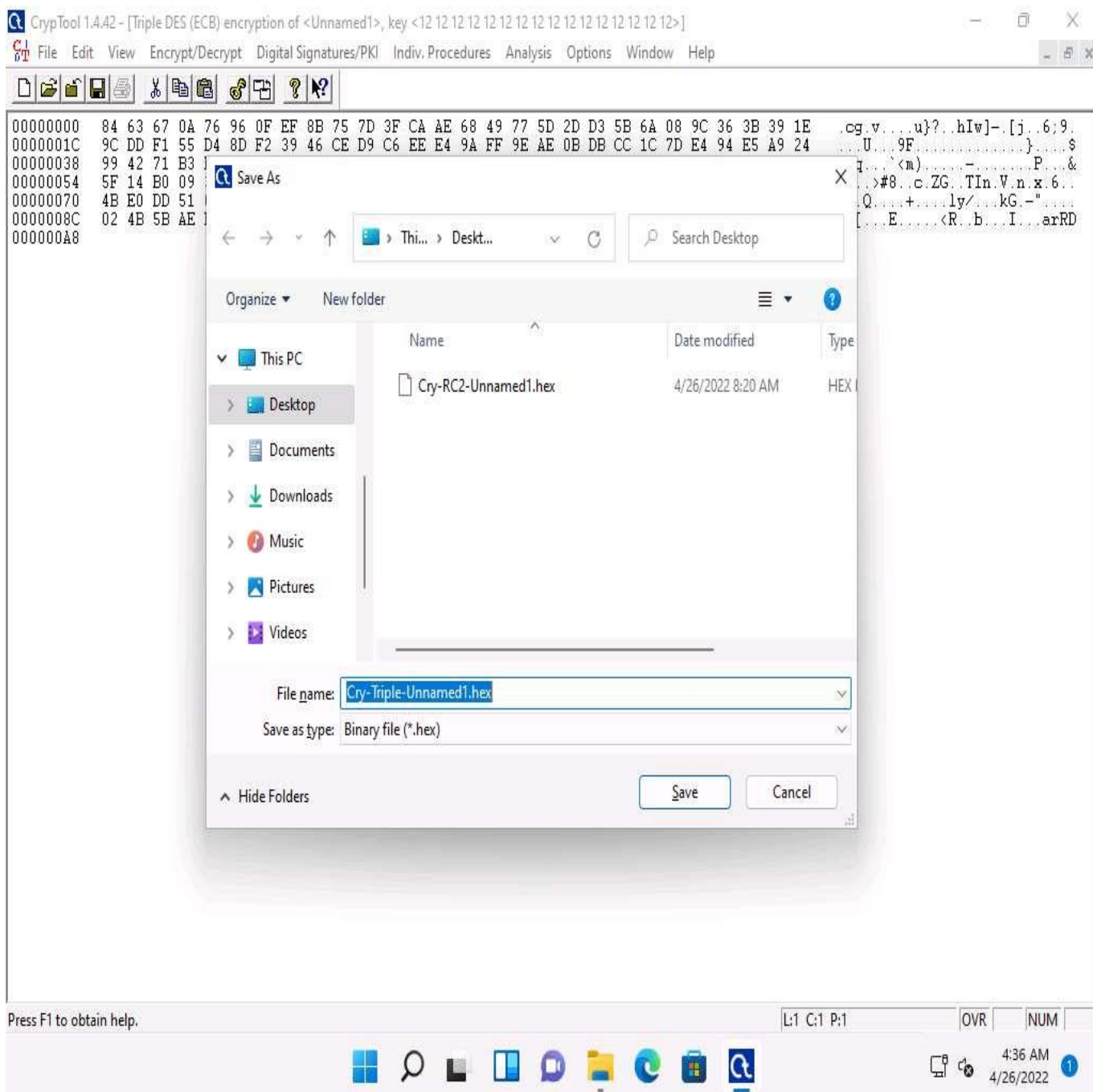


30. ☐ The **Triple DES (ECB) encryption of Unnamed1** notepad appears, as shown in the screenshot.

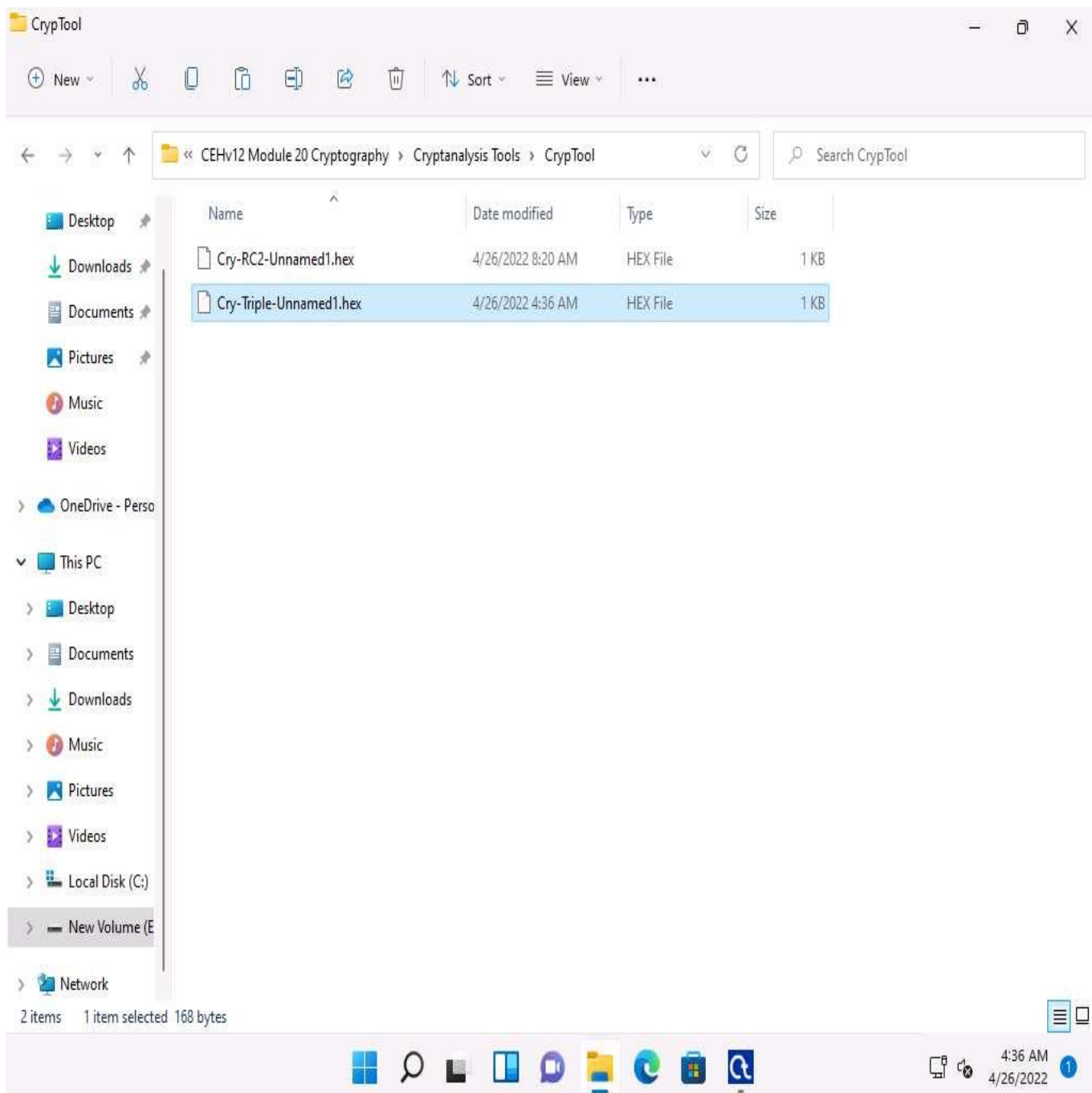


31. ☐ To save the file, click **File** in the menu bar and select **Save**.
32. ☐ The **Save As** window appears; choose the save location (here, **Desktop**) and click **Save**.

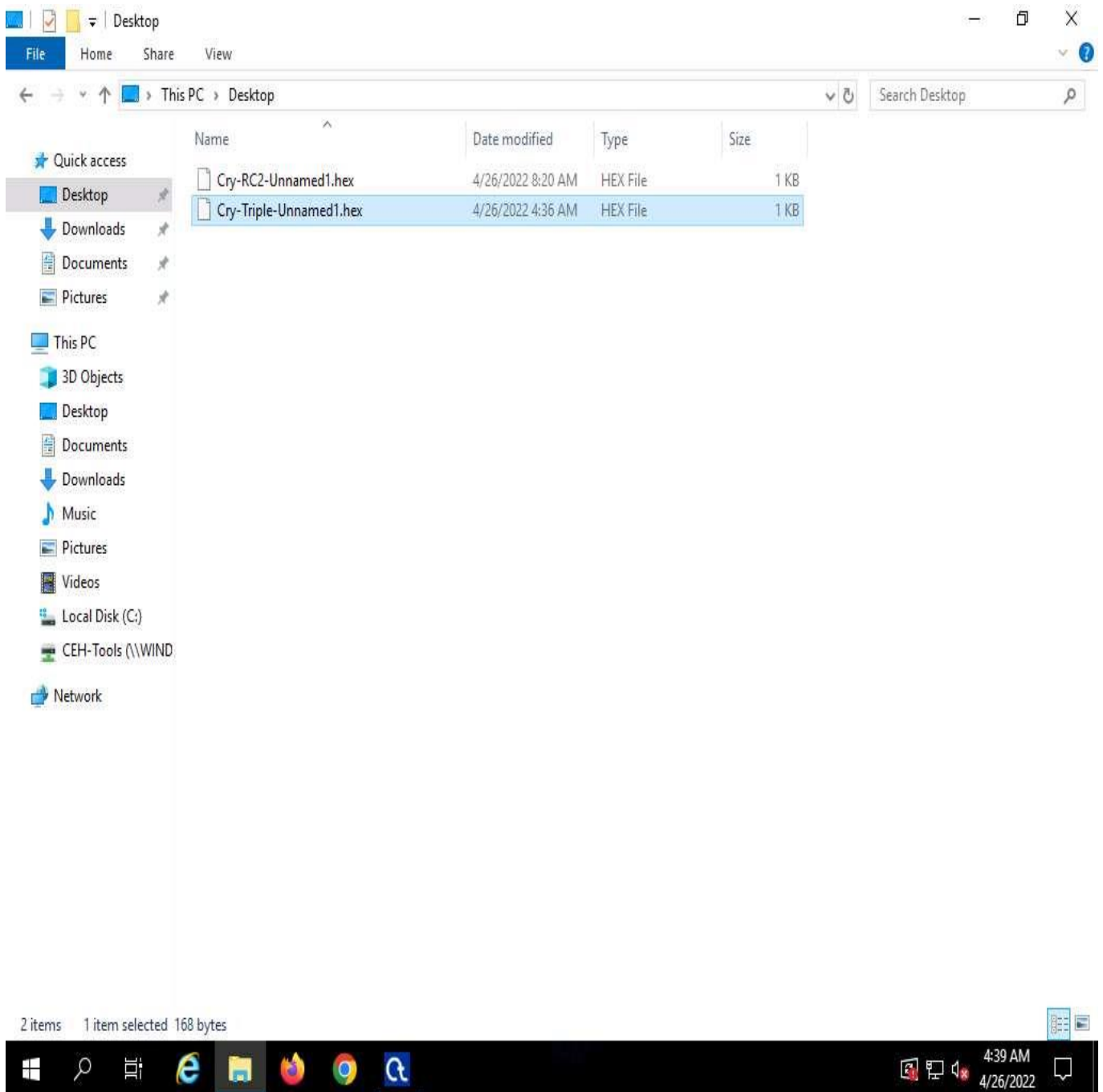
The file name may differ in your lab environment.



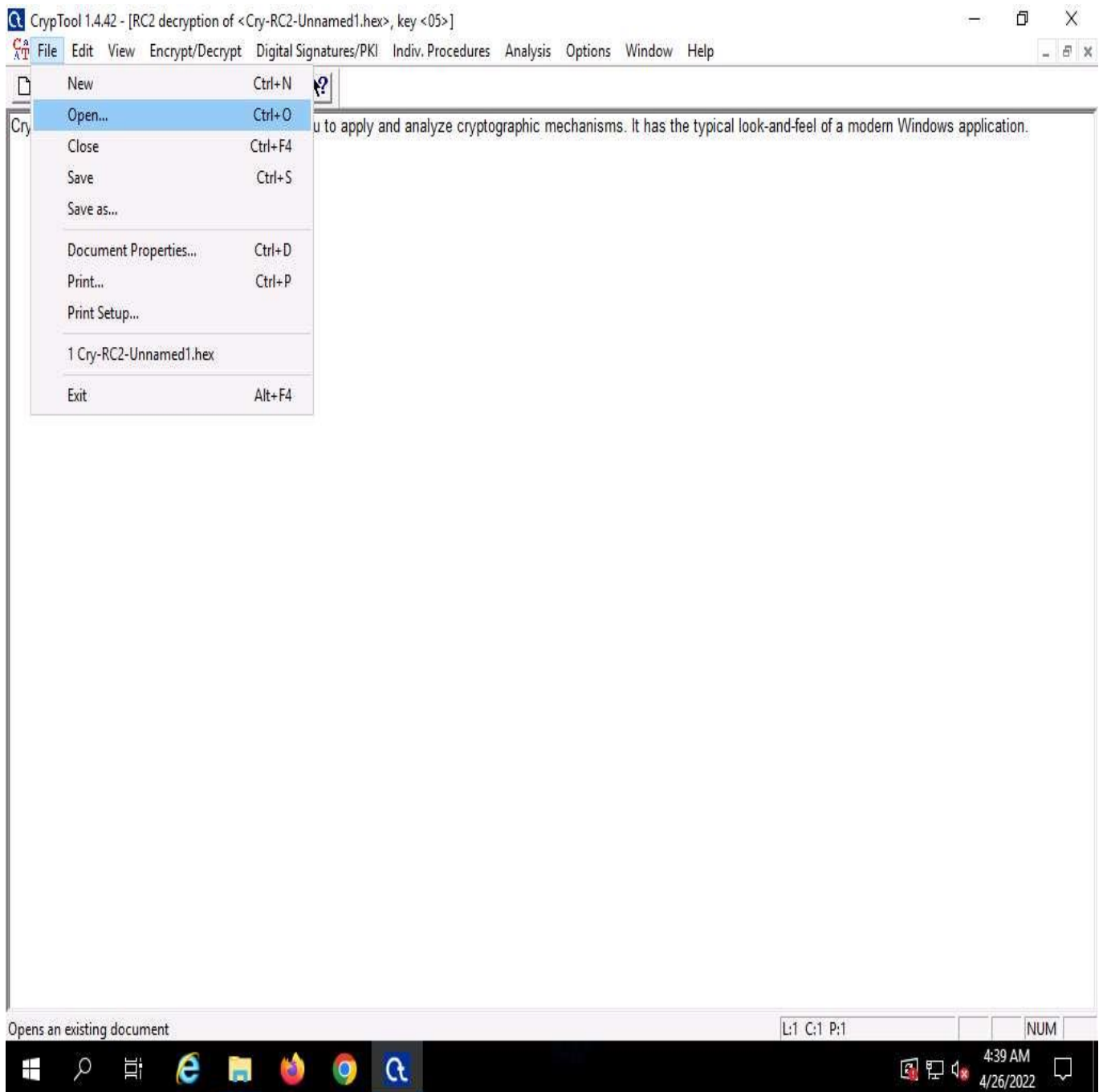
33. ☐ To share the file, you may copy the encrypted file (**Cry-Triple-Unnamed1.hex**) from **Desktop** to **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\CrypTool**.



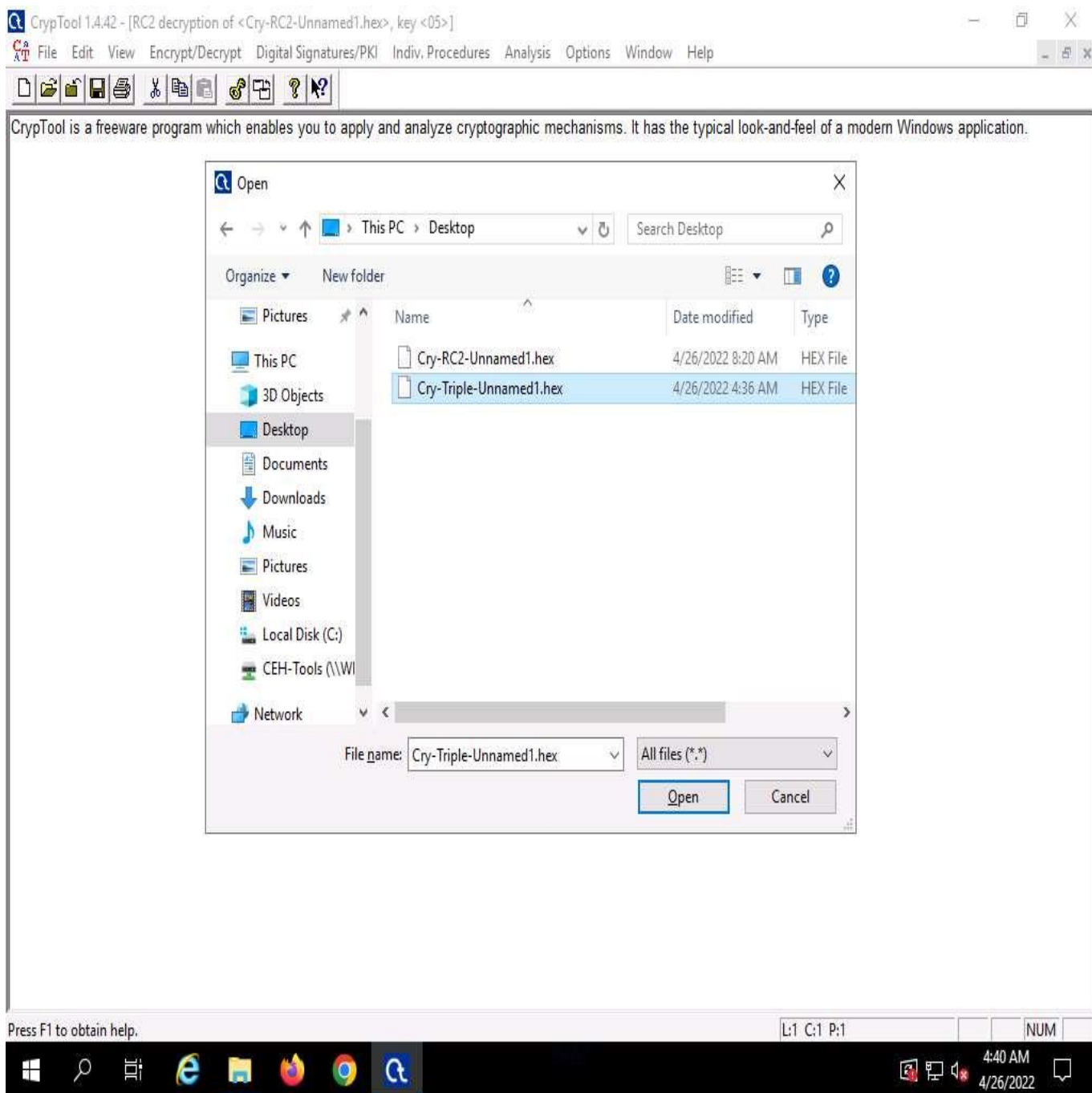
34. ☐ Click [Windows Server 2019](#) to switch to **Windows Server 2019**; copy the encrypted hex file (**Cry-Triple-Unnamed1.hex**) from **Z:\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\CrypTool** and paste on **Desktop**.



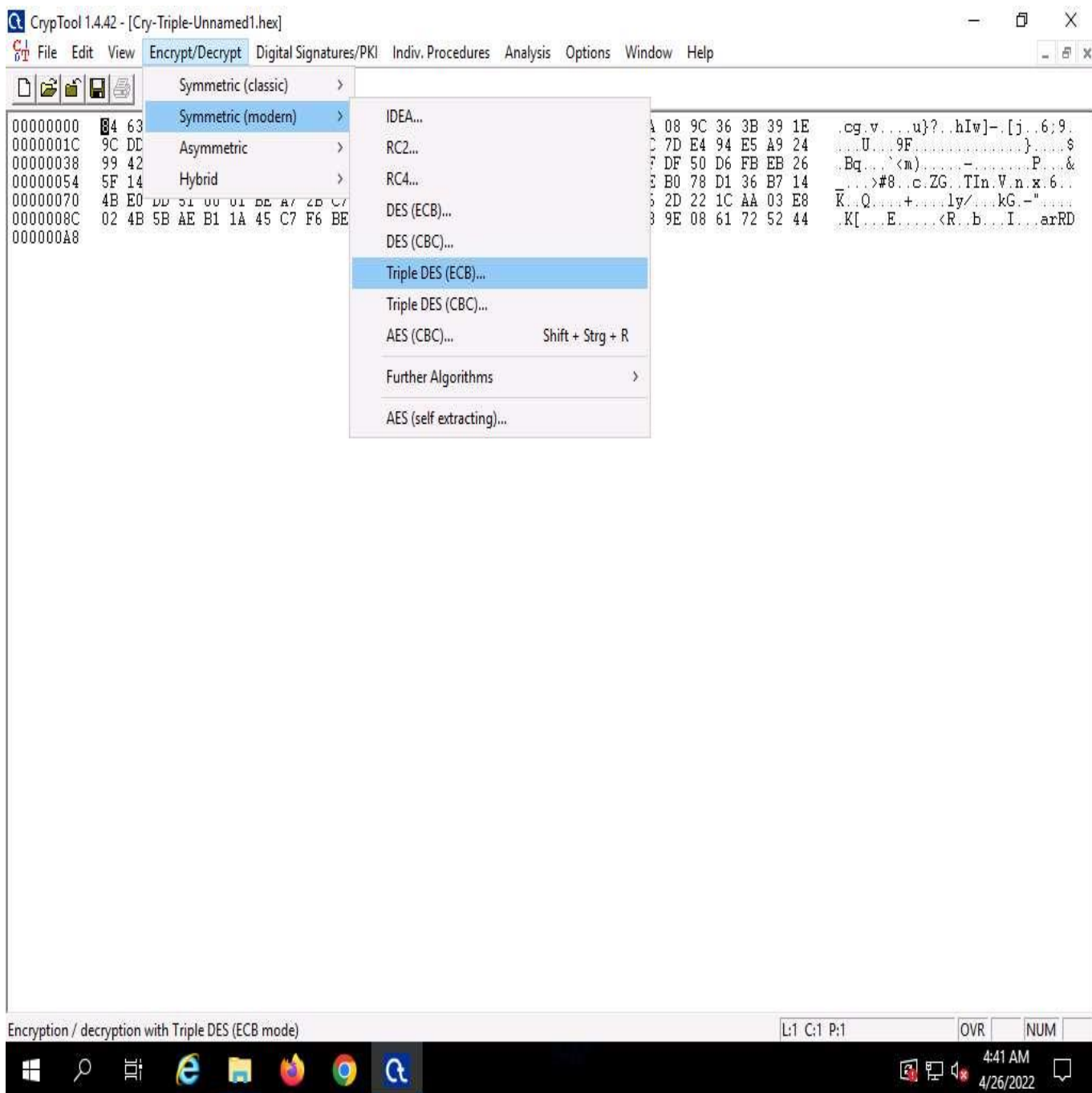
35. ☐ Switch to the **CrypTool** window to **decrypt** the data; click **File** in the menu bar and select **Open...**



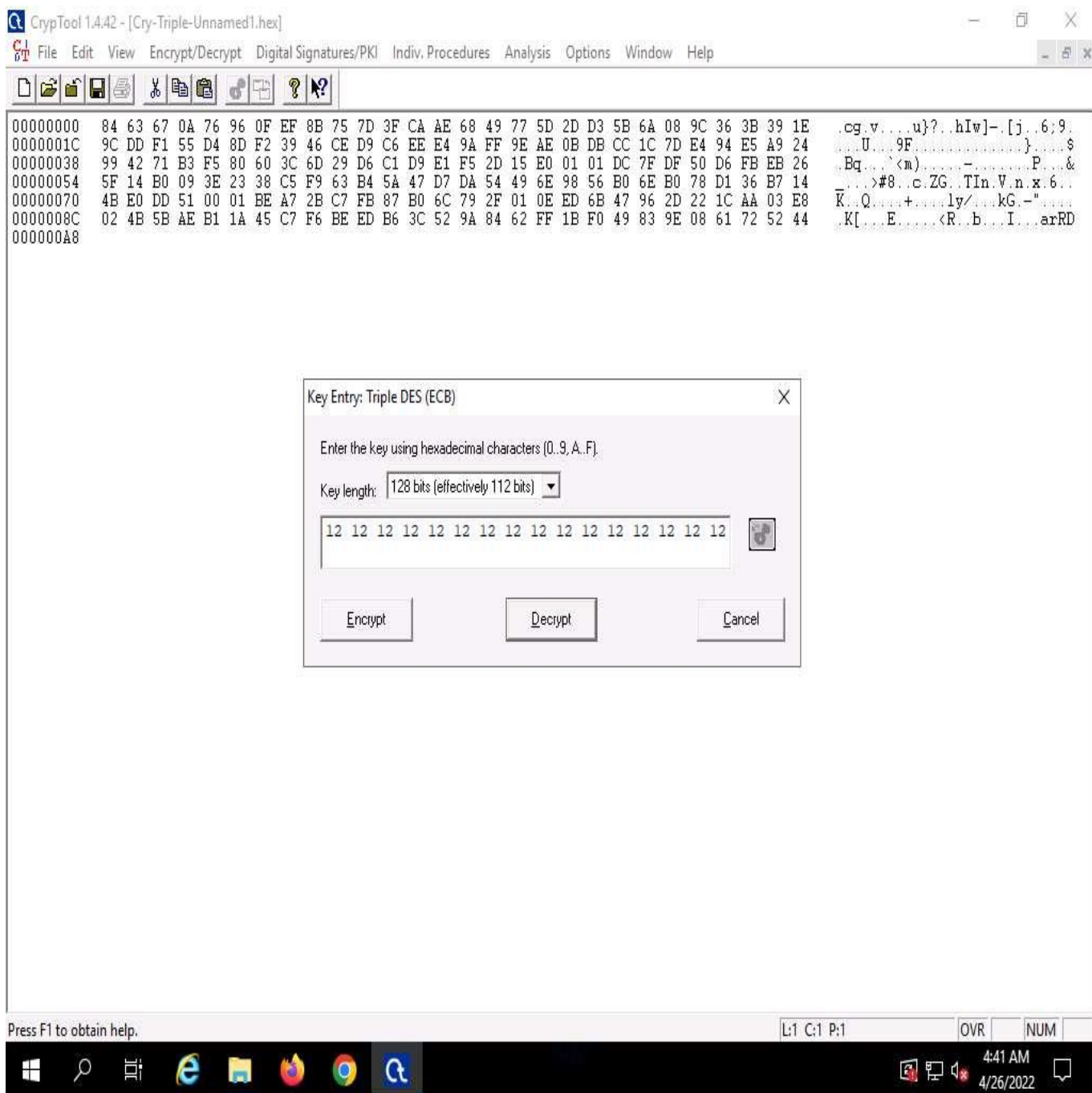
36. ☐ The **Open** window appears; select **All files(*.*)** from the drop-down list in the file type option, navigate to the location of the file (here, **Desktop**), select, and click **Open**.



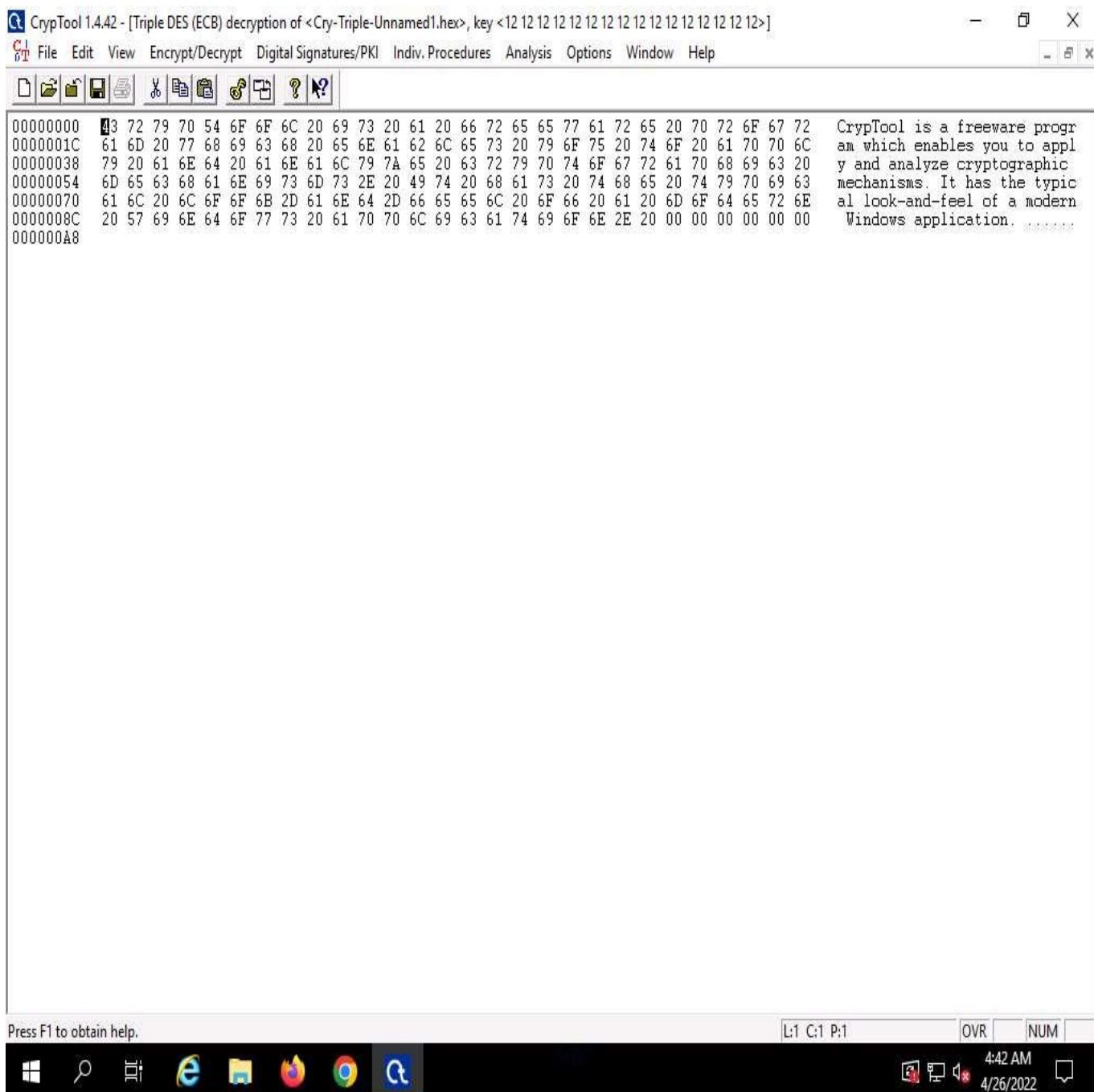
37. ☐ From the menu bar, click **Encrypt/Decrypt** and navigate to **Symmetric (modern)** -- > **Triple DES (ECB)**...



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.




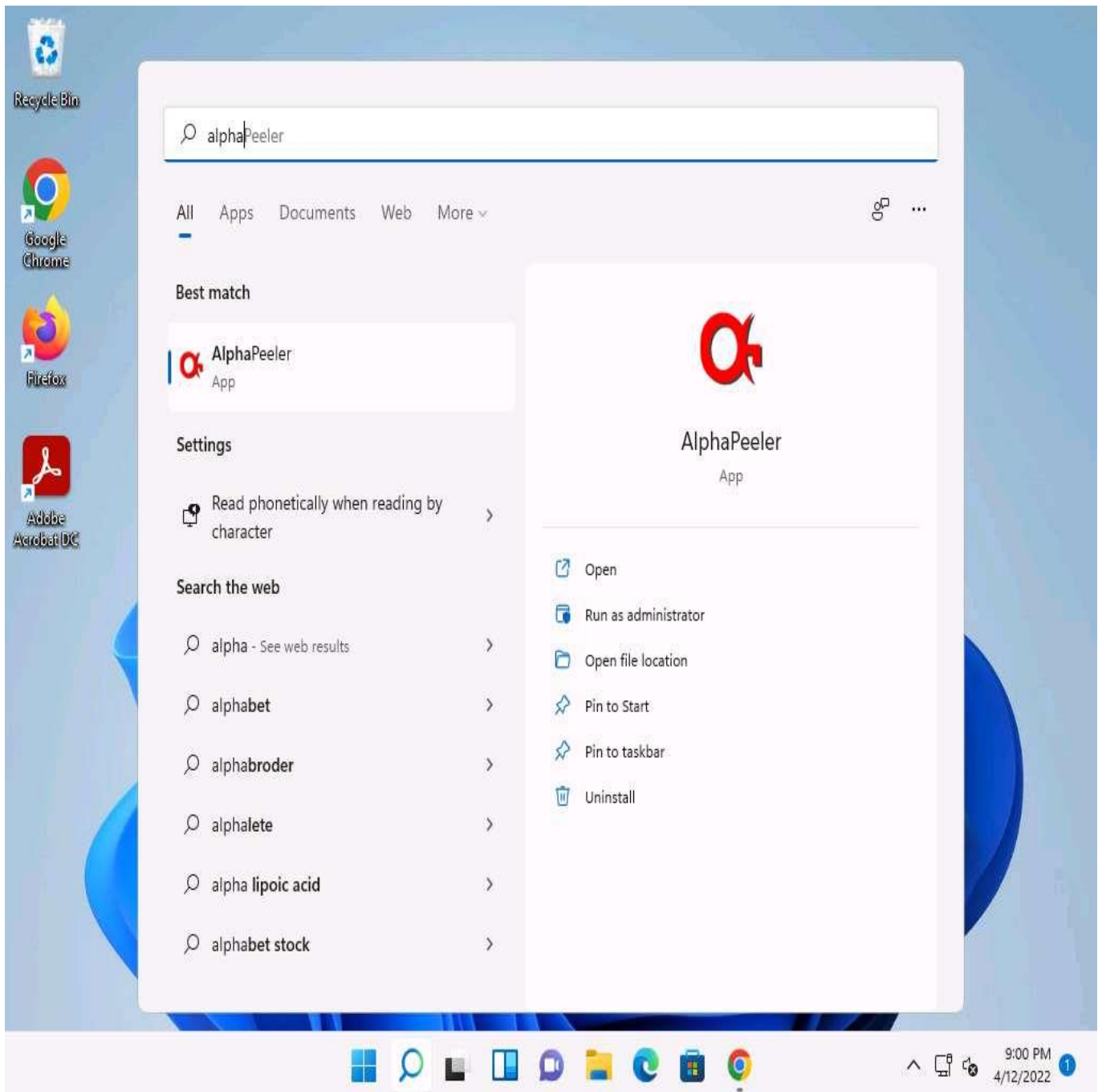
41. ☐ Using this method, files can be encrypted using CrypTool and shared with an individual in a secure manner, so that no one can intercept the data.
42. ☐ This concludes the demonstration of performing cryptanalysis using CrypTool.
43. ☐ Close all open windows and document all the acquired information.

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.

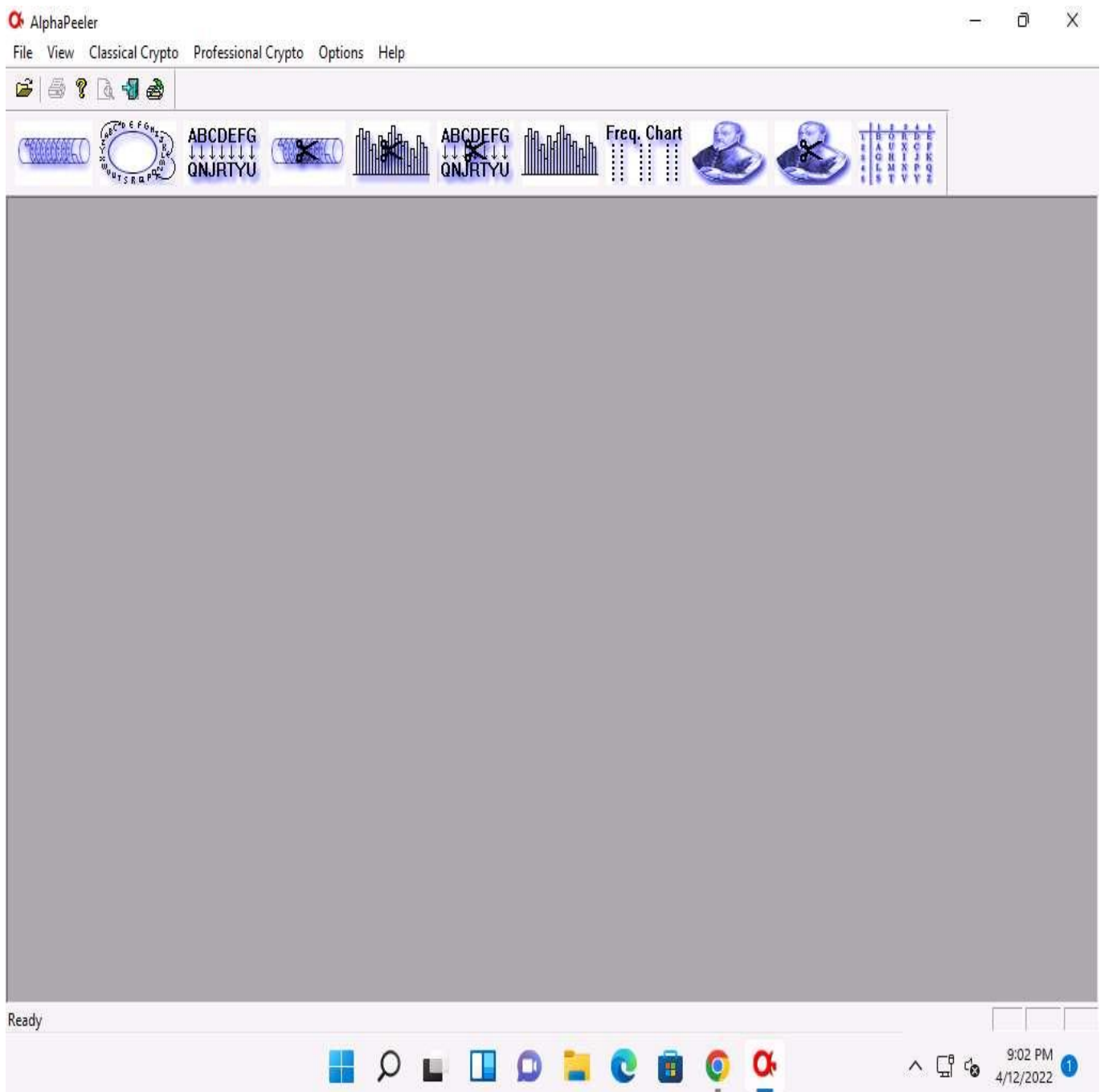
Here, we will use the AlphaPeeler tool to perform cryptanalysis.

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.

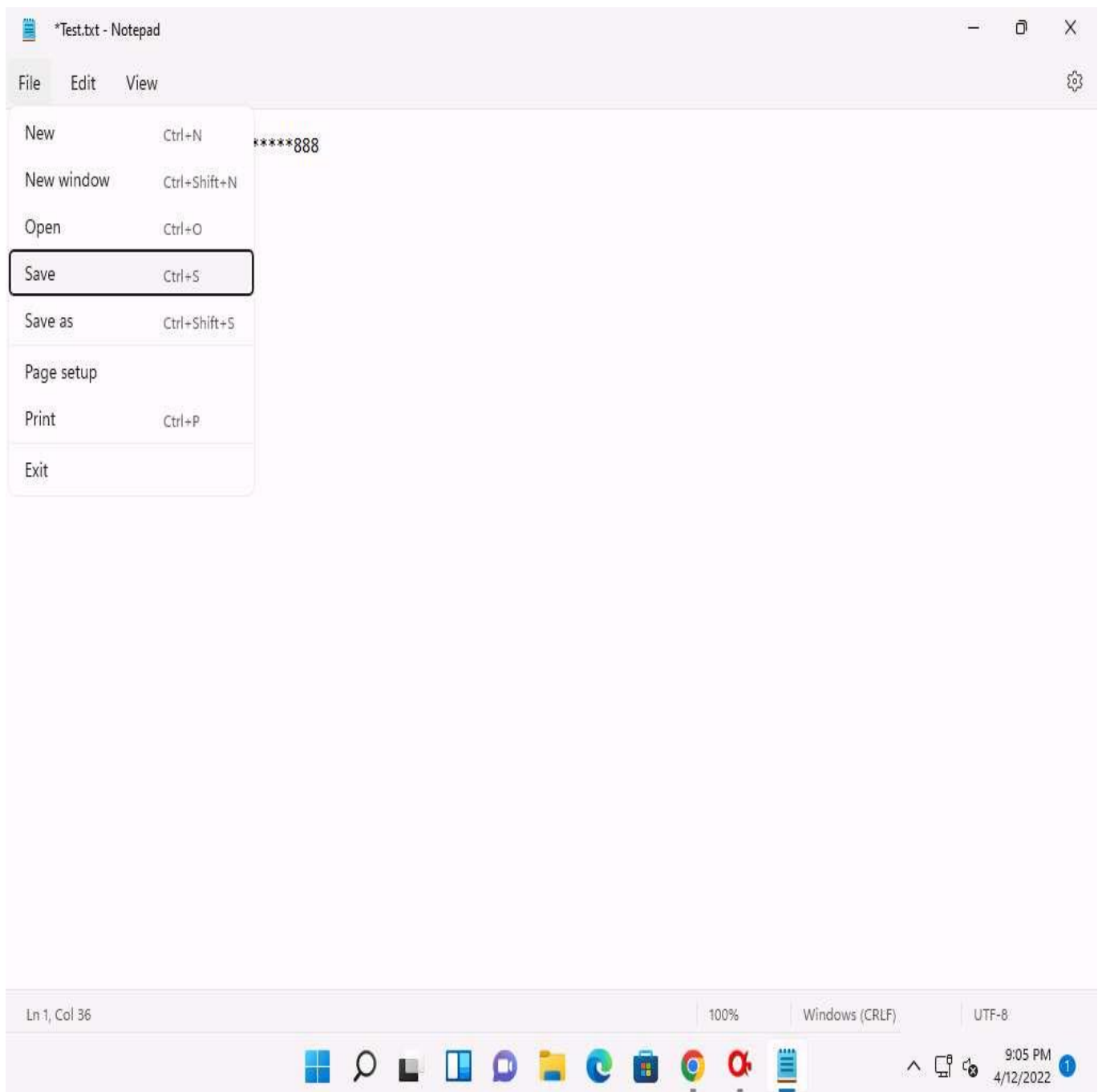


If an **Open File - Security Warning** pop-up appears, click **Run**.

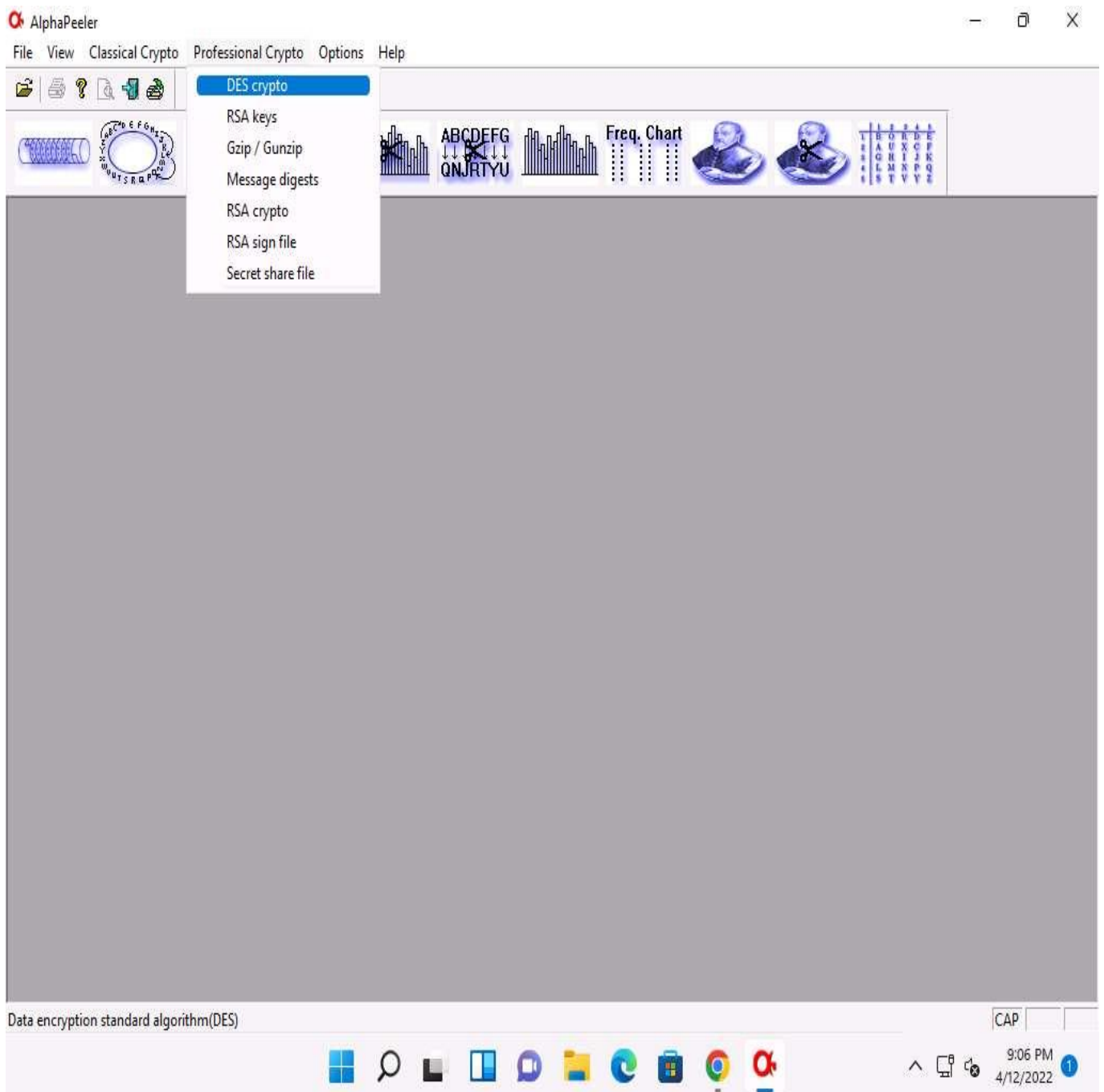
2. ☐ **AlphaPeeler Professional** initializes and the **AlphaPeeler** main window appears, as shown in the screenshot.



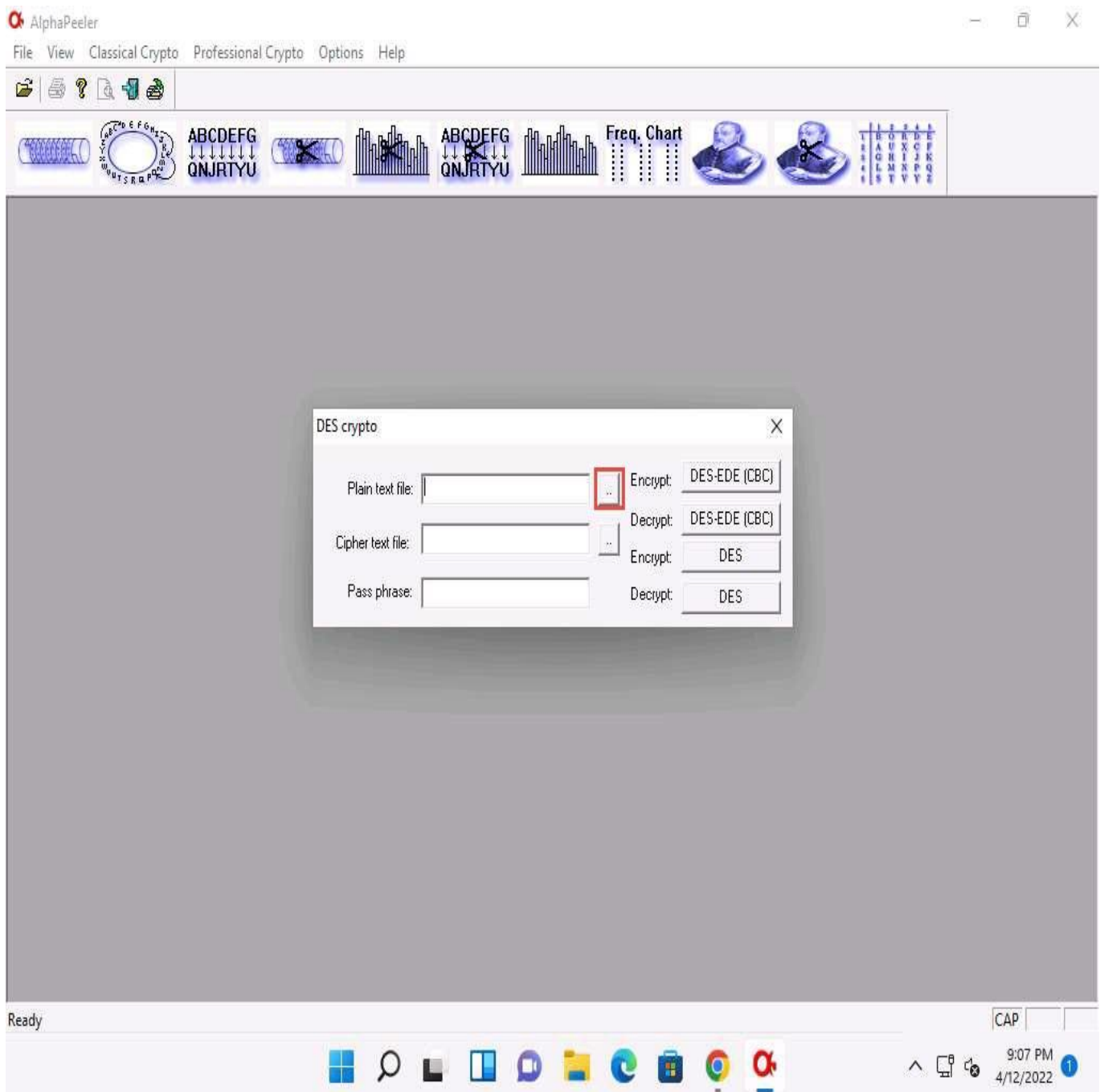
3. ☐ Now, minimize the AlphaPeeler window and create a text file on **Desktop**. Name it **Test**, open the file, and insert some text.
4. ☐ Click **File** in the menu bar and click **Save**.



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

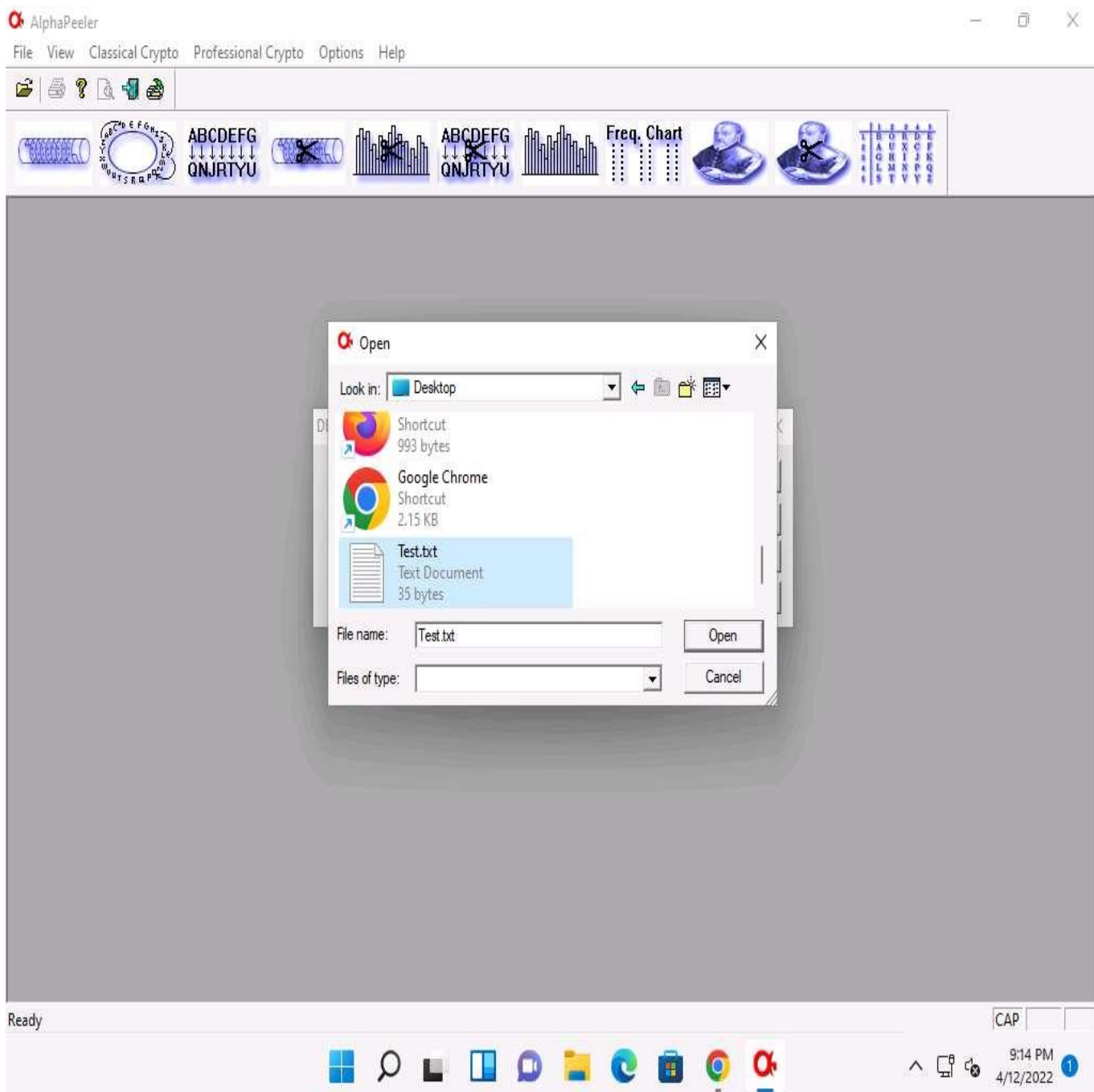


6. ☐ The **DES crypto** pop-up appears; click the ellipsis icon under the **Plain text file** option.

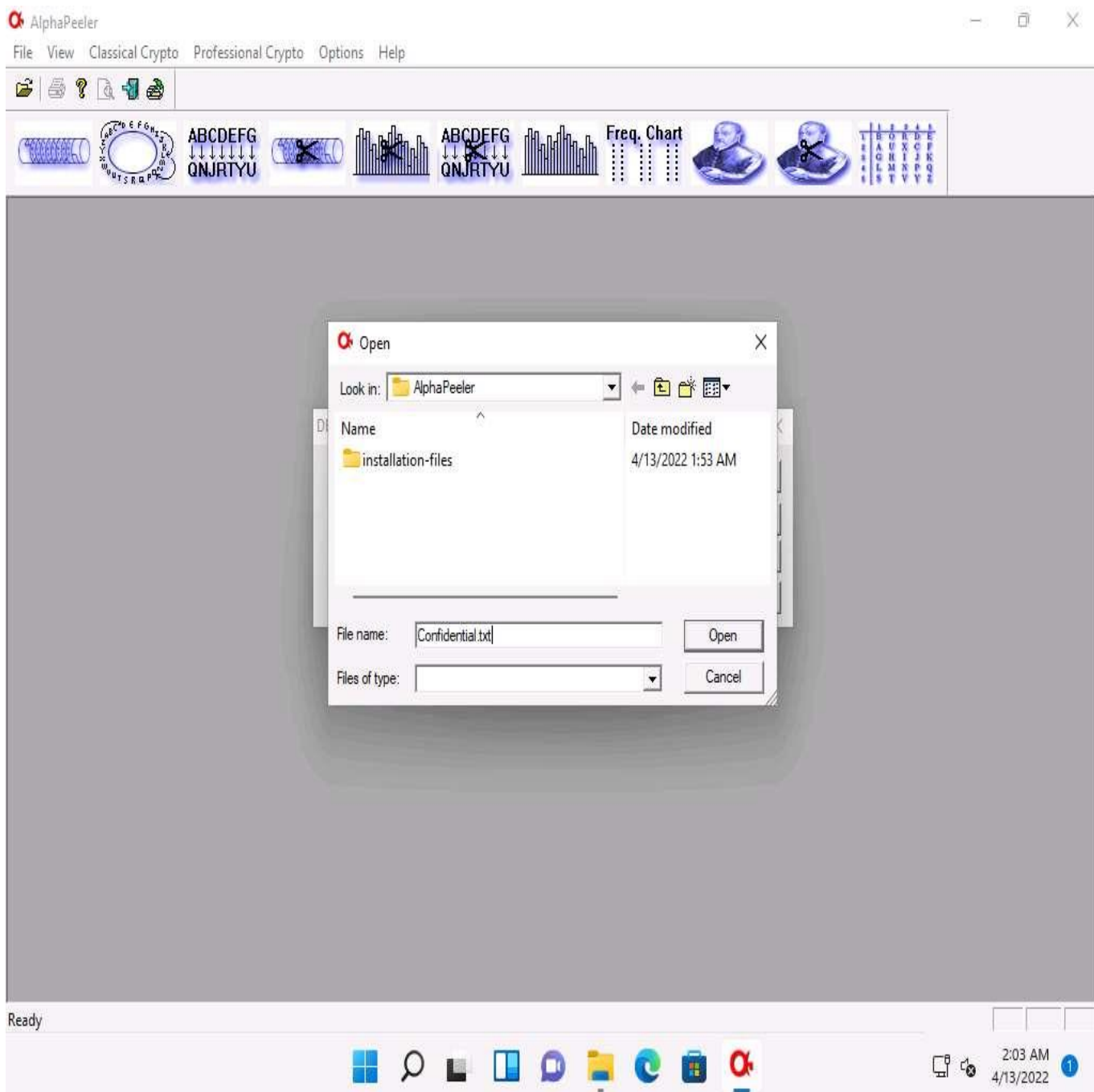


7. ☐ The **Open** window appears; navigate to **Desktop** and select **Test.txt** file; then, click **Open**.

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

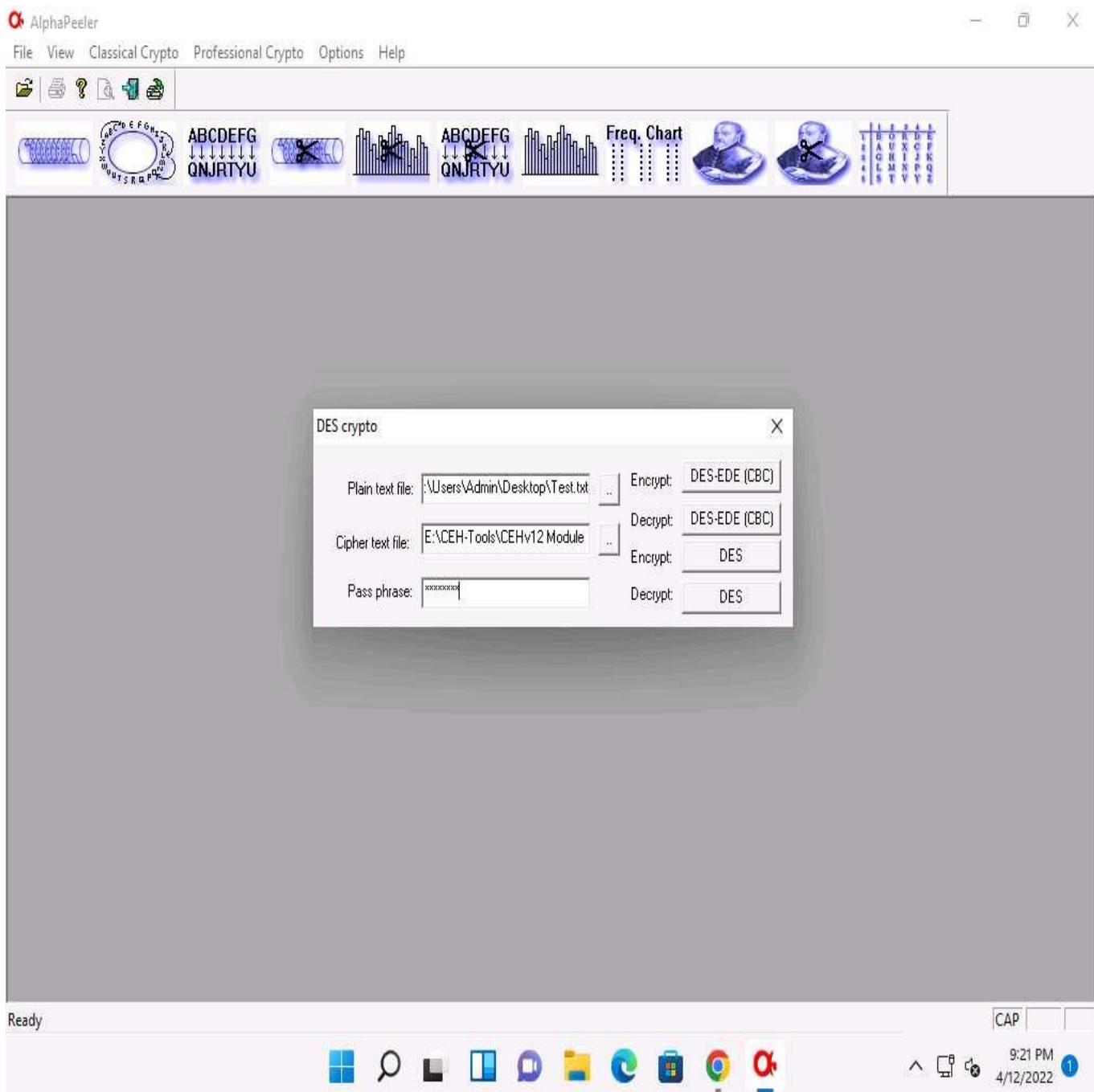


8. ☐ In the **DES crypto** pop-up; click the ellipsis icon under the **Cipher text file** option.
9. ☐ The **Open** window appears; select the save location (here, **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**) and name the file as **Confidential.txt**; then, click **Open**.

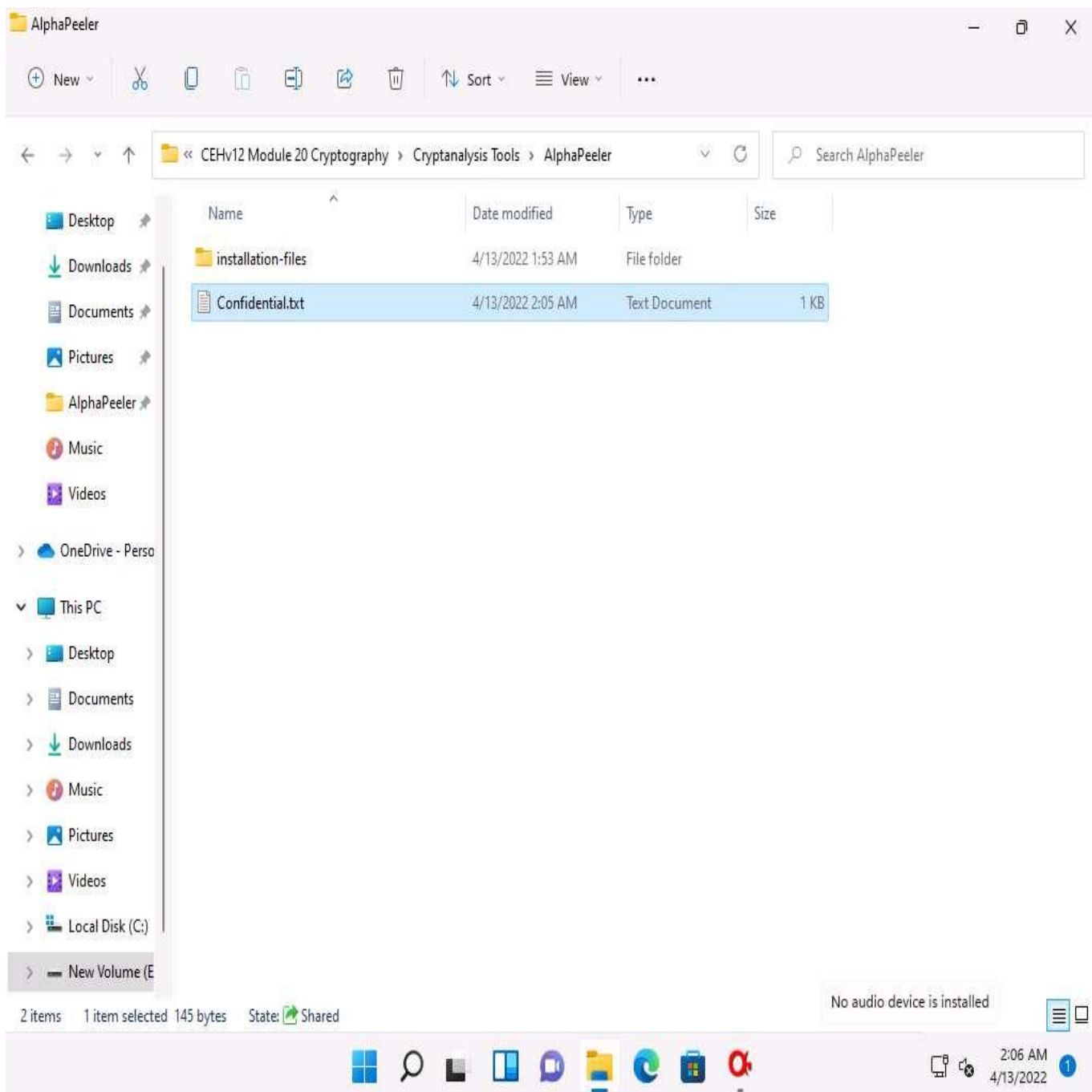


10. ☐ In the **DES crypto** pop-up; insert the password into the **Pass phrase** field and click **DES-EDE (CBC)** button under **Encrypt** option to encrypt the text file.

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

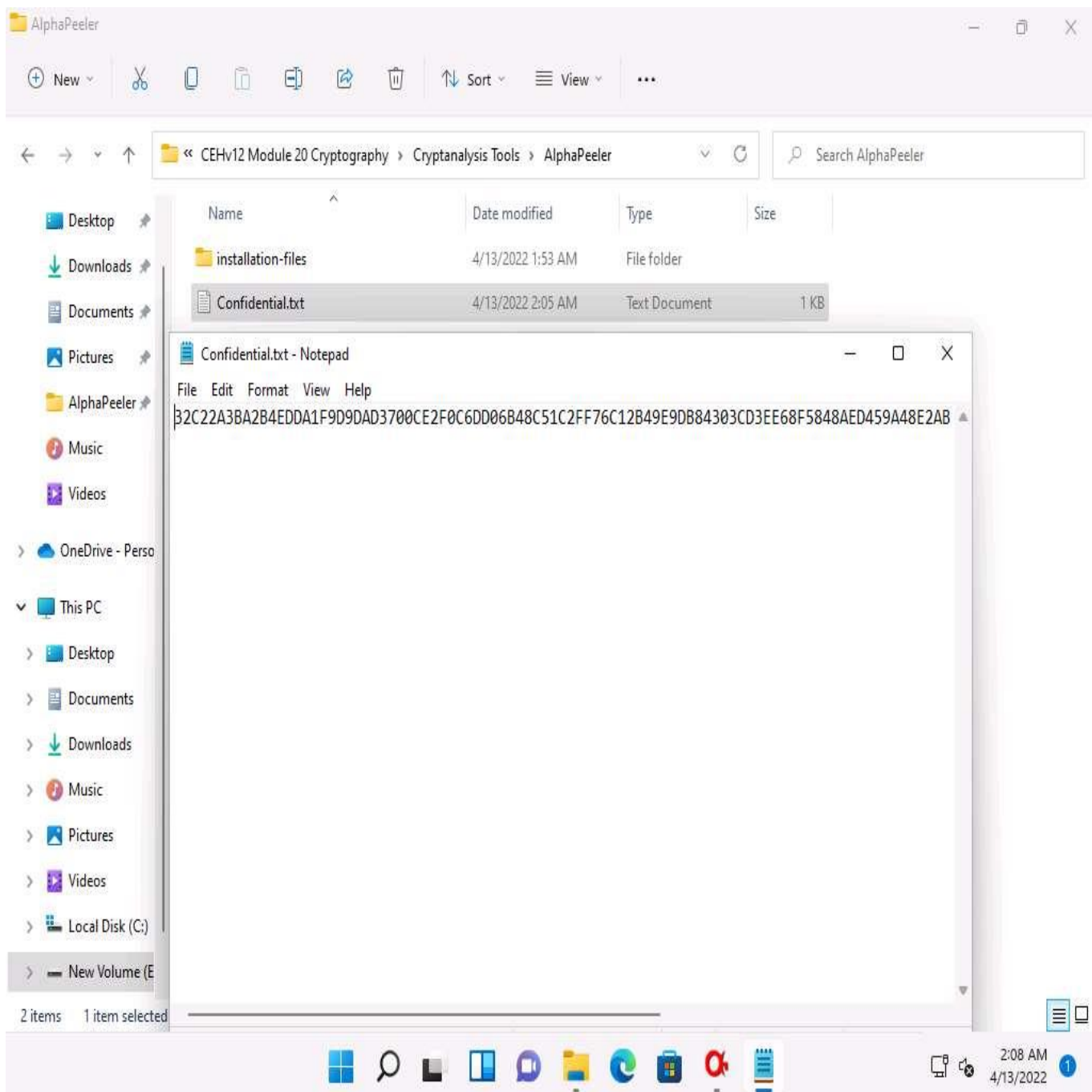



11. ☐ A new file **Confidential.txt** appears at location **E:\CEH-Tools\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler**, as shown in the screenshot.



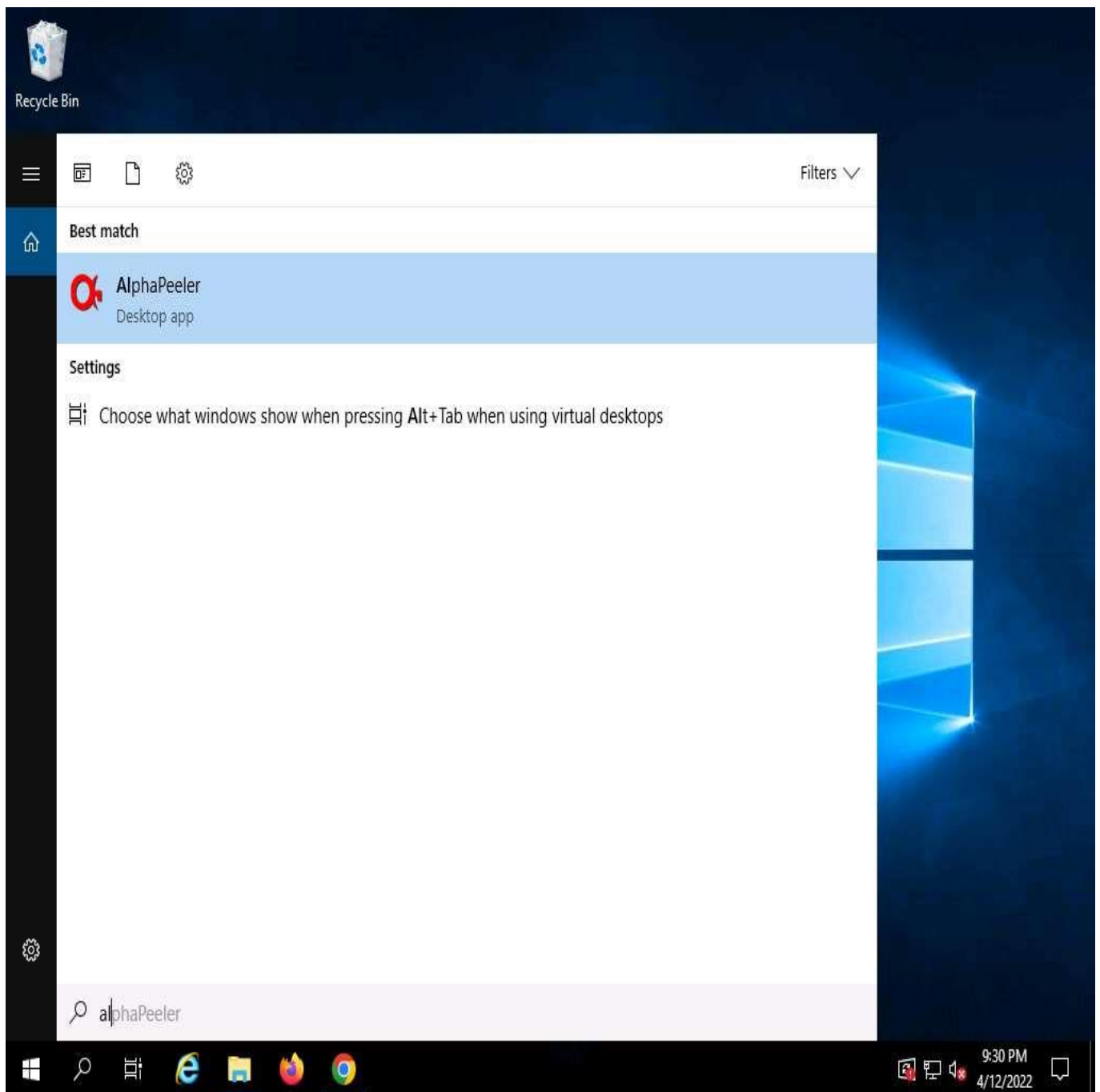
12. ☐ Double-click **Confidential.txt** to open, and you can observe that the file's content is encrypted.

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.

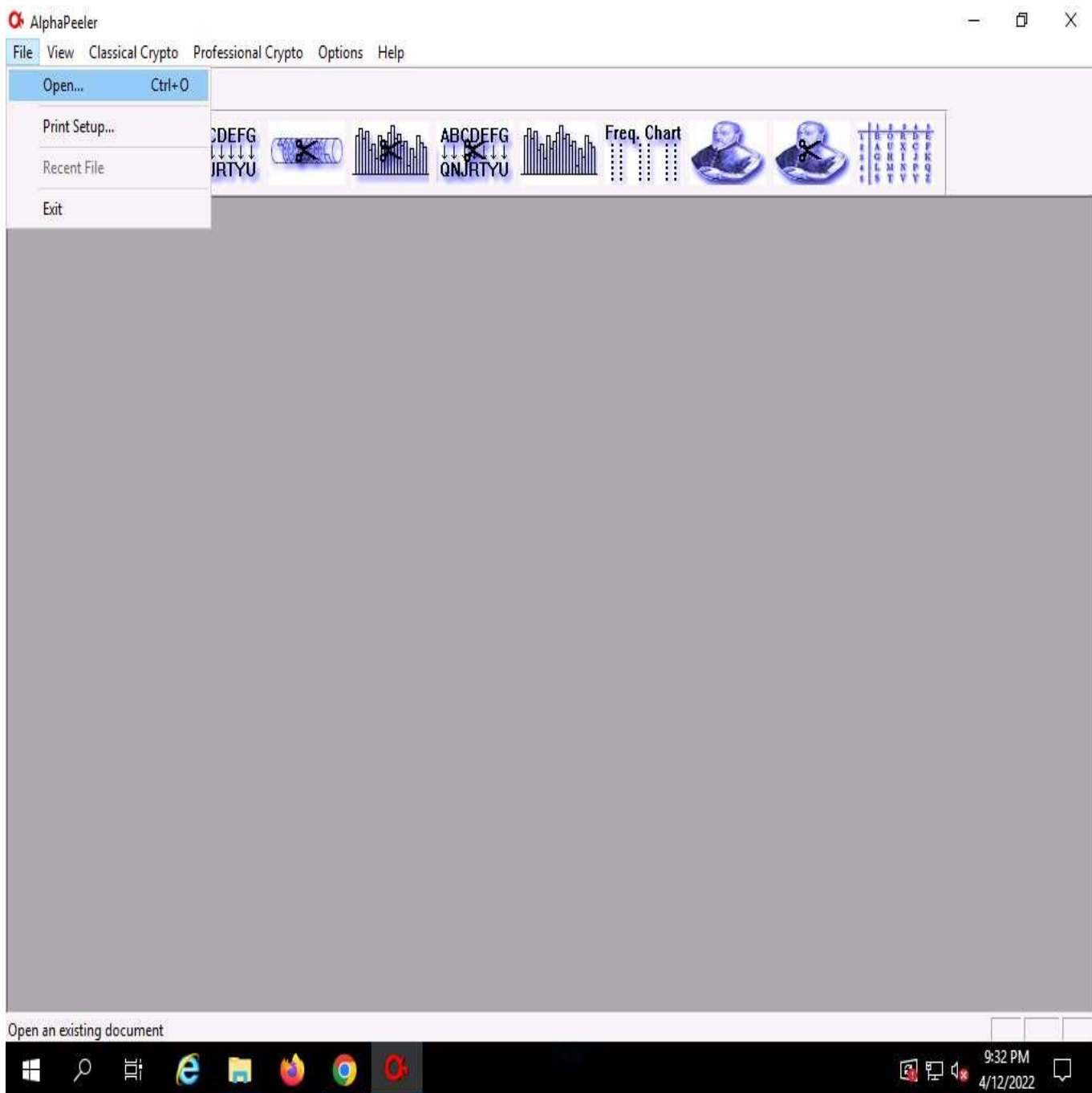


13. ☐ Close the **DES crypto** pop-up and the **AlphaPeeler** window.
14. ☐ Click on [Windows Server 2019](#) to switch to **Windows Server 2019**; Click **Search** icon () on the **Desktop**. Type **alpha** in the search field, the **AlphaPeeler** appears in the results, double click to launch it.

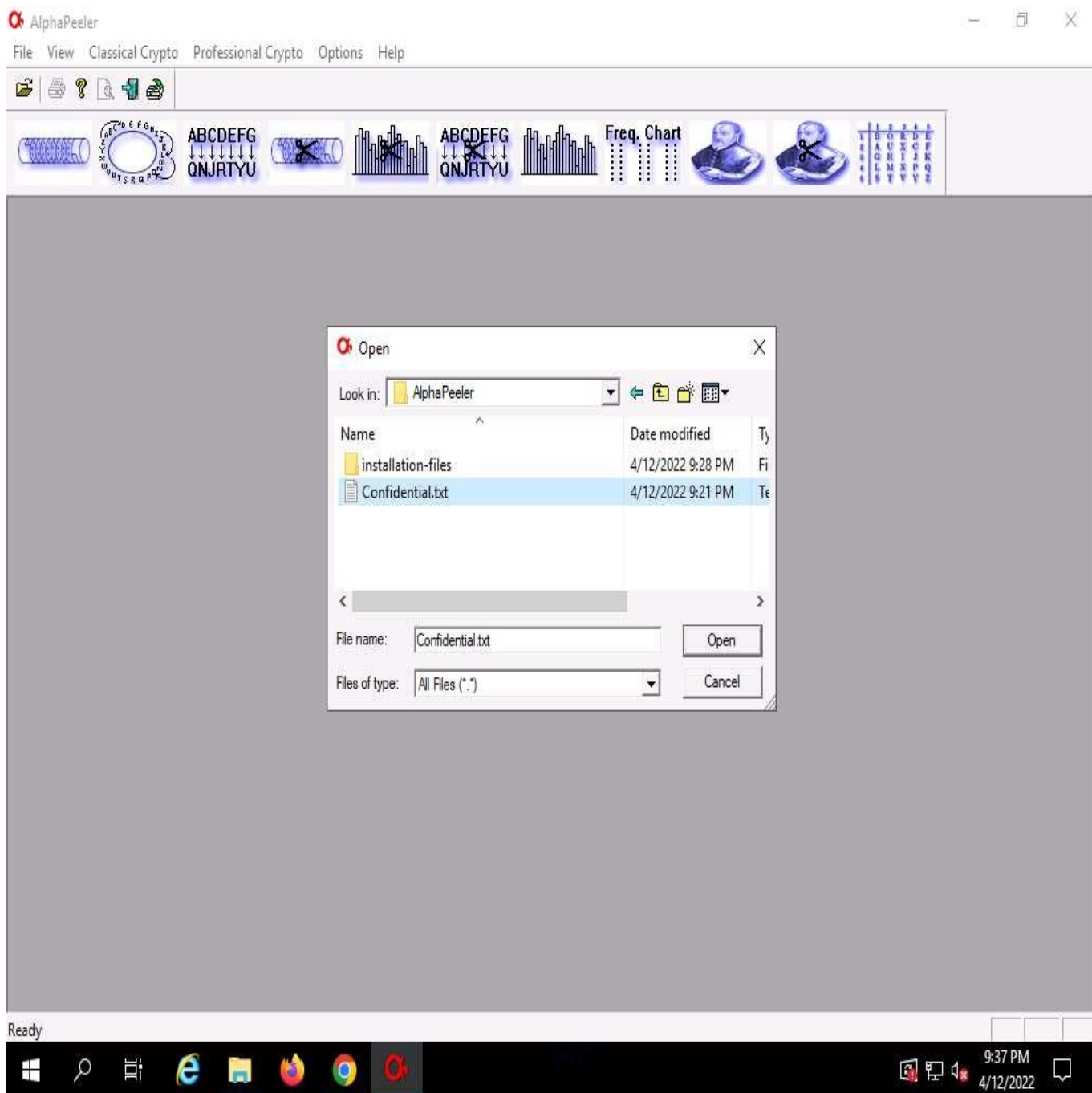
If an **Open File - Security Warning** pop-up appears, click **Run**.



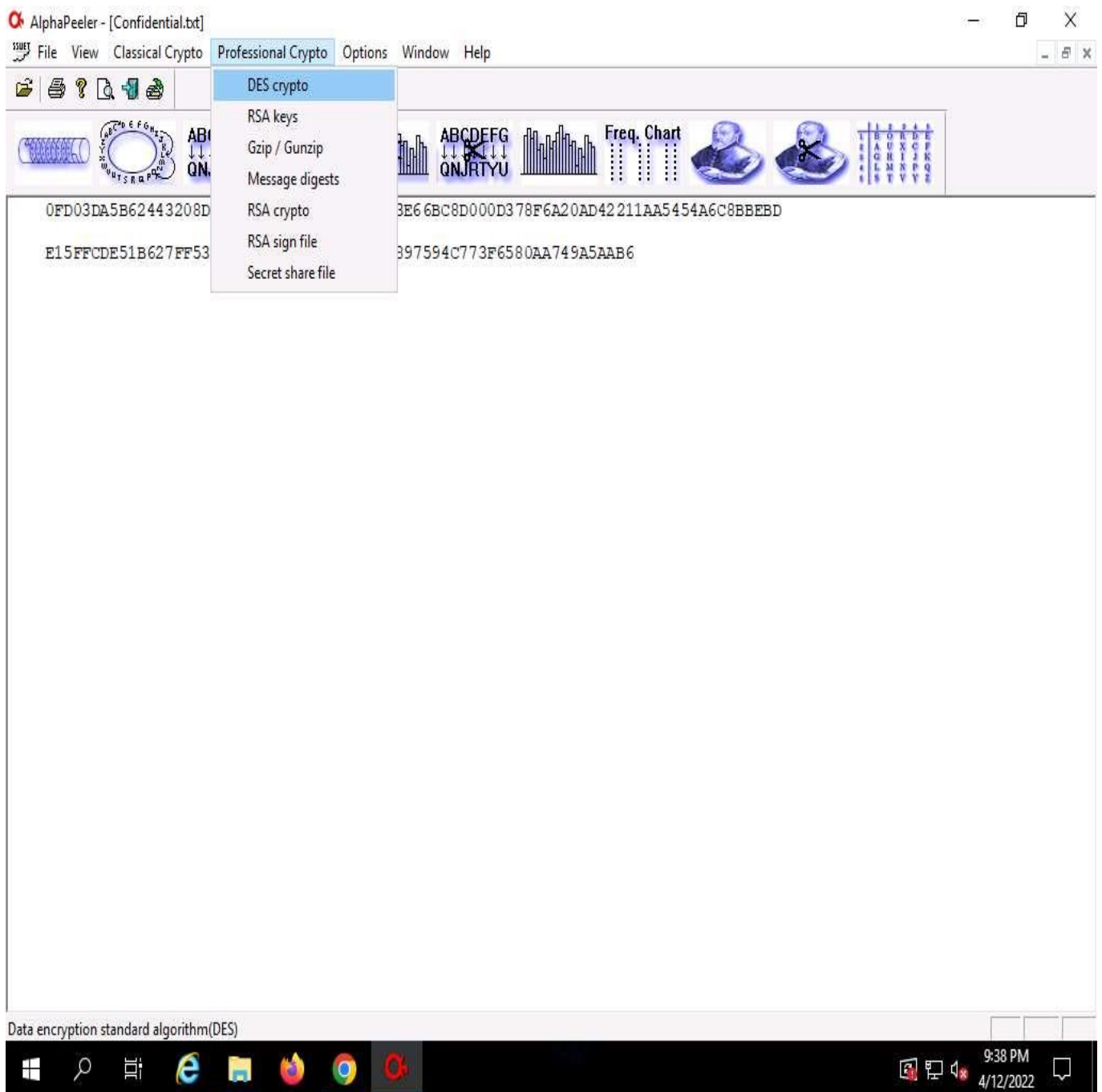
15. ☐ The **AlphaPeeler** main window appears; click **File** from the menu bar and click **Open...**



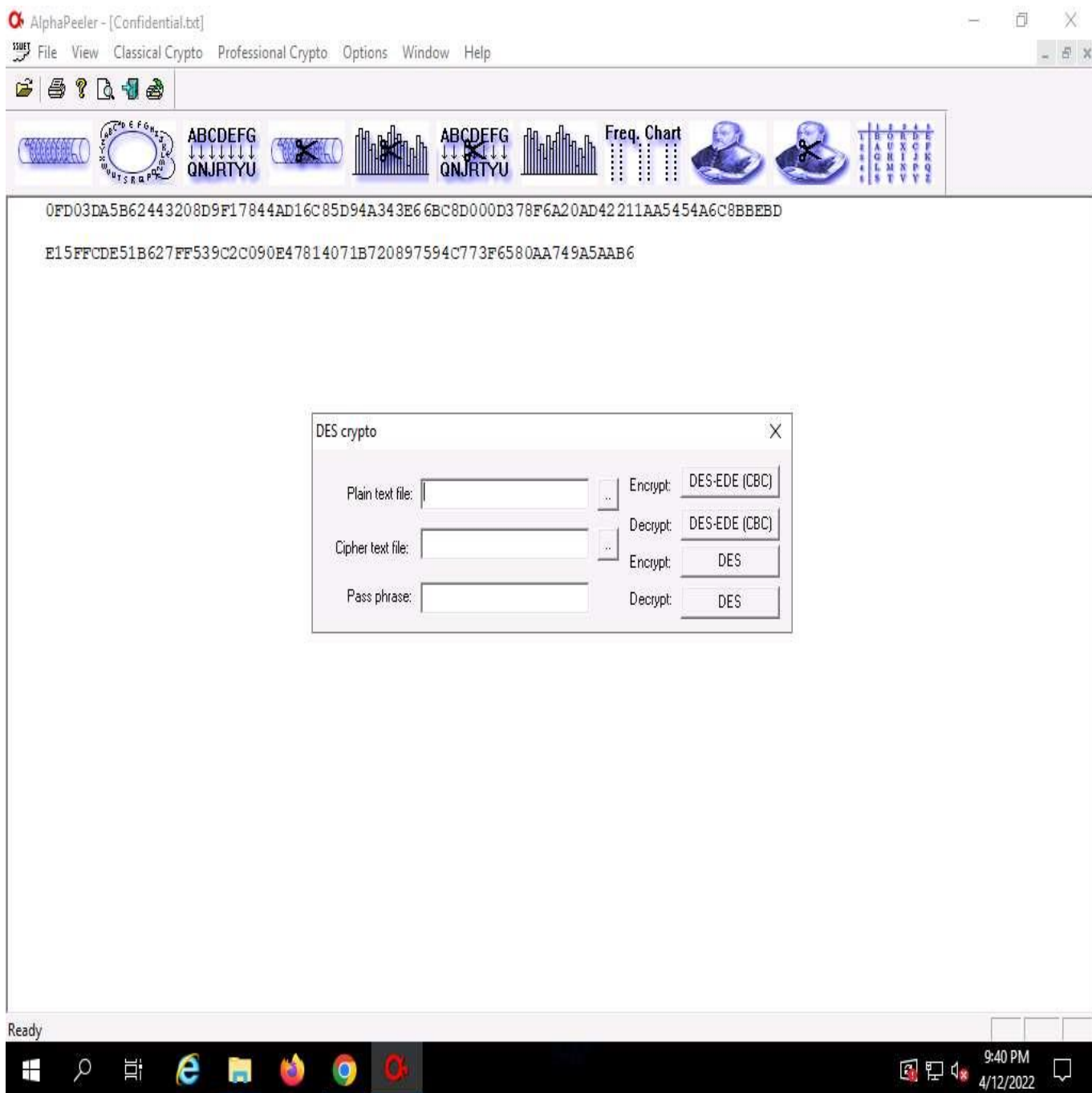
16. ☐ The **Open** window appears; in the **Look in** field, navigate to the location of **Z:\CEHv12 Module 20 Cryptography\Cryptanalysis Tools\AlphaPeeler** and select **Confidential.txt** file; then, click **Open**.



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



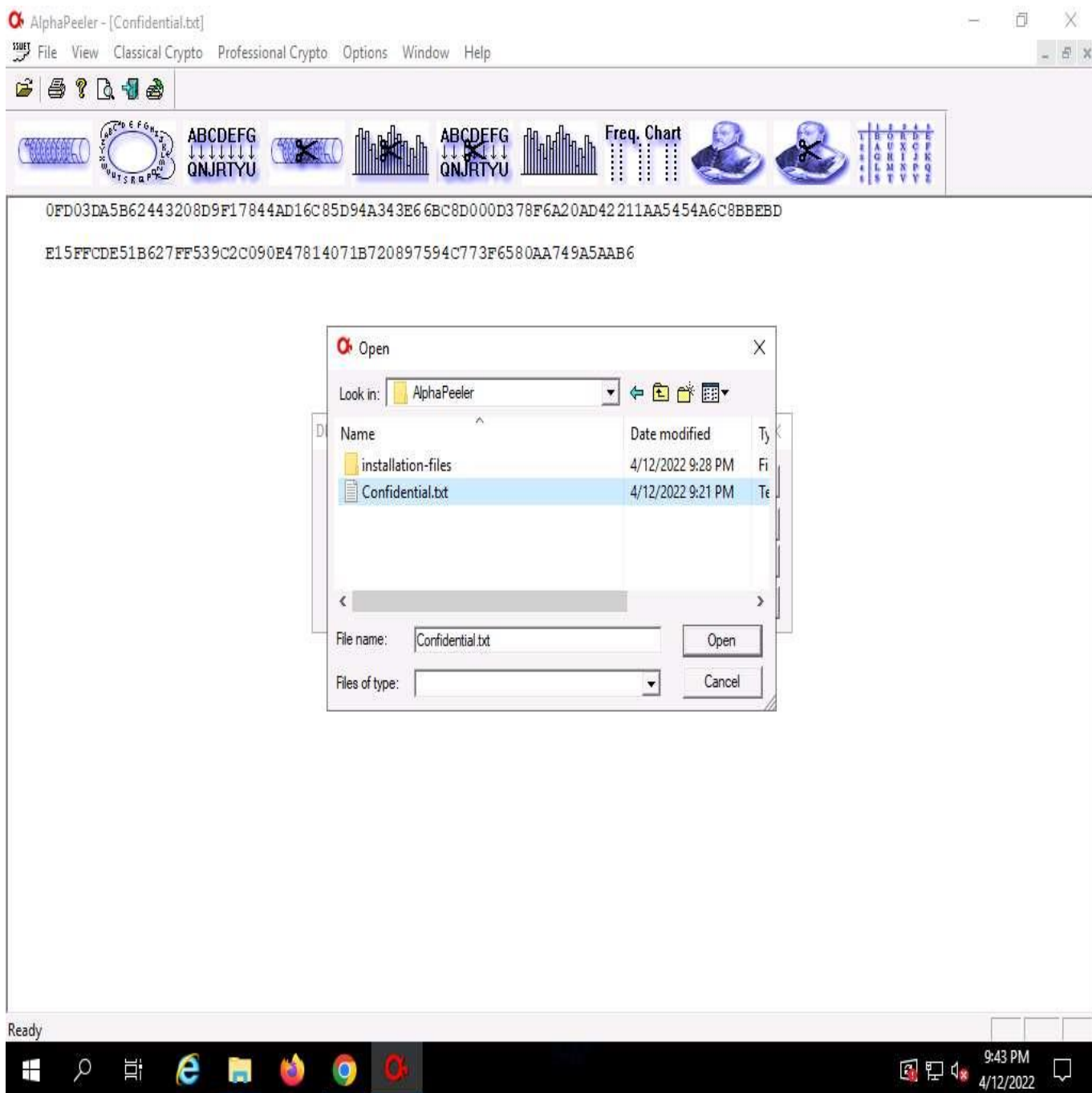
18. ☐ The **DES crypto** pop-up appears; click the ellipsis icon next to the **Plain text file** option.



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

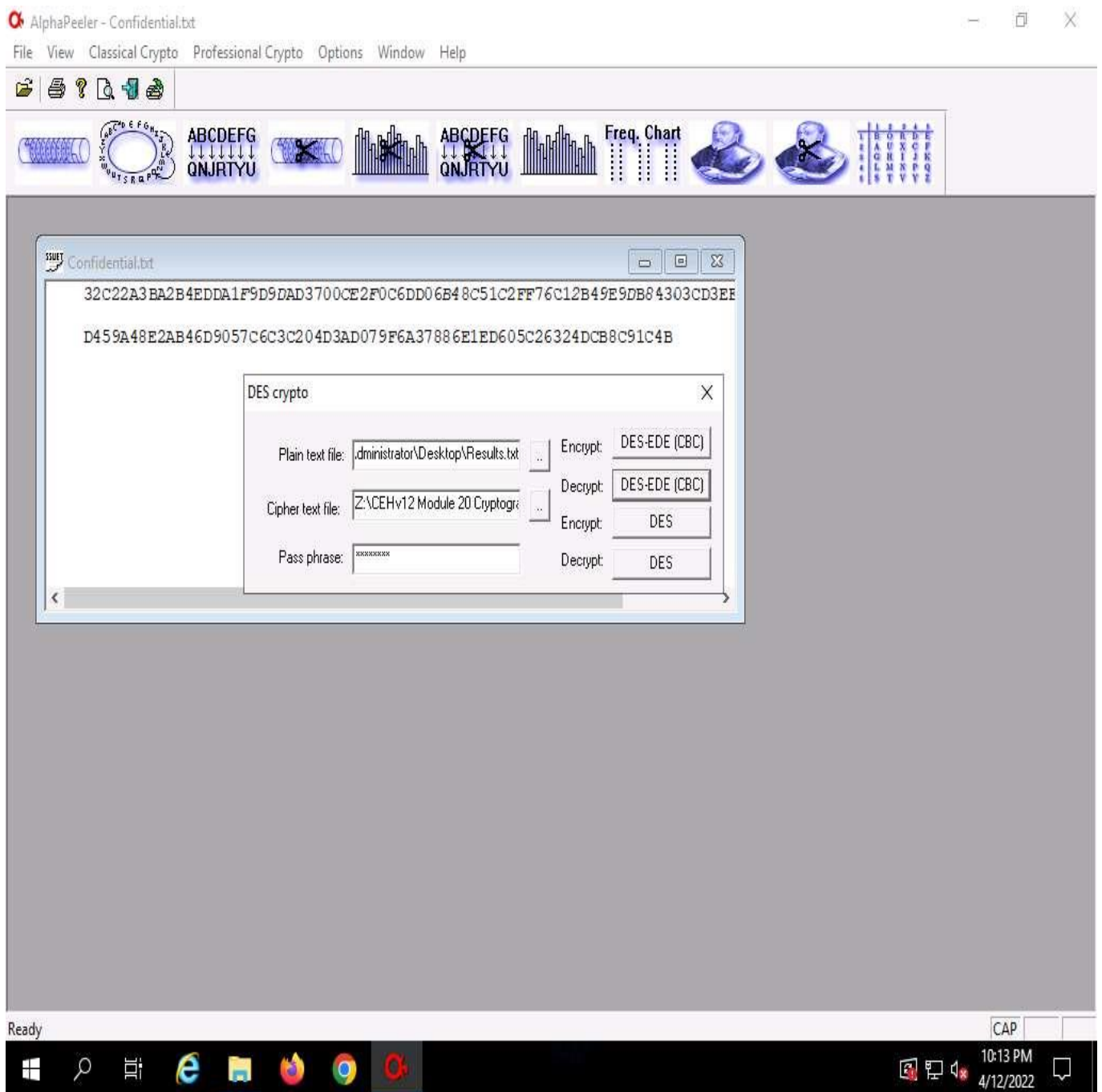
Here, we are creating an output file that will be in plain-text.

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**.

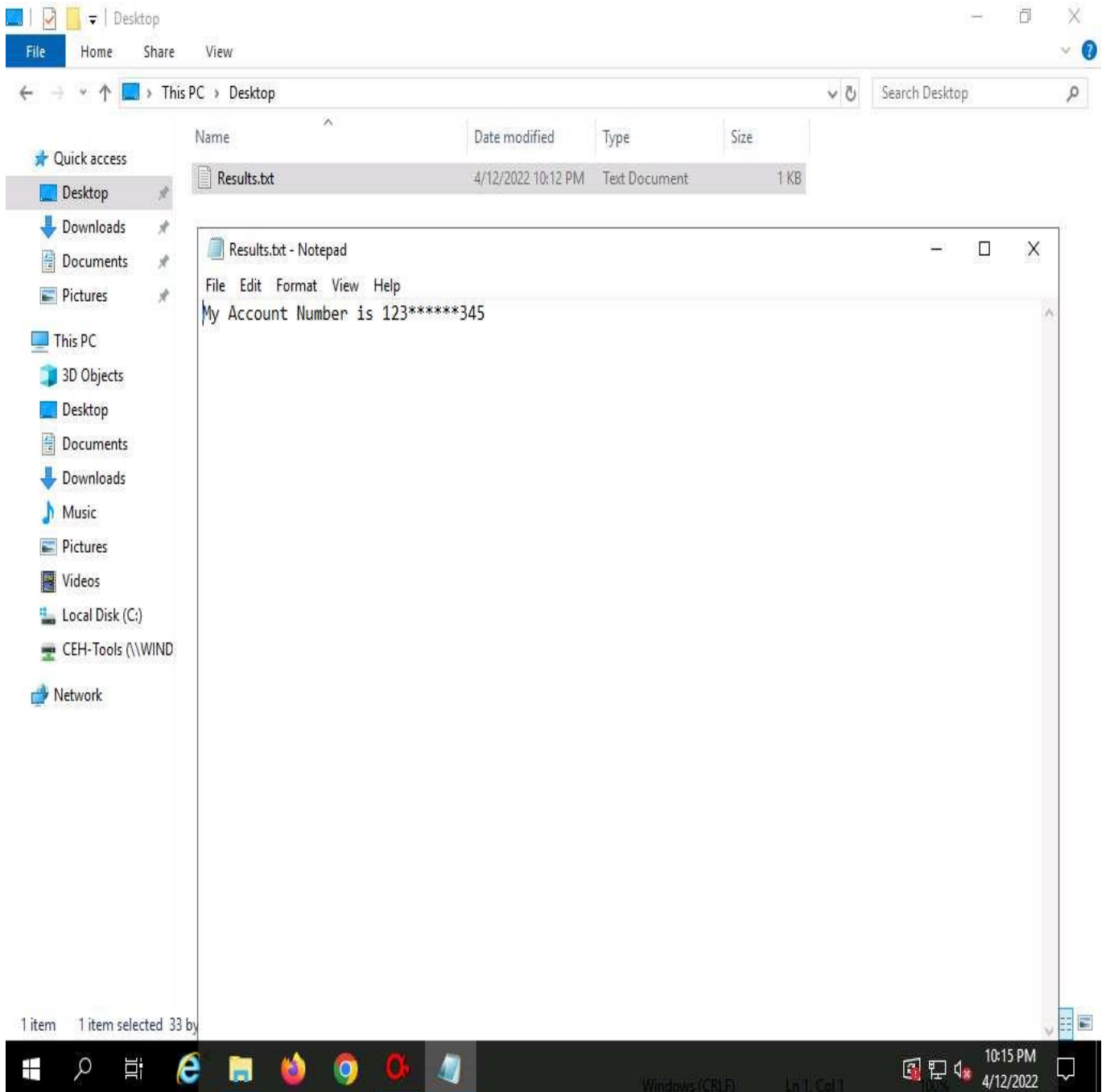


22. ☐ In the **DES crypto** pop-up, enter the password that you provided in **Step#10** into the **Pass phrase** field and click the **DES-EDE (CBC)** button next to **Decrypt** to decrypt the text file.

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.