



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



School of
Applied Computing

Advanced Cyber Security (ACS)

Lab – Cryptography

**Faculty of Architecture, Computing &
Engineering
School of Applied Computing
IQ Building, Room 205
Swansea
SA1 8EW**

Cryptography is the study and art of hiding meaningful information in an unreadable format.

Task 1: Basic Data Encryption Using CrypTool

CrypTool is a freeware program that enables you to apply and analyze cryptographic mechanisms. It has the typical look and feel of a modern Windows application. CrypTool includes every state-of-the-art cryptographic function and allows you to learn and use cryptography within the same environment.

Lab Scenario

Most security initiatives are defensive strategies aimed at protecting the perimeter of the network. But these efforts may ignore a crucial vulnerability sensitive data stored on networked servers are at risk from attackers who only need to find one way inside the network to access this confidential information. Additionally, perimeter defenses like firewalls cannot protect stored sensitive data from the internal threat employees with the means to access and exploit this data. Encryption can provide strong security for sensitive data stored on local or network servers. To be an expert ethical hacker and penetration tester, you must have knowledge of cryptography functions.

Lab Objectives

This lab will give you experience on encrypting data and show you how to do so. It will teach you how to:

- Use encrypting/decrypting command
- Visualize several algorithms
- Calculate hash values and analysis

Pre- Activity exercise

To carry out the lab, you need:

- CrypTool located on the shared drive lecturer PC.
- Windows running on virtual machine
- You can also download the latest version of CrypTool from the link <http://www.cryptool.org/en/download-ct1-en>
- If you decide to download the latest version, then screenshots shown in the lab might differ

Overview of Lab

CrypTool is a free, open-source e-learning application used in the implementation and analysis of cryptographic algorithms. It was originally designed for internal business application for information security training.

Activity:

Note: Screenshot may varies from the one in this lab. Though the lab says Windows server 2008, use Windows 7 and/or Windows 10 if the Windows server 2008 is not available.

1. Navigate to the shared drive on lecturer PC for CrypTool, double-click **SetupCrypTool_1_4_31_Beta6b_r3670_VS2008_en.exe**, and follow the wizard driven installation steps to install the application.
2. On completing the installation, launch **CrypTool** application from the **Apps** screen.

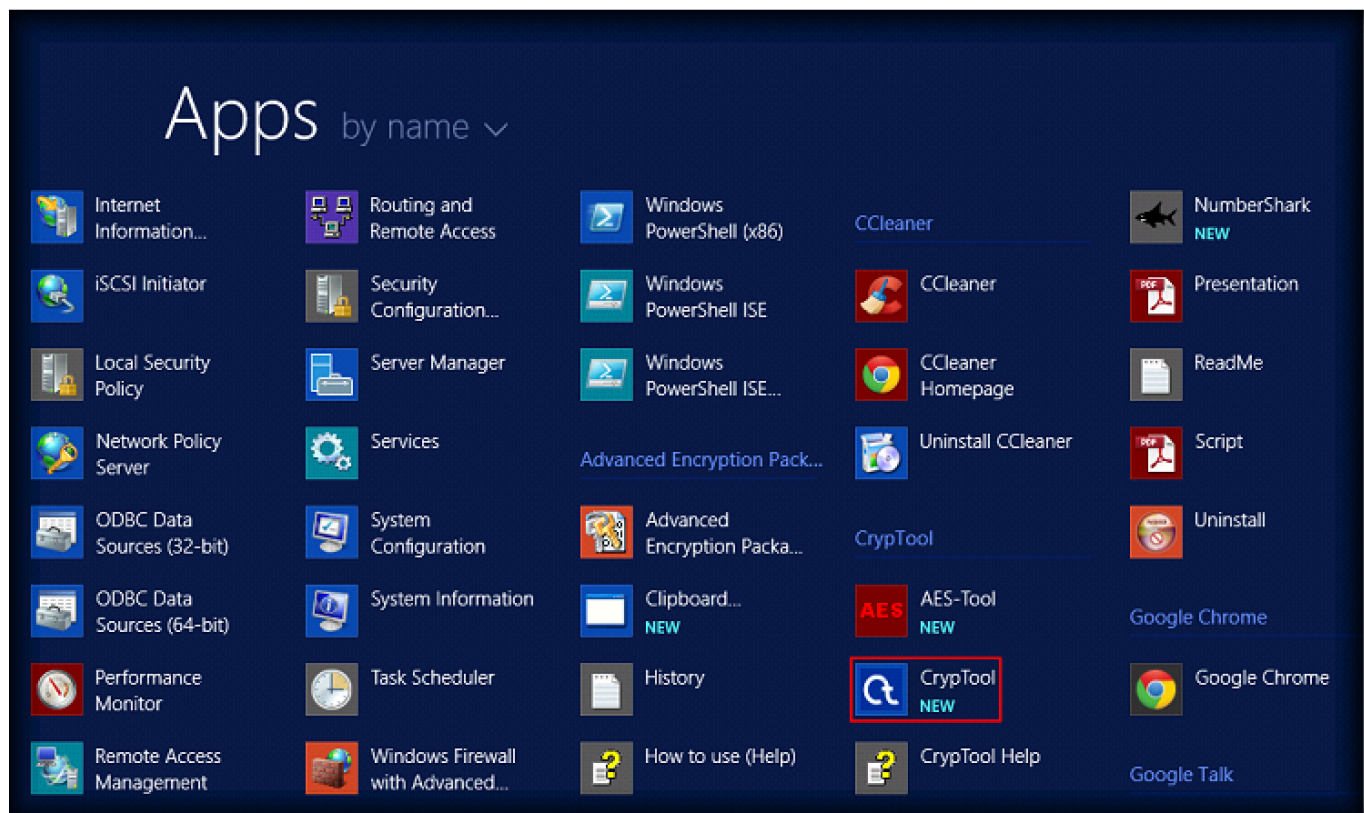


FIGURE 11.1: Launching CrypTool from Apps screen

3. The **How to Start** dialog box appears; check **Don't show this message again**, and click **Close**.

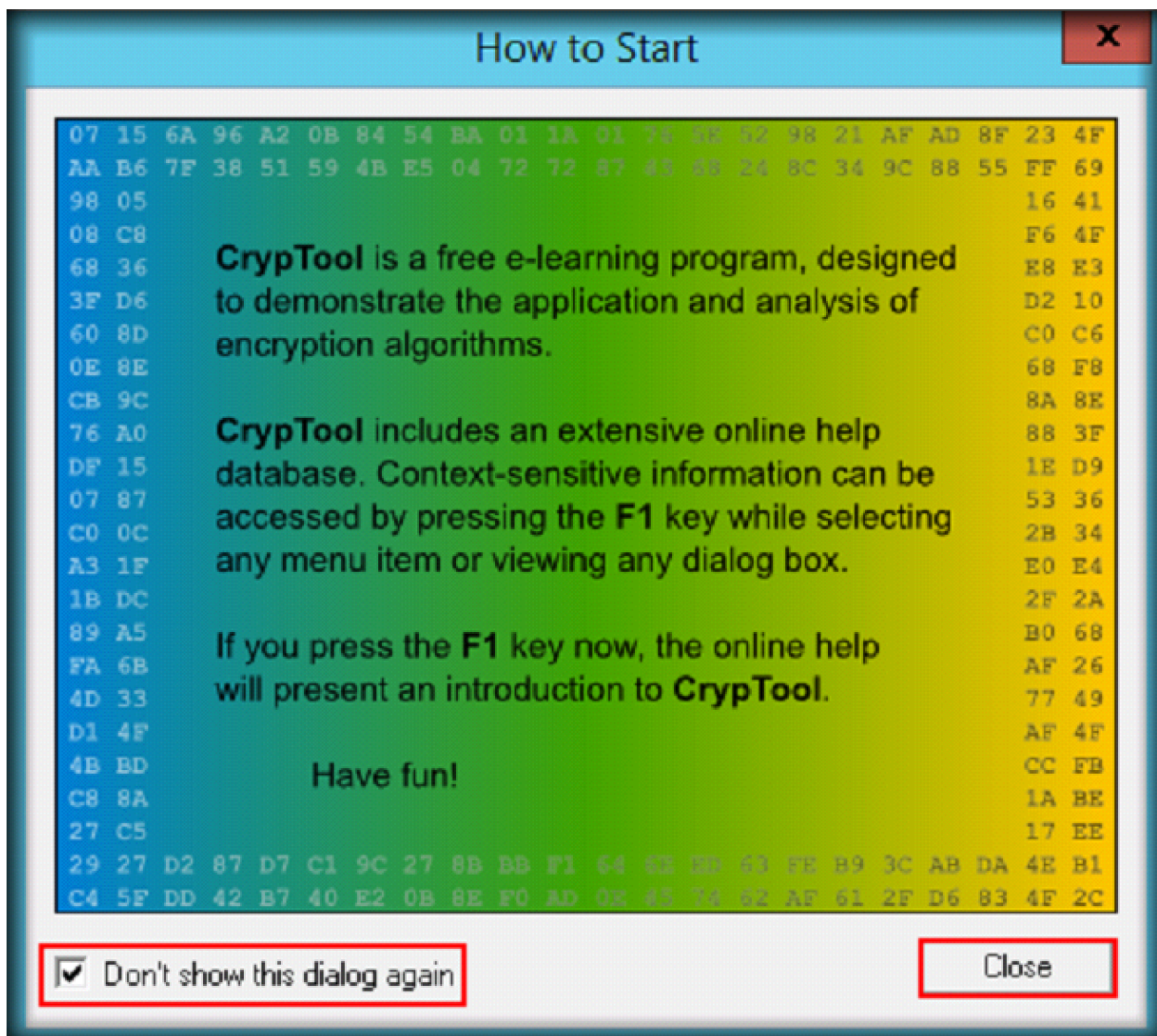


FIGURE 11.2: How to Start Dialog box

4. The main window of **CrypTool** appears; close the **startingexample-en.txt** window.

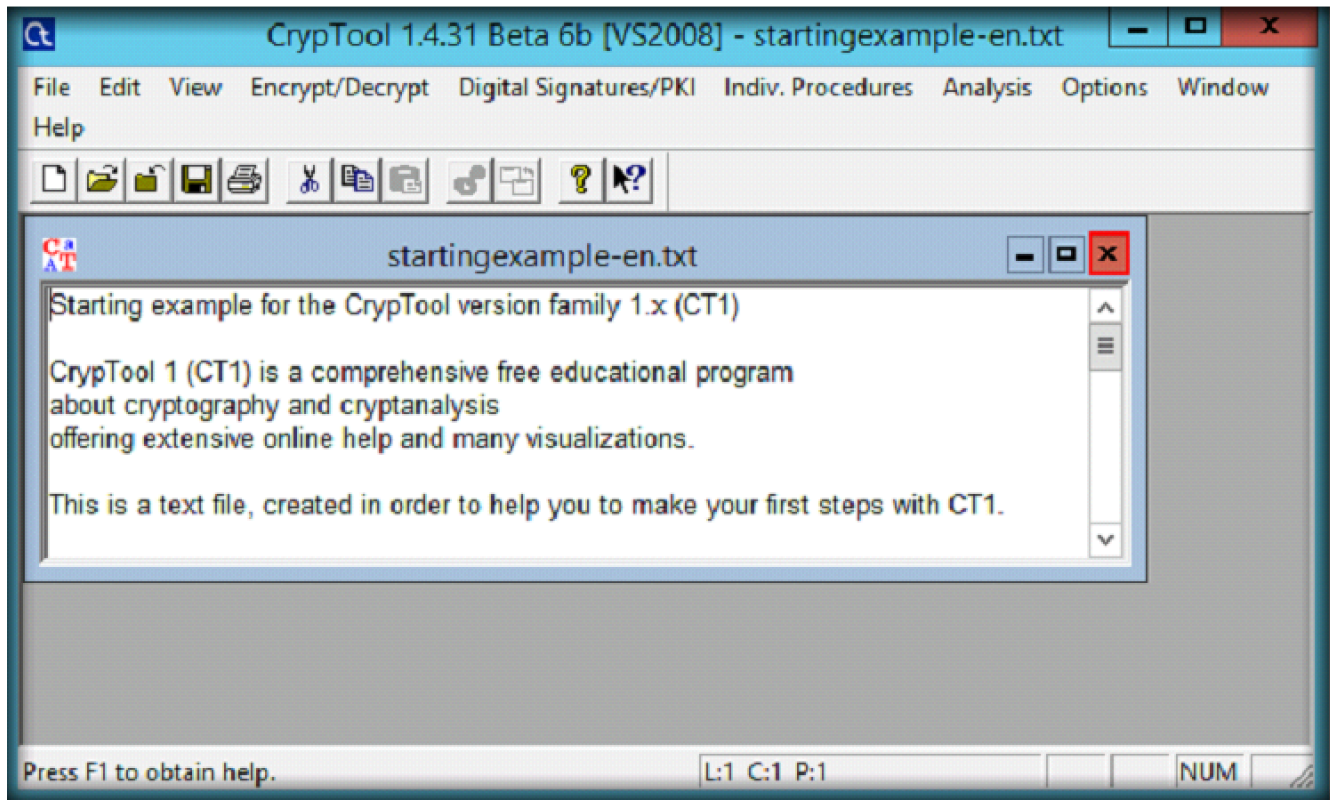


FIGURE 11.3: startingexample-en.txt window in CrypTool

5. To **encrypt** data, click the **File** option from the menu bar, and select **New**.

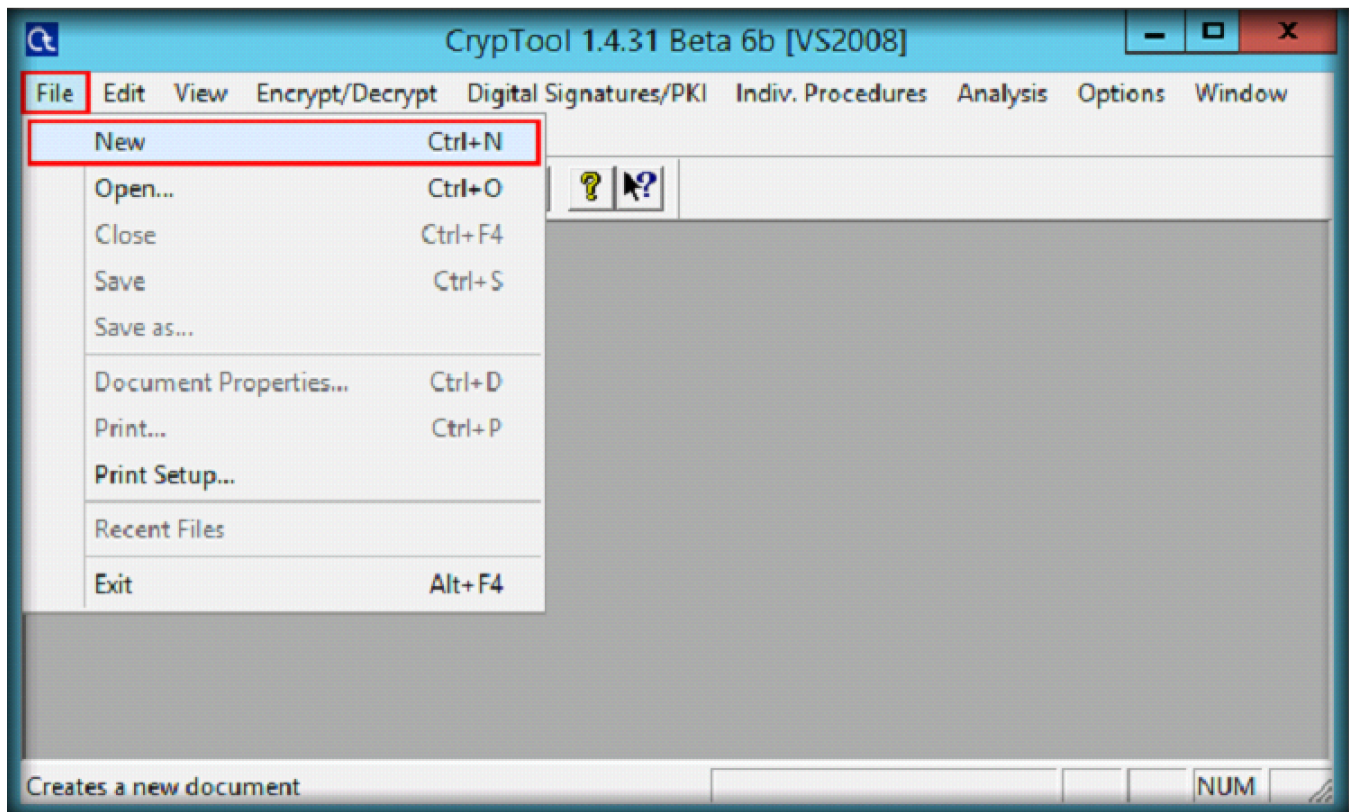


FIGURE 11.4: Choosing a new file to crypt

6. Type some content in the opened **Unnamed1** Notepad of CrypTool. You will be encrypting this content.
7. Select **Encrypt/Decrypt → Symmetric (modern) → RC2...** in the Menu bar.

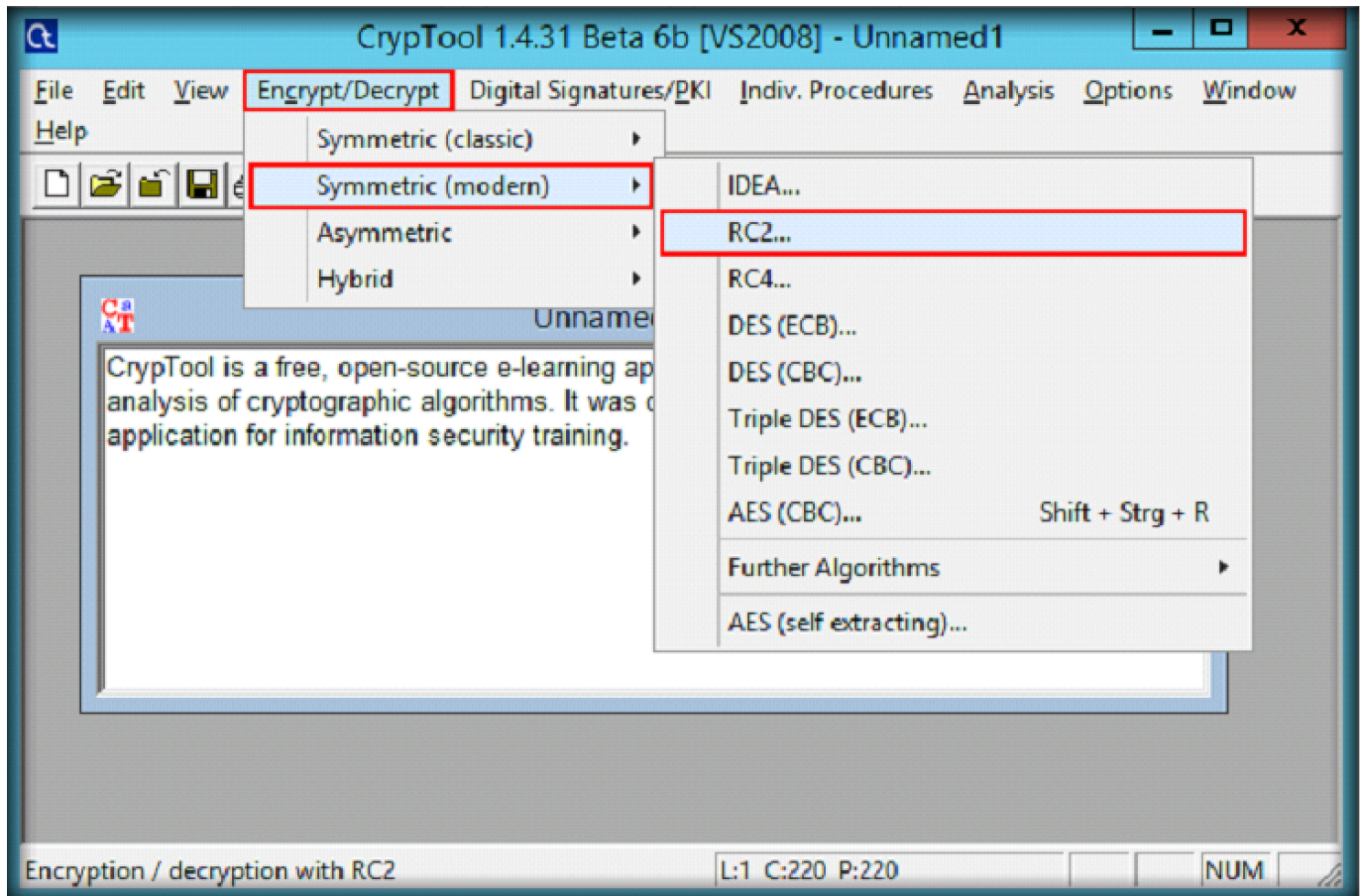


FIGURE 11.5: Encrypting the file

8. The **Key Entry: RC2** dialog box appears; select **Key length** (here, **8 bits**) from the drop-down list.
9. Enter the key using hexadecimal characters (**05**), and click **Encrypt**.

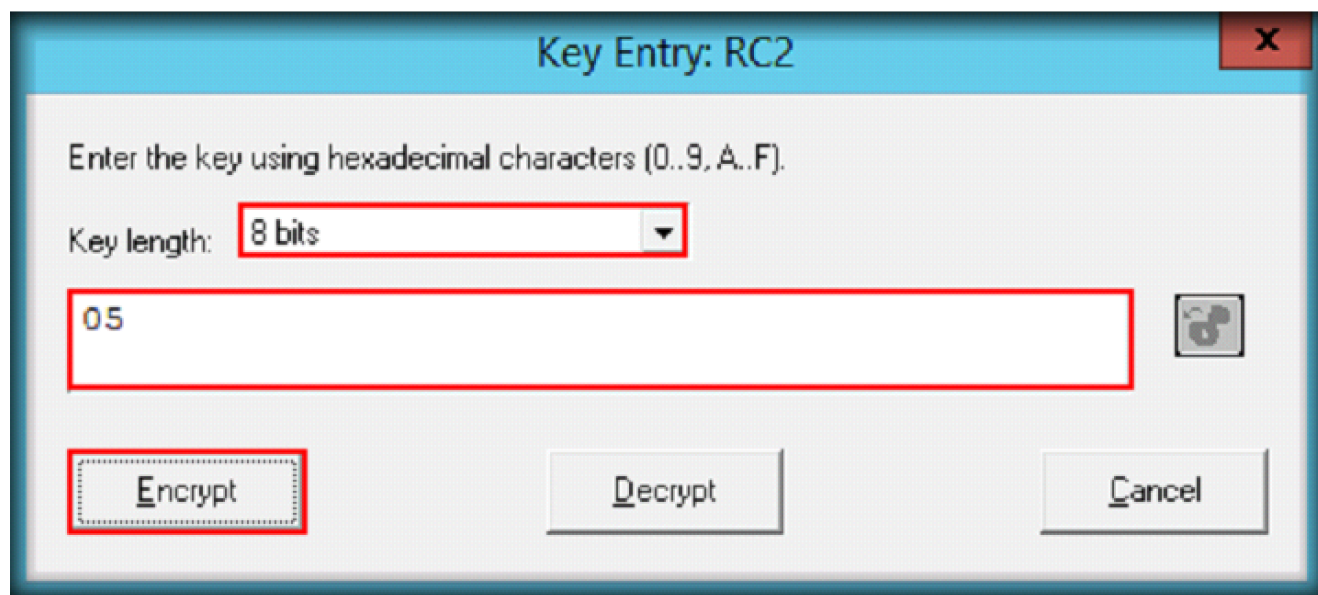


FIGURE 11.6: Encrypting the file

10. The RC2 encryption of **Unnamed1** notepad displays, as shown in the screenshot:

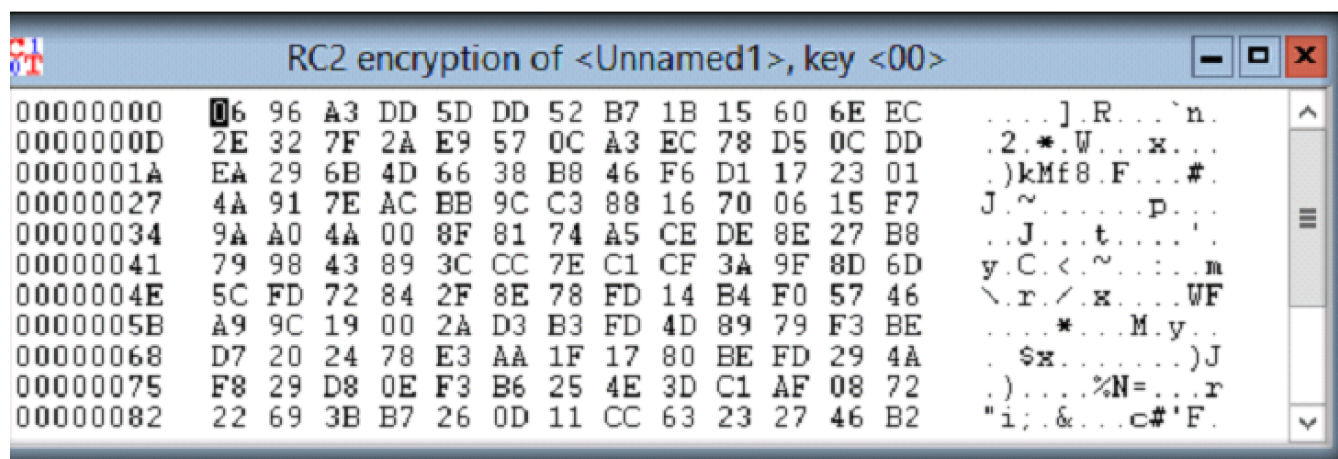


FIGURE 11.7: Output of RC2 - encrypted data

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

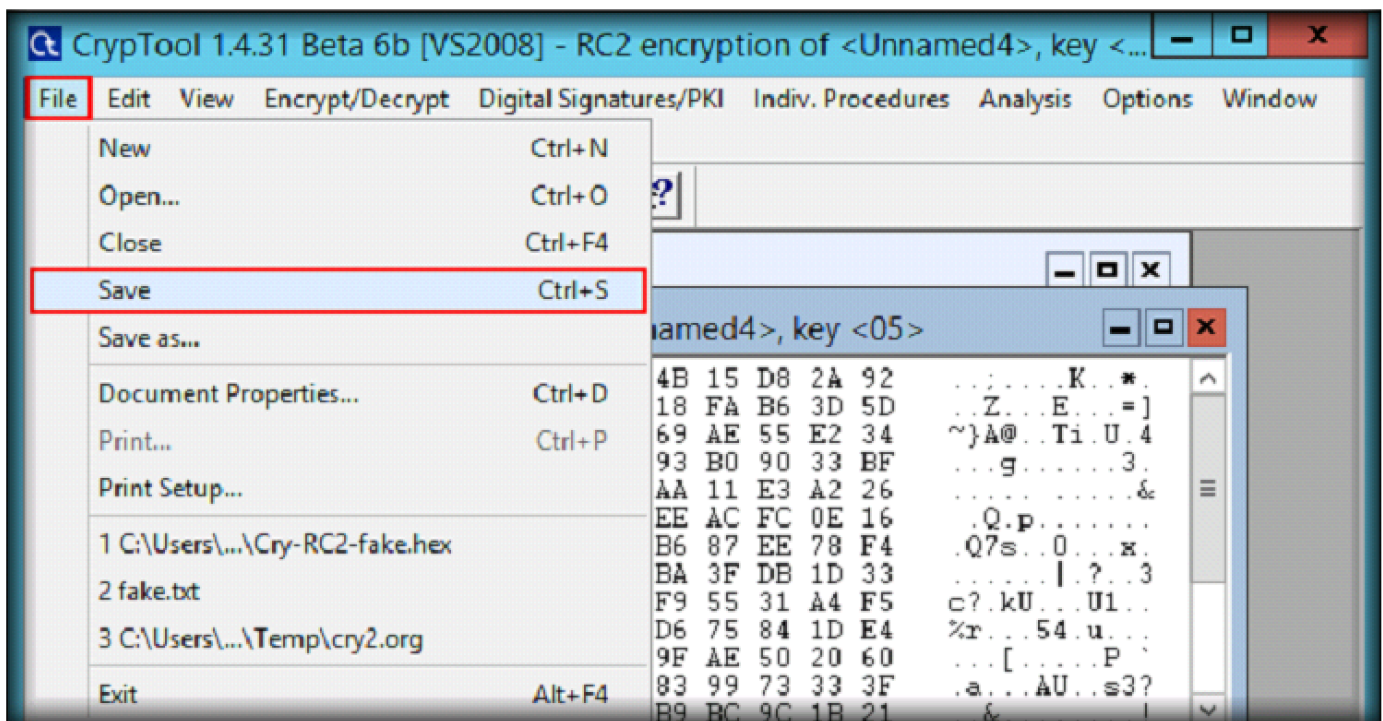


FIGURE 11.8: Saving the encrypted file

12. The **Save As** dialog-box appears; choose a location where you want to save the file (**Desktop**), specify a file name (**Cry-RC2-Unnamed4.hex**), and click **Save**.

Note: The file name may differ in your lab environment.

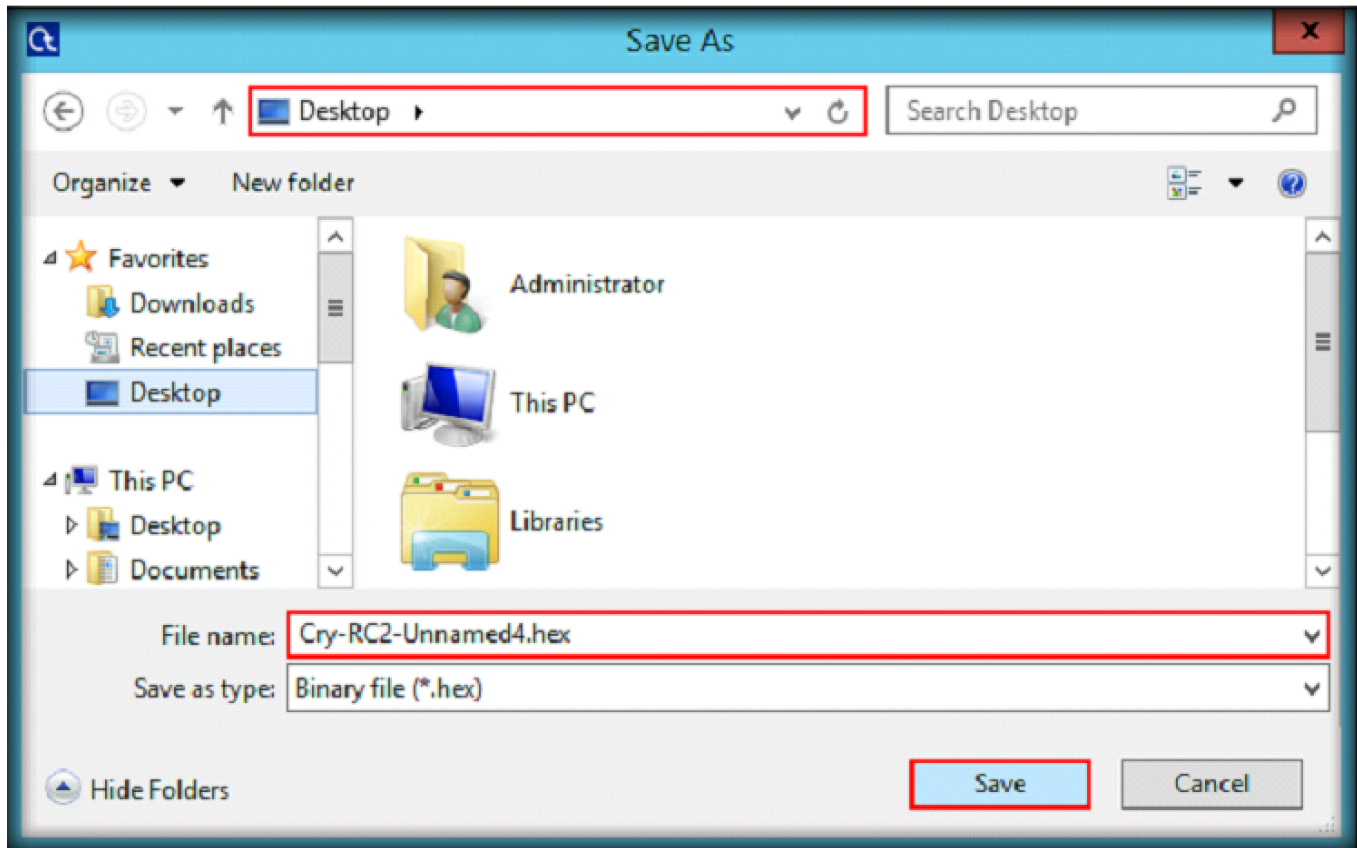


FIGURE 11.9: Saving the encrypted file

13. 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.
14. To share the file, you may copy the encrypted file from the Desktop to **D:\CEH-Tools\CEHv9 Module 18 Cryptography\Cryptanalysis Tools\CrypTool**.
15. Assume that you are the intended recipient (working on Windows 8.1) of the Crypted file through the shared network drive.
16. Log into the Windows virtual machine, navigate to the shared drive on lecturer PC for CrvpTool. double-click **SetupCrypTool_1_4_31_Beta6b_r3670_VS2008_en.exe**, and follow the steps to install the application.
17. In the meanwhile, copy the Crypted hex file (**Cry-RC2-Unnamed4.hex**) from CrypTool on the shared drive on lecturer PC, and save it to the desktop
18. Launch the **CrypTool** application.
19. The **How to Start** dialog box appears; check **Don't show this message again**, and click **Close**.

20. The main window of **CrypTool** appears; close the **startingexample-en.txt** window.

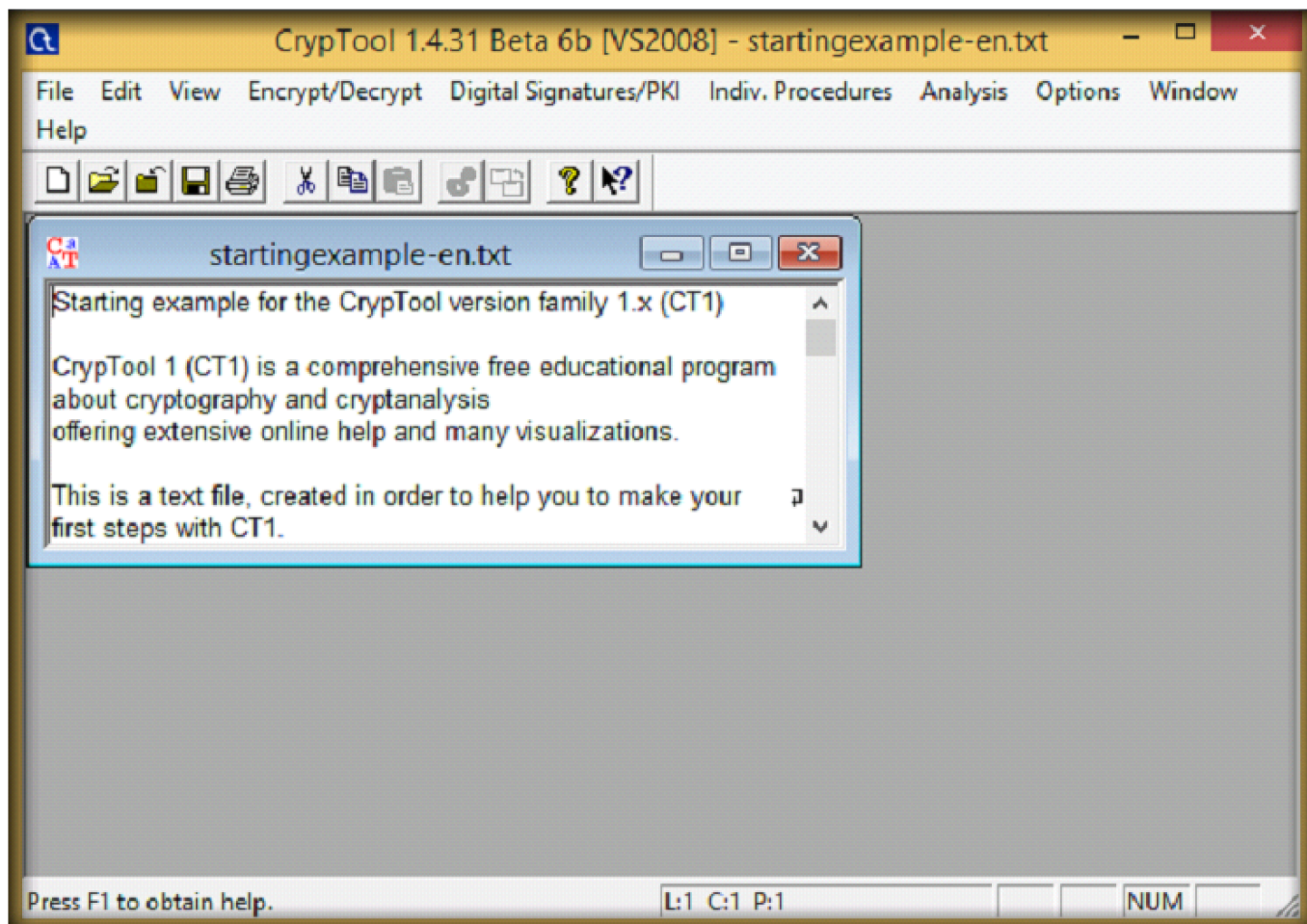


FIGURE 11.10: startingexample-en.txt window in CrypTool

21. To **decrypt** data, click **File** in the menu bar, and select **Open....**

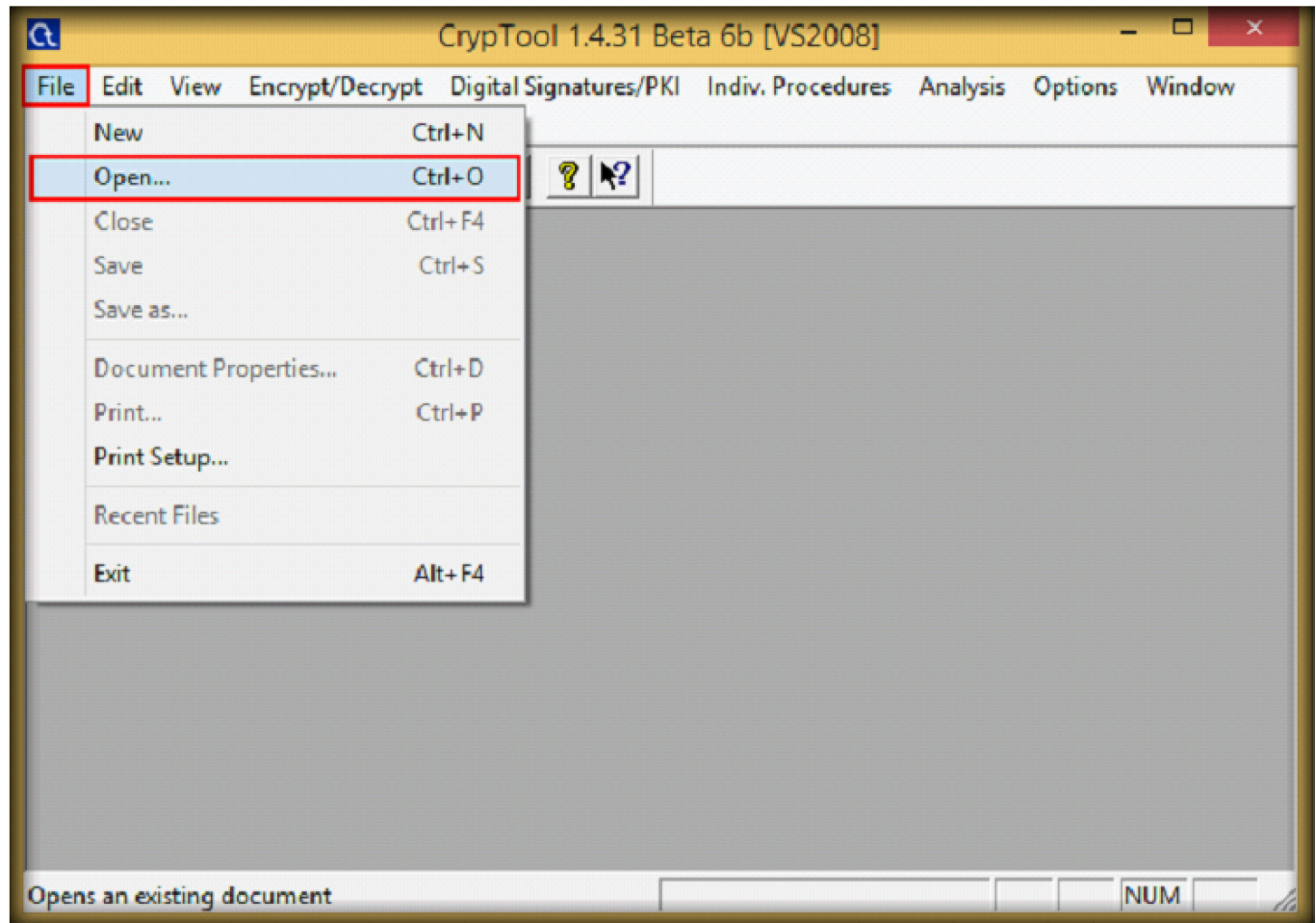


FIGURE 11.11: Opening a Crypted file

22. The **Open** dialog-box appears; select **All files** from the drop-down list, navigate to the location of the file (**Desktop**), select it, and click **Open**.

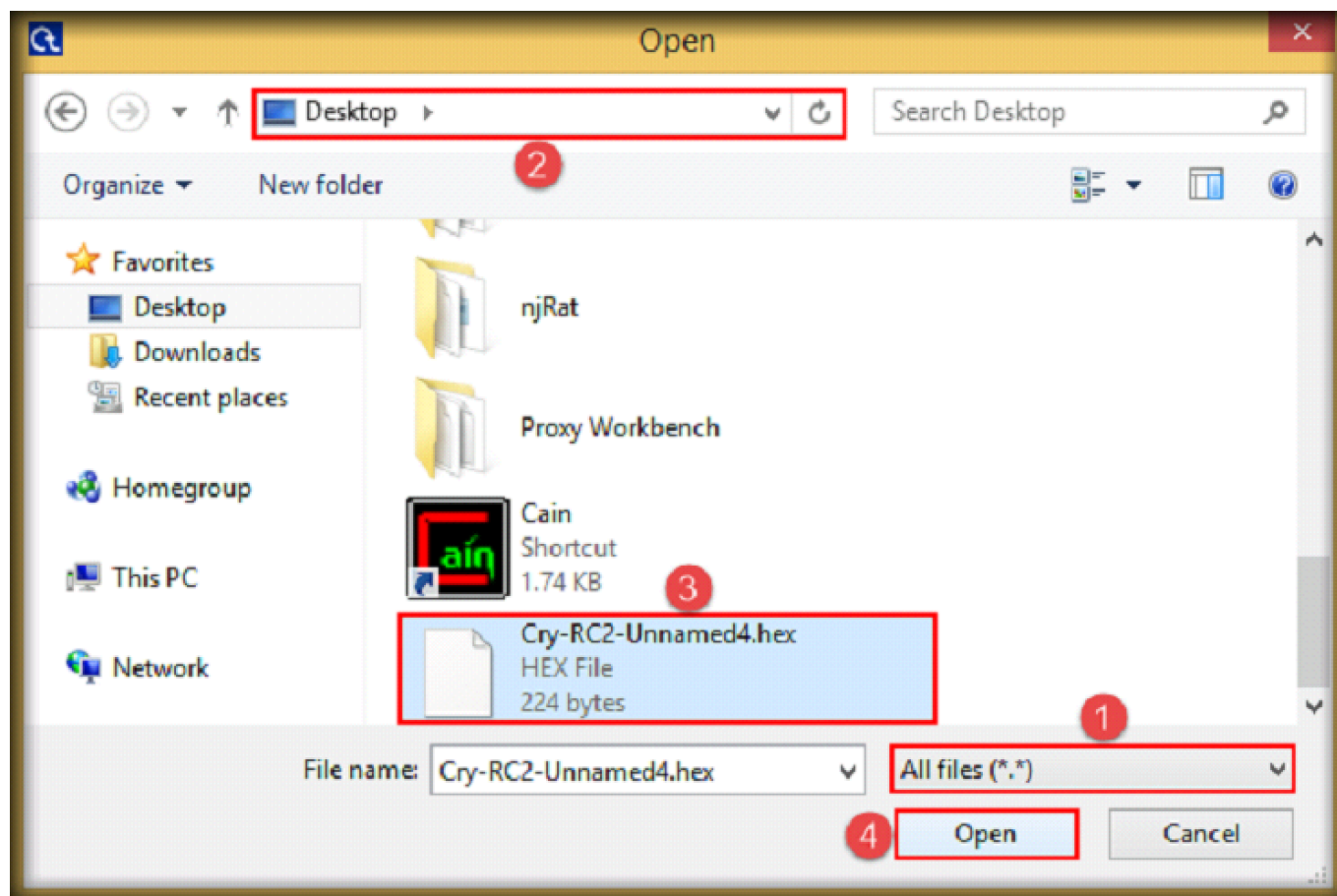


FIGURE 11.12: Opening a Crypted file

23. Select **Encrypt/Decrypt** → **Symmetric (modern)** → **RC2...** from the menu bar.

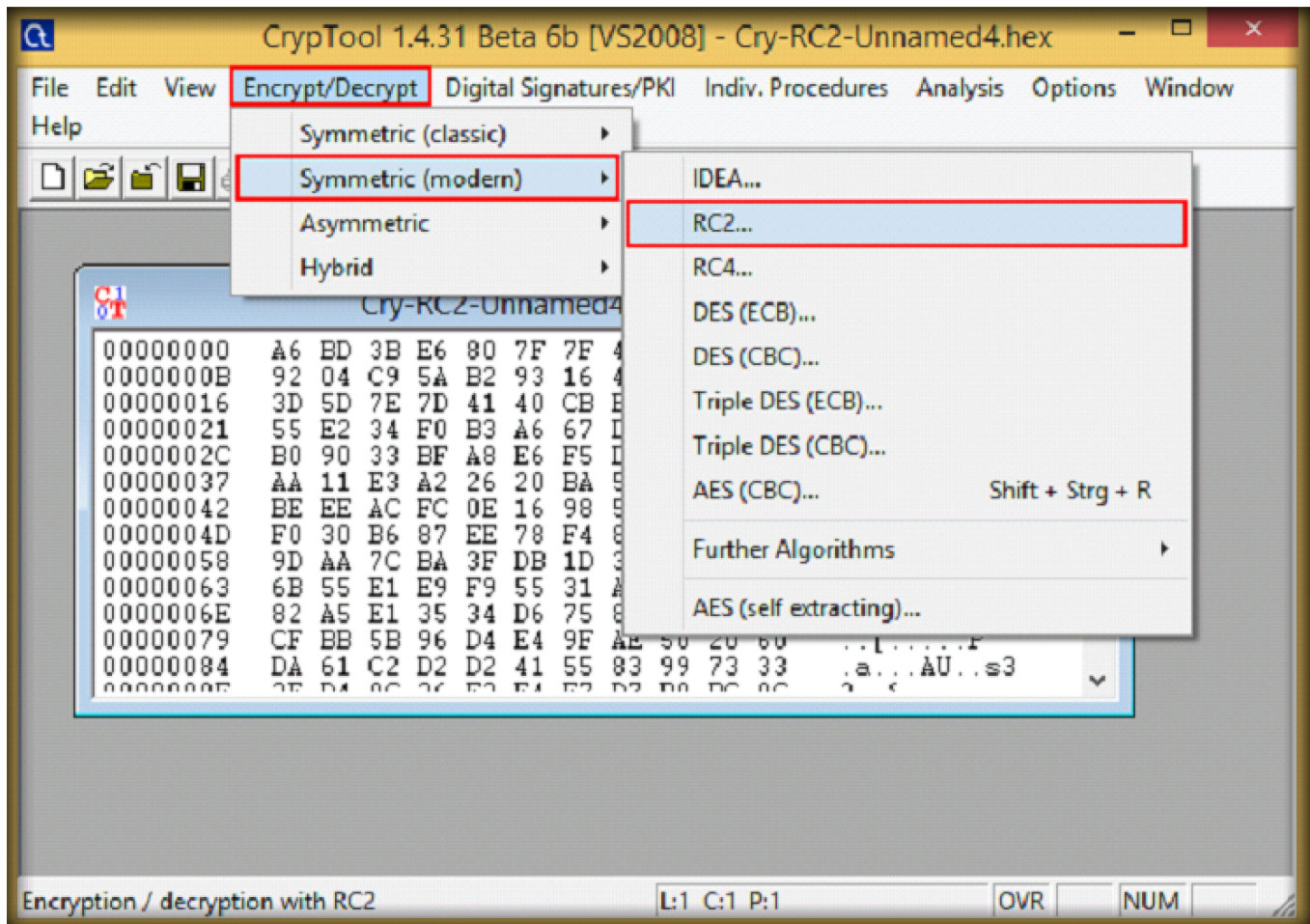


FIGURE 11.13: Select the RC2 Encryption algorithm

24. The **Key Entry: RC2** dialog-box appears; select **Key length** (here, **8 bits**) from the drop-down list.
25. Enter the hexadecimal key (**05**) that was used to encrypt the file, and click **Decrypt**.

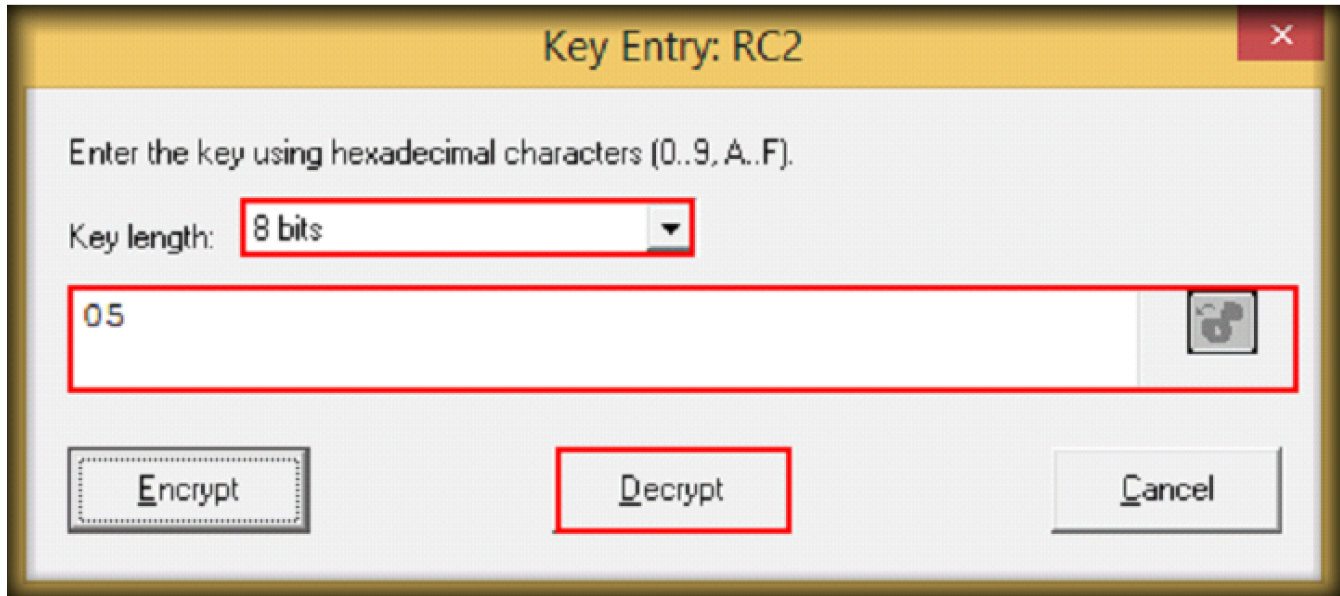


FIGURE 11.14: Decrypting the file

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

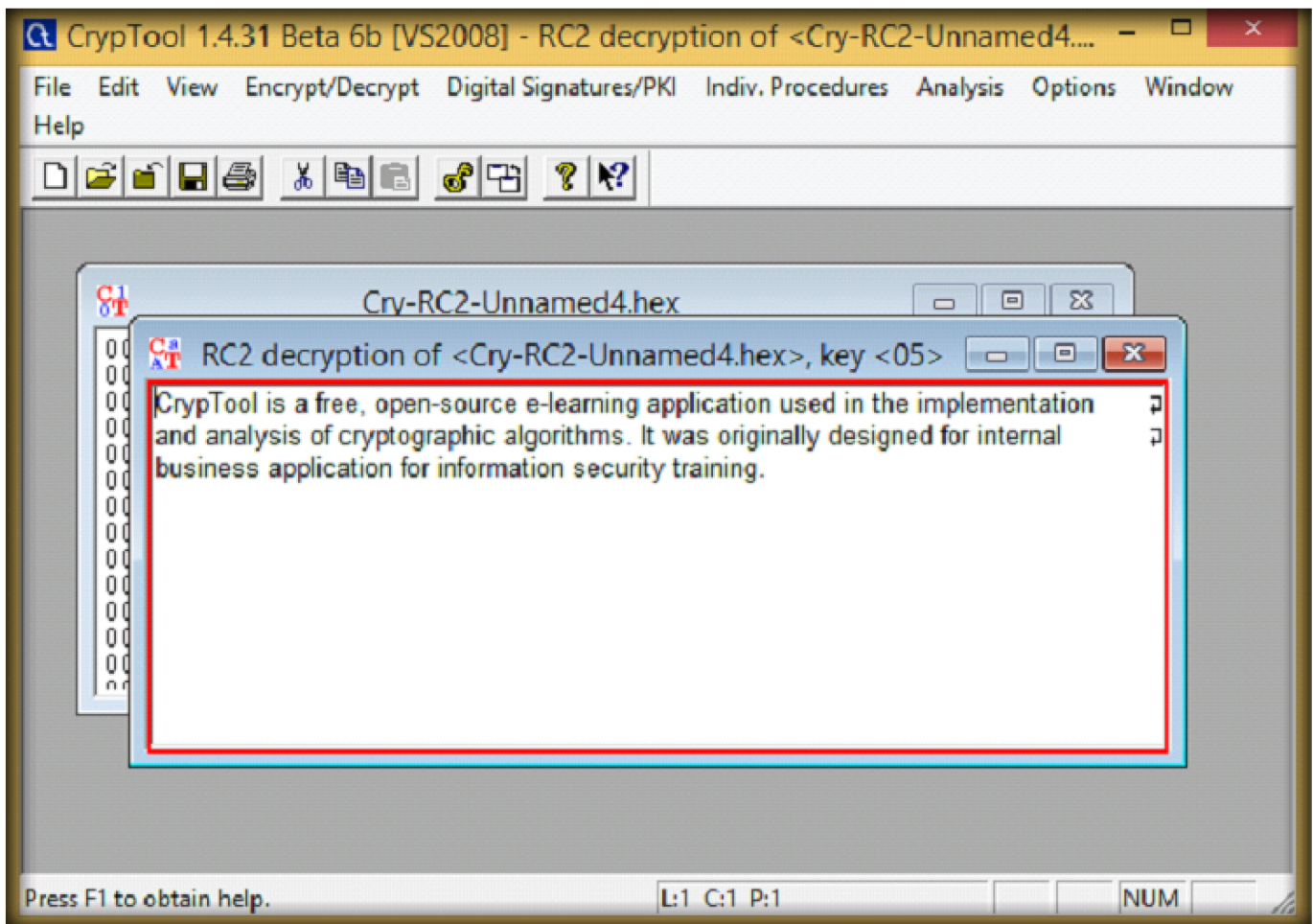


FIGURE 11.15: Decrypted the file successfully

27. This way, files can be encrypted using CryTool and shared with an individual in a secure manner, so that no one can intercept its data.

Lab Analysis

Analyze and document the results related to this lab exercise.