



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



School of
Applied Computing

Advanced Cyber Security (ACS)

Lab – Cryptography

**Wales Institute of Science and Art
Applied Computing
I.Q 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

To attain maximum network security, use strong encryption for all the traffic placed onto the transmission media, without considering its type and location. Attackers tend to focus on easy to compromise targets. If an attacker wants to break into encrypted network, he or she has to face decrypting a whole slew of encrypted packets, which is a difficult task. Therefore, the attacker is likely to move on to try and find another target that is easy to compromise or will simply abort the attempt. Use the latest encryption algorithms that provide strong security. 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 is located on the shared Onedrive https://uowtsd-my.sharepoint.com/:f:/g/personal/carlene_campbell_uwtsd_ac_uk/EgdTO51JxWhFi5BH3KMUwyMBPjDko_uerB1O2XhcAaCl3A?e=u5jUjx

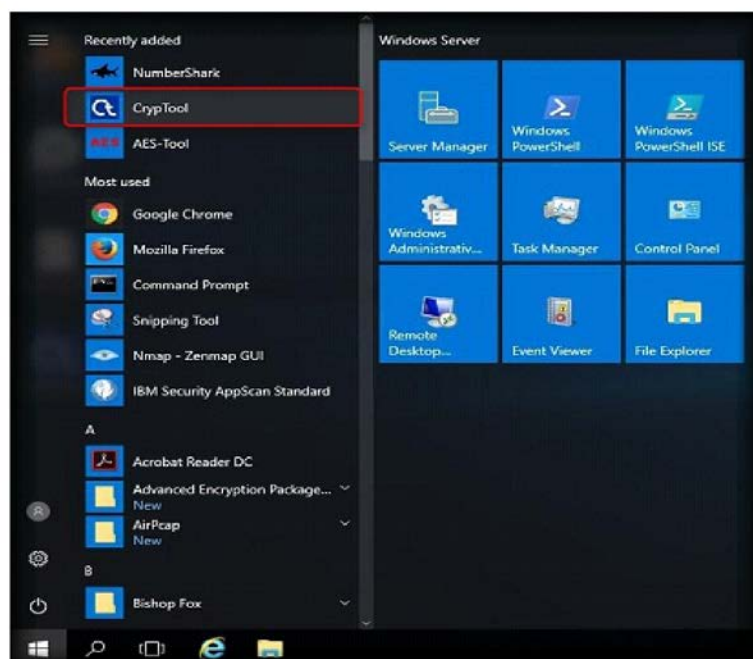
- You can also download the latest version of CrypTool from the link <http://www.cryptool.org/en>
- If you decide to download the latest version, then screenshots shown in the lab might differ
- Windows Server 2016 running on host machine
- Windows 10 running on virtual machine
- Administrative Privileges to run the tool

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:

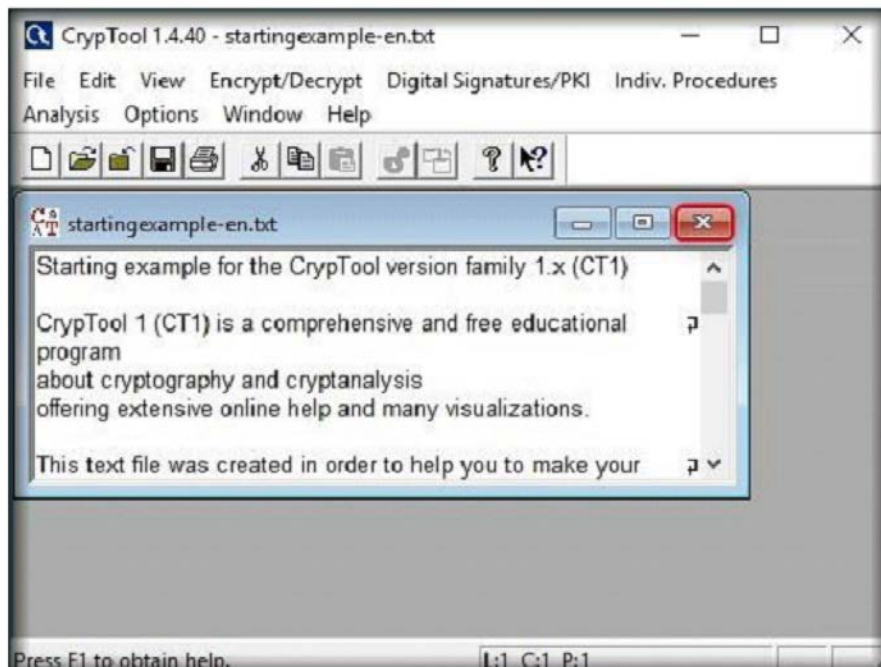
1. Navigate to https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uowtsd_ac_uk/EgdTO51JxWhFi5BH3KMUwyMBPjDko_uerB1O2XhcAaCI3A?e=u5jUjx for CrypTool, double-click **SetupCrypTool_1_4_40_en.exe**, and follow the wizard driven installation steps to install the application.
2. On completing the installation, launch **CrypTool** application from the **Apps** list.



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



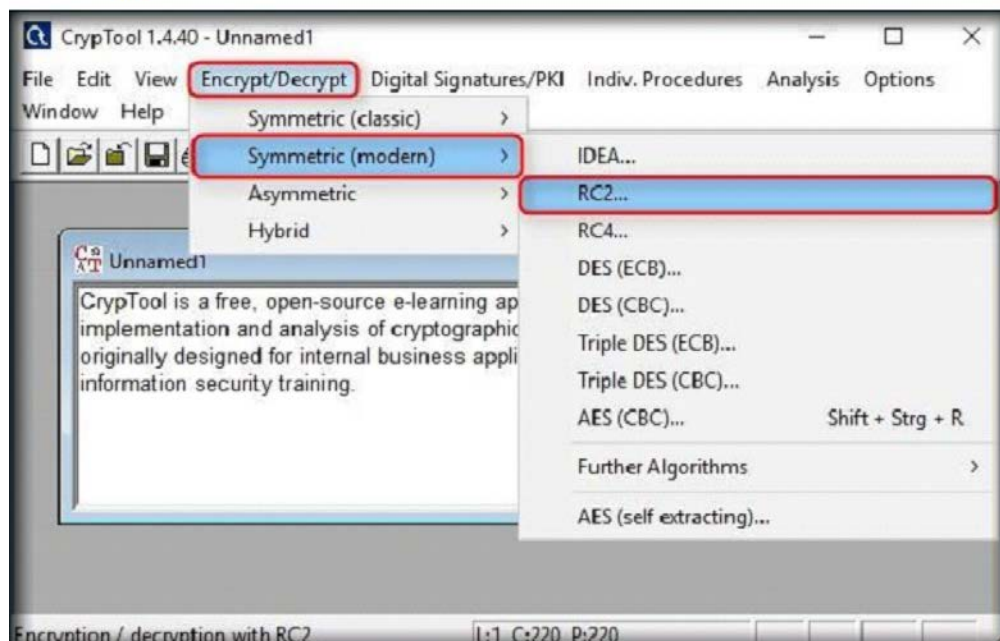
4. The main window of **CrypTool** appears; close the **startingexample-en.txt** window.



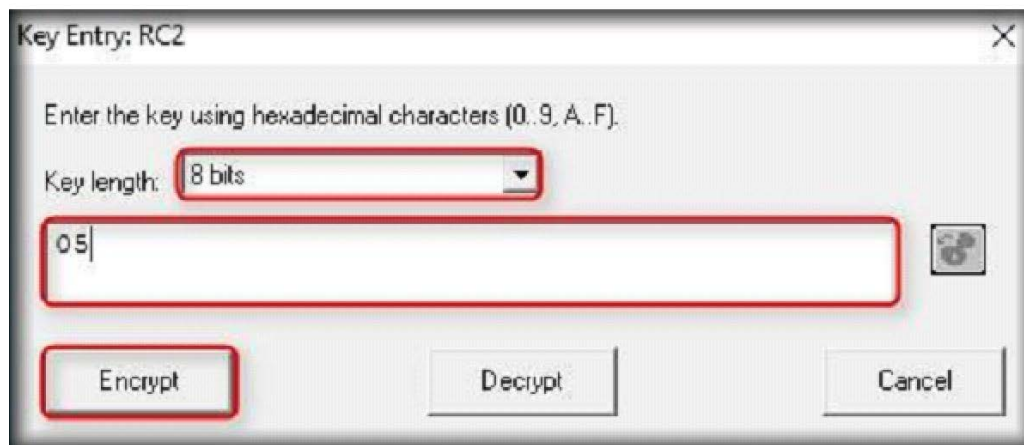
5. To **encrypt** data, click the **File** option from the menu bar, and select **New**.



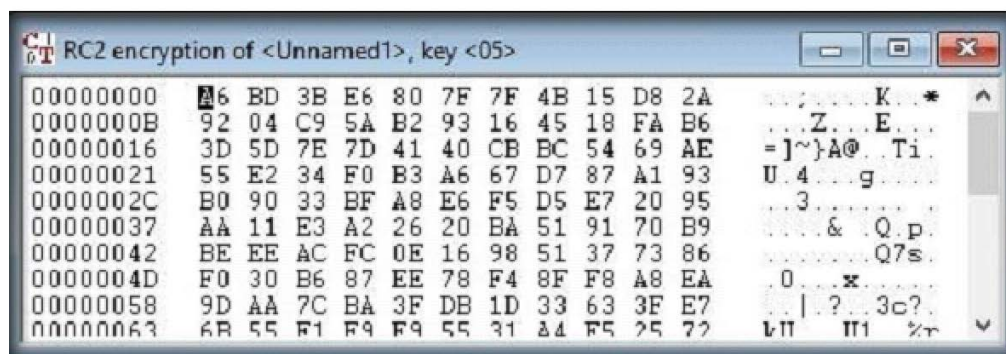
6. Type some content in the opened **Unnamed1** Notepad of CrypTool. You will be encrypting this content.
7. Select **Encrypt/Decrypt** → **Symmetric (modern)** → **RC2...** in the Menu bar.



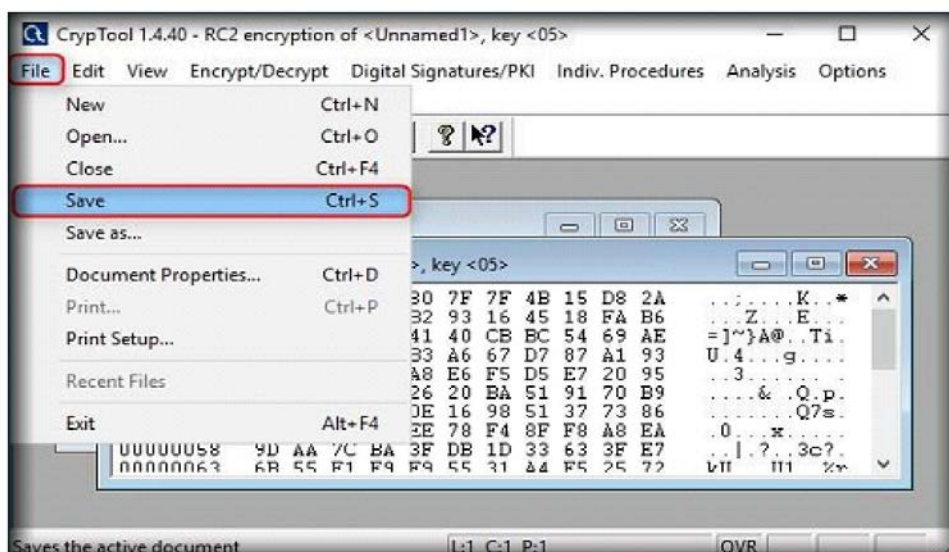
8. The **Key Entry: RC2** dialog box appears; select **Key length** (here, **8 bits**) from the drop-down list.
9. Enter the key using **hexadecimal characters (05)**, and click **Encrypt**.



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

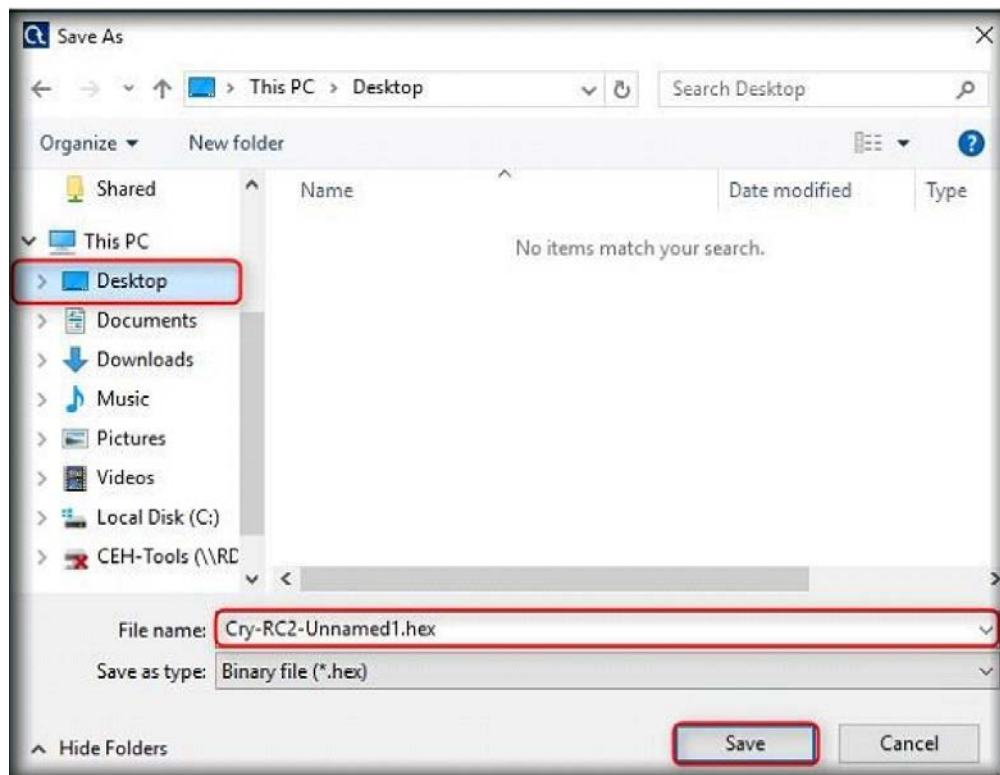


11. To save the file, click **File** in the menu bar, and select **Save**.



12. The **Save As** dialog-box appears; choose a location where you want to save the file (**Desktop**), specify a file name (**Cry-RC2-Unnamed1.hex**), and click **Save**.

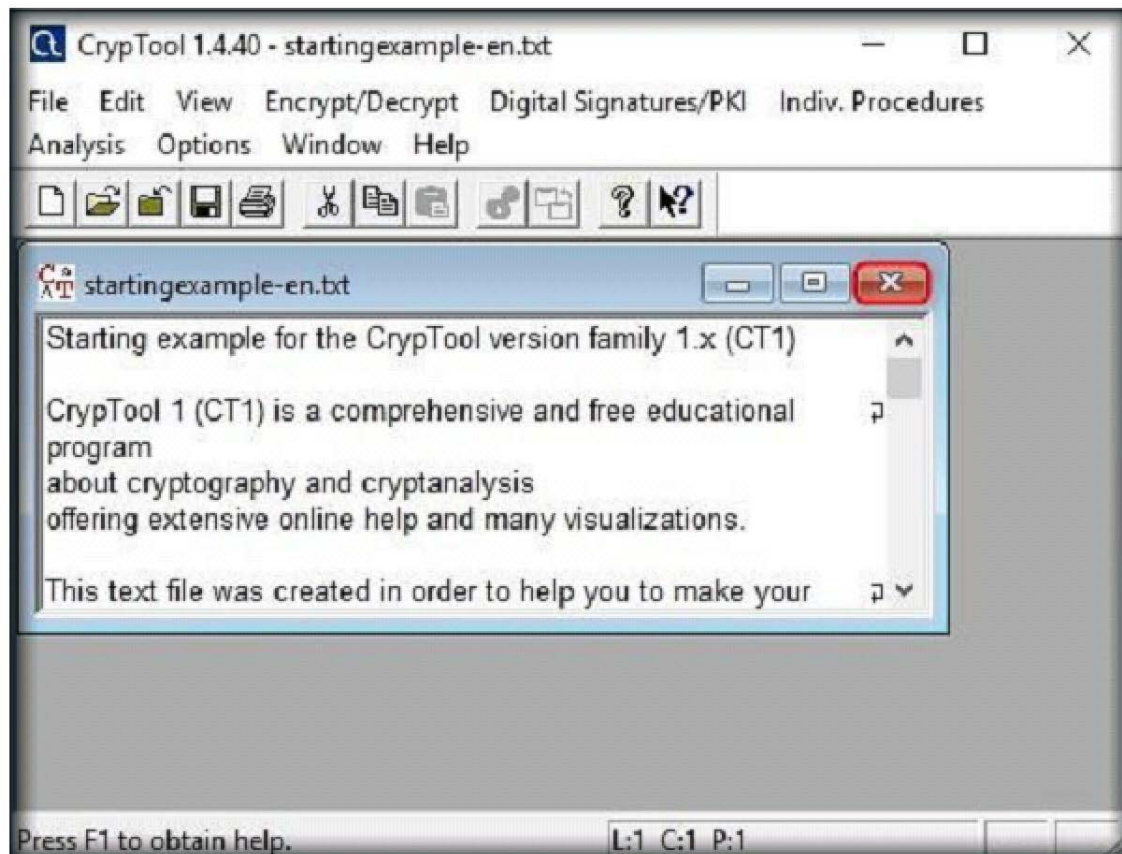
Note: The file name may differ in your lab environment.



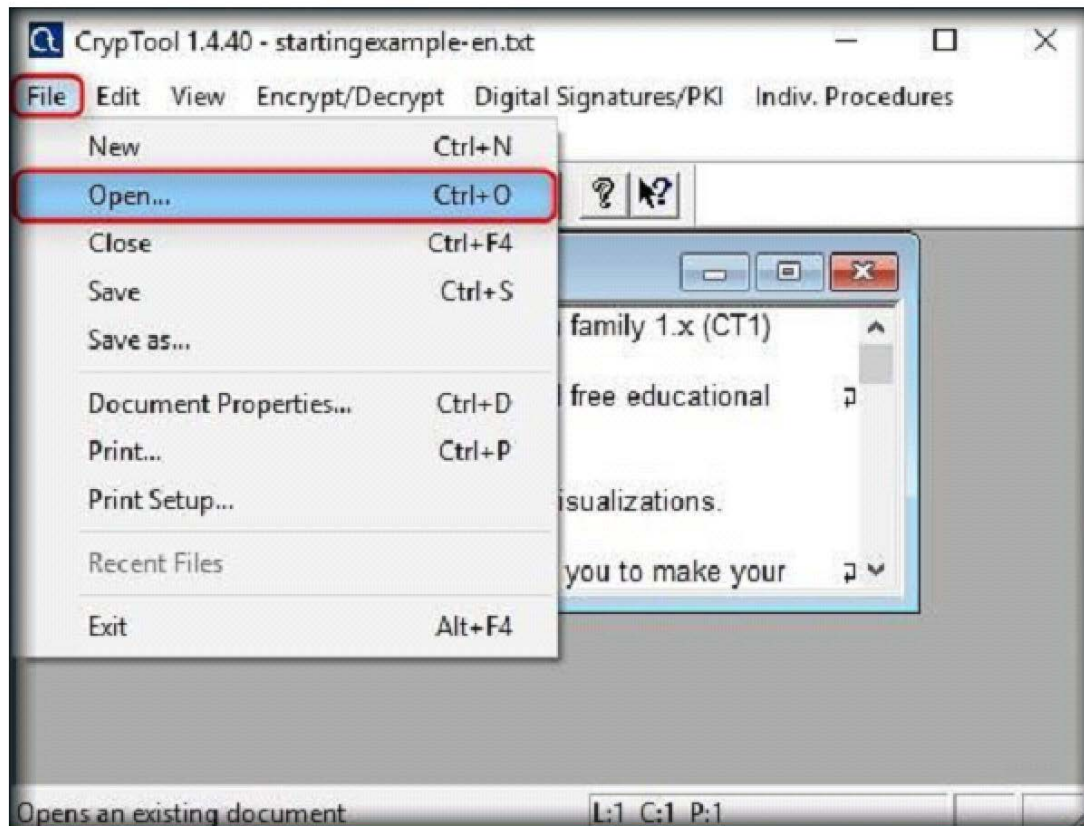
13. Now, you can send this file to the intended person by email or any other means and provide him/her with the hex value, which will be used to decrypt the file.
14. To share the file, you may copy the encrypted file from the Desktop to https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uwtsd_ac_uk/EgdTO51JxWhFi5BH3KMUwyMBPjDko_uerB1O2XhcAaCI3A?e=u5jUjx
15. Assume that you are the intended recipient (working on Windows 10) of the Crypted file, through the shared network drive.
16. Log into **Windows 10** virtual machine, navigate to https://uowtsd-my.sharepoint.com/:f/g/personal/carlene_campbell_uwtsd_ac_uk/EgdTO51JxWhFi5BH3KMUwyMBPjDko_uerB1O2XhcAaCI3A?e=u5jUjx double click SetupCrypTool_1_4_40_en.exe, and follow the steps to install the application.
17. In the meanwhile, copy the Crypted hex file (**Cry-RC2-Unnamed4.hex**)

from https://uwotds-my.sharepoint.com/:f/g/personal/carlene_campbell_uwotds_ac_uk/EgdTO51JxWhFi5BH3KMUWyMBPjDko_uerB1O2XhcAaCI3A?e=u5jUjx and save it to Desktop.

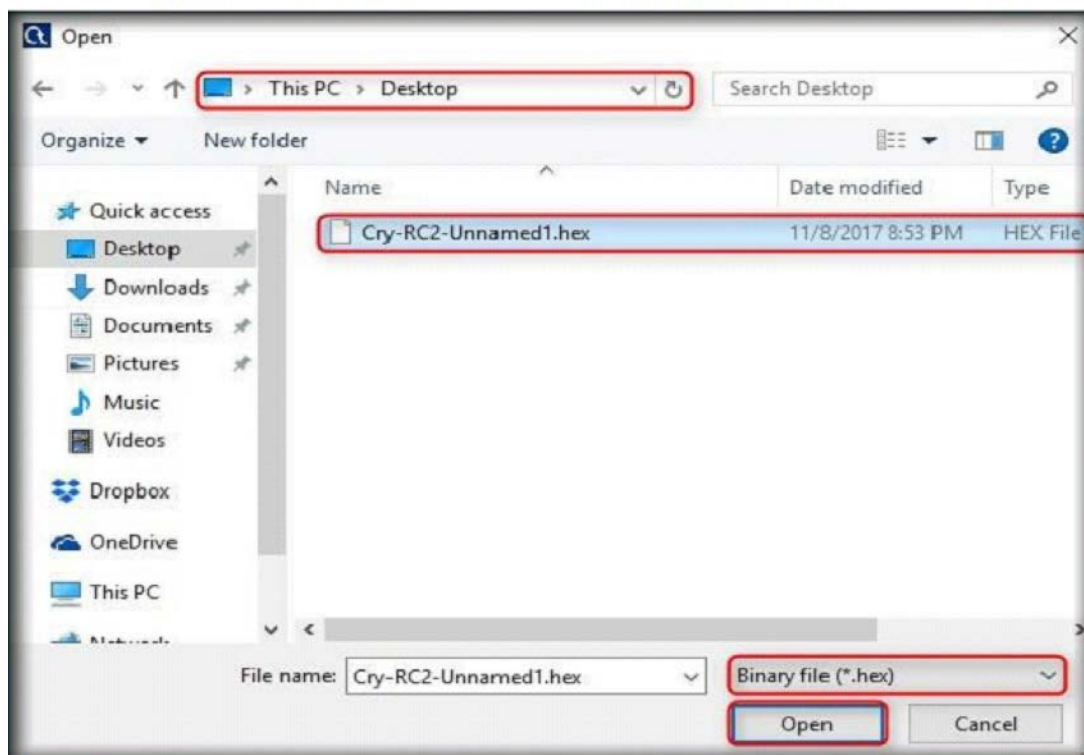
18. Launch the **CrypTool** application.
19. The **How to Start** dialog box appears; check **Don't show this dialog again**, and click **Close**.
20. The main window of **CrypTool** appears; close the **startingexample-en.txt** window.



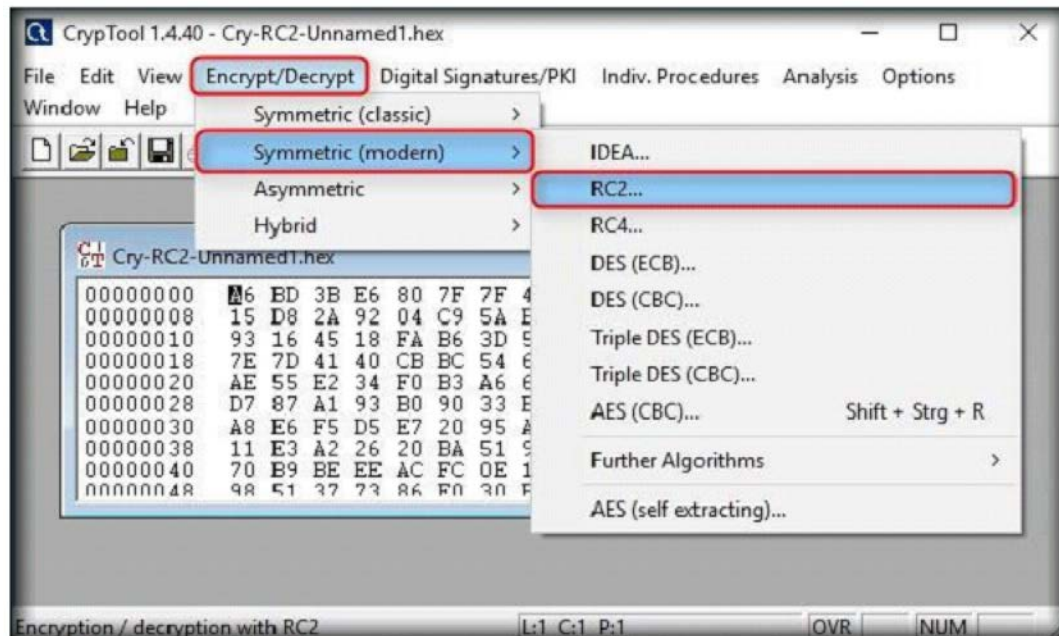
21. To **decrypt** data, click **File** in the menu bar, and select **Open....**



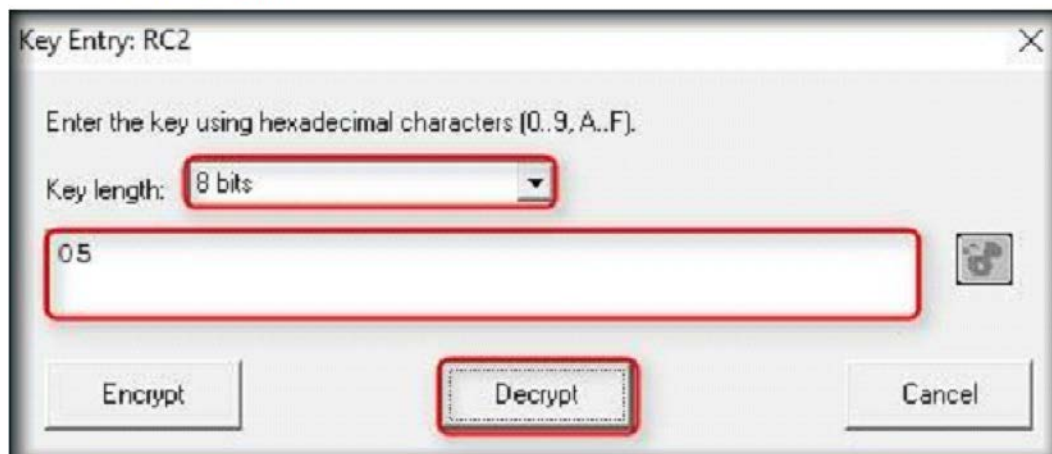
22. The **Open** dialog-box appears; select **All files** from the drop-down list, navigate to the location of the file (**Desktop**), select it, and click **Open**.



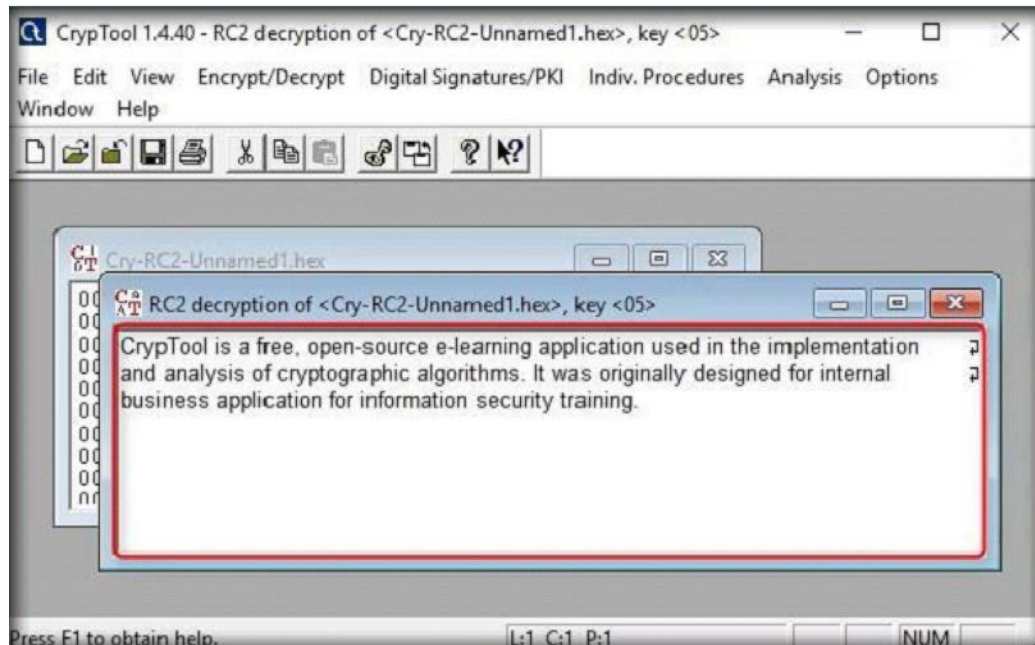
23. Select **Encrypt/Decrypt** → **Symmetric (modern)** → **RC2...** from the menu bar.



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**.



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



27. This way, files can be encrypted using CrypTool 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.