Symmetric Algorithms

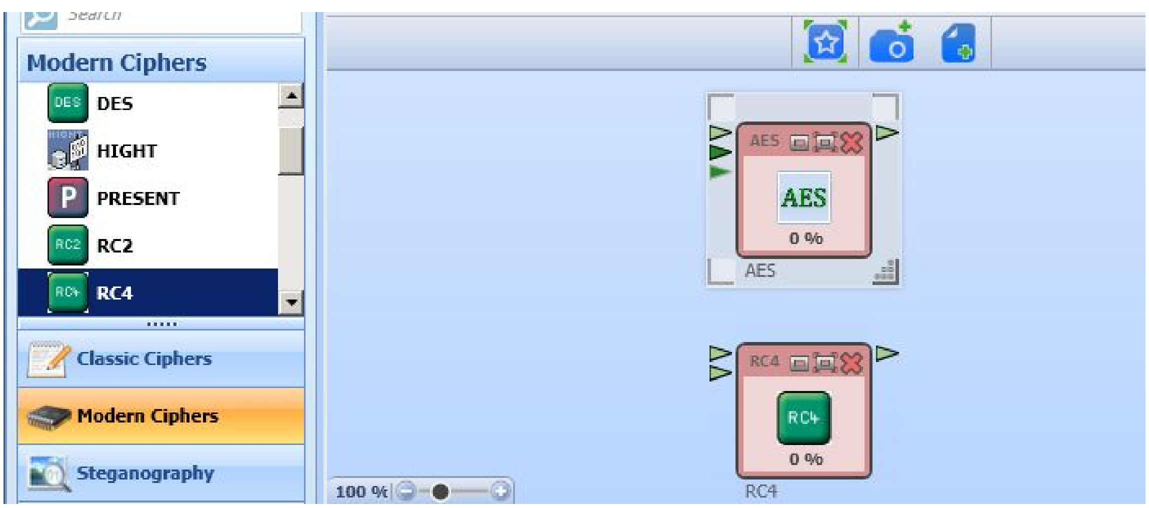
Learning Objectives: In this exercise, you will learn to test cryptographic strength of various symmetric ciphers.

Summary: You will use CrypTool 2.0 for this exercise.

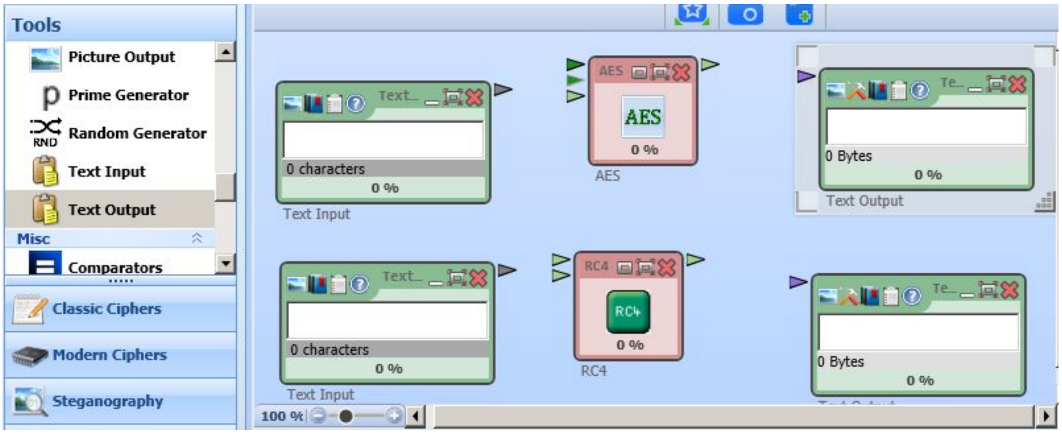
Deliverables: Submit a lab report by answering the review questions. In some review questions, you may provide screen captures.

Comparing RC4 and AER Cipher

1. Start CrypTool 2.0 via the **Desktop Shortcut** or **Start menu.**.
    a. (Start > Programs > CrypTool > CrypTool 2.0).
2. Under the **Home** tab, select new to create a new workspace.
3. Next you will need to go to the **Modern Ciphers** row. Drag and drop both the **AES Cipher** and the **RC4 Cipher** into your workspace.

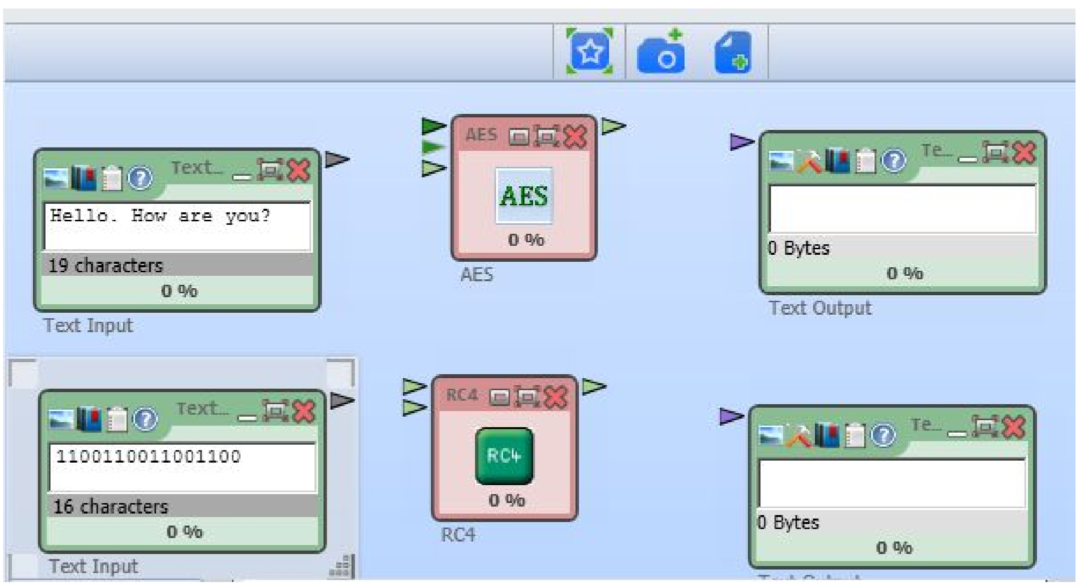


4. Now you will need to go to the **Tools** row. In the tools drag two text input boxes and two text output boxes into the workspace.

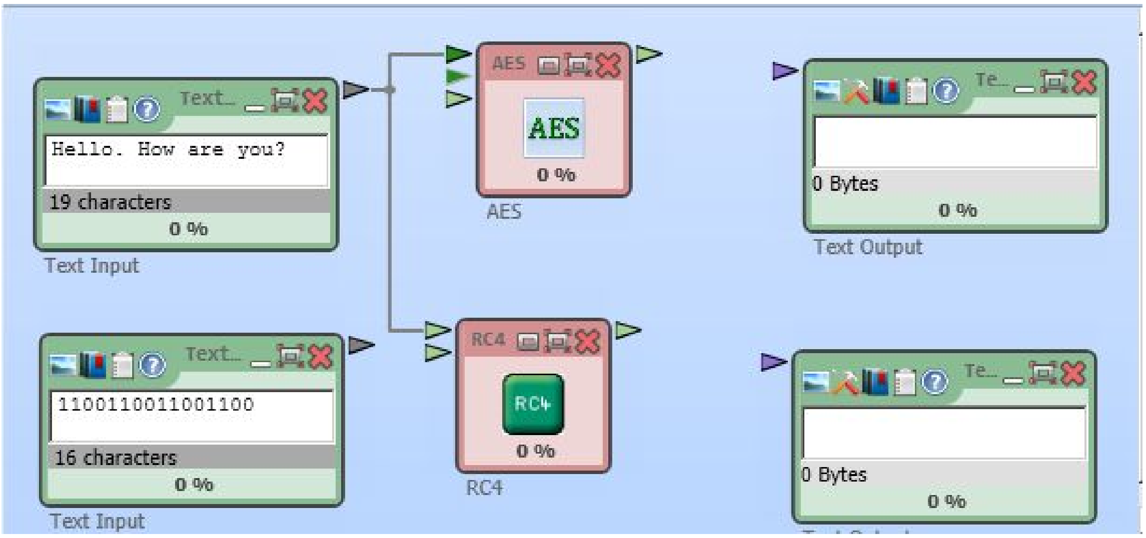


5. Now you will write something simple in the first text input box. In this example, "**Hello. How are you?**" was used.

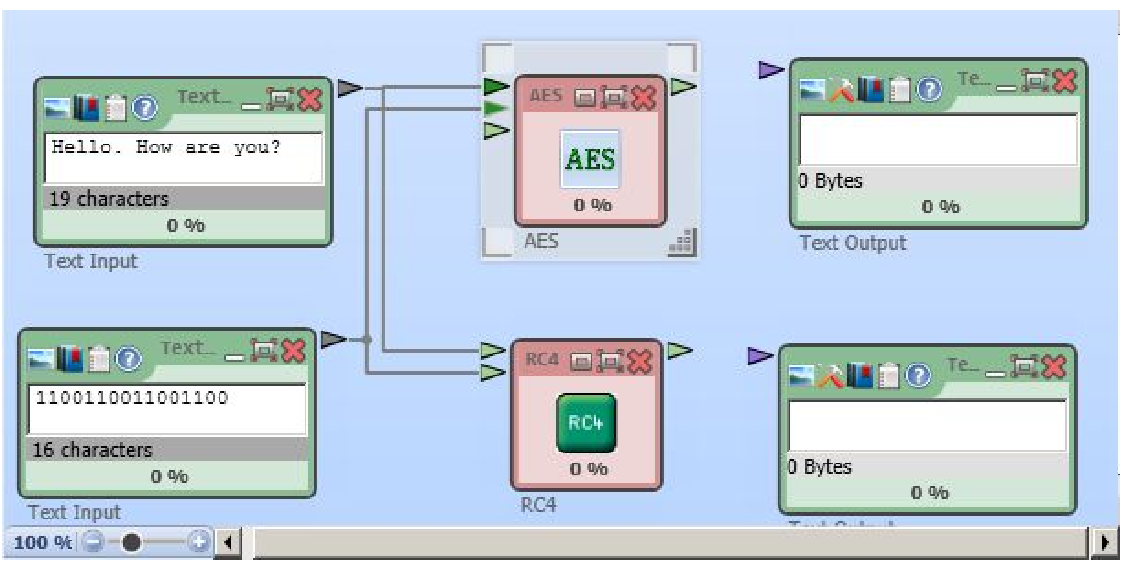
6. In the second text input box you will enter a key. Use **1100110011001100**.



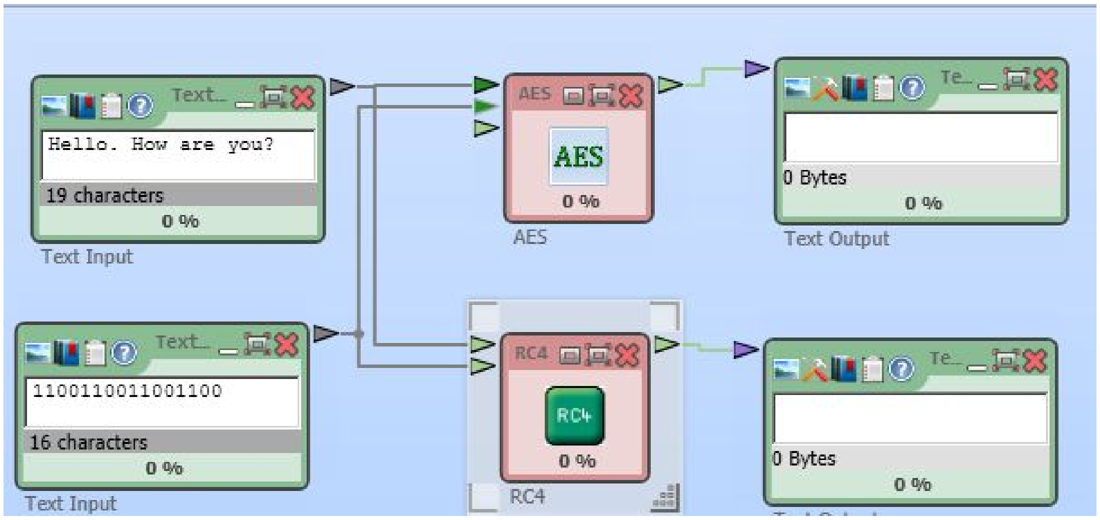
7. Now you will need to attach the boxes to each other. Start by connecting the **first text input** box to the **first arrow** on both the **RC4** and **AES Ciphers**. See the image below.



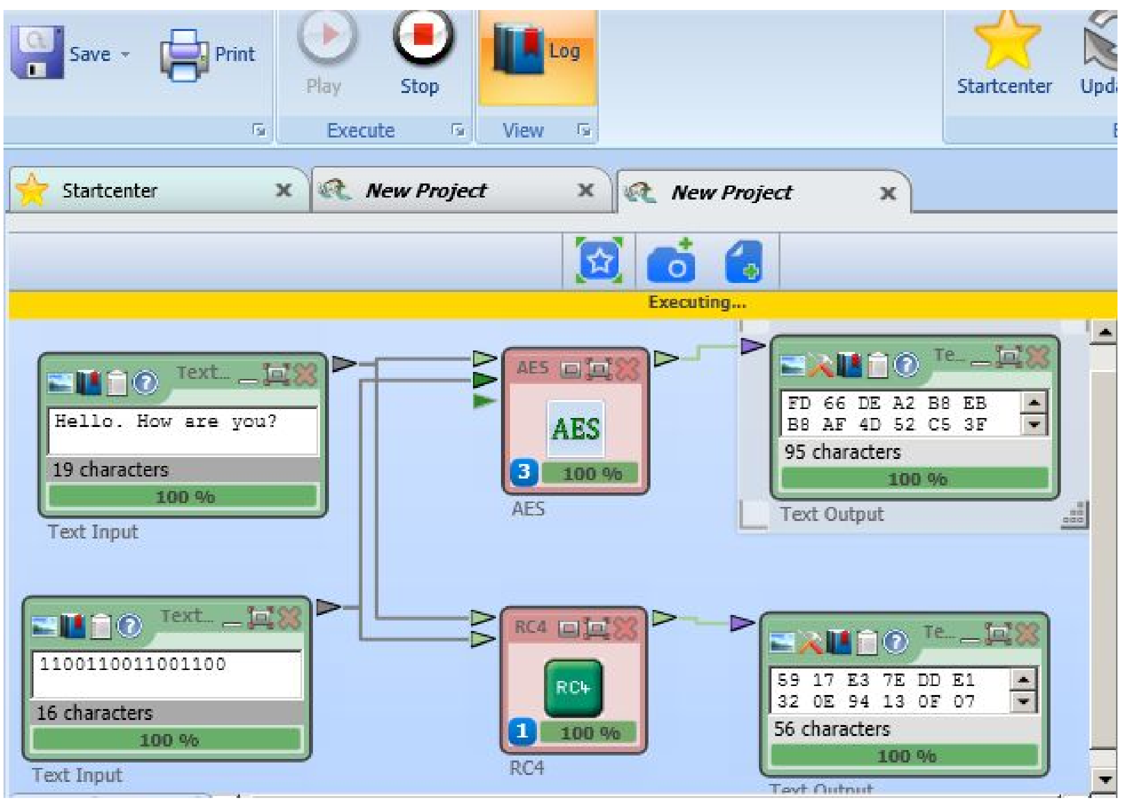
8. Next you will connect the **KEY** to the **second arrow** on both the **RC4** and **AES Cipher**.



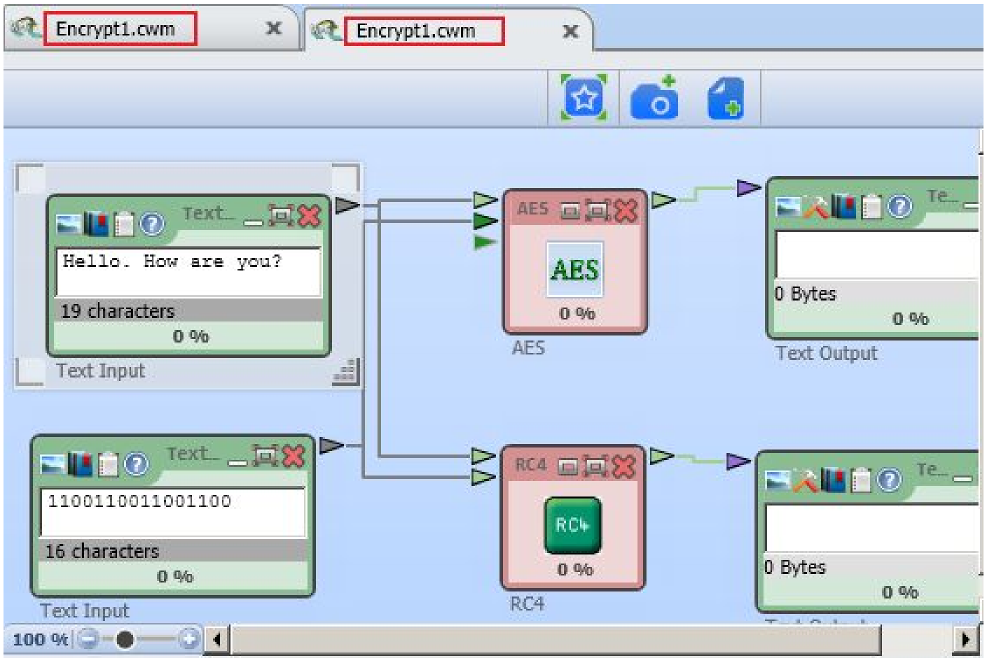
9. Connect the **AES Cipher** to the **first text output box** and the **RC4 Cipher** to the **second text output box**.



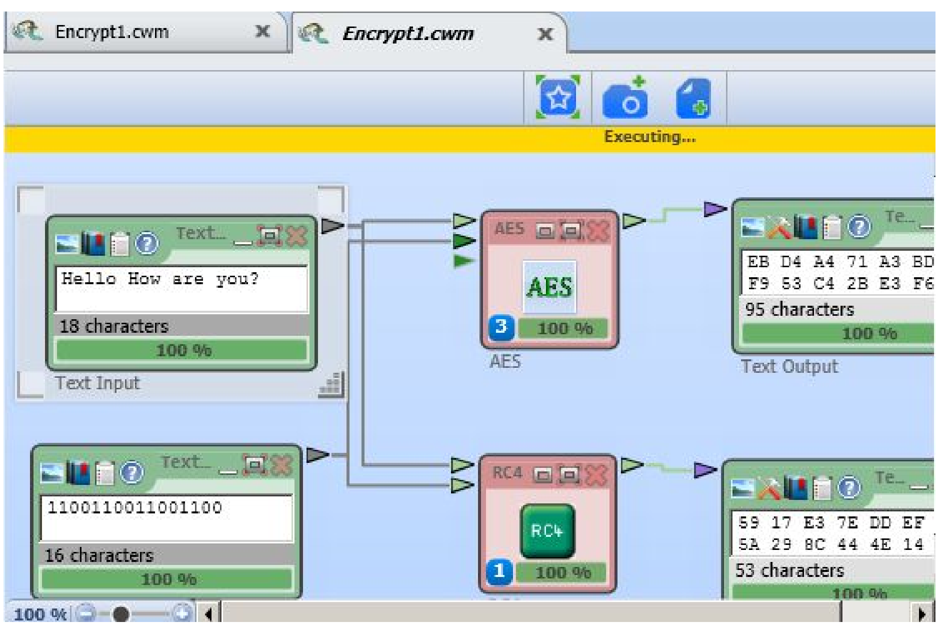
10. Now you can press **Play** to encrypt the text. The Cipher Encryptions will appear in their respective text output boxes.



11. Save the project as **Encryption1** to the desktop and open it a second time. You should have two of the same project up as in the image below.



12. In the **second Encryption1 project**, remove the period behind Hello and press play to encrypt. Compare the two projects.



13. Leave both projects up and answer the questions below.

Review Questions (to be submitted)

- How much similar the ciphertext of the original file to the ciphertext of the modified file of each Cipher type?
- What are your observations from this experiment? Does RC4 or AES significantly modify the ciphertext even for minor changes in the message? Why might this be a desired future of a cipher?
- Try another experiment as follows. This time do not change the message, but change a single bit of the secret key. Does the ciphertext significantly change when you change a single bit of the key in RC4 and AES. Summarize your findings.