Lab 4 - Cryptography

- This is an assignment, and worth 2 points.
- The due date is <mark>the same day midnight</mark>. It will be graded as pass/fail (2 or 0 points).

Answer the following questions.

1. Were you able to crack the text encrypted with Caesar/Rot-13 using Analysis > Symmetric Encryption (classic)?   (Y   /   N   )

   Yes

2. How long did it take to brute force the key for the text encrypted with DES (ECB) when the last four hex codes of the key are not known?

   It took about 45 seconds to a minute for the 3 brute-force analysis to run, and then it prompted me with the "Accept Selection" box.

3. How long did it take to brute force the key for the text encrypted with Reijndael (AES) when the last four hex codes of the key are not known?

   I did not finish the brute force search because of time constraints, but it prompted me with a message saying it would take about 2 hours and 45 minutes.

4. Were you able to verify the digital signature? (Y   /   N   )

   Yes

5. Are the hash values for CrypTool 1.4.41 (what you have calculated and the one on the cryptool.org website) the same? (Yes   /   No   )

   Yes