# Crypto Lab Tasks

Name: \_\_\_\_William Brown\_\_\_\_\_\_\_\_\_\_\_

Answer the following questions. (each 2 points)

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

Yes, I was able to encrypt the text with the Caesar/Rot-13 and using the analysis I was able to decrypt back to normal text.

1. 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?

About 2 seconds

1. 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?

About 1 second

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

Yes I was able to verify my digital signature by creating the key pairs and a pin, and concurrently signing the document with my digital signature. Finally I was able to verify the signature as mine.

1. Are the hash values for CrypTool 1.4.30 (what you have calculated and the one on the cryptool.org website) the same? ( Yes / No )

It isn’t the same due to the hash, and I hashed with MD5 instead of Sha256 and ended with a different end result.