In this laboratory, you will use some features of OpenSSL in a Linux environment and do some relevant reading and investigation. In Linux the “man openssl” command can be used to get some basic information about OpenSSL. You can also use Internet to get information about it. For the lab, you should also know about the script command in Linux, that lets you record your entire session in a default file called “typescript”. Note that multiple uses of the command may erase the previous contents, so you should learn to give your own file names. Again use “man script” to figure out how to do that. You will have to turn in a recoding of all the commands you use for the following exercises.

1. First, use the pseudorandom number generator in OpenSSL to generate a key of 192 bits that will be used for the following exercises. Does OpenSSL allow you to use a seed for this purpose? If so, choose your seed carefully and justify your choice in your submission.

2. Use OpenSSL to compare DES, 3DES and AES encryption (with and without CBC mode) of the message “Betty bought a bit of butter, but the butter was bitter, so Betty bought a bit of better butter to make the bitter butter better butter” and a 1-page English text document of your choice. Choose your document carefully so that you can compare and contrast the three algorithms and justify your choice in your submission. For DES use the 1st 56 bits of the 192 bit key that you generated in item 1 above. For 3DES use the appropriate number of bits starting from the leftmost bit of the same 192 bit key and for AES use the whole 192 bit key if possible in OpenSSL. After you have encrypted the message and the chosen document, you need to answer the following questions: (i) How did you convert the message and the text document into blocks of bits for encryption? Explain. (ii) How many bits out of 192 bits were you able to use for 3DES and why? Same question for AES. (iii) Based on the message given and the document you chose for encryption, can you differentiate between the level of security provided by the six different methods? For this compare first the non-CBC versions against one another, then the CBC versions against one another and finally the non-CBC version of algorithm X against the CBC version of algorithm X, where X = DES, 3DES and AES. Explain in detail by putting yourself in the shoes of an attacker who has your ciphertexts but not the key or the plaintexts. Creativity is encouraged and expected in this exercise. Hint: At a minimum, for this question, you should consider the two properties confusion and diffusion and study the relationship (statistically, tests of randomness, or using any other means you can think of) between the key and ciphertext and the plaintext and ciphertext.

In your submission, besides the answers to the above questions make sure to include as many details as possible including but not limited to: any seed used for the random number generation and how it was derived, the key used for each part, the plaintext document used, the conversion process to get the blocks from the plaintexts, the results of the conversion process, the commands that you typed, the tests that you used to study the relationships in the Hint, etc.

Academic Honesty Policy: No collaboration with anyone or anything in or outside the course is allowed on any homeworks, exams and programming assignments (yes, that excludes the internet as well) except if it is explicitly allowed on a problem. The appropriate help of the instructor and (if applicable) the TA is of course allowed and encouraged. Special Note for this assignment: Parts of this assignment specifically allow you to use the Internet, but it is still prohibited for the parts that do not explicitly ask you to use it.