ENEE457 – Computer Systems Security
Project 3 Rubric

Note: Make sure to document your responses in a separate (.doc or .pdf) file, with details and screenshots of each task.

Task #	Description	Points
	Secret-Key Encryption Lab	
2	Get familiar with openssl command line and provide observations in your report.	4
3	I. Encrypt *pic_original.bmp* with ECB and CBC modes and report your observations. (10) II. Select a picture of your choice, repeat the experiment, and report your observations. (5)	15
4	I. Use ECB, CBC, CFB, and OFB modes to encrypt a file, and report which modes have paddings and which ones do not. For those that do not need paddings, please explain why. (8) II. Figure out what paddings are added to the three files containing 5 bytes, 10 bytes, and 16 bytes. (7)	15
5	I. Decrypt the corrupted cyphertext using ECB, CBC, CFB and OFB modes. (8) II. Answer the question. (8)	16
6	I. Encrypt the same plaintext using [1] two different IVs, and [2] the same IV, and describe your observations. (10) I. Answer the 2 questions from Task 6.2 and describe how you figured them out. (10) II. Successfully construct a message and ask Bob to encrypt it and give you the ciphertext and figure out whether the actual content of Bob's secret message is *Yes* or *No*. (10)	30
7	Successfully write a program to find out the encryption key based on the given plaintext and a cyphertext, and report your steps and observations.	20
	TOTAL POINTS:	**100**