CMPS 485 - Computer Security - Fall 2018
Homework 3

You need to submit homework 3 Word document to your GitHub repository.

In this homework you will conduct a performance testing to figure out the relative computing time for some key encryption algorithms by *encrypting* and *decrypting* the text file available at https://www.dropbox.com/s/79oos41y63tw6k6/TenDaysBook.txt using:

- RC4
- AES 128 and 256 with the following modes: ECB, CBC, OFB, CFB, and CTR
- DES with the following modes: ECB, CBC, OFB, CFB, and CTR
- Triple DES with the following modes: ECB, CBC, OFB, CFB, and CTR

1. For each cipher you need to measure the Encryption Time (in Sec), Decryption Time (in Sec), Ciphertext File Size (in MB). Present the results in a table.
2. Include all your openssl or python scripts used to produce the data.
3. Analyze and interpret the results then draw the main conclusions (e.g., highlight the best performing and the worst performing ciphers, compare the ciphertext file size).