### Qatar University College of Engineering CMPT 642/742 Information Security Fall 2020

### Assignment 2 Solution Template

Use the following table to enter your answers.

|  |  |
| --- | --- |
| **Questions** | **Your commands and answers** |
| **Question 1** | |
| Command to generate the key | openssl rand 16 > "me.key" |
| Command to encrypt using ECB (a) | openssl aes-128-ecb -e -in me5times.txt -nosalt -nopad -out me5tims.ecb.enc -kfile me.key 2>/dev/null |
| Command to encrypt using CBC (b) | openssl aes-128-cbc -e -in me5times.txt -nosalt -nopad -iv 00000000000000000000000000000000 -out me5tims.cbc.enc -kfile me.key 2>/dev/null |
| Your observation on the ciphertexts (d) | Ecb has the same cipher text for each block !  CBC has different cipher-text for each block |
| **Question 2** | |
| First line of the plaintext file q2file.txt | THE GLORIOUS QURAN |
| **Question 3** | |
| Describe the hardware and software of your machine | -VM Fusion Linux ubuntu 5.3.0-64-generic #58-Ubuntu  -RAM 2404GB  - Intel(R) Core(TM) i7-4960HQ CPU @ 2.60GHz quad-core  -OpenSSL 1.1.1c 28 May 2019 |
| *Algorithm* | *Bandwidth (MBits/sec)* |
| SHA256 | 3670.66544 |
| AES-128-CBC | 2781.872 |
| AES-256-CBC | 2036.19552 |
| RSA2048  (sign with private key) | 1751 (signatures/second) |
| RSA2048  (verify with public key) | 35480 (verifications/second) |
| **Question 4** | |
| Prime parameters ***p*** & ***q*** | 11,29 |
| Public key **(e,n)** | (23,319) |
| Private key **d** | 207 |
| C=Encrypt(**e,n**) (10) | 98 |
| Decrypt**d** (C) | 10 |