(a) Create a 128-bit AES key, encrypt and decrypt each of the two files using AES in the CBC mode.

(b) Create a 128-bit AES key, encrypt and decrypt each of the two files using AES in the CTR mode.

(c) Repeat part (b) with a 256-bit key. two files using AES in the CTR mode.

(d) Compute a hash of each of the files using hash functions SHA-256, SHA-512, and SHA3- 256.

(e) Create a 2048-bit RSA key, encrypt and decrypt the files above with PKCS #1 v2 padding (at least v2.0, but v2.2 is preferred; it may also be called OAEP).

(f) Repeat part (e) with a 3072-bit key.

(g) Create a 2048-bit DSA key, sign the two files and verify the corresponding signatures. If creating a key takes two parameters, use 224 bits for the exponent sizes. If the hash function algorithm needs to specified separately, use SHA-256. (

h) Repeat part (g) with a 3072-bit DSA key (if the second parameter is required, use 256).