BLM 442e Spring 2018

Homework

In this homework, you are expected to implement the following (in any programming language):

1) Generate an RSA public-private key pair. K_A^+ and K_A^-.
2) Generate a 128 bit symmetric key K_S. Encypt it with K_A^+, print the result, and then decrypt it with K_A^-. Again print the result.
3) Consider a long text *m*. Apply SHA2 Hash algorithm (Obtain the message digest, H(m)). Then encrypt it with K_A^-. (Thus generate a digital signature.) Then verify the digital signature. (Decrypt it with K_A^+, apply Hash algorithm to the message, compare).
4) Consider a text *m*. Apply HMAC using K_S and SHA2 algorithms.
5) Encypt a long text using AES algorithm in CBC mode. Print the result. (IV should be randomly generated, Key = K_S) Then decrypt it. Again print the result.