CSE4057 Fall 2018

Homework 1

Due: November 16th (but start ASAP)

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 two symmetric keys: 128 bit K_1 and 256 bit K_2. Print values of the keys on the screen. Encypt them with K_A^+, print the results, and then decrypt them with K_A^-. Again print the results. Provide a screenshot showing your results.

3) Consider a long text m. Apply SHA256 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). Print m, H(m) and digital signature on the screen. Provide a screenshot. (Or you may print in a file and provide the file).

4) Consider a text m. Apply HMAC using K_1 and SHA256 algorithms. Print m and result of HMAC on the screen and provide a screenshot.

5) Generate or find any file of size 1MB. Now consider following three algorithms:

i) AES (128 bit key) in CBC mode.

ii) AES (256 bit key) in CBC mode.

iii) DES in CBC mode (you need to generate a 56 bit key for this).

For each of the above algorithms, do the following:

a) Encrypt the file of size 1MB. Store the result (and submit it with the homework) (Note: IV should be randomly generated, Key = K_1 or K_2).

b) Decrypt the file and store the result. Show that it is the same as the original file.

c) Measure the time elapsed for encryption. Write it in your report. Comment on the result.

d) For the first algorithm, change Initialization Vector (IV) and show that the corresponding ciphertext chages for the same plaintext (Give the result for both).

Optional: Generate a symmetric key using Elliptive Curve Diffie Helman with a two public/private key pairs.

You may do this homework in groups of two.

What to submit: Submit all your commented codes, output files and a report including your results, screenshots and comments to cse457submit@gmail.com.

In your codes, please clearly describe which code parts do which job. If you do not complete all the items asked above, please clearly indicate which items are completed.