CSE4057 Spring 2022

Homework 1

Due: May 10th, Tuesday 23:59

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

1) Generation of public-private key pairs.

a. Generate an RSA public-private key pair. K_A^+ and K_A^-. The length of the keys should be at least 1024 bits (the number of bits in the modulus). Provide a screenshot to show the generated keys.

b. Generate two Elliptic-Curve Diffie Helman public-private key pairs. (K_B^+, K_B^-) and (K_C^+, K_C^-).

2) Generation of Symmetric keys

a. Generate two symmetric keys using a secure key derivation function: 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.

b. Generate a 256 bit symmetric key using Elliptic key Diffie Helman using K_C^+ and K_B^-. This is K_3. Generate a symmetric key using K_B^+ and K_C^- and show that the generated key is the same. Print value of the generated keys and provide a screenshot.

3) Generation and Verification of Digital Signature

Consider any text of at least 1000 characters. 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) AES Encryption

Generate or find a text or image file of size at least 1MB. Now consider the following three algorithms:

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

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

iii) AES (256 bit key) in CTR mode.

For each of the above algorithms, do the following:

a) Encrypt the file. Store the results (and submit it with the homework) (Note: Initialization Vector (IV) in CBC mode and nonce in CTR mode should be generated randomly, For 128 bit ıse K_1 as the symmetric key. For 256 bit you may use either K_2 or K_3).

b) Decrypt the ciphertexts and store the results. Show that they are the same as the original files.

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 changes for the same plaintext (Give the result for both).

5) Message Authentication Codes

a) Generate a message authentication code (HMAC-SHA256) using any of the symmetric keys.

b) Apply HMAC-SHA256 to K_2 in order to generate a new 256 bit key.

You may do this homework in groups of two or three.

What to submit: Submit all your commented codes, output files and a report including your results, screenshots and comments via google classroom. 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**.