SENG2250/6250 System and Network Security

School of Electrical Engineering and Computing

Semester 2, 2020

Lab 3: Topic 2 – Cryptographic Techniques II

Objectives

1) Review the knowledge of Topic 2.
2) Apply cryptographic techniques for security system design.
3) Implement CFB mode for the understanding of operation modes.

Part 1 Review Questions

1. What is a one-way function?
2. What is a one-way trapdoor function?
3. Describe the RSA cryptosystem, including the key generation, encryption, and decryption.
4. What is the message authentication code?
5. What properties are provided by digital signatures?

Part 2 Exercises

6. **Message Authentication Code (MAC)**:
    a. Describe the MAC system for message authentication.
    b. Why do we use double hash in HMAC algorithm?
    c. What are the differences between MAC and Digital Signatures?
    d. Considering the functionalities (security properties), is it fine to use digital signatures to replace MAC?
        - If yes, why do we still widely use both?
        - If no, why?

7. **Security Design**

    Considering a messaging system, it aims to securely deliver a message from user A to user B. The system needs to provide both the message confidentiality and integrity.

a. Use symmetric-key based cryptographic techniques (e.g., block cipher, hash function) to design a mechanism.
    - Write down the assumptions/pre-requisites of using the system, for example, anything required for (pre)sharing.
    - Write down the steps for message preparation, delivery and receiving process.

b. Do the same task as 7.a, but use public key based cryptography only.

c. *Challenge*: do the same task as 7.a, but use both of symmetric-key and asymmetric-key cryptography. The designed mechanism should achieve better performance and/or provide with more functionality/properties.

d. What would be the differences between "encrypt-then-sign" and "sign-then-encrypt" patterns for a message delivery system?

8. **Programming**
Implement a (k-bit) CFB mode with the following specifications.
    - The underlying block cipher is as
        - Plaintext (P) block size: 16 bits, represented by hexadecimal, e.g., "A7B3"
        - Key (K) size: 16 bits, represented by hexadecimal, e.g., "ED89"
        - Encryption: $C = P \oplus K$, C is a ciphertext.
        - Decryption: $P = C \oplus K$.
    - If an input message of CFB encryption process is not a multiple of 16-bit, pad "0"s for blocking.
    - Output the used Initialisation Vector (IV) and the ciphertext.
    - Implement CFB decryption process.
    - You need to select IV, key K and the shift bits k.

Part 3 Discovery

This self-study is for the understanding of many public key based cryptographic algorithms, such as RSA. This part (knowledge) is OPTIONAL and NOT examinable.

9. Self-study: Extended Euclidean algorithm (EEA)

a. Refer to the slides of lab 03 for EEA description.

b. Answer the following questions.
    - $19 \; mod \; 13 \; = ?$
    - $4 \; mod \; 13 = ?$
    - $\gcd(3,13) = ?$
    - $\gcd(4,42) \; = ?$
    - What does it mean if $\gcd(a, b) = 1$?
    - Let $a = 11, m = 24$, find b, s.t $ab = 1 \; mod \; m$, where b is so-called the multiplicative inverse of a mod m. (Use the Extended Euclidean algorithm).