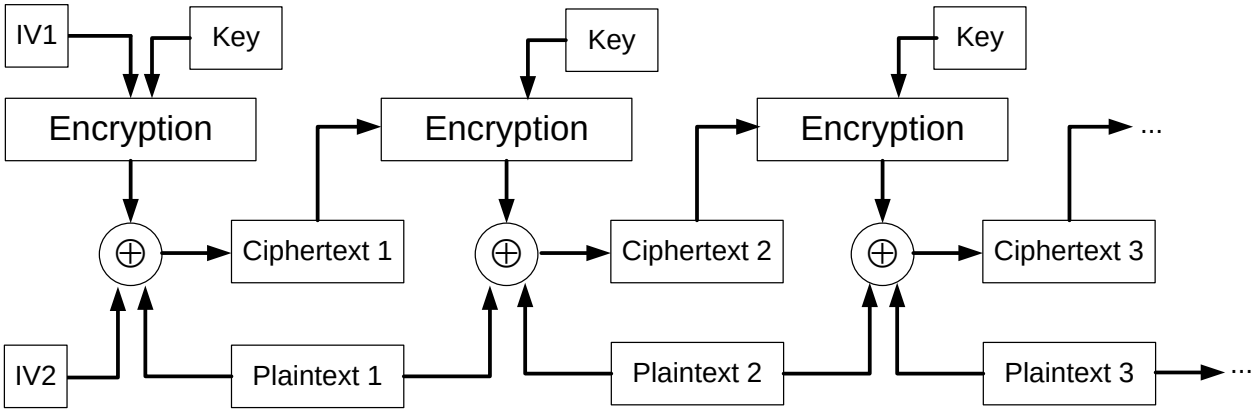
FINAL EXAMINATION

Course: **CS434 – COMPUTER SECURITY**	
Time: **90** minutes	Term: 3 – Academic year: **2020-2021**
Lecturer(s): **Assoc. Prof. Tran Minh Triet, Mr. Tran Anh Duy**	
Student name:	Student ID:

(Notes: Neither books nor laptops, phones allowed)

Question 1: Mode of Operation (*3.0 marks*)

Consider the following mode of operation for a block cipher:



Notes:

P_i: Plaintext

C_i: Ciphertext

IV_1 and IV_2: Initialization Vectors

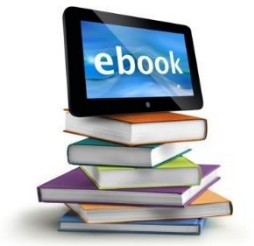
$$C_0 = \text{IV1}, P_0 = \text{IV2},$$
$$C_i = P_{i-1} \oplus P_i \oplus E_K(C_{i-1})$$

a) Describe the corresponding decryption process. *Hint*: draw the diagram of the decryption operation *(1.0 mark)*

b) Evaluate the parallel processing of the encryption and decryption schemes. *(1.0 mark)*

c) Assume that, in the transmission of encrypted data, there were an error at the ***i*th bit of the *first* block (C_1)** and an error at the ***j*th bit of the *second* block** (C_2). Evaluate the error propagation after decrypting all the received data. *(1.0 mark)*

Question 2: Message Authentication Code (MAC) *(2.0 marks)*



When a customer signs up for an e-bookstore service, the online bookstore issues the customer a membership number (ID) and a secret key (K).

For each customer, the store stores the customer's information (such as full name, address, phone...) along with the customer's membership number and secret key.

The customer must keep the key content (K) secret, only the customer and the store know this code of the customer.

When making a purchase, the customer will send the store a message consisting of two parts:

Part 1: order content (M), including membership number (ID).

Part 2: hash value (H) calculated from order content (M) combined with customer's secret key (K):

$$H = \text{Hash}\ (\text{Hash}(M) \mid K)$$

a) Please discuss about the meaning of using hash value (H) in customer order message?

b) Does using a hash value (H) in a customer's order message help the store prove that the order was actually placed by the customer if the customer intentionally denies the order? Why?

Question 3: Supermarket Shopping Support System (S^4) *(3.0 marks)*

SmartMarket is a system of supermarkets deployed in many cities and countries around the world. SmartMarket provides a utility on mobile devices that helps customers ***find product-related information based on the product's barcode***, such as promotional information, buyer comments about products and services. product. In addition, this utility also allows users to ***select products and place orders via mobile devices***.

When entering the supermarket, your mobile device (C) will automatically connect to the server (S) of the supermarket. You can use your mobile device to ***capture barcodes*** to identify product numbers. You can then select the function on your mobile device to ***send the product number*** to the supermarket's server (S) and ***receive information related to this product***. Alternatively, you can ***order products*** directly on your mobile device.

Here are some information security issues in the purchase support system:

- Because SmartMarket has many supermarkets, every time a customer enters a specific SmartMarket supermarket, his/her mobile device (C) needs to make sure that it is properly connected to the server (S) of this supermarket to avoid mistakenly connecting to another server (for the purpose of providing customers with false information about products).
- The server (S) of each supermarket needs to check if the user is a valid registered user.
- After establishing a secure connection and communication channel between the mobile device (C) and the server (S) of the supermarket, all information transmitted/received between the mobile device (C) and the server (S) are encrypted by a pre-defined symmetric encryption method using a secret key K that is generated and shared between S and C for that session.

The solution to protect information security in the system are proposed as follows:

- ***The server at each supermarket*** has its own ***asymmetric key pair*** (registered for digital certificates at the common Certificate Authority - CA).
- ***Each user*** has his own ***unique ID*** and a ***secret key*** K_c registered with SmartMarket's central server. The secret key K_C is stored on the user's mobile device (C).
- The server at each supermarket can automatically connect to SmartMarket's central server to get all the ***ID information*** and all ***secret keys*** (K_c) of all registered users.

The protocol used to initiate a secure communication channel is defined as follows:

Step 1: The server (S) periodically sends (***broadcast***) the message ① to ***all mobile devices*** within the supermarket's range.

① = Connection invitation, Cert(SName, $PublicKey_S$)

Message ① includes: ***connection invitation*** and a ***valid digital certificate of the server*** (S). The certificate clearly states the name of the supermarket and the public key $\mathbf{PublicKey_S}$ of the server (S) at this supermarket.

Step 2: When receiving the message ①, a mobile device (C) will check the validity of the certificate. If this is a valid certificate, the mobile device (C) will send the message ② to the server (S).

② = $E_{PublicKeyS}(ID_C)$

The content of the message ② is the ***user's identifier*** $\mathbf{ID_C}$ that is ***asymmetrically encrypted*** with the public key $\mathbf{PublicKey_S}$ of the server (S).

Step 3: The server (S) ***connects to the central server*** of the SmartMarket supermarket system on a ***secure channel*** to ***check the validity*** of the $\mathbf{ID_C}$ and receive the user's ***secret key*** $\mathbf{K_C}$. Then, the server (S) sends the message ③ to the mobile device (C).

③ = Hash(①|②|ID_C)

Message ③is the digest message of the messages ① and ②, and the identifier $\mathbf{ID_C}$.

Step 4: Mobile device (C) sends message ④ to server (S)

④= Hash(①|②|③)

Message ④ message is a digest message of the threee messages ①, ②, and ③.

After finishing step 4, all communication messages between the mobile device (C) and the server (S) are encrypted with the secret key $\mathbf{K_C}$.

a) In the protocol, the mobile device (C) does not send any random value $\mathbf{Random_C}$ to the server (S). Do you think this may lead to the security risk for the system? If so, please describe a practical situation that could desecrate the system. *(1.0 mark)*

b) In the protocol, can the mobile device (C) be sure that the server (S) is the owner of the $PublicKey_S$? Why? If not, please suggest a simple solution for mobile device (C) to check that server (S) really owns $PublicKey_S$. *(1.0 mark)*

c) In the protocol, can the **server** (S) be able to check that the **user with the** mobile device (C) really has an **identifier** ID_C? If not, provide a simple solution to make sure the server (S) is really communicating with the **user who is using the** mobile device that has the identifier ID_C stored. *(1.0 mark)*

Question 4: Computer and Information Security (*2.0+ marks*)

a. Describe a real world problem in information security. You should choose a problem that you actually love and describe in detail that problem: the scenario, the threats when that problem appears. Which security issue(s) that your chosen problem belongs to: secrecy/confidentiality, integrity, authentication, non-repudiation, or privacy. *(1.0 mark)*

b. Describe ***a possible solution*** for your chosen problem. *(1.0 mark)*

GOOD LUCK TO YOU 😊