11210/IIS500200 Network Security, Fall 2023 **7-Nov-2023**

Midterm

Instructor: Prof. Amir Rezapour

1. Which of the following activities might be considered as a possible breach of security to a company's network? (12 points)

   (a) The daily carrier personnel who drop off and picks up packages.

   (b) Former employees who left the company because of downsizing.

   (c) An employee traveling on company business to another city.

   (d) The building management company where an organization has its offices has decided to install a fire sprinkler system.

2. Consider a sensor X that periodically sends a 64-octet measurement to a receiver Y. One day the administrator decides that X should encrypt the measurement data using DES in CBC mode. How many octets does X now send for each measurement? Explain your answer. (8 points)

3. DES is insecure because of its short key length (56 bits). A modified DES algorithm has key length of 120 bits, $k = (k_1, k_2)$, where k_1 is 56 bits and k_2 is 64 bits. The new encryption algorithm is as follows.

$$DES'(k, m) = k_2 \oplus DES(k_1, (k_2 \oplus m)). \tag{1}$$

   Explain how decryption is done. (10 points)

4. Briefly explain the Shift Rows and Byte Substitution layers in AES algorithm. What happens if we change their order in the AES algorithm (Shift Rows and then Byte Substitution)? (10 points)

5. In Counter mode (CTR) mode of operation:

   (a) Describe the encryption and decryption process. (10 points)

   (b) Suppose that there is a transmission bit error in c_i. Show how many plaintext blocks are affected due to the transmission bit error in c_i. (10 points)

6. We consider a banking system, where message m of the form *fromAccount*, *toAccount*, and *amount* are sent within the bank network, with the meaning that *amount* dollars should be transferred from *fromAccount*, to *toAccount*. Each message consists of three blocks, with each block holding one of the three parameters. Messages are encrypted with AES in Counter Mode as follows:

$$K_j = E(k, T_j),\ C_j = M_j \oplus K_j \tag{2}$$

   Each of the three parts of a message is sixteen characters, i.e., one block, so messages consist of three blocks.

(a) The adversary has an account in the bank and can intercept and changes messages. Imagine now that he know the *toAccount* for a particular message $m = C_1C_2C_3$. Explain how he can modify the message so that the amount is transferred to his own account. (10 points)

(b) Explain how the use of MAC would prevent this attack? (10 points)

7. When one signs an electronic document using digital signature, one often performs the signature operation on a message digest produced by passing the document through a cryptographically strong hash function $h = H(m)$. Why it is important that it is difficult to find two documents with the same message digest? (10 points)

8. In RSA algorithm, is it possible for more than one d to work with a given e, p, and q? *Hint (Is it possible to have d and u s.t. $ed = 1 \mod \phi(n)$ and $eu = 1 \mod \phi(n)$?)* (10 points)