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

Homework 1

Instructor: Prof. Amir Rezapour

1. Consider a system that provides authentication services for critical systems, applications, and devices. Give examples of confidentiality, integrity, and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement. (10 points)

2. Consider a desktop publishing system used to produce documents for various organizations. (15 points)

   (a) Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.

   (b) Give an example of a type of publication in which data integrity is the most important requirement.

   (c) Give an example in which system availability is the most important requirement.

3. Alice was told to design a scheme to prevent messages from being modified by an attacker. Alice decides to append to each message a hash (message digest) of that message. Why doesn't this solve the problem? (10 points)

4. What RC4 key value will leave S unchanged during initialization? That is, after the initial permutation of S, the entries of S will be equal to the values from 0 through 255 in ascending order. (10 points)

5. With the ECB mode, if there is an error in a block of the transmitted ciphertext, only the corresponding plaintext block is affected. However, in the CBC mode, this error propagates. For example, an error in the transmitted C_1 obviously corrupts P_1 and P_2. Are any blocks beyond P_2 affected? (10 points)

6. Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? How about decryption? (15 points)

7. Suppose $H(m)$ is a collision-resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all messages x, x' with $x \neq x'$, we have $H(x) \neq H(x')$? Explain your answer. (10 points)

8. It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible? (10 points)

9. In an RSA system, the public key of a given user is $e = 3$, $n = 667$. What is the private key for this user? (10 points)