University of Dhaka
Department of Computer Science and Engineering
4th Year 1st Semester B. Sc. Final Examination, 2020
CSE-4137: Cryptography and Security

Total Marks: 60 **Time: 2 Hours**

(Answer any three (3) of the following questions)

1. a) Differentiate between passive and active attacks? Discuss any two active attacks. 1.5+2.5
   b) State the important property of XOR that makes it suitable for an encryption operation. Prove the validity of the property with an example. Prove One Time Pad has perfect secrecy. 3+2
   c) Construct a Playfair matrix with the key **LARGEST**. Now encrypt the following sentence explaining each transformation: 1+4

   JUDI MUST KNOW JOHN

   d) Why GF (2^n) is important? Consider a set of polynomials that belong to the finite field GF (3^2). List all the polynomials and explain the reasons. 3+3

2. a) Explain the notion of semantic security. Discuss why stream ciphers are semantically secure. 3+3
   b) Using the Extended Euclidean algorithm, find the multiplicative inverse of 551 mod 1761. 4
   c) Suppose you perform encryption and decryption using the Feistel structure. What is the relationship between the output of the second encryption round (consisting of RE2 and LE2) and the output of the fourteenth round of decryption (consisting of RD14 and LD14)? Prove that this relationship holds in the Feistel structure. 5
   d) AES decryption is not identical to AES encryption. Explain the changes you need to make to perform the AES encryption and decryption using the same circuit. Draw the AES decryption circuit after you make the necessary changes. 3+2

3. a) Describe Diffie Hellman key exchange protocol and discuss how it can suffer from man in the middle attack? 5+5
   b) Find the out come of Shift Row Transformation step in AES algorithm for the following scenario: 5

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

   c) How the key expansion algorithm work in case of AES? 5

4. a) Consider an Elgamal public key scheme with a common prime **q** = 71 and a primitive root **α** = 7. 4
      1. If **B** has a public key $\mathbf{Y_B}$ = 3 and **A** chooses the random integer **k** =2, what is the ciphertext of **M** = 30?
      2. If **A** now chooses a different value of **k** so that the encoding of **M** = 30 is **C = (59, C_2)**, what is the integer C_2?
   b) Explain how the Birthday Paradox attack can be performed on the cryptographic hash function and derive the computational complexity of this attack. List some application scenarios that can use the cryptographic hash function. 3+1+2
   c) Discuss the concept of a chain of certificates using an example. 5
   d) Why is the result produced by Bio-metric not always accurate? Discuss in detail the impact of selecting threshold values on bio-metric data. 5

5. a) Consider the following threats and describe how each is handled using SSL: 6

   i. Brute-Force Cryptanalytic Attack: An exhaustive search of the key space for a conventional encryption algorithm.
   ii. Replay Attack: Earlier handshake messages are replayed.
   iii. IP Spoofing: Uses forged IP addresses to fool a host into accepting bogus data.

   b) Explain the Transport mode and Tunnel mode operation of IPSec. Also, discuss the application scenarios where they can be used. 3+3

   c) Compare AES to DES with respect to the following elements of DES. Indicate comparable element in AES or explain why it is not needed in AES. 8

   (i) XOR of subkey material with the input to the f function.
   (ii) XOR of the f function output with the left half of the block.
   (iii) f function.
   (iv) Permutation P.
   (v) Swapping of the halves of the block.