Mid Term Examination
4th year, 2nd Semester B.Sc (Hons.)'2020
Department of Computer Science and Engineering
University of Dhaka

Total Mark: 30 **Total Time: 1 hour 20 minutes**

Answer Q3 and choose any Four (4) from the remaining questions:

1. What is "unconditional security" and "~~conditional~~ computational security"? Explain with an example why EX-OR operation is important for encryption operation. 2+4=6

2. In onetime pad you cannot use the same key to encrypt more than one messages. Suppose you encrypt two messages of same length with the same key. Describe elaborately what kind of vulnerabilities exist if you are provided only with the ciphertexts of these two messages. 4+2=6
(ii) Is it possible to reuse a key without creating any security vulnerabilities? Argue in favour of your answer.

3. Consider a set of polynomials that belong to the finite field GF (2^3) using the irreducible polynomial $m(x) = x^3 + x + 1$. 3+3=6
(i) List all the polynomials. Explain the reasons.
(ii) Construct the multiplication table and list the multiplicative inverse for each polynomial.
(iii) Find the result of

4. (i) Find the multiplicative inverse of each element of Z_5. 2+4=6
(ii) List out the steps to find the multiplicative inverse using the Extended Euclidean algorithm for 135 mod 61.

5. Define confusion and diffusion. Describes how these two properties are achieved in AES. (Mention the AES algorithm steps and explain their operations). 6

6. 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. 4+2=6

7. Explain the working procedure with the underlying design principle of Cipher Block Chaining. What are advantages and disadvantages of CBC and Output Feedback mode? 6