University of Dhaka
Department of Computer Science and Engineering
Professional Masters in Information and Cyber Security (PMICS)
Mid Term Examination
CSE 802: Information Security Fundamentals

Total Mark: 30 **Total Time: 1 Hour 30 Minutes**

Answer any Three (3) Questions

4. (a) Discuss how key-signing keys are used to validate a DNS record. 5

   (b) Suppose A received a certificate from CA X_1 and B received a certificate from CA X_2. X_3 is an intermediate CA having certificates $X_3\langle\langle X_1\rangle\rangle$ and $X_3\langle\langle X_2\rangle\rangle$. Now suppose A has access to B's certificate and wants to verify the public key of B through X_1, X_2 and X_3. Describe how this can be achieved. 5

5. (a) Draw the block diagram of the operations of the public key crypto systems. 4

   (b) Discuss the properties of a cryptographic hash function. 2

   (c) Consider the scenario shown in the figure below. Here, A wants to communicate with B. You should explain the purpose of each message involved in the communication. 4