Department of Computer Engineering

Internal Assessment Test - 1

FH-2021

Subject: Cryptography and System Security **Class/Div/Sem: TE/A,B,C/VI**
Subject Code: CSC604

Q.6 Descriptive Questions (5 Marks Each)

Question (6A)

In RSA Given n=221 and e=5 find d?

OR

In Diffie-Hellman protocol g=7, p=23, x=3 and y=5
i) What is symmetric key
ii) What is value of R1 and R2

Question (6B)

Describe Digital Certificate X.509 standard?

OR

Explain MAC and HMAC for checking message integrity in the communication?