राष्ट्रीय प्रौद्योगिकी संस्थान हमीरपुर
हमीरपुर (हि॰प्र॰) – 177 005 (भारत)
NATIONAL INSTITUTE OF TECHNOLOGY HAMIRPUR
HAMIRPUR (H.P.) - 177 005 (INDIA)
(An Institute of National Importance under Ministry of HRD)
संगणक विज्ञान एवम् अभियांत्रिकी विभाग
Department of Computer Science & Engineering

Information Security (CSD-410) Assignment-2

AS02/2019

SEMESTER-VII

CLASS-Dual Degree (CSE) VIII Sem + B.Tech. (CSE) VIII Sem, (IIITU)

1. What are application of Pseudo random number generators (PRNGs)? Specify the use of PRNG in Digital Signature Applications.
2. Using RSA algorithm, Find n, d, and c, if p=11, q=3, e=3. Encrypt "NITH" Message.
3. Describe HMAC algorithm. Comment on the security of HMAC.
4. What is TCP Session Hijacking? How is it done?
5. Explain in detail the operation of Internet Key Exchange with an example.
6. Differentiate the Host and Network-Based Intrusion Detection Systems.