

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT
TEST -3 EXAMINATION- Dec 2018
B.Tech(ECE/CSE/IT/BI) VII Semester

COURSE CODE: 10B1WCI735

MAX. MARKS: 35

COURSE NAME: Network Security and Cryptography Techniques

MAX. TIME: 120min

COURSE CREDITS: 3

Note: All questions are compulsory. Carrying of mobile phone during examinations will be treated as case of unfair means.

Q.1. [5 Marks. Each part is one mark]

- a) Differentiate between symmetric and asymmetric encryption.
- b) Describe structure of a virus program.
- c) Describe components of access control.
- d) List methods to generate random numbers.
- e) Discuss general structure of a firewall system?

Q.2. [5 marks] In our computing labs, print billing is often tied to the user's login. People login, they print, they get a bill. Sometimes people call to complain about bills for printing they never did, only to find out that the bills are, indeed, correct. What do you think might be wrong here? As a security expert what is your solution to the problem?

Q.3. [5 marks] The IT folks got a number of complaints that one of our campus computers was sending out spam. They checked it out, and the reports were true: a hacker had installed a program on the computer that made it automatically send out tons of spam email without the computer owner's knowledge. How do you think the hacker got into the computer to set this up? What is the remedy for such intrusions?

Q.4. [5 marks] How is AES different from DES? Describe the key expansion algorithm used in AES.

Q.5. [5 marks] What are the different modes of operation of symmetric ciphers? What are their properties? When would you use each mode?

Q.6. [5 marks] What are properties of MAC functions? Describe HMAC algorithm.

Q.7. [5 marks] What is SSL protocol? Describe how web services may be secured using SSL.