

**B.Tech. – VIEP – COMPUTER SCIENCE AND
ENGINEERING (BTCSVI)**

Term-End Examination

December, 2017

00941

**BICSE-016 : CRYPTOGRAPHY AND NETWORK
SECURITY**

Time : 3 hours

Maximum Marks : 70

Note : Answer any *five* questions. All questions carry equal marks.

1. (a) What is an Attack ? Explain and differentiate between active and passive attacks with a suitable example. 7
- (b) What do you mean by Cryptography ? Explain public key and private key cryptography. 7
2. (a) What is PGP ? Mention the services provided by the Pretty Good Privacy (PGP). 7
- (b) What is a Trusted System ? Explain the basic concept of data access control in trusted systems. 7

3. (a) Explain the significance and design details of S/MIME. 7
- (b) Describe the design details of a secure electronic transaction. 7
4. (a) What is Cipher ? Explain and differentiate between substitution cipher and transposition cipher. 7
- (b) Explain the procedure of RSA algorithms in detail with example. 7
5. (a) How is security provided at transport layer, network layer and application layer ? Discuss. 7
- (b) What is Single Sign-On (SSO) ? Explain in detail. 7
6. (a) What do you mean by Network Security ? Explain with the help of example and suitable diagram. 7
- (b) What is HASH function ? Explain the security of hash function and MACs. 7
7. Write short notes on the following : 14
- (a) IP Header
- (b) Intruder Detection
- (c) Digital Signature Standard
- (d) MD5 Algorithm