

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

**00293 Term-End Examination**

**December, 2018**

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

*Time : 3 hours*

*Maximum Marks : 70*

---

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

---

1. Explain the term Cryptography. Also explain the various security attacks and their types. 14
2. What is DES ? Using suitable diagram, explain its one complete iteration in detail. 14
3. (a) What is meant by Block Cipher ? 7  
(b) What are the key algorithms used in S/MIME ? 7
4. Using a suitable example, explain the Diffie-Hellman key exchange algorithm. 14

5. How does symmetric key cryptography and asymmetric key cryptography get used in digital signatures ? 14
6. (a) What are the different approaches to produce message authentication ? 7
- (b) What is the difference between a message authentication code and a one-way hash function ? 7
7. Explain the MD5 message-digest algorithm in detail. 14
-