B.Sc.(E.C.S.)-III (Sem-VI)

System Security

Time: -3 hrs. Marks: - 80

Instructions: 1) All Questions are compulsory.

2) Figures to the right indicate full marks.

3) Use of log tables and calculators allowed

4) Draw a neat labelled diagram wherever necessary.

**Q. 1. A) Choose the correct alternative. 10**

**1.The …………… Uses 64 bits and a key of 56 bits to produce a ciphertext.**

**A.RSA B.DES C. AES D.RC5**

**2. A person who uses his or her expertise to gain access to other people’s computers to get information illegally or do damage is a**

**A. Hacker B. Analyst C. Spammer D. Programmer**

**3.** **\_\_\_\_\_\_\_\_is a form of virus explicitly designed to hide itself from detection by anti-virus software**

**A.Parasitic virus B.Polymorphic virus**

#### **C.Stealth virus D.Macro virus**

**4.** **……….programs can be used to accomplish functions indirectly that an unauthorized user could not accomplish directly.**

**A.Zombie B.Worm C.Trojan Horses D.Logic Bomb**

**5.HASH function is useful for message………….**

**A.Confidentiality B. Non Repudiation C.Integrity D.Authentication**

**6A digital signature is\_\_\_\_\_\_\_\_\_\_**

**A.Encrypting information B.Handwritten signature**

**C.Scanned signature D.None**

**7. In which of the following encryption key is used to encrypt and decrypt the data?  
A. Public key B.Private key C.Symmetric key D.Asymmetric key**

**8. What is used for database security ?**

**A.data encryption B.a view C.finger print D. all of the above**

**9. …………….. are used in denial of service attacks, typically against targeted web sites.**

**A.Worm B.Zombie C.Virus D. Trojan horse**

**10. The phrase ……… describe viruses,worms, Trojans and attack scripts.**

**A.Spam B.Phishing C.Malware D.None**

**Q. 1. B) Fill in the blanks. 6**

**1. The granting of a right or permission to a system entity to access a system resource is called as…………**

**2……………is used to gain access to user passwords without the use of a password cracking tool.**

**3.** **…………. are called as “crimeware”.**

**4.** **………….overload the network capacity on some link to a server.**

**5. The information transfer path by which unauthorized data is obtained is referred to as an ………… channel.**

**6. The ……….. is code embedded in the malware that is set to “explode” when certain conditions are met.**

**Q. 2. Answer the following (any eight ) 16**

**1. Passive Attack**

**2. Flooding Attack.**

**3. Symmetric Cryptography**

**4. Denial of service**

**5. Rootkit**

**6. subjects in access control.**

**7. authentication.**

**8. biometric authentication.**

**9. stream cipher.**

**10. denial of service.**

**Q.3 A) Attempt the following.(any two) 10**

**1. Explain various flooding attacks.**

**2. Explain security issues in user authentication.**

**3. Explain** **general approaches to attacking a symmetric encryption scheme.**

**Q. 3 B) Explain role based acess control. 6**

**Q.4 A) Attempt the following. (any two) 8**

**1. Explain Digital Envelope.**

**2. Explain advanced persistent threat.**

**3. Password cracking strategies.**

**Q.4 B) Explain reflection and amplifier attack. 8**

**Q. 5. Attempt the following.(any two) 16**

**1.Explain Discretionary Access control in detail.**

**2.Explain token based authentication.**

**3.Explain digital signature with diagram.**