M.C.A. (Sem - IV)
Network Security
(May-2017)

Q.P. Code :02180

[Time: 3 Hours] **[Marks:100]**

Please check whether you have got the right question paper.

1. Question No. 1 is Compulsory.
2. Attempt any four from the remaining six questions.
3. Assume a suitable data whenever required, clearly state the assumptions.

Q.1 a)Explain in detail the DES algorithm and a DES Round. **10**
b)Explain SSL Architecture. **10**

Q.2 a)What is hash function? How is MAC different from HMAC? **10**
b)Explain the different categories of Passive and Active Security Attacks? **10**

Q.3 a)Discuss the various pitfalls in security handshake or authentication. **10**
b)Discuss E-mail Security in detail. **10**

Q.4 a)What is Firewall? Explain different configurations of Firewalls. **10**
b)What is security policy? Explain different security policies. **10**

Q.5 a)Explain Diffie – Hellman key distribution algorithm with example. And list the disadvantages of Diffie-Hellman key distribution algorithm? **10**
b)Explain in detail PGP. **10**

Q.6 a)What is Public-Key Cryptography ? Explain RSA asymmetric key cryptographic algorithm with suitable example? **10**
b)What is a digital Signature ? Explain EI-Gamal Signature? **10**

Q.7 Write short note on **any four:** **20**
a)Kerberos V5
b)Reflection Attack
c)Triple DES
d)ECB and CBC
e) Stream Cipher and Block Cipher.
