1. Answer question 1 and any FOUR from questions 2 to 7.
2. Parts of the same question should be answered together and in the same sequence.

Time: 3 Hours Total Marks: 100

1. What are strong primes and are they necessary for the RSA system?
   b) Write a note on Computer virus.
   c) What is Risk? What are the objectives of performing risk management to enable the organization to accomplish its mission(s)?
   d) What is the most significant difference between biometric and traditional technologies for authentication?
   e) Which are the four primary classes of threats to network security? Explain each in detail.
   f) Write a short note on Kerberos.
   g) Explain block cipher in short.

   (7x4)

2. What are the advantages and disadvantages of public-key cryptography compared with secret-key cryptography?

   (10+8)

3. What are the basic types of firewalls?
   b) Explain MD5 and SHA1 algorithms.

   (9+9)

4. How secure is HTTPS today?
   b) What are the motivations for Public Key Infrastructure?
   c) Write a short note on secure digital signature.

   (6+4+8)

5. IEEE 802.11 specifies standard for wireless networking. Draw and explain protocol architecture of it.
   b) Symbian OS is used in some Mobile phones as Operating System. What are the characteristics of Symbian OS?
   c) WEP is the privacy protocol specified in IEEE 802.11 to provide wireless LAN users protection against casual eavesdropping. What are the weaknesses of WEP?

   (6+6+6)

   b) Short note on: Firewall Design Principles.
   c) How does SSL (Secure Socket Layer) certificates work?

   (5+6+7)
7. Write a Short Note on following:
   a) What are types of DoS (Denial of Service) Attacks?
   b) What are the benefits of IPSec?
   c) Draw and explain SNMP architecture in detail.

(6+6+6)