Q.P. Code: 40274

Total Marks: 80

(3 Hours)

N.B. : 1) Question No.1 is **compulsory.**
　　　 2) Attempt any **three** from the remaining questions.
　　　 3) Figures to the right indicate full marks.

Q1.　(a)　Discuss the RSA with a suitable example　　　　　　　　　　　　　　　　　[10]

　　　(b)　What is Denial of service attack? Explain its type. How we can defenses against　[10]
　　　　　 Denial of service attack.

Q2.　(a)　Explain the four Phases operation of IEEE 802.11i in detail　　　　　　　　　[10]

　　　(b)　Explain mutual authentication and reflection attack with the help of diagram　　[10]

Q3.　(a)　What are algorithm modes uses for secret key cryptography?　　　　　　　　　[10]

　　　(b)　What are the needs for DB security? Explain Inference in brief.　　　　　　　 [10]

Q4.　(a)　Explain how SET ensures a secure E-commerce transaction.　　　　　　　　　[10]
　　　(b)　Define Firewall. What are the different types of Firewalls? Explain in brief.　　[10]

Q5.　(a)　What do you mean by IDEA algorithm? Explain the detailed working principles　[10]
　　　　　 of IDEA.

　　　(b)　Explain MD5 in detail. Compare SHA1 and MD5.　　　　　　　　　　　　　 [10]

Q6.　　　 Short Note (Solve Any Four)　　　　　　　　　　　　　　　　　　　　　[20]
　　　a)　SOAP
　　　b)　Intrusion detection and it's type
　　　c)　TKIP
　　　d)　XML
　　　e)　Digital Signature

****