(3 Hours) **Total Marks: 80**

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)	Explain Information Security principles.	**[5]**
	(b)	Explain algorithm mode CBC uses for secrete key cryptography	**[5]**
	(c)	Explain HMAC.	**[5]**
	(d)	Explain SOAP web service	**[5]**
Q2.	(a)	Explain Mutual authentication and reflection attack with the help of diagram.	**[10]**
	(b)	What is message digest? Explain the working of MD5 in detail.	**[10]**
Q3.	(a)	Write short note on a) PGP b) Digital Signature	**[10]**
	(b)	Explain and differentiate between various architectures of firewall and its implementation.	**[10]**
Q4.	(a)	Explain overview of DES with one round in details	**[10]**
	(b)	Discuss SSL as an internet security protocol and discuss three major protocol used at SSL	**[10]**
Q5.	(a)	What is a Digital certificate? Explain the stepwise process of certificate generation and validation.	**[10]**
	(b)	What is Intrusion Detection? What are various systems used for detecting Intrusion?	**[10]**
Q6.	(a)	Explain Euclidean Algorithm. Using Euclidean algorithm find the Greatest Common Divisor of the following. a) 272 and 192 b) 252 and 105	**[10]**
	(b)	What are the need for Data Base security? Explain Inference in brief.	**[10]**