[Time: 3 Hours] **[Marks:80]**

Please check whether you have got the right question paper.

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

1.	a)	Explain Information Security principles.	**5**
	b)	Explain Kerberos.	**5**
	c)	Describe working of S/MIME.	**5**
	d)	Explain DOS attack.	**5**
2.	a)	What is SSL? Explain three major protocols use at SSL.	**10**
	b)	What is Message Digest? Explain MD5 in detail.	**10**
3.	a)	Discuss Inference. What are the various approaches to deal with it?	**10**
	b)	What is Firewall? Discuss its types in detail.	**10**
4.	a)	What is IDS? Explain Statistical Anomaly Detection and Rule based Detection.	**10**
	b)	What is PKI? How does PKI work?	**10**
5.	a)	Explain Euclidean algorithm. Using Euclidean algorithm, find the greatest common divisor of the following: i) 285 and 741 ii) 88 and 220	**10**
	b)	Explain RSA algorithm with example.	**10**
6.	a)	Explain Digital Encryption Standard (DES) in detail.	**10**
	b)	What is MAC? Explain HMAC in detail.	**10**

****