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

N.B. (1) Question No. **1** is **Compulsory.**

(2) Attempt any **three** questions from the remaining **five** questions.

(3) Answers to **sub-questions** should be **grouped** and written **together.**

Q1.	**Answer following questions. Each question of five marks.**	**20**
A.	State and explain the principles of information security	
B.	What are browser attacks?	
C.	What is the inference problem in database security?	
D.	Explain PKI and its components	
Q2. A	Describe the modes of operation of block ciphers (ECB, CBC, CFB, OFB). Compare their security and performance.	**10**
Q2. B	Describe approaches for intrusion detection with examples.	**10**
Q3. A	Explain database access control mechanisms.	**10**
Q3. B	Discuss IPSec architecture and explain the AH and ESP protocols in detail	**10**
Q4. A	Explain the structure of X.509 digital certificate and steps of creating the digital certificate.	**10**
Q4. B	In an RSA system, the public key of a given user is E=31, N=3599. What is the private key?	**10**
Q5. A	Explain the characteristics and types of firewalls with neat diagrams.	**10**
Q5. B	Explain HMAC in details	**10**
Q6. A	Explain different types of security attacks with examples.	**10**
Q6. B	Explain mutual authentication and reflection attack with suitable examples.	**10**

****