1	a) Why Kerckhoffs argued that cryptographic algorithms should be made public and the secrecy of the code should only depend upon the key. b) Discuss One Time Pad and show the working of One Time Pad with suitable Diagram and example.
2	a) “Pseudo Random Must be Unpredictable”. What is the meaning of this statement. Prove the correctness of the statement. b) Two Time Pad is insecure. Prove using any method of proof.
3	a) Write a short Note of Salsa 20. Show the construction of Salsa 20. b) DES block cipher was used for many years as a crypto standard. Make the model of DES and show various components of DES architecture.
4	Discuss the Following a) Nonce Based Encryption b) Message Authentication Codes and Their Security
5	Write Short Notes on the following a) Security Model should depend on the power of the adversary you are anticipating b) All System do not require fool proof security c) Three Main Principles of Modern Cryptography d) Basic key Exchange Model