

GUJARAT TECHNOLOGICAL UNIVERSITY**M.E –IIst SEMESTER–EXAMINATION – JULY- 2012****Subject code: 725104****Date: 04/07/2012****Subject Name: PKI and Biometrics****Time: 10:30 am – 13:00 pm****Total Marks: 70****Instructions:**

1. Attempt all questions.
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.

- Q.1** (a) What are the basic principles of cryptography? Give the model of cryptography system and explain role of each element. **07**
(b) What are the limitations of the symmetric key cryptography? How do we overcome them? What are its strengths? **07**
- Q.2** (a) Give the structure of DES algorithm with brief explanation. Compare it with other symmetric key algorithms. **07**
(b) What are the important parameters to be taken care in order to realize the Feistel cipher structure? List and explain them. **07**
- OR**
- (b) What are the different cryptography attacks? List them and explain any one of them in detail. **07**
- Q.3** (a) Explain principles of the public-key cryptosystems in detail. **07**
(b) What do you mean by digital signature? Explain the digital signature standard. **07**
- OR**
- Q.3** (a) What do you mean by authentication? Explain any one of the authentication method or protocol. **07**
(b) Explain the important fundamentals of the PKI. **07**
- Q.4** (a) Explain any one of the PKI standard. **07**
(b) Explain the possible key management solution for the symmetric key cryptography. **07**
- OR**
- Q.4** (a) Explain the Diffie-Hellman Key exchange algorithm. **07**
(b) Explain how to design a secured system with combination of both symmetric and asymmetric cryptography systems. **07**
- Q.5** (a) What do you mean by single sign-on solution? Explain with at least one example. **07**
(b) Explain the implementation of the secure e-mail system with example. **07**
- OR**
- Q.5** (a) What are the practical issues to be considered while implementing a security system for an organization? **07**
(b) Discuss the legal issues in the network security. **07**
