| Seat No. | | o.: Enrolment No | | |
|----------|---|---|-----------|--|
| | GUJARAT TECHNOLOGICAL UNIVERSITY | | | |
| | | M.E –II st SEMESTER–EXAMINATION – JULY- 2012 | | |
| | • | ect code: 1720205 Date: 12/07/201 | 12 | |
| | Subject Name: Cryptography & Network Security | | | |
| | | e: 10:30 am – 13:00 pm Total Marks: 7 | 70 | |
| | | ructions: | | |
| | 2. | Attempt all questions. Make suitable assumptions wherever necessary. Figures to the right indicate full marks. | | |
| | 3. | rigures to the right mulcate run marks. | | |
| Q.1 | (a) | What do you mean by Database Access Control? How it can be implemented? | 07 | |
| | (b) | Explain Following: | 07 | |
| | | a. Threats b. Vulnerabilities c. Integrity d. Confidentiality e. Anonymity, f. Authentication g. Authorization | | |
| Q.2 | (a) | What do you mean by PKI? Explain Digital certificate in detail. How will you obtain Digital Certificate? | 07 | |
| | (b) | Note down the Security and Privacy Issues in RFIDs | 07 | |
| | ` , | OR | | |
| | (b) | How will you ensure Message integrity? Enlist method for Message integrity & explain one of them. | 07 | |
| Q.3 | (a) | How will you ensure authenticity of a digital message or document? Explain in detail. | 07 | |
| | (b) | Enlist various types of Firewall. Explain any one of them. | 07 | |
| | | OR | | |
| Q.3 | | Which protocol is responsible for establishing a session key between two parties on a network? Explain in detail. [Hint: it's a Symmetric Key Protocol] | 07 | |
| | (b) | Point out basic aim to establish Kerberos server? Also explain how Kerberos server works. | 07 | |
| Q.4 | (a) | Explain IP security. Reveal the fact that IP security plays important role in Network Security. | 07 | |
| | (b) | Explain RSA Algorithm. Explain RSA by taking Example for two prime number: $p = 61$ and $q = 53$. [Take other parameter as per your choice] OR | 07 | |
| Q.4 | (a) | How Data Encryption Standard (DES) works? | 07 | |
| Q.4 | (b) | Explain the difference of Worm & viruses. Provide example of each. | 07 | |
| Q.5 | (a) | Explain SSL protocol. | 07 | |
| - | (b) | Write a brief note on Biometric Authentication. | 07 | |
| | | OR | | |
| Q.5 | (a) | Give your ideas: How will you short out the issue of vulnerability in case of E-Transaction? | 07 | |

(b) Differentiate Message Authentication Code and Hash Function. Discuss various

properties that Hash function.

07