Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME – SEMESTER II– EXAMINATION – WINTER - 2016

Subject Code: 3725104 Date: 21/11/ 2016

Subject Name: PKI and Biometrics

Time: 2:30 pm to 5:00 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)** **07**

(i) Identify the attacks

a. The contents of the test is not confidential on the day of the test, it is confidential before the test day. **03**

b. The value of the check is changed (from $10 to $100).

c. so many e-mails may crash the server and the service may be interrupted.

(ii) Atbash was a popular cipher among Biblical writers. In Atbash, "A" is encrypted as "Z", "B" is encrypted as "Y" and so on. Similarly "Z" is encrypted as "A", "Y" is encrypted as "B" and so on. Suppose that the alphabet is divided into two halves and the letters in the first half are encrypted as the letters in the second half and vice versa. Find the type of cipher and key. Encipher the message "an exercise" using Atbash cipher. **04**

(b) Explain single sign on and single sign off property. Write about one application that is based on this property. **07**

Q.2 **(a)** Explain the four ways in which public keys are distributed. **07**

(b) Write the RSA public key algorithm. What are the security issues with RSA? **07**

OR

(b) Describe PKI trust models. **07**

Q.3 **(a)** Describe the modules included in generic biometric system. **07**

(b) Write applications of biometric. How performance of biometric is measured? **07**

OR

Q.3 **(a)** Write the legal issues involved in network security. **07**

(b) How public key infrastructure is deployed? **07**

Q.4 **(a)** Explain how authentication can be achieved with digital signature. **07**

(b) How E-mail can be secured? **07**

OR

Q.4 **(a)** What is cryptanalysis? Describe cryptanalytic and brute force attack. **07**

(b) How public key cryptography can be used to achieve authentication and confidentiality? Explain with block diagram. **07**

Q.5 **(a)** What are the problems with biometric? **07**

(b) How fingerprint can be used as authentication in biometric? **07**

OR

Q.5 **(a)** Explain file encryption solution. **07**

(b) How face detector can be used as authentication in biometric? **07**

****