Navrachana University
School of Business & Law
M.Sc. (IT)
End-Semester Examination May 2017
FYM.Sc.IT (Semester II)
Network Administration & Security (IT118)

Date: 08/05/2017
Time: 01.00 PM to 03.00 PM

Marks: 40
Weightage: 40%

Answer the following questions.

1) Name the parameters and design features of a Fiestel Cipher Structure. (2)
2) If the key size is 32 bits, then how many alternate keys have to be used for exhaustive key search? (2)
3) List and briefly define three uses of a public-key cryptosystem. (2)
4) In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is $e = 5$, $n = 35$. What is the plaintext M? (2)
5) In an RSA system, the public key of a given user is $e = 31$, $n = 3599$. What is the private key of this user? (2)
6) Explain line coding schemes in detail. (5)
7) Give examples of passive and active security attacks along with the security services/mechanism to protect against those attacks. (5)
8) Perform encryption and decryption using the RSA algorithm for the following: (10)
   a. $p = 3$; $q = 11$, $e = 7$; $M = 5$
   b. $p = 5$; $q = 11$, $e = 3$; $M = 9$
9) The new network administrator for your university has asked you to help him document and evaluate the university's network. He requests that you begin by addressing the following questions about Internet access and Internet use:
   - Tabulate all ways your own university is using the Internet?
   - What other ways do you believe the Internet could be better used for staff and students at your university? Do you believe the newer social networking aspects of the Internet could or should be used in an educational environment?
   - List out all the devices used in your university to establish network. Also, differentiate use and role of all those devices. (10)