COMP/IT 424 Midterm October 17 Winter 2014

Name _____ Student No. _____

No aids allowed. Answer all questions on test paper. Use backs of sheets if necessary.

Total Marks: **30**

[10] 1. Define each of the following four terms:

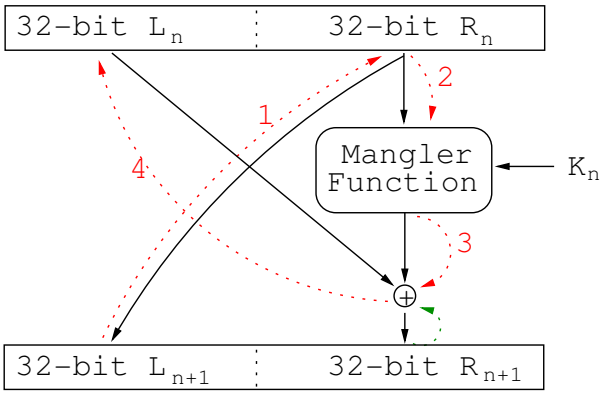
(a) Confidentiality

(b) Integrity

(c) Availability

(d) Authentication

[10] 2. Explain how to invert a single round of DES using the diagram below.



[10] 3. Explain how WEP is based on RC4; in particular, discuss the following:

(a) the difference between IV and the key; how long are they?

(b) the difference between the key and the key-stream.

(c) how is the XOR function used.

(d) how is decryption accomplished.