# FEDERAL UNIVERSITY OF TECHNOLOGY MINNA
# SCHOOL OF INFORMATION & COMMUNICATION TECHNOLOGY
# DEPARTMENT OF INFORMATION & MEDIA TECHNOLOGY
# FIRST SEMESTER EXAMINATION 2012/2013 SESSION
# CIT 315: INTERNET SECURITY

**INSTRUCTION:** ANSWER ALL QUESTIONS IN SECTION A AND TWO (2) QUESTIONS IN SECTION B

**TIME ALLOWED:** 2 HRS

## Section A

1. a) A cryptographic hash function *h* must have certain properties in order to be considered secure. State these properties. (6 *marks)*

   b) Briefly describe the concept of asymmetric (or public-key) cryptography as disclosed by Diffie and Hellman. (3 *marks)*

   c) In practice, a variant of the Data Encryption Standard (DES) called the Triple-DES is being used and is much more popular. Discuss why? (2 *marks)*

   d) What is a Virtual Private Network (VPN)? (2 *marks)*

   e) Briefly describe how a challenge-response protocol is used by an authentication system. (2 *marks)*

2. a) The latest trend in the industry tends towards selling Intrusion Prevention Systems (IPS) rather than Intrusion Detection System (IDS). Discuss the pros and cons of this trend. (4 *marks)*

   b) Describe the **limitations** of each of the two basic methods for Intrusion Detection. (3 *marks)*

   c) Describe Host-Based Intrusion Detection Systems (HIDS). (2 *marks)*

   d) Describe extensively the three techniques used to crack passwords (6 *marks)*

## Section B

1. a) What are Malwares? (5 *marks)*

   b) Clearly explain the similarities and the differences between a virus and a worm (5*marks)*

   c) Explain the three basic functional mode of antivirus software (5 *marks)*

2. a) Explain in a few sentences how NAT works (5 *marks)*

   *b)* What is the difference between Static NAT and Dynamic NAT? (5 *marks)*

   c) What are the advantages of NAT? (5 *marks*)

3. Consider the following basic principles: Least Privileges, Default Deny, Defense in Depth, Choke Point, Simplicity and User Participation in the context of configuring a firewall, discuss each principle. (15 *marks*)