TECHNICAL UNIVERISTY OF MOMBASA

Faculty of Engineering & Technology

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

UNIVERSITY EXAMINATION FOR DEGREE IN:
BACHELOR OF TECHNOLOGY IN INFORMATION TECHNOLOGY
BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY
(BTIT/BSIT – Y4 S2)

EIT 4414: CRYPTOGRAPHY & NETWORK SECURITY

END OF SEMESTER EXAMINATION
SERIES: DECEMBER 2014
TIME: 2 HOURS

Instructions to Candidates:
You should have the following for this examination
- *Answer Booklet*

This paper consists of **FIVE** questions. Attempt question **ONE (Compulsory)** and any other **TWO** questions
Maximum marks for each part of a question are as shown
This paper consists of **TWO** printed pages

Question One (Compulsory)

a) Define the following terms as used in Network Security: **(10 marks)**
(i) Confidentiality
(ii) Integrity
(iii) Non-repudiation
(iv) Authenticity
(v) Accountability

b) Explain TWO main draw backs of mono-acphasetic substitution ciphers. **(4 marks)**

c) You are working from an internal work station with an IP address of 192.168.2.65 within Technical University of Mombasa. Explain how you are able to browse the Internet (i.e. send requests to a remote Internet based host and receive replies. **(4 marks)**

d) Security is the ability of a system to protect information and system resources with respect to confidentiality, availability and integrity state and explain THREE examples of security violations **(6 marks)**

e) State and explain THREE characteristics of cryptographic systems **(6 marks)**

Question Two

a) You wish to register for a master degree at TUM. The University requires your transcripts before admission. Explain clearly how you can send the transcripts securely. How would the admissions office authenticate the transcripts **(6 marks)**

b) Compare and contrast symmetric and asymmetric key cryptography **(4 marks)**

c) Explain the operation of the following Pretty Gord Privacy (PGP) services with references to email security **(10 marks)**

(i) Confidentiality

(ii) Authentication

Question Three

a) Explain THREE challenges of designing network security **(6 marks)**

b) Explain with justification how message digests can be applied in the realization of an efficient message integrity scheme **(6 marks)**

c) Distinguish between stream and block ciphers identify and explain TWO advantages and TWO disadvantages of each. **(8 marks)**

Question Four

a) Name and explain FOUR types of active attacks in network security **(8 marks)**

b) Explain FOUR ways that two parties A and B can achieve key distribution **(4 marks)**

c) Explain FOUR basic tasks in designing a particular security service **(8 marks)**

Question Five

a) See attached diagram.

b) Describe any TWO techniques used by firewalls to offer protection **(4 marks)**

c) Distinguish between digital signature and digital certificate citing a suitable application of each **(4 marks)**

d) What do you understand by the term “reusable password”? Explain how such passwords can be made more secure **(4 marks)**