TECHNICAL UNIVERISTY OF MOMBASA

Faculty of Engineering & Technology

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

UNIVERSITY EXAMINATION FOR:
BACHELOR OF TECHNOLOGY IN INFORMATION TECHNOLOGY
(BTIT 11M)
EIT 4414: CRYPTOGRAPHY & NETWORK SECURITY

END OF SEMESTER EXAMINATION
SERIES: AUGUST 2013
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** 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) Using the Rail-fence cipher, encrypt the message.
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG **(2 marks)**

b) Explain the following objectives of computer security:
(i) Availability
(ii) Confidentiality
(iii) Integrity
(iv) Authenticity
(v) Non-repudiation **(10 marks)**

c) Explain the **THREE** services provided by the OSI security architecture. **(6 marks)**

d) State the format's theorem **(2 marks)**

e) Briefly explain the following terms:
- **(i)** Enciphering
- **(ii)** Symmetric algorithm
- **(iii)** Digital signature
- **(iv)** Vulnerability
- **(v)** Cryptosystem **(10 marks)**

Question Two

a) Discuss any **FOUR** properties of digital signatures. (**4 marks)**

b) There are several general means of authenticating a user's identify which can be used alone or in combination. Discuss any **FOUR** of them giving suitable examples. **(8 marks)**

c) (i) Explain the term "IP Security" **(2 marks)**

(ii) Discuss any **FOUR** benefits of IP security **(8 marks)**

Question Three

a) Using Caesar Cipher, decrypt the message:
PHHW PH DIWHU WKH WRJD SDUWB **(4 marks)**

b) Explain the difference between the following terms:
- **(i)** "cryptography" and "steganography"
- **(ii)** "stream cipher" and "block cipher" **(8 marks)**

c) With an aid of an appropriate diagram, discuss:
- **(i)** Public key encryption
- **(ii)** Private key encryption **(8 marks)**

Question Four

a) Virtually in all distributed environment, electronic mail is the most heavily used network-based application. Hence there is demand for authentication and confidentiality services.
- **(i)** Explain the security enhancement schemes
- **(ii)** "Pretty-Good Privacy (PGP)"
- **(iii)** Secure/Multipurpose Internet Mail Extension (SMIME) Security **(4 marks)**

b) Discuss any **FIVE** reasons for the PGP'S wide use and explosive growth. **(10 marks)**

c) Explain the following concepts relating to web security.
- **(i)** Secure Socket Layer (SSL)
- **(ii)** Transport Layer Security (TLS)
- **(iii)** Secure Shell (SSH) **(6 Marks)**

Question Five

a) As a system administrator of TUM, discuss any **FOUR** attacks that may modify data or disrupt the system **(8 marks)**

b) Explain the difference between the following terms:

(i) "Passive Attack" and "Active Attack"
(ii) "Masquerader" and "Misfeasor"
(iii) "Intrusion Deletion System" and "Firewall" **(12 marks)**