TECHNICAL UNIVERISTY OF MOMBASA

Faculty of Engineering & Technology

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY

UNIVERSITY EXAMINATIONS FOR DEGREE IN:
BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY
(BSIT 12J – Y4 S1)

BTIT 2317: FUNDAMENTALS OF COMPUTER SECURITY

END OF SEMESTER EXAMINATION
SERIES: APRIL 2015
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) Distinguish between the following terms:
(i) "Firewall" and "Intrusion Detection system"
(ii) "Stream Cipher" and "Block Cipher"
(iii) "Computer Security" and Network Security"
(iv) "Steganography" and "Cryptography"
(v) "Hot site" and "Cold site" **(10 marks)**

b) Explain the following terms:
(i) Web security
(ii) IP security
(iii) Hash algorithms
(iv) Message digest
(v) Computer crimes
(vi) S-MIME **(12 marks)**

c) State any FOUR properties of a digital signature **(4 marks)**

d) State any FOUR methods of user authentication **(4 marks)**

Question Two

a) Consider an Automated Teller Machine (ATM) in which users provide a personal identification Number (PIN) and a card for account access. Give examples of confidentiality, integrity, availability and authenticity requirements associated with the system and in each case indicate the degree of importance of the requirement **(8 marks)**

b) For each of the following assets, assign a Low, Moderate, or High impact level for the loss of a confidentiality, availability and integrity respectively. Justify your answers.

(i) An organization managing public information on its web server
(ii) A law enforcement organization managing extremely sensitive investigative information
(iii) A financial organization managing routine administrative information (non privacy-related information) **(6 marks)**

c) Using rail fence techniques, encode the message "THE QUICK BROWN FOX JUMPS OVER DOG" the toga party **(3 marks)**

d) Using Caesar Cipher, decode the message "PHHW PH DIWHU WKH WRJD 5DUWB" **(3 marks)**

Question Three

a) Explain the difference between: "Cryptanalysis" and Brute-force" **(4 marks)**

b) Using an illustration, explain the FIVE ingredients of symmetric encryption scheme **(12 marks)**

c) Distinguish between "symmetric cipher" "asymmetric cipher" **(4 marks)**

Question Four

a) Risk-based taxonomy is based on a vast number of reported instances of actual attacks. Describe any FIVE attacks to information systems, citing suitable examples **(10 marks)**

b) Describe any THREE methods that can be used to prevent attacks to information systems **(6 marks)**

c) There are many good reasons to perform a risk analysis in preparation for creating a security plan. Despite the advantages of risk analysis, there are several arguments against using it to support decision making. Describe any TWO reasons for and against risk analysis **(4 marks)**

Question Five

a) Security management must manage risks in terms of causes, effects and costs of a security loss. This means that systematic security management allows counter-measures to be chosen in a planed and managed way, since too much security wastes money while too little security wastes information systems resources capability. Describe the FOUR distinct stages of security management **(16 marks)**

b) Explain the following terms:

(i) IP address spoofing
(ii) Data Encryption standard **(4 marks)**