JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATION SYSTEMS

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE

COMPUTER SECURITY

3RD YEAR 1ST SEMESTER 2013/2014 ACADEMIC YEAR

KISUMU LEARNING CENTRE

COURSE CODE: IIT 3315

COURSE TITLE: FUNDAMENTALS OF CRYPTOPGRAPHY AND STEGANOGRAPHY

EXAM VENUE: **STREAM: (BSc. Comp Security)**

DATE: 24/04/14 **EXAM SESSION: 9.00 – 11.00 AM**

TIME: 2.00 HOURS

Instructions:

1. **Answer question 1 (Compulsory) and ANY other 2 questions**
2. **Candidates are advised not to write on the question paper.**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room.**

QUESTION ONE (30 MARKS)

a) Differentiate between passive and active security threats [2 marks]
b) List and briefly define at least three of the categories of passive and active security attacks. [8 marks]
c) For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers. [8 marks]

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 (not privacy related information).
iv. An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

d) Explain the Playfair cipher. [5 marks]
e) Use Playfair Cipher technique to decrypt the following ciphertext. VRFKAFGONVNBULMLIZIHEIFESHZV. The keyword is ANOTHER. [7 marks]

QUESTION TWO (20 MARKS)

a) Differentiate between a mono-alphabetic cipher and a polyalphabetic cipher. [3 marks]

b) Briefly explain your understanding of a block cipher and a stream cipher. [4 marks]
c) List and briefly define types of cryptanalytic attacks based on what is known to the attacker. [6 marks]
d) Briefly explain the Hill Cipher; apply this principle to ciphertext the word "COE" using ANOTHERBZ as the key. [7 marks]

QUESTION THREE (20 MARKS)

a) Briefly explain the Caesar cipher. [3 marks]
b) Applying the principle of Caesar cipher, where k takes on a value in the range 1 to 25.The decryption algorithm is $p = D(k, C) = (C - k) \bmod 26$. Decrypt the following ciphertext. PHHW PH DIWHU WKH WRJD SDUWB. [5 marks]

c) The following shows a plaintext and its corresponding ciphertext. Is the cipher mono-alphabetic? Justify your answer. [2 marks]

Plaintext: HELLO
Ciphertext: ABNZF

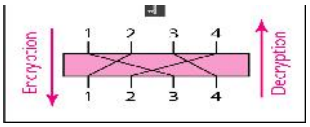
d) 

Fig.1. Encrypt the message "HELLO MY DEAR," using the key shown in fig.1. [4 marks]

e) Explain the drawbacks of substitution ciphers [3 marks]

f) List the elements of Information security and explain each in brief [3 marks]

QUESTION FOUR (20 MARKS)

a) Explain the operational security model with block diagram [2 marks]
b) Explain the various components of Asymmetric and Symmetric encryptions [4 marks]
c) Explain the working of DES in detail [5 marks]
d) Compare and contrast Rijndael and AES? [4 marks]
e) Explain FIVE parameters and design choices that determine the actual algorithm of a Feistel cipher. [5 marks]

QUESTION FIVE (20 MARKS)

a) Draw a matrix that shows the relationship between security services and attacks [6 marks]
b) What is the difference between a block cipher and a stream cipher? [4 marks]
c) List and briefly define types of cryptanalytic attacks based on what is known to the attacker. [5 marks]
d) State three advantages and two limitations of Rijndael [5 marks]