JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING

UNIVERSITY EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN SECURITY AND FORENSICS

3RD YEAR 1ST SEMESTER 2020/2021 ACADEMIC YEAR

SPECIAL RESIT TWO

MAIN CAMPUS

COURSE CODE: IIT 3315

COURSE TITLE: FUNDAMENTALS OF CRYPTOGRAPHY AND STEGANOGRAPHY

EXAM VENUE: **STREAM: COMPUTER SECURITY & FORENSICS**

DATE: **EXAM SESSION: 2 HRS.**

TIME:

INSTRUCTIONS

1. **Answer Question 1 (Compulsory) and ANY other TWO 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) Define the following terms
   i) Cryptography. **(2 mark)**
   ii) Cryptoanalysis. **(2 mark)**
   iii) Cryptology. **(2 mark)**
   iv) Cyber terrorism **(2 mark)**
   v) Ciphertext **(2 mark)**

b) Differentiate clearly between symmetric and asymmetric encryption. **(6 marks)**

c) Mention any four characteristics of a good cipher? **(4 marks)**

d) Compare and contrast steganography and digital watermarking. (6 Marks)

e) Distinguish between substitution and transposition as applied in cryptography(4 Marks)

QUESTION TWO 20 MARKS

a) State and explain the four different types of attacks applied in cryptology (8 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 SDUWB. (8 marks)

c) Explain the drawbacks of substitution ciphers (4 Marks)

QUESTION THREE 20 MARKS

"Functions are used in encryption to ensure that information is hidden from anyone for whom it's not intended"

a) State and explain the four main purposes of cryptography **(8 marks)**

b) If function of f(x) = (x-2)/(3x-1) is an encrypting function for a message, find the function g(x) that is its decrypting function. **(8 marks)**

c) Differentiate between passive and active security threats (4 marks)

QUESTION FOUR 20 MARKS

a) Using appropriate examples, briefly explain the following terms as applied to security of data. . (8 marks)
   i. Non-Repudiation
   ii. Authentication
   iii. Confidentiality
   iv. Integrity

b) Differentiate between stream and block ciphers. **(4 marks)**

c) Identify both the advantages and disadvantages of: **(8 marks)**
   i. S
   tream Ciphers

ii. Block Ciphers.

QUESTION FIVE 20 MARKS

a) Define the following terms: **(10 marks)**

i) S
teganography

ii) C
omputer Emergency Response Team (CERT)

iii) K
ey

iv) H
activism

v) Root access .

b). Describe the working principles behind the following security features (10 marks)

i) H
ash functions

ii) D
igital signatures

iii) C
ertificate of authority

iv) Industrial control system (ICS)