JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING

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

3RD YEAR 1ST SEMESTER 2022/2023 ACADEMIC YEAR

MAIN,KISUMU CAMPUS

COURSE CODE: ICB 1307

COURSE TITLE: FUNDAMENTAL S CRYPTOGRAPHY AND STEGANOGRAPHY

EXAM VENUE: **STREAM:**

DATE: **EXAM SESSION:**

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 1 [30 marks]

a) Define the following terms
   i) Cryptography **(2 marks)**
   ii) Steganography **(2 marks)**
   iii) Cryptanalysis **(2 marks)**
   iv) Steganalysis **(2 marks)**

b) Differentiate between diffusion and confusion encryption processes **(4 marks)**

c) Give a distinction between ***secrecy*** and ***security*** for steganographic protocols **(4 marks)**

d) Explain what is Quantum error-correcting code **(4 marks)**

e) Give the advantages of end to end encryption **(4 marks)**

f) Describe how data confidentiality is achieved using Public Key cryptography **(6 marks)**

Question 2 [20 marks]

a) Discuss the Steganographic approaches **(8 marks)**

b) Discuss the classification of cryptography **(6 marks)**

c) Discuss the challenges facing any image steganographic system **(6 marks)**

Question 3 [20 marks]

a) Kirchhoff's' principle states that the adversary knows all the details of the cryptosystem including its algorithms and their implementations. Discuss the attacks that may be carried out on the secrecy of an encryption scheme **(10 marks)**

b) Statistical Steganalysis is more robust than signature Steganalysis since mathematical analysis is more accurate than visual analysis. Discuss the categories of statistical analysis **(10 marks)**

Question 4 [20 marks]

a) Discuss the requirements of Public Key cryptography **(10 marks)**

b) Discuss how the symmetric encryption model works **(10 marks)**

Question 5 [20 marks]

a) User "A" receives the cipher-text "C" and recovers the message "M" by decrypting it using its own Private Key (d, n): $M = C^d mod\ n$ .Prove that decrypted value of a cipher-text at the recipient end is an exact copy of the plaintext encrypted at the sender end where M is relatively prime to n. **(10 marks)**

b) A plaintext M is encrypted using RSA and two Public Keys (n, e) and (n, f) such that $GCD(e, f) = 1$. It produces cipher-texts C_c and C_f

$$C_e = M^{\boldsymbol{e}}\ mod\ n$$
$$C_e = M^f\ mod\ n$$

Show how a common modulus attack can be carried out on the above **(10 marks)**