UGANDA MARTYRS UNIVERSITY
NKOZI

UNIVERSITY EXAMINATIONS

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & INFORMATION SYSTEMS

SEMESTER I 2021-2022
SECOND YEAR EXAMINATION FOR BSC. COMPUTER SCIENCE
CRYPTOLOGY & CODING THEORY
CSC 2108

DATE: 20th January 2022

TIME: **9:30 AM – 12:30 PM**

DURATION: 3HRS

Instructions:

1. *Carefully read through ALL the questions before attempting*
2. *This paper consists of two sections, Section A and Section B*
3. *Answer* ***ALL*** *Questions in Section A*
4. *Answer any* ***TWO*** *Questions in Section B*
6. *Write your answers in the answer booklet provided*
7. *No* ***names*** *should be written anywhere on the examination book.*
8. *Ensure that your* ***Reg number*** *is indicated on all pages of the examination answer booklet.*
9. *Ensure your work is* ***clear*** *and* ***readable****. Untidy work shall be penalized*
10. *Any type of examination Malpractice will lead to automatic disqualification*
11. *Do not write anything on the question paper.*

SECTION A (60 MARKS)

QUESTION 1: Explain the following types of coding. **[8 MARKS]**

a) Data compression (also known as source coding)
b) Error control (also known as channel coding)
c) Cryptographic coding
d) Line coding

QUESTION 2:

a) Explain four security services provided by cryptography. **[8 MARKS]**
b) Explain the following cryptographic primitives. **[8 MARKS]**
   i. Digital signatures
   ii. Message Authentication Code (MAC)
   iii. Hash function
   iv. Encryption

QUESTION 3:

a) In a group of *n* people, to enable 2-party communication between any two persons, the number of keys required for the group is given by $n * (n - 1) / 2$. How many keys are required to communicate between any two parties in a group of 5 persons in a symmetric key cryptosystem? Show how you work out your answer. **[4 MARKS]**

b) Explain three (3) characteristics that distinguish modern cryptographic practices from classical or traditional cryptographic practices. **[6 MARKS]**

QUESTION 4: Using a diagram, identify and describe the different parts of a cryptosystem (also known as a cipher system). **[10 MARKS]**

QUESTION 5:

a) Name two types of cryptosystems and explain two differences between them. **[6 MARKS]**
b) Name one advantage and one disadvantage of each type of cryptosystem. **[4 MARKS]**

QUESTION 6:

a) Distinguish between a *passive* and an *active*, cryptographic attack. **[2 MARKS]**
b) Explain the following types of cryptographic attacks **[4 MARKS]**
   i. Ciphertext Only Attach (COA)
   ii. Known Plaintext Attack (KPA)

SECTION B (40 MARKS)

QUESTION 7:

a) What is the difference between a block cipher and a stream cipher? **[4 MARKS]**

b) Use a block diagram to illustrate the design model for a Feistel block cipher. **[10 MARKS]**

c) Describe the encryption and description processes in a Feistel block cipher. **[6 MARKS]**

QUESTION 8: The Data Encryption Standard (DES) is a symmetric-key block cipher whose design is based on the Feistel block cipher.

a) Use a block diagram to illustrate the structure of the DES **[10 MARKS]**

b) Explain the *Avalanche effect* and *Completeness* properties of block ciphers. **[6 MARKS]**

c) Give two examples of block ciphers. **[4 MARKS]**

QUESTION 9:

a) Use a block diagram to illustrate the structure and relationship between the different components of a public key encryption scheme. **[10 MARKS]**

b) Secure communication using the Rivest, Shamir, and Adleman (RSA) encryption scheme requires one to generate a public-private key pair. Given two prime numbers $p = 7$ and $q = 13$, and a derived number $e = 5$ such that $1 < e > (p-1)(q-1)$ to satisfy the requirements of the scheme. Generate a public key for this cryptosystem. Show how you work out the solution. **[4 MARKS]**

c) Explain the following properties of hash functions. **[6 MARKS]**

   i. Pre-image resistance

   ii. Collision resistance

THE END!