CHUKA UNIVERSITY

UNIVERSITY EXAMINATIONS

EXAMINATION FOR THE AWARD OF BSC (COMPUTER SCIENCE) AND BSC (APPLIED COMPUTER SCIENCE)

COMP 424: Cryptography and Computer Security

STREAMS: BSC (COMP. SCI) Y4S2 **TIME: 2 HOURS**

DAY/DATE: MONDAY 08/4/2019 **2.30 P.M. – 4.30 P.M.**

INSTRUCTIONS

- Attempt **Question 1** and any other **TWO** from **SECTION B**
- Marks are awarded for clear and concise answers
- ONLY the first **THREE** Questions attempted will be marked **(Question one inclusive)**

SECTION A-COMPULSORY

Question One [30 Marks]

(a) What is the key distinguishing characteristic between a stream cipher and a block cipher [4 Marks]

(b) What is the effect of the key size on the strength of a security algorithm [4 Marks]

(c) Briefly describe the following concepts as applied in database security [6 Marks]

(i) Subject

(ii) Object

(iii) Access right (privileges)

(d) Write an SQL statement that gives user U_1 the **select** privileges on **branch** table and allows U_1 to grant this privilege to others [4 Marks]

(e) A company employee has been using the password **"APPLE"** for the past six months to access a database. Discuss why this poses a security risk and suggest ways in which the company could improve password management [4 Marks]

(f) Give **ONE** similarity and **ONE** difference in the way Ms-windows and UNIX stores their passwords [4 Marks]

(g) Public key infrastructure refers to the CAs and digital certificate procedures that are accepted by all parties. Identify **FOUR** items found on a digital certificate [4 Marks]

SECTION B-Attempt TWO questions in this section

Question TWO [20 Marks]

(a) Describe key characteristic(s) of each of the following cryptographic schemes.

(i) Secret key cryptography [3 Marks]

(ii) Public key cryptography [3 Marks]

(iii) Hash functions [3 Marks]

(b) The **DES** cipher function enables the algorithm to achieve confusion so that the relationship between the statistics of the ciphertext and the values of the encryption key is as complex as possible. Using a diagram, illustrate how a DES cipher function operates [11 Marks]

Question THREE [20 Marks]

(a) While giving examples, give key differences between Discretionary access control and mandatory access control [4 Marks]

(b) Human element is an important consideration in any security issue because it contributes heavily to realization of attacks primarily because a human attacker is behind the development of an attack tool and will still be the one to run the first attack command. Describe **FIVE** phases of the hacking methodology [10 Marks]

(c) Briefly describe the challenge handshake authentication protocol (CHAP) [6 Marks]

Question FOUR [20 Marks]

(a) Explain and with the support of a diagram how you can use public key cryptography to encrypt and distribute/share public key [10 Marks]

(b) Explain and with the support of a diagram how you can combine public key cryptography and hash functions to create a digital signature [10 Marks]

Question FIVE [20 Marks]

(a) Illustrate using a diagram a basic security model that can be used to protect networks [8 Marks]

(b) Briefly describe the first **THREE** steps of security risk assessment in an organization that has invested heavily in computer based systems [6 Marks]

(c) Describe while giving examples **THREE** types of controls that can be used to manage security risks in an organization [6 Marks]
