CHUKA  **UNIVERSITY**

UNIVERSITY EXAMINATIONS

EXAMINATION FOR THE AWARD OF DEGREE OF BACHELOR OF SCIENCE IN APPLIED COMPUTER SCIENCE

ACSC 462: COMPUTER AND NETWORK SECURITY

STREAMS: BSC (ACSC) Y4S2 **TIME: 2 HOURS**

DAY/DATE: MONDAY 06/04/2020 **2.30 PM – 4.30 PM**

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 Ciphers. **[4 Marks]**

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

(c)Briefly describe **THREE** key technical security mechanisms that are commonly employed to provide security in networked systems. **[6 Marks]**

(d) Differentiate between a threat and a vulnerability in relation to computer network security. **[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 **[2 Marks]**
(ii)Public key cryptography **[2 Marks]**
(iii)Hash functions **[2 Marks]**

(b)Briefly describe the purpose of the following information security policies when implemented in an organization.

(i)Information classification **[2 Marks]**
(ii) Access control **[2 Marks]**
(iii) Backup **[2 Marks]**
(iv)Asset disposal **[2 marks]**
(v) Clear desk **[2 Marks]**
(vi) Incidence response **[2 Marks]**
(vii) Log review **[2 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 run the first attack command. Social engineering is an instance of human element in computer security.
(i)Describe how password pilfering attack may be carried out using social engineering. **[4 Marks]**

(iii)Describe T**HREE** other techniques for password pilfering and corresponding preventive measures. **[6 Marks]**

(c)Identity spoofing attacks allow attackers to impersonate a victim without using the victim's passwords. Describe **THREE** forms/types of Network spoofing attacks. **[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 **THREE**physical controls that need to be put in place in order to protect networked resources in an organization. **[6 Marks]**

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