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: **TIME: 2 HOURS**

DAY/DATE: TUESDAY18/4/2023 **11.30 P.M. – 1.30 P.M.**

INSTRUCTIONS:

1. **Answer question ONE and any other TWO questions**
2. **Marks are awarded for clear and concise answers**

SECTION A – COMPULSORY

Question ONE [30 Marks]

(a)While describing the following tools, indicate the role played by each in protecting computer Systems i.e servers and clients **[10 Marks]**

(i)Antivirus

(ii)Authentication

(iii)Access Controls

(iv)Personal firewalls

(v)Intrusion detection

(b)Give **TWO** advantages and **TWO** disadvantages of biometric based authentication **[4 Marks]**

(c) A successful cyber-attack can cause major damage to a business. Briefly describe THREE key consequences that security breaches can impact on a business **[6 Marks]**

(d) Describe **TWO** limitation of passwords when used to authenticate users logging in a remote server **[2 Marks]**

(e)Describe **TWO** key characteristic(s) of each of the following cryptographic algorithms:

(i) Symmetric algorithms **[2 Marks]**

(ii)Asymmetric algorithms **[2 Marks]**

(f)While giving examples, distinguish between active and passive computer security attacks

[4 Marks]

SECTION B- Answer any TWO questions

Question TWO [20 Marks]

(a)Given a Key: 4 3 1 2 5 6 7. Using Rail fence show how you can encrypt the message **"Attack will be at ten o'clock"** **[6 Marks]**

(b)Using the word "MASTER**"** as the key word, encrypt the message "**honey"** based on play fair cipher **[6 Marks]**

(c)An encryption scheme is either unconditionally secure or computationally secure. Discuss

[4 Marks]

(d) Describe **FOUR** ways of protecting Servers and Clients in a network from **disruption** and **unauthorized disclosure** of data held in them **[4 Marks]**

Question THREE [20 Marks]

(a) Alice and Bob have agreed to use the Diffie Hellman key exchange mechanism. Given p = 37 and g = 13. Suppose Alice chooses her secret key **x =10** while Bob chooses his secret key **y=7**.

(i)Determine Alice's Public key **[3 Marks]**

(ii)Determine Bob's public key **[3 Marks]**

(iii)Determine the shared session key **[4 Marks]**

(b)Describe the main strength of challenge authentication protocol (CHAP) and further demonstrate **FOUR** steps that describe its operation **[10 Marks]**

Question FOUR-20 Marks

(a)Given the key below, Use Hill Cipher to encrypt the message **"liar" [5 Marks]**

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

(b) Given p = 5; q = 11, e = 3; M = 9,use RSA algorithm to answer the following questions.

(i)Determine the value n [**3 Marks]**

(ii)Determine f(n) **[3 Marks]**

(iii)Determine Public Key **[3 Marks]**

(iv)Determine Private Key **[3 Marks]**

(v)Encrypt **"M"** **[3 Marks]**

Question FIVE [20 Marks]

(a)A digital envelope addresses weaknesses of both Asymmetric and Symmetric key encryption. Using a diagram, illustrate how Asymmetric encryption can be used to create a digital envelope as well as digital signature **[10 Marks]**

(b)Use the expression E(x) = (9x + 7) MOD 26 to encrypt the message: "shoot him" **[4 Marks]**

(c)Illustrate using a diagram how SSL protocol provides the following security services:

(i)Confidentiality **[3 Marks]**

(ii)Integrity **[3 Marks]**

……