

CHUKA



UNIVERSITY

UNIVERSITY EXAMINATIONS

FOURTH YEAR EXAMINATION FOR THE AWARD OF BACHELOR OF SCIENCE
IN COMPUTER SCIENCE

COSC 464: CRYPTOGRAPHY AND COMPUTER SECURITY

STREAMS: BSC. COMP. SCI (Y4S2)

TIME: 2 HOURS

DAY/DATE: FRIDAY 26/03/2021

11.30 A.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) Consider RSA with $p = 5$ and $q = 7$. What are the values of n and $f(n)$ [4 Marks]
- (d) Describe **FOUR** limitations to encryption solutions [4 Marks]
- (e) 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]
- (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) Bell Lapudula model assumes a Read down; write up approach while Biba model assumes a Read up; write down approach.
- (i) Describe **TWO** key conditions that guide operation of Bell lapudula model [6 Marks]
 - (ii) Describe **TWO** key conditions that guide operation of Biba model [6 Marks]
 - (iii) What is the difference between the security service provided by Bell lapudula model and that provided by Biba Model [4 Marks]
- (b) Differentiate between Discretionary access control and Mandatory access control [4 Marks]

QUESTION THREE [20 MARKS]

- (a) One of the known password pilfering methods is dictionary attack.
- (i) Illustrate **THREE** key dictionary attack steps [6 Marks]
 - (ii) Give **TWO** countermeasures to dictionary attack password pilfering technique [4 Marks]
- (b) Describe **FIVE** key technical differences between DES and AES algorithms [10 Marks]

QUESTION FOUR [20 MARKS]

- (a) Give a brief description of access control mechanisms that employ the following [10 Marks]
- (i) IP address
 - (ii) Domain Name
 - (iii) User name and password
 - (iv) Client certificates
- (b) DES encryption algorithm design prescribes 16 rounds of operation on **L** and **R** blocks. State the formulae applied on each iteration to compute [4 Marks]
- (i) L_n
 - (ii) R_n
- (c) Describe **THREE** key design principles employed by DES encryption algorithm [6 Marks]

QUESTION FIVE [20 MARKS]

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