CHUKA  **UNIVERSITY**

UNIVERSITY EXAMINATION
RESIT/SUPPLEMENTARY / SPECIAL EXAMINATIONS
EXAMINATION FOR THE AWARD OF DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE

COSC 464: CRYPTOGRAPHY AND COMPUTER SECURITY

STREAMS: **TIME: 2 HOURS**

DAY/DATE: TUESDAY 02/11/2021 **8.30 A.M - 10.30 A.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 network infrastructure **[10 Marks]**

(i)Firewall

(ii)Proxy servers

(iii)Virtual private network

(iv)Secure sockets layer (SSL)

(v)Intrusion detection systems

(b)Give **TWO** advantages and **TWO** disadvantages of host IP address and/or DNS name based authentication **[4 Marks]**

(c)Briefly describe **FOUR** main services provided by cryptography in a netcentric system **[4 Marks]**

(d)Describe **FOUR** forms of authorization that can be applied on a database to control access **[4 Marks]**

(e) Describe **FOUR** limitations to encryption solutions **[4 Marks]**

(f)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- Answer any TWO questions

Question TWO [20 Marks]

(a)Describe the following security threats that an organization conducting business online may face **[6 Marks]**

i. Phishing
ii. Spoofing
iii. Sniffing

(b)Authentication based on user ID and password requires user to provide protected information in order to be authenticated. Give **TWO** advantages and **TWO** disadvantages of this authentication approach when employed on online systems **[4 Marks]**

(c)Highlight the key features that illustrate and/or differentiate symmetric encryption and public key encryption while giving atleast one standard/algorithm in each **[10 Marks]**

Question THREE [20 Marks]

(a)Some firms hire outsiders to crash their systems in order to test their security readiness.

i. What are "grey" and "black" hats and why do firms avoid them as security testers **[6 Marks]**
ii. Give **TWO** countermeasures to denial of service attacks **[4 Marks]**

(b) Using a diagram, give a detailed description of RC4 encryption algorithm **[6 Marks]**

(c)What are the key differences between DES and AES algorithms **[4 Marks]**

Question FOUR-20 Marks

(a)Describe the **FIVE** technical objectives of computer security listed below **[5 Marks]**

(i) Integrity
(ii)Availability
(iii)Confidentiality
(iv) Authentication
(v)Non-repudiation

(b)Identify **FIVE** vulnerable parts of a typical e-commerce transaction model **[5 Marks]**

(c)Using a diagram, illustrate an SSL connection setup **[10 Marks]**

Question FIVE [20 Marks]

(a)Briefly explain the operation of the following protocols:

i. CHAP **[5 Marks]**

ii. Kerberos **[5 Marks]**

(b)A digital envelope addresses weaknesses of both public key encryption and Symmetric key encryption. Illustrate how:

(i)Double encryption can be used to ensure authenticity and non-repudiation **[5 Marks]**

(ii)Public key cryptography can be used to create a digital envelope **[5 Marks]**

……