MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY

P.O. Box 972-60200 – Meru-Kenya.
Tel: +254 (0)799529958, +254 (0)799529959, +254 (0)712524293
Website: www.must.ac.ke Email: info@must.ac.ke

University Examinations 2021/2022
SECOND YEAR, SECOND SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF COMPUTER SCIENCE, BACHELOR OF COMPUTER TECHNOLOGY, BACHELOR OF COMPUTER SECURITY & FORENSICS,BBIT,BIT

CCS 3402: COMPUTER SECURITY AND CRYPTOGRAPHY

DATE: MAY 2022 **TIME: 2 HOURS**

INSTRUCTIONS: Answer Question ONE and ANY OTHER TWO QuestionsSECTION A-COMPULSORY

Question One [30 Marks]

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

a) Given Key: 4 3 1 2 5 6 7 Using Rail fence show how you can encrypt the message "Attack postponed till two AM" [6 Marks]

(b)Describe key characteristic(s) of each of the following cryptographic algorithms

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

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

c) Given the key below ,Use Hill Cipher to encrypt the message " am ready (6 Marks)

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

Show your calculations and the result. (6 Marks)

(d) For each of the following computer threats, give **ONE** vulnerability exploited to realize an attack and ONE control that can be implemented to prevent an attack from being successful

(i)Dictionary attack **[2 Marks]**

(ii)Password sniffing **[2 Marks]**

(e) Define the following terms as used in security (6marks)

I. Confidentiality

Ii. Integrity

Iii. Availability

SECTION B-Attempt TWO questions in this section

Question TWO [20 Marks]

a) Use play fair cipher to encrypt the message " cryptograhy" Use the word " **MASTER"** as the key word (5 Marks)

b) Using RSA show how two users can exchange key give p = 5; q = 11, e = 3; M = 9 (5 Marks)

a) Alice and Bob have agreed to use the Diffie Hellma key exchange mechanism. Explain how this system works. Given the p = 37 and g = 13, show how this mechanism can be used to send keys secretly.
[5 Marks]

b) Discuss any five requirements for a hash function (5 marks)

Question THREE [20 Marks]

(a)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. Describe how password pilfering attack may be carried out using social engineering **[4 Marks]**

(b)In NOV 1999,http://www.slashdot.org released an online poll asking which was the best graduate school in Computer Science. As is the case with online polls, IP address of voters were recorded in order to prevent single users from voting more than once. However, students at Carnegie Melon University (CMU) found a way to cast the ballots using programs that voted for CMU thousands of times.CMU's score started growing rapidly. The next day, students at Massachusetts institute of technology (MIT) wrote their own program and the poll became a contest between software robots.MIT finished with 21,156 votes while CMU finished with 21,032 votes. Others got less than 1,000.

(i)Briefly explain how the students at **MIT** and **CMU** were able to bypass the IP address restriction of not voting more than once **[4 Marks]**

(ii)Suggest **TWO** ways to mitigate such an attacks **[4 Marks]**

(c)Give **TWO** ways of protecting Servers and Clients **[4 Marks]**

(d)Briefly describe Challenge Authentication Protocol (CHAP) **[4 Marks]**

Question FOUR [20 Marks]

(a)The design of most of symmetric cryptographic algorithms involve combining two or more transformations/operations in a manner that the resulting cipher is more secure than if individual transformations/operations was employed. Describe **FIVE** such transformations employed in the design of DES cryptographic algorithm **[5 Marks]**

(b)Explain and with the support of a diagram how you can combine asymmetric cryptographic algorithms and hash functions to create a digital signature **[10 Marks]**

c) Discuss the following types of firewalls

i)Packet filtering (2 Marks)

ii)Application level Gateway firewall (3 Marks)

Question FIVE [20 Marks]

a) Discuss how the following access control mechanisms work. For each, state any benefits of implementing them. (6marks)

   i. Access control lists

   ii. Capability lists

   iii. Role based access control

b) An encryption scheme is unconditionally secure or computationally secure. Discuss (4 Marks)

c) Use the expression E(x) = (9x + 5)MOD26 to encrypt the message " The game has been postponed" (5 Marks)

d) $\Sigma = \{A, \ldots, Z\}, l = 2, k = XY$: Use this to encrypt the message The game has been postponed" using autokey cipher (5 Marks)

e) Discuss the two requirements for secure use of conventional encryption (4 Marks)