CHUKA UNIVERSITY

UNIVERSITY EXAMINATIONS

FIRST YEAR EXAMINATION FOR THE AWARD OF DEGREE OF MASTER OF SCIENCE IN COMPUTER SCIENCE

COSC 851: ADVANCED COMPUTER SECURITY

STREAMS: MSC COM SCI Y1S1 P/T **TIME: 3 HOURS**

DAY/DATE: FRIDAY 9/08/2019 **2.30 P.M - 5.30 P.M.**

INSTRUCTIONS

- Answer question 1 in section **A** and any other **TWO** from section **B**
- Marks are awarded for clear and concise answers
- Note that only Question ONE (Section A) and the first TWO attempted questions in section B will be marked.

SECTION A-COMPULSORY
QUESTION ONE [30 MARKS]

(a) There are rumors of widespread layoffs in a company. A programmer that feels at risk modifies his programming to execute malicious device encryption code if he is unemployed at the end of the month. The infected device(s) will display instructions requiring payment to regain control of the device(s). How would you categorize this action. **[4 Marks]**

(b) Differentiate between application level and database level security. **[4 Marks]**

(c) Hash function maps bit strings of arbitrary finite length to bit strings of fixed length (n bits).Illustrate the following **THREE** desirable properties of hash functions.

i) Weak collision resistance /2nd pre-image resistance **[3 Marks]**
(ii)Strong collision resistance **[3 Marks]**
(iii)One-way property /pre-image resistance **[3 Marks]**

(d) Briefly articulate the concept behind the following principles

(i)Kerckhoff's Principle **[3 Marks]**
(ii)Shannon's maxim **[2 Marks]**

(e) A random number is a number that cannot be predicted by an observer before it is generated. Briefly describe **FOUR** desirable properties of pseudo random numbers **[4 Marks]**

(f) Describe the concept of the following adversary models **[4 Marks]**
(i)Ciphertext-Only attack
(ii)Known-Plaintext attack

SECTION B: ANSWER ANY TWO QUESTIONS

QUESTION TWO [15 MARKS]

(a)Briefly describe two fundamental rules/properties associated with each of the following security models:

(i) Bell-LaPadula model **[3 Marks]**
(ii) Biba Model **[3 Marks]**
(iii) Chinese Wall **[3 Marks]**

(b)While giving illustrations, differentiate between:

(i)Discretionary access control and mandatory access control **[3 Marks]**
(ii)Diffusion and confusion in secret key cryptography. **[3 Marks]**

QUESTION THREE [15 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. Describe **FIVE** phases of the hacking methodology [**5 Marks]**

(b) While describing the following vulnerabilities, discuss their effect on a database and at least one mitigation strategy **[6 Marks]**
(i) Unencrypted database
(ii) Misconfigured Databases
(iii) Programmers

(c)In relation to mandatory access control, give the **THREE** possible security labels in their order of dominance from the highest to the lowest **[4 Marks]**

QUESTION FOUR [15 MARKS]

(a) Highlight the key features that differentiate symmetric encryption and public key encryption while giving atleast one standard/algorithm in each **[6 Marks]**

(b) Highlight and mathematically illustrate **THREE** desirable properties of MAC functions **[3 Marks]**

(c) Various parameters are used to measure performance of cryptographic algorithms. Analyze the performance of the DES, 3DES,AES and RC4 based on key size, computation and security strength **[6 Marks]**

QUESTION FIVE [15 MARKS]

(a) When satisfying a design criteria of a block cipher,acomplex encryption function can be built by composing several simple operations which offer complementary. But individually insufficient protection.

(i) Highlight **THREE** elements of a block cipher design criteria **[6 Marks]**

(ii) Give at least **FOUR** simple operations that can be combined to make a complex encryption function in a manner that the resulting cipher is more secure than the individual components

[**4 Marks]**

(b)Briefly describe atleast one known attack on each of the following cryptographic algorithms: DES, 3DES, AES, RSA, DIFFIE-HELMAN **[5 Marks]**

……