NATIONAL SCHOOL OF BUSINESS MANAGEMENT

BSc in Management Information Systems (Special) (NSBM)– 19.2/20.1
BSc (Honours) in Software Engineering (NSBM)– 19.2/20.1
BSc (Honours) in Computer Science (NSBM)– 19.2/20.1

Year 03 Semester 01 Examination

28th May 2022

CS306.3 - Information Assurance and Security

Instructions to Candidates

1) **Answer ONLY FIVE questions.**
2) **Time allocated for the examination is five (05) hours (Including downloading and uploading time)** . (Note: **No email submissions are accepted under any condition.)**
3) Weightage of Examination: 60% out of final grade
4) Download the paper, provide answers to the selected questions in a word document.
5) **Please upload the document with answers (Answer Script) to the submission link before the submission link expires**
6) Answer script should be uploaded in PDF Format
7) Under any circumstances E-mail submissions would not be taken into consideration for marking. Incomplete attempt would be counted as a MISSED ATTEMPT.
8) The Naming convention of the answer script – Module Code_Subject name_Index No

9) You must adhere to the online examination guidelines when submitting the answer script to N-Learn.

10) Your answers will be subjected to Turnitin similarity check, hence, direct copying and pasting from internet sources, friend’s answers etc. will be penalized.

Question 01

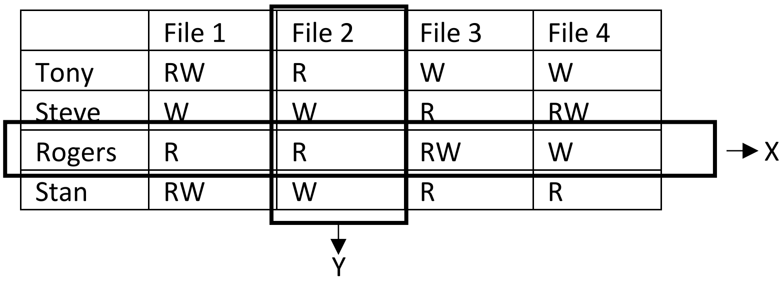
1. Briefly explain the CIA triad providing one example for each category (6 marks).
2. List down the 3 security rules of the Bell La Padula model and briefly explain how confidentiality is assured in this model. You may use diagrams if necessary (5 marks)
3. List down the 3 security rules of the Biba model and briefly explain how integrity is assured in this model. You may use diagrams if necessary (5 marks)
4. Given below is a table showing objects, their clearance levels along with the Need to know. Answer the following questions based on the table given below.

	Objects			
	File 1	File 2	File 3	File 4
File Clearance Level	Secret	Confidential	Top Secret	Unclassified
Need to know	Alpha	Charly	Bravo	Alpha & bravo

A user called ‘Stark’ has a security clearance of ‘Secret’ and his need to know is about ‘Charly and ‘Bravo’. Write down the access rights (read/write/no permission) that ‘Stark’ has for each object (file 1, file 2, file 3, file 4) with related to the Bell-La Padula model. (4 marks)

Question 02

1. List down 3 physical access control mechanisms (3 marks)
2. Identify X and Y with reference to Access Control Matrix given below (2 marks)



	File 1	File 2	File 3	File 4
Tony	RW	R	W	W
Steve	W	W	R	RW
Rogers	R	R	RW	W
Stan	RW	W	R	R

3. State what is meant by a security policy and list down 2 factors to be considered when developing a security policy. (4 marks)
4. Briefly explain what is meant by Discretionary Access Control (DAC) while providing examples (4 marks)
5. In order to determine how subjects and objects interact, an organization has chosen 'Role Based Access Control'. Assuming you are the hired security consultant to evaluate this decision, briefly discuss the advantages and disadvantages of the above approach. (7 marks)

<u>Question 03</u>

1. State what is meant by symmetric encryption and list down 3 shortcomings of it. (4 marks)
2. According to Claude Shannon there are two primitive operations with which strong encryption algorithms are built upon namely confusion and diffusion. State what is meant by confusion and diffusion with reference to the Claude Shannon principle. (4 marks)
3. A student states that 2DES provides double the security than what is provided by DES (Data Encryption Standard). Do you agree with this statement? Provide necessary facts to justify your statement.(3 marks)
4. Eight (8) users are involved in a communication process using symmetric cryptography. Calculate the total number of keys involve in the process. (3 marks)
5. Briefly discuss the issues with True Random Number generators and Pseudorandom Number generators and explain why they are not suitable to be used in cryptography. (You may use examples where appropriate) (6 marks)

<u>Question 04</u>

1. List down 3 different types of Cross Site Scripting (XSS) attacks (3 marks)
2. List down 2 secure software characteristics (2 marks)
3. Briefly explain how a SQL injection attack works and list down one mitigation technique. You may use diagrams if necessary. (5 marks)
4. Briefly explain what is meant by "Insecure Direct Object Reference (IDOR)" using a practical example. (4 marks)
5. Briefly explain 3 secure software requirement types, providing 2 examples for each category (6 marks)

<u>Question 05</u>

1. Compare and contrast computer security with computer forensics (3 marks)
2. List down the stages involved in a digital forensic investigation process (5 marks)
3. State what is meant by Anti – Digital Forensics (ADF) and list down 2 ADF techniques (3 marks)
4. State what is meant by Chain of Custody (CoC) and briefly explain why it is essential to maintain a CoC (4 marks)
5. "Data acquisition is the process of obtaining data from a digital device using peripheral equipment and media". List down the 2 main data acquisition methods and briefly explain them (5 marks)

Question 06

1. State why non-Repudiation is ensured in Digital Signatures but not in Message Authentication code (MAC) (2 marks)
2. Briefly explain how a hybrid cryptographic system function. You may use flow diagrams if necessary (4 marks)
3. Compare and contrast the hashing with encryption. (3 marks)
4. List down 3 security properties of a hash function and briefly explain them (5 marks)
5. Briefly explain the digital signature signing and verification process. Use diagrams where necessary (6 marks)

- End of the paper -