NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE, BACHELOR OF INFORMATICS, BACHELOR OF COMPUTER SCIENCE IN CYBER SECURITY	
QUALIFICATION CODE: 07BACS, 07BAIF, 07BCCY	**LEVEL: 6/7**
COURSE: INFORMATION SYSTEMS SECURITY ESSENTIALS/IT SYSTEMS SECURITY	**COURSE CODE:** ISS611S/ISS610S
DATE: JULY 2022	**SESSION:** 2
DURATION: 3 HOURS	**MARKS:** 100

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER (S)	**MRS UAKOMBA UHONGORA** **MS JOVITA MATEUS** **MR EDWARD NEPOLO** **MS VIKTORIA SHAKELA**
MODERATOR	**MR ISAAC NHAMU**

THIS EXAM QUESTION PAPER CONSISTS OF 5 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions in the ***answer booklet*** provided.
2. Write clearly and neatly.
3. Number the answers clearly.
4. When answering questions you should be guided by the allocation of marks in [ ]. Do not give too few or too many facts in your answers.
5. Submit both your examination booklet and this question paper to the exam invigilator.

PERMISSIBLE MATERIALS

1. Non-programmable calculator.

Question 1: Multiple Choice [10 marks]

Circle ONLY one correct answer among the choices provided.

1. A denial-of-service, or DoS attack is an attempt to defeat which security principle of the CIA Triad? [1]
   a) Integrity
   b) Availability
   c) Confidentiality
   d) Accountability

2. _____ encryption covers communication between a browser and the remote web host. [1]
   a) TSL
   b) SLS
   c) Web browser
   d) SSL

3. The right to control who knows certain things about you is called: [1]
   a) Secret
   b) Privacy
   c) Rights
   d) Encryption

4. Intrusion _______ System, is a technology with built-in protective response to try and block or stop harm. [1]
   a) Protective
   b) Prevention
   c) Detection
   d) Detention

5. If Alice crushes Bob's operating system, which CIA triad or its additional principles are violated? [1]
   a) Availability
   b) Confidentiality
   c) Non-repudiation
   d) Accountability

6. If Company A does not honour the contract agreed with Company B, which CIA triad or its additional principles is violated? [1]
   a) Availability
   b) Non-repudiation
   c) Authentication
   d) Integrity

7. Given the website address *news.nust.na* which is the Subdomain name? [1]
   a) news
   b) .na
   c) www.nust.na
   d) news.nust

8. Given the website address *www.nust.na* which is the Top-level domain name? [1]
   a) na
   b) news
   c) nust.na
   d) None of the above.

9. _____ define what kind of service is needed from the cloud service provider. [1]
   a) Deployment models
   b) Cloud
   c) Service models
   d) Infrastructure models

10. DES encrypts ______ blocks by using a 56-bit key. [1]
    a) 64-bit
    b) 256-bit
    c) DES can encrypt any block size
    d) 56-bit

Question 2: True or False [10 marks]

True or False.

T F 1. Service interruption is one of the reasons/motivations for committing cybercrimes. [1]

T F 2. An external attack occurs when there is a breach of trust from employees—or other people like former employees, working within the target organization who have legitimate access to its computing systems. [1]

T F 3. Substitution is a string of data used to lock or unlock cryptographic functions. [1]

T F 4. Cryptanalysis is the process used to secure data and communication. [1]

T F 5. The availibility service is one that protects a system to ensure its availability and addresses the security concerns raised by denial- of- service attacks. [1]

T F 6. Eradication in the incident response methodology eliminates incompetent members of the Incident Response Team. [1]

T F 7. Risk exposure is the likelihood that the event will occur. [1]

T F 8. Data mining uses statistics, machine learning, etc. to discover patterns and relations in large datasets. [1]

T F 9. RSA and 3DES are an example of Asymmetric encryption. [1]

T F 10. The purpose of cryptography is to investigate digital evidence related to computer crimes. [1]

Question 3 [15 marks]

i. Define the terms below:

a) Security plan [1]

b) Incident response plan [1]

c) Business continuity plan [1]

ii. List any two (2) of the seven (7) contents of a Security Plan. [2]

iii. List and explain the five (5) steps of the Incident Response Methodology. [10]

Question 4 [12 marks]

i. A misconfigured firewall is an example of a configuration vulnerability. State and explain two other types of vulnerabilities. [4]

ii. Classify each of the following as a violation of confidentiality, integrity, availability, or non-repudiation.

a) Hularia copies Mweulwa's assignment. [2]

b) Joe changes the amount on Gary's cheque from N$100 to N$1000 without Gary's knowledge. [2]

iii. Define the following terms:

a) Attack [1]

b) Exploit [1]

iv. What is the difference between a Denial of Service (DoS) attack and a Distributed Denial of Service (DDoS)? [2]

Question 5 [6 marks]

i. Explain how multi-factor authentication improves authentication mechanisms. [2]

ii. What is the correct rule assignment when using Unix for accessibility to the *IS Financial Application* for all the users listed in the access control table below. [2]

User	Hello Text File	IS Financial App	Active Directory	Client Database
Root	rwx	rwx	rwx	rwx
Group	rwx	rw-	-	r--
Others	rwx	r--	rwx	rwx

iii. What is the correct rule assignment when using Unix for accessibility to the *Hello Text File* for all the users listed in the access control table below. [2]

User	Hello Text File	IS Financial App	Active Directory	Client Database
Root	rwx	rwx	rwx	rwx
Group	rwx	-	-	r--
Others	rwx	r--	rwx	rwx

Question 6 [15 marks]

i. List and explain the six (6) controls used to block threats by neutralizing vulnerabilities. [6]

ii. Controls can be grouped into three largely independent classes. The following table shows the classes and several examples of each type of control. Match the examples to the correct classes. Use the Roman characters on the left of the table and write the corresponding letters representing the correct answers on the right. [3]

Control classes	Example
i. Administrative controls	(a) Laws, regulation
ii. Technical controls	(b) Locks, fences, human guards
iii. Physical controls	(c) Network protocols, firewalls
	(d) Intrusion attempts
	(e) Skimming

iii. Risk analysis is an organized process for identifying the most significant risks in a computing environment, determining the impact of those risks and weighing the desirability of applying various controls against those risks.

a) How can you identify risk? [2]

b) What are the first two steps of risk analysis? [2]

c) Which two types of costs are associated with Risk Analysis? [2]

Question 7 [10 marks)

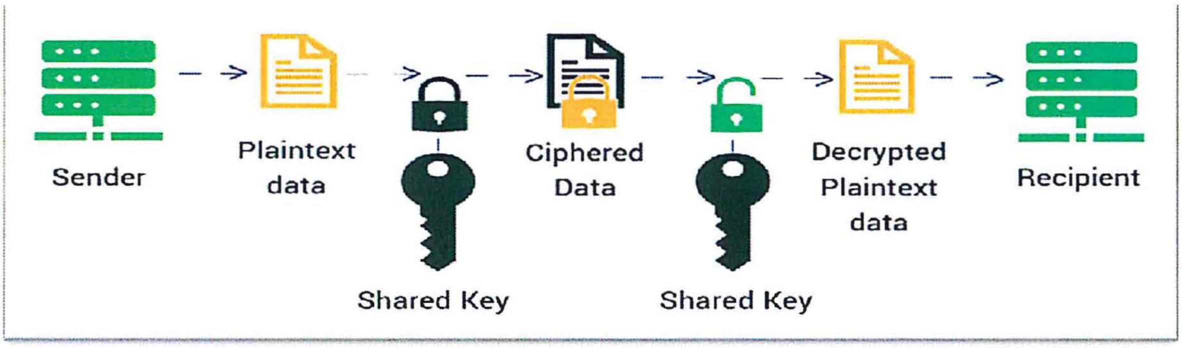
i. Name the three (3) cloud service models, and discuss any security issues associated with each model. (No abbreviations of the names) [6]

ii. Outline any four (4) security considerations to be taken into account before an organization moves it functionality or data to a cloud environment. [4]

Question 8 [10 marks]

i. A cryptosystem involves a set of rules for how to encrypt the plaintext and decrypt the ciphertext. The number of keys used are determined by the encryption algorithm.

a) The following diagram shows which encryption algorithm? [2]



b) Explain how the encryption algorithm mentioned in (a) above performs the encryption and decryption process. [2]

ii. Name and explain the two (2) types of operations used for transforming a plaintext to a ciphertext. [4]

iii. How is identification different from authentication? [2]

Question 9 [12 marks]

i. What is the role of a DNS server on a network? [2]

ii. What is an "A Record" and what is a "PTR Record" in DNS? [4]

iii. What could happen if the DNS server stopped working on the network? [2]

iv. Given the hostname www.apache.com and the IP address 192.168.112.129, what is the forward translation? [2]

v. Given the hostname www.apache.com and the IP address 192.168.112.129, what is the reverse translation? [2]