



**NAMIBIA UNIVERSITY**  
OF SCIENCE AND TECHNOLOGY

**FACULTY OF COMPUTING AND INFORMATICS**

DEPARTMENT OF COMPUTER SCIENCE

<b>QUALIFICATION:</b> BACHELOR OF COMPUTER SCIENCE	
<b>QUALIFICATION CODE:</b> 07BACS	<b>LEVEL:</b> 6
<b>COURSE:</b> IT Systems Security	<b>COURSE CODE:</b> ISS610S
<b>DATE:</b> July 2019	<b>SESSION:</b> 2
<b>DURATION:</b> 3 hours	<b>MARKS:</b> 100

<b>SUPPLEMENTARY / SECOND OPPORTUNITY EXAMINATION QUESTION PAPER</b>	
<b>EXAMINER(S)</b>	Mr. Edward Nepolo Mr. Attlee Gamundani Mr. Julius Silaa Mrs. Uakomba Mbasuva Ms. Jovita Mateus
<b>MODERATOR:</b>	Mr. Isaac Nhamu

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

**INSTRUCTIONS**

1. Answer ALL the questions.
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.

**PERMISSIBLE MATERIALS**

1. Non programmable Scientific Calculator.

**Question 1 True or False [10 Marks]**

1. Computer security is the protection of the items you value, called the assets of a computer or computer system.  
(True / False)
2. A vulnerability is a weakness in the system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm.  
(True / False)
3. A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.  
(True / False)
4. The principles of the CIA Triad are Confidence, Integrity, Availability.  
(True / False)
5. Examples of human threats include natural disasters like fires or floods.  
(True / False)
6. Non-malicious kinds of harm include someone's accidentally spilling a soft drink on a laptop, unintentionally deleting text.  
(True / False)
7. Operating Systems don't store passwords in plaintext.  
(True / False)
8. Authentication based on Passwords can be classified as "Something as user has" authentication mechanism.  
(True / False)
9. A Trojan horse is malicious code that, in addition to its primary effect, has a second, nonobvious, malicious effect.  
(True / False)
10. A keystroke logger (or key logger) can only be a software.  
(True / False)

**Question 2 Multiple Choice [10 Marks]**

1. A \_\_\_\_\_ is a puzzle that supposedly only a human can solve, so a server application can distinguish between a human who makes a request and an automated program generating the same request repeatedly.  
A. OTP  
B. CAPTCHA  
C. Stack  
D. Jig-Saw
2. A \_\_\_\_\_ is a faux environment intended to lure an attacker.  
A. Jellypot  
B. LurePot  
C. KillerPot  
D. Honeypot

3. A denial-of-service, or DoS, attack is an attempt to defeat which security principle of the CIA Triad?
- A. Integrity
  - B. Confidentiality
  - C. Availability
  - D. Accountability
4. Encryption can be employed in a network through two general modes: End-to-End Encryption and...
- A. Link Encryption
  - B. Protocol Encryption
  - C. IP Encryption
  - D. Layer Encryption
5. In 1999, the Internet Engineering Task Force upgraded SSL 3.0 and named the upgrade \_\_\_\_\_, which is also sometimes referred to as SSL 3.1.
- A. TLS
  - B. TSL
  - C. TSS
  - D. TTS
6. \_\_\_\_\_ encryption covers communication between a browser and the remote web host.
- A. SSS
  - B. SSL
  - C. TSL
  - D. SLS
7. A \_\_\_\_\_ is a device that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network.
- A. Hub
  - B. Repeater
  - C. Switch
  - D. Firewall
8. A \_\_\_\_\_ cloud is composed of two or more types of clouds, connected by technology that enables data and applications to be moved around the infrastructure to balance loads among clouds.
- A. Private
  - B. Public
  - C. Hybrid
  - D. Community
9. The right to control who knows certain things about you is called.
- A. Privacy
  - B. Right
  - C. Secret
  - D. Private
10. The logical structure of a database is called a:
- A. Logic
  - B. Syntax
  - C. Logical DB
  - D. Schema

**Question 3 [14 Marks]**

- i. Mention and explain the 3 principles of the CIA Triad. (6)
- ii. The CIA Triad has two additional principles. (a) Mention and (b) explain how those two principles help in IT Systems Security. (4)
- iii. What is the difference between a page-in-the-middle attack, and Man-in-the-middle attack? (4)

**Question 4 [21 Marks]**

- i. The cloud has five defining characteristics. Mention and explain them. (10)
- ii. List the 3 cloud service models (No Abbreviations) (3)
- iii. Name the four cloud computing deployment models. (4)
- iv. You are the Security Administrator of a certain company. The company deals with forensics investigations and the company would like to seek for cloud services that will allow you to store confidential data, and also allow you to publish some findings of your investigations with the general public.
  - (a) Which cloud computing deployment model would you recommend the company to use in order to ensure that confidential information is kept safe, while allowing you to share some information with the general public. (2)
  - (b) Explain how your recommendation will help in achieving the objective in (a). (2)

**Question 5 [15 Marks]**

- i. Discuss the concept of Single-Sign-On (SSO). (2)
- ii. How is Authentication different from Identification in IT Systems security? (4)
- iii. Authentication is the first step in access control, and there are three common factors used for authentication. (a) Name and (b) give an example of each authentication mechanisms. (6)
- iv. For each example given in (iii), give one short coming for each authentication mechanism. (3)

**Question 6 [10 Marks]**

Vitjitua is a System Administrator for Matisa Travel Agency CC. She created a file that runs an online application through the company's website. She needs to share it with group members but wants to make sure that only she has full rights over the file, while her group members and other users should only be able to execute file.

- i. Give the permissions that Vitjitua must assign to that file using a Debian operating system. (2)

```
#mkdir Files
#touch Files/information.exe
#chmod ___ ___ ___ Files/information.exe
```

ii. Vitjitua realises that an intruder made a modification to the file, which led to a compromise of the online application on the website.

(a) Which principle of the CIA triad will Vitjitua be addressing? (2)

(b) Vitjitua wants to encrypt this file using symmetric encryption to avoid future intrusions. Suggest any encryption algorithm that she can use. (2)

iii. Which type of encryption uses two keys, a public key and a private key to encrypt and decrypt? (1)

iv. Give 3 examples of algorithms that use the type of encryption mentioned in 11.a. (3)

**Question 7 [5 Marks]**

i. What is Buffer overflow in computing? (2)

ii. What is a query in Database Management? (2)

iii. Apart from NSLOOKUP, name any other command line tool that are useful in troubleshooting DNS services. (1)

**Question 8 [8 Marks]**

(a) Network communications face several threats. Define the following terms that are related to network communication threats by matching the terms to the correct definitions. Use the Roman characters on the left of the table and write the corresponding letters representing the correct answers on the right. (4)

(i) Interception	(A) Prevention of authorized access to data
(ii) Modification	(B) Unauthorized Sharing of Data
(iii) Fabrication	(C) Unauthorized change of data
(iv) Interruption	(D) Unauthorized creation of data
	(E) Prevention of Data interception
	(F) Unauthorized viewing of data, communication goes on as normal.

(i) \_\_\_\_ (ii) \_\_\_\_ (iii) \_\_\_\_ (iv) \_\_\_\_

(b) Match the following terms to the corresponding threats. (4)

(i) Interception	(A) SQLi
(ii) Modification	(B) Masquerading
(iii) Fabrication	(C) Cross-Site-Scripting
(iv) Interruption	(D) Man-in-the-Middle
	(E) Denial of Service
	(F) Eavesdropping/Wiretapping

(i) \_\_\_\_ (ii) \_\_\_\_ (iii) \_\_\_\_ (iv) \_\_\_\_

**Question 9 [6 Marks]**

i. Intrusion Detection Systems (IDS) can be classified into two categories. Mention them. (2)

ii. How are Intrusion Prevention Systems (IPS) different from Intrusion Detection Systems (IDS)? (4)

**Question 10 [1 Mark]**

Which Wi-Fi security protocol is preferred over its predecessor due to its security improvements?  
(No Abbreviations) (1)

---End of Question Paper---