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: JUNE 2022	**SESSION:** 1
DURATION: 3 HOURS	**MARKS:** 100

FIRST OPPORTUNITY 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. ______ is a small application, or string of code, that infects host applications. It is a programming code that can replicate itself and spread from one system to another requiring user intervention. [1]
   a) Worm
   b) Backdoor
   c) Spyware
   d) Virus

2. The CIA triad consists of the following three main principles: [1]
   a) Confidentiality, Integrity, Authentication
   b) Confidentiality, Integral, Availability
   c) Confidentiality, Integrity, Availability
   d) Confidentiality, Integrity, Accountability

3. Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy. This infrastructure includes: [1]
   a) Critical sector
   b) People sector
   c) Food and agriculture sector
   d) Rights sector

4. An original intelligible message fed into the algorithm as input is known as __________, while the coded message produced as output is called the __________. [1]
   a) decryption, encryption
   b) plaintext, ciphertext
   c) deciphering, enciphering
   d) cipher, plaintext

5. If both sender and receiver use the same key, the system is referred to as: [1]
   a) Public-key encryption
   b) Two-key
   c) Asymmetric
   d) Secret-key encryption

6. A branch of forensic science that uses scientific knowledge for collecting, analyzing, documenting, and presenting digital evidence related to computer crime for using it in a court of law is known as: [1]
   a) Mobile forensics
   b) Forensic science
   c) Digital forensics
   d) Network forensics

7. Which is a processes of incident response? [1]
   a) Control
   b) Containment
   c) Assume
   d) Seizure

8. Which IT Security mechanism is used to determine the accessibility of objects to certain subjects? [1]

a) Interception
b) Cryptography
c) Access control
d) Substitution

9. ______ an attack is a control that discourages an attacker to cause harm due to the cost of the attack outweighing the benefits. [1]

a) Deflecting
b) Dettering
c) Modification
d) Detecting

10. ______ is an example of a technical control. [1]

a) Policy
b) Locking a server room
c) Mitigation control
d) Intrusion Detection System

Question 2: True or False [10 marks]

True or False.

T F 1. A common technique for masking contents of messages or other information traffic so that opponents can not extract the information from the message is known as masquerade. [1]

T F 2. A loss of confidentiality is the unauthorized disclosure of information. [1]

T F 3. Verifying that users are who they say they are and that each input arriving at the system came from a trusted source is credibility. [1]

T F 4. A integrity 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 5. The command **# chmod 600 /etc/apache2/ssl/*** is used to set permissions to some files contained in the ssl directory. [1]

T F 6. A loss of confidentiality is the unauthorized disclosure of information. [1]

T F 7. Digital forensics is investigating crimes committed using computing devices like computers, tablets and textbooks. [1]

T F 8. A loss of confidentiality is the unauthorized disclosure of information. [1]

T F 9. An integrity 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 10. Auditability is one of the security requirements of databases. [1]

Question 3 [25 marks]

i. Mention and explain the 3 principles of the CIA Triad. [6]

ii. List and explain the additional principles of the CIA triad. [4]

iii. Match the following threats faced by the principles outlined in the table below. Use the Roman characters on the left of the table and write the corresponding letters representing the correct answers on the right. [4]

Principle	**Threat**
(i) Integrity	(a) Cause of incident elimination
(ii) Confidentiality	(b) Modification of message in transit
(iii) Denial of Service	(c) Theft of information from server
(iv) Authentication	(d) Impersonation of legitimate users
	(e) Computational power required
	(f) Legitimate users unable to access a network resource

(i) ____ (ii) ____ (iii) ____ (iv) ____

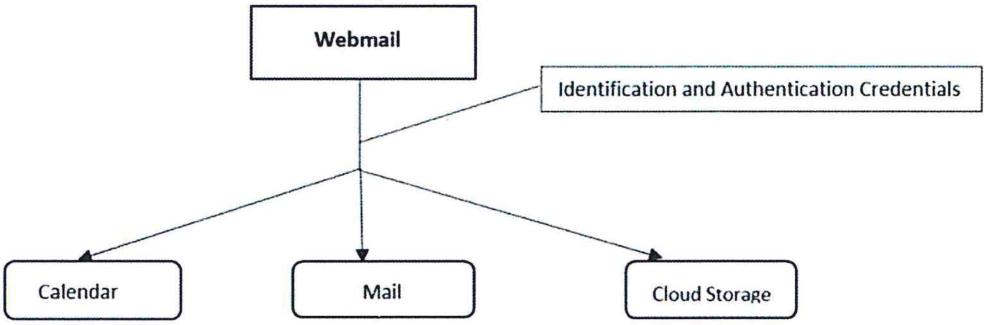
iv. Authentication is the first step in access control, and there are three common factors used for authentication.

(a) Name the three factors used for authentication. [3]

(b) Give an example for each authentication method listed in (a) above. [3]

(c) For each of the example given in (b) above, list one shortcoming for each of the authentication mechanisms. [3]

v. The following diagram depicts which authentication method? [2]



Question 4 [6 marks]

Mobile forensics consists of three process namley; Seizure, Acquisition and Analysis. Name and discuss the three methods used for the acquisition of evidence from mobile devices. [6]

Question 5 [8 marks]

i. Discuss three ways computers are used in a crime. [4]

ii. How is an Intrusion Prevention System (IPS) different from an Intrusion Detection System (IDS). [4]

Question 6 [10 marks]

i. A browser is a software that connects to a particular web address, fetches and displays content from that address and transmits data from a user to that address.

a) Why are browser attacks popular? [1]

b) State three browser attack vectors. [3]

c) Explain man-in-the-browser attack. [2]

d) What is the difference between page-in-the-middle attack and man-in-the-browser attack? [2]

e) Explain the difference between a defaced website and a fake website. [2]

Question 7 [5 marks]

i. What is the difference between a threat and a vulnerability? [2]

ii. Classify whether each of the following is a threat or a vulnerability?

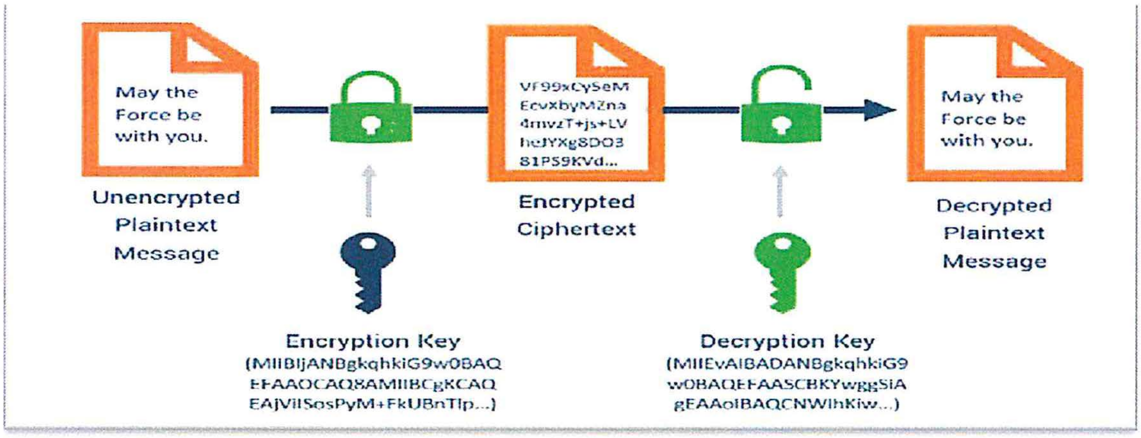
a) A misconfigured firewall. [1]

b) A computer virus. [1]

c) A computer with no password. [1]

Question 8 [5 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 diagram below shows which encryption algorithm? [2]


May the Force be with you.
Unencrypted Plaintext Message
VF99xCySeM EcvxbyMZna 4mvzT+js+LV heJYXg8DO3 81PS9KVd...
Encrypted Ciphertext
May the Force be with you.
Decrypted Plaintext Message
Encryption Key
(MIIBIjANBgkqhkiG9w0BAQ EFAAOCAQ8AMIIBCgKCAQ EAjVilSosPyM+FkUBnTlp...)
Decryption Key
(MIIEvAIBADANBgkqhkiG9 w0BAQEFAASCBKYwggSiA gEAAoIBAQCNWlhKiw...)

b) Explain how the encryption algorithm mentioned in (a) above performs the encryption and decryption process. [3]

Question 9 [11 marks]

i. A risk is a potential problem that the system or its users may experience.

a) What are the six risk analysis steps? [6]

b) State two advantages of doing a risk analysis [2]

c) What is the difference between *risk control, risk impact and risk exposure*? [3]

Question 10 [10 marks]

i. List any of the four (4) cloud deployment models. [4]

ii. List and explain any three (3) privacy principles and policies. [6]