NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF CYBER SECURITY

QUALIFICATION: *BACHELOR OF COMPUTER SCIENCE (HONS INFORMATION SECURITY)*	
QUALIFICATION CODE: 08 BHIF	**LEVEL:** **8**
COURSE: APPLIED CRYPTOGRAPHY	**COURSE CODE:** APC811S
DATE: JUNE 2023	**SESSION:** THEORY
DURATION: 2 HOURS 30 MINUTES	**MARKS:** **70**

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	DR ATTLEE M. GAMUNDANI
MODERATOR:	MR STANFORD MUSARURWA

THIS QUESTION PAPER CONSISTS OF 2 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions in Section A and Section B.
2. Write clearly and neatly.
3. In answering questions, be guided by the allocated marks.
4. Number your answers clearly following the numbering used in this question paper.

PERMISSIBLE MATERIALS

1. None

SECTION A: 20 Marks [Answer all Questions]

Question 1: [10 Marks]

Scenario: *You are a security analyst working for a government agency that needs to share classified information with a foreign government.*

(a) What type of encryption would you recommend for secure communication, and why? **[5 marks]**

(b) Discuss the potential legal and ethical implications of sharing classified information with a foreign government. **[5 marks]**

Question 2: [10 Marks]

Scenario: *You are a security consultant working for a multinational corporation that operates in countries with different data protection laws.*

(a) What factors would you consider when designing an encryption policy for the corporation? **[6 marks]**

(b) How would you ensure compliance with different data protection regulations? **[4 marks]**

SECTION B: 50 Marks [Answer all Questions]

Question 3: [15 Marks]

Based on the following questions, identify a practical application of Cryptography and answer each of the following questions precisely.

(a) What are the security requirements? **[4 marks]**

(b) What are the application constraints which influence decision-making? **[2 marks]**

(c) Which cryptographic primitives are deployed? **[2 marks]**

(d) Which cryptographic algorithms and key lengths are supported? **[4 marks]**

(e) How is key management conducted? **[3 marks]**

Question 4: [15 Marks]

(a) Come up with practical examples that demonstrate the relationship between security services provided by cryptography as outlined by the contrasting reviews below: -

i. **Data Origin Authentication** is a strong notion than **Data Integrity**. **[4 marks]**

ii. **Non-repudiation** of a source is a stronger notion that **Data Origin Authentication**.
n

[4 marks]

iii. **Data Origin Authentication** and **Entity Authentication** are different. **[4 marks]**

(b) Complete the following table **[3 marks]**

	Relationship between Keys	Encryption Key	Decryption Key
Symmetric Cryptosystem			
Public-Key Cryptosystem			

Question 5: [20 Marks]

(a) With detailed explanations and clear workings, demonstrate how we may know how many bits long a symmetric key should be, to guarantee a key space of at least one million. **[10 marks]**

(b) How do stream ciphers and block ciphers differ in their response to errors? Please provide examples of at least two specific errors and describe how the differences manifest in each case.

[6 marks]

(c) Stream ciphers have several attractive properties, which makes them the favoured encryption mechanism in several important applications. Identify and explain any two such attractive properties. **[4 marks]**

*******END OF EXAMINATION PAPER*******