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 2024	**SESSION: THEORY**
DURATION: 2 HOURS 30 MINUTES	**MARKS: 80**

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

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

INSTRUCTIONS

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

PERMISSIBLE MATERIALS

1. None

Question 1: Overview of Cryptography

Critically evaluate the legal implications of encryption technologies in the context of personal privacy vs national security. Provide examples from current legislation or notable cases to support your arguments. **[10 marks]**

Question 2: Mathematical Foundations of Cryptography

Demonstrate how prime numbers are used in the RSA encryption algorithm. Include key generation, encryption, and decryption in your answer. **[10 marks]**

Question 3: Symmetric Key Cryptography

(a) Discuss the Advanced Encryption Standard (AES) and its application in secure file transfer protocols. **[8 marks]**

(b) How does AES ensure data integrity and confidentiality? **[2 marks]**

Question 4: Asymmetric Key Cryptography

(a) Describe how the Diffie-Hellman key exchange algorithm enables secure communication over an insecure channel. **[6 marks]**

(b) Discuss the significance of the Diffie-Hellman key exchange algorithm in developing secure internet protocols. **[4 marks]**

Question 5: Hash Functions and Digital Signatures

(a) Compare and contrast the security features of SHA-256 and MD5 hash functions. **[6 marks]**

(b) Discuss the implications of hash collisions in digital signatures. **[4 marks]**

Question 6: Cryptographic Protocols

(a) Evaluate the security features of the IPSec protocol in VPNs. **[2 marks]**

(b) How does the IPSec protocol provide confidentiality, integrity, and authentication? **[8 marks]**

Question 7: Advanced Topics

(a) Discuss the concept of homomorphic encryption and its potential applications in cloud computing. **[6 marks]**

(b) What challenges must be addressed to make homomorphic encryption practical for widespread use? **[4 marks]**

Question 8: Applications of Cryptography

(a) Analyse the use of cryptography in securing mobile banking applications. **[3 marks]**

(b) Discuss the combination of cryptographic techniques that ensure transaction security. **[7 marks]**

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