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

SECOND OPPORTUNITY/ SUPPLEMENTARY 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

(a) Discuss the role of cryptography in enforcing data protection laws such as the General Data Protection Regulation (GDPR) or the Data Protection Bill in Namibia. **[2 marks]**

(b) How does cryptography aid in compliance with these regulations, and what are the potential challenges or limitations? **[8 marks]**

Question 2: Mathematical Foundations of Cryptography

(a) Describe the role of elliptic curve cryptography (ECC) in securing mobile devices. **[2 marks]**

(b) Compare its efficiency and security level to RSA's in this specific application. **[8 marks]**

Question 3: Symmetric Key Cryptography

Evaluate the security and performance implications of using block cipher modes of operation, such as CBC and GCM, in network security protocols. **[10 marks]**

Question 4: Asymmetric Key Cryptography

Explain the concept of public key infrastructure (PKI) and how it supports digital signatures and certificates in e-commerce transactions. **[10 marks]**

Question 5: Hash Functions and Digital Signatures

(a) Explain the process of generating and verifying a digital signature using the ECDSA algorithm. **[7 marks]**

(b) Discuss its application in cryptocurrency transactions. **[3 marks]**

Question 6: Cryptographic Protocols

Describe the SSL/TLS handshake process and how it ensures secure web browsing. Include in your discussion the roles of asymmetric and symmetric encryption in this process. **[10 marks]**

Question 7: Advanced Topics

(a) Explain the threat of quantum computers to current cryptographic algorithms. **[3 marks]**

(b) Discuss post-quantum cryptography and its importance in future-proofing cryptographic practices. **[7 marks]**

Question 8: Applications of Cryptography

(a) Evaluate the role of cryptography in IoT devices. **[1 mark]**

(b) Discuss the challenges and propose solutions for implementing cryptographic security in resource-constrained environments. **[9 marks]**

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