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 2023 | **SESSION:** THEORY |
| **DURATION:** 2 HOURS 30 MINUTES | **MARKS:** **70** |

| **SECOND OPPORTUNITY/ SUPPLEMENTARY 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 company that stores customer data. Your company has been targeted by a cyber-attack, and the attackers have gained access to the customer data. The data is encrypted using a symmetric key algorithm, but the attackers have also obtained the encryption key.*

**(a)** What steps would you take to mitigate the damage caused by the breach? **[6 marks]**

**(b)** What measures would you implement to prevent similar breaches in the future? **[4 marks]**

### Question 2: [10 Marks]

***Scenario:*** *You are a security consultant working for a financial institution that is considering implementing a new key management system for its encrypted data.*

**(a)** What factors would you consider when selecting a key management system? **[2 marks]**

**(b)** What challenges might you encounter during the implementation process? **[4 marks]**

**(c)** Discuss potential solutions to these challenges. **[4 marks]**

## SECTION B: 50 Marks [Answer all Questions]

### Question 3: [15 Marks]

Considering the practical application of Cryptography on the Internet, 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** and **Entity Authentication** are different. **[4 marks]**

ii. **Data Origin Authentication** plus a **Freshness Check** can provide **Entity Authentication.** **[4 marks]**

iii. **Confidentiality** does not imply **Data Origin Authentication.** **[4 marks]**

**(b)** Anna and Mary have chosen p=53 and g=17. Their private keys are as follows, Anna = 5 and Mary =7. Calculate Anna and Mary's public key pairs using the **Diffie-Hellman** Key exchange algorithm. **[3 marks]**

**Question 5: [20 Marks]**

**(a)** Using the 7 days of the week, demonstrate the concept of modular arithmetic and explain how it is applied to cryptography. **[10 marks]**

**(b)** Suppose Alice and Bob have RSA public keys in a file on a server. They communicate regularly using authenticated, confidential messages. Eve wants to read the messages but is unable to crack the RSA private keys of Alice and Bob, However, she can break into the server and alter the file containing Alice's and Bob's public keys.

i. How should Eve alter that file so that she can read confidential messages sent between Alice and Bob, and forge messages from either? **[5 marks]**

ii. How might Alice and / or Bob detect Eve's subversion of the public keys? **[5 marks]**

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