NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE	
QUALIFICATION CODE: 08BHIS	**LEVEL:** 8
COURSE: APPLIED CRYPTOGRAPHY	**COURSE CODE:** APC811S
DATE: JUNE 2019	**PAPER:** THEORY
DURATION: 2 HOURS	**MARKS:** 70

FIRST OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER (S):	DR ATTLEE M. GAMUNDANI
MODERATOR:	MR ATUMBE J BARUANI

THIS QUESTION PAPER CONSISTS OF 1 PAGE
(Excluding this front page)

INSTRUCTIONS

1. Answer **ALL the questions** on the answer scripts.
2. When writing take the following into account: The style should **inform** than impress, it should be **formal**, in third person, paragraphs set out according to ideas or issues and the paragraphs flowing in a **logical** order. Information provided should be **brief** and **accurate**.
3. Number the answers clearly; ensure that your writing is **legible**, **neat** and **presentable**.

PERMISSIBLE MATERIALS

1. Calculator.

Question 1

(a) **John** and **Mary** want to share secret messages without **Anna** knowing it. They both agree to use symmetric cipher. Provided that, they have already securely exchanged the key and agreed on **K** as a shared key. Outline the steps that **John** and **Mary** must follow when they encrypt and decrypt their messages respectively. **[6]**

(b) Two different ciphers have been applied to the following cipher text: **QRH**. Given the following intel on the ciphers applied, deduce the original plaintext, the names of the ciphers used in **(i)** and **(ii)**

(i) The first cipher swapped the positions of the original plaintext (that did not change any original characters in the original plaintext but only their positions).

(ii) The second cipher was applied to the first cipher's results (i.e. the first cipher text), to obtain the presented cipher text above (i.e. **QRH**). This cipher operates by mathematically adding a constant k to the position of any given input's position on the alphabet, to obtain a character that is then picked to formulate the cipher characters. **[6]**

(c) With illustrations, explain how a **man-in-the middle attack** can attack a simple key distribution scheme between two communicating parties **A** and **B**. **[6]**

(d) How does a polyalphabetic substitution cipher improve the mono alphabetic substitution cipher? **[2]**

Question 2

(a) Explain the context of diffusion and confusion as building blocks for any cryptographic system. **[6]**

(b) With the aid of illustrations, explain the statement: "**An encryption function Ee is a bijection from M to C**" **[4]**

(c) Which two fundamental difficulties do **one–time pads** present in their quest to provide full security? **[4]**

(d) Encrypt the following message mathematically using the **Vigenere cipher *'STEMISSECURE'***. **[6]**

Question 3

(a) Suppose **A** and **B** have **RSA** public keys in a file on a server. They communicate regularly using authenticated, confidential messages. **C** wants to read the messages but is unable to crack the **RSA** private keys of **A** and **B**, However, **C** is able to break into the server and alter the file containing **A**'s and **B**'s public keys. How should **C** alter that file so that he/she can read confidential messages sent between **A** and **B**, and forge messages from either? **[6]**

(b) Design and explain any encryption scheme for cloud-based databases. **[8]**

(c) Copy and complete Table 1 below **[6]**

Table 1: Types of attacks

Type of attack		What is known to the cryptanalyst?
(i)	Cipher text only	
(ii)	Chosen cipher text	
(iii)	Chosen plaintext	

Question 4

(a) Prove that two users who perform a **Diffie-Hellman** key exchange will have the same-shared key. **[8]**

(b) Explain the representation: **gcd(a,b)= max(k, such that k|a and k|b).** **[2]**

****End of Examination Paper*****