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: JULY 2019	**PAPER:** THEORY
DURATION: 2 HOURS	**MARKS:** 70

SECOND OPPORTUNITY/SUPPLEMENTARY 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) Explain any three **Fiestel cipher** design features. **[6]**

(b) Given that a cryptosystem is made up of **E, D, M, K, C** where **M**=Plaintext; **K**= Key(s); **C**=Cipher text; **E**= Encryption and **D** = Decryption. Formulate an equation in terms of **C**, **K** or **M** to represent

a. **E.** **[3]**

b. **D.** **[3]**

(c) Cryptography can be useful towards information protection; under what circumstances would you consider this statement to be true? **[4]**

(d) Under timing attacks, DES proves certain strengths. Identify and explain any two such strengths. **[4]**

Question 2

(a) **Alice** and **Bob** decides to use the **Diffie-Hellman** key exchange technique with a common prime **q**=47 and a primitive root **α** = 7.

(i) If **Alice** has a private key X_{Alice}= 5, what is **Alice**'s public key Y_{Alice}? **[3]**

(ii) If **Bob** has private key X_{Bob} =12, what is **Bob**'s public key Y_{Bob}? **[3]**

(iii) What is the shared secret key between **Alice** and **Bob**? **[5]**

(b) **Anna** wants to send a message **P** with a digital signature **kP** to **Peter**. **Anna** and **Peter** have an authentic copy of each other's public keys, and have agreed on using a specific hash function **h**.

(i). Outline the steps that **Anna** must follow when signing **P**. **[4]**

(ii). What steps must **Peter** follow upon receipt of **P**, for validating the signature **kP?** **[5]**

Question 3

(a) Why would you consider a **one-time pad** a perfect encryption scheme? **[2]**

(b) Given the communication between **Susan** and **Jay**, such that **Susan** intends to send a message to **Jay** by preserving the message integrity. Outline briefly the cryptographic steps that **Susan** and **Jay** must follow to ensure the integrity of the message by creating and verifying a **MAC.** **[6]**

(c) Using brute force attack, decrypt, "**GQ RMBYW RFC BYW MD CVYK.**" **[5]**

(d) Explain in detail, how a smart card can protect **PGP** electronic e-mail on a PC running windows against malware. **[7]**

Question 4

(a) Consider the **RSA** cryptosystem. Show that the cipher texts corresponding to the messages **0, 1** and **n-1** are the messages themselves. **[8]**

(b) Give and explain any two real world usages of public key encryption. **[2]**

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