NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION: BACHELOR OF COMPUTER SCIENCE HONOURS (INFORMATION SECURITY)	
QUALIFICATION CODE: 08BHIF	**LEVEL:** 8
COURSE: APPLIED CRYPTOGRAPHY	**COURSE CODE**: APC811S
DATE: JULY 2022	**SESSION:** 1
DURATION: 2 HOURS	**MARKS:** 60

SECOND OPPORTUNITY / SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**DR MERCY CHITAURO**
MODERATOR:	**MS ESNA MANGUNDU**

THIS QUESTION PAPER CONSISTS OF 4 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Answer **all questions**.
2. Write all your answers in the answer booklet provided and number every question.
3. Please, ensure that your writing is **legible, neat** and **presentab*le.***
4. Marks/scores per question are given in square brackets [ ].
5. Calculators are permitted
6. Do not use or bring into the examination venue books, mobile devices and other material that may provide you with unfair advantage. Should you be in possession of one right now, draw the attention of the examination officer or invigilator.
7. All things that should **not** be marked, e.g. any "rough work", have to be crossed out unambiguously.

1. Cryptolocker is a malware released in September 2013, CryptoLocker spread through email attachments and encrypted the user's files so that they couldn't access them. The hackers then sent a decryption key in return for a sum of money, usually somewhere from a few hundred pounds up to a couple of grand (Norton.com, 2017).

   a. Which information security property is breached when a user is not able to access files that they are authorised to view and modify? [1]

   b. Explain why the legitimate users are not able view or access their files. [2]

   c. If the hacker gives the users, the correct decryption key will the users be able to access their files? [1]

   d. If your answer in '1c' is yes explain how the users will be able to access their files. If your answer is no explain why the users will not be able to access their files.

   e. Given that the users are able to access the encrypted files. Why would the users still not be able to understand what is contained in their files? [2]

   f. Suppose the users had already encrypted their files before the hackers encrypted them. Would the users have been able to access their files after they had been encrypted by the hackers? Explain your answer. [3]

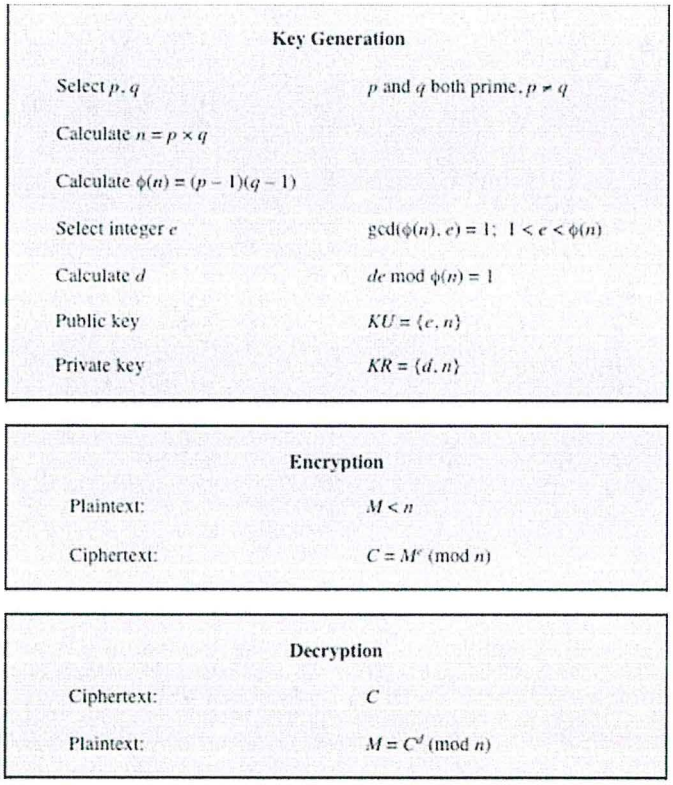
   g. Which security property/objective would the users have achieved against the hackers given the description in (1f). [1]

2. Public key encryption algorithms are used to distribute public keys and private (session) keys for symmetric encryption algorithms.

   a. Explain how a public key is distributed using public key encryption algorithms. [3]

   b. Explain how a session key is distributed using public key encryption algorithms. [3]

3. Given the RSA algorithm shown in Figure 1



Key Generation

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

Figure 1: RSA Algorithm

a. Using the RSA algorithm depicted in Figure 1 and given two prime numbers 5 and 7. Generate the public key and the private key. ***For e and d use the smallest value of d and e possible.*** [8]

b. Paul Kocher, a cryptographic consultant, demonstrated that a hacker can determine an RSA private key by keeping track of how long a computer takes to decipher messages. State and explain three countermeasures that can be used to circumvent this attack. [6]

4.

a. Explain how to get a public-key certificate [3]

b. Explain how Zenane can verify Adelino's public-key certificate. [8]

5.

a. DES is an example of which type of encryption algorithm? [1]

b. DES decryption rule is as follows: Use the ciphertext as input to the DES algorithm, but use the subkeys K_n in reverse order. That is, use K_{16} on the first iteration, K_{15} on the second iteration, and so on until K_1 is used on the 16th and last iteration.

i. Which key is used on the first iteration? [1]

ii. Which key is used on the sixth iteration? [1]

c. Given: the hexadeximal plaintext: 0123456789ABCDEF.

i. Convert it to binary [2]

d. The first step of DES enciphering plaintext is the initial permutation (IP) given by:

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

What is the result of applying IP on your plaintext you got in (5c)? [5]

e. IP you got in (5d) is then divided into two equal sizes block; left half (L) and right half (R). What is the size of each half? [1]

f. Write down left half (L_0). [1]

g. Write down right half (R_0). [1]

e) Backformation [1]

f) Eponym [1]

g) Conversion [1]

Total Marks [7]

Question 3

Complete the following table. Re-draw the table in your examination booklet.

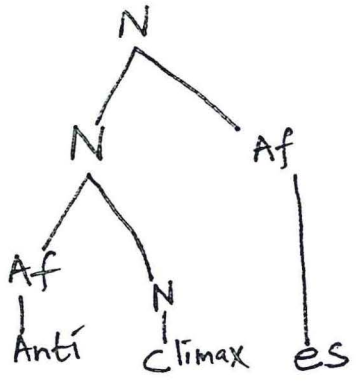
Word	Free morpheme [5 marks]	Bound morpheme [5 marks]
Keys	***Key***	***s***
Waiter	***Wait***	***er***
Completion	***Complete***	***ion***
Poetic	***Poet***	***ic***
Healthy	***Health***	***y***
Considering	***Consider***	***ing***
Agreeing	***Agree***	***ing***
redness	***Red***	***ness***
rotation	***Rotate***	***ion***

Total marks [10]

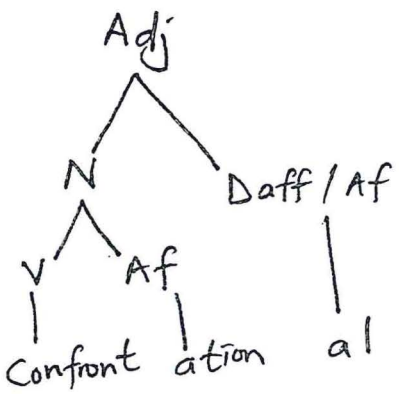
Question 4

For each word below, draw a morphological tree diagram. Please note a word may belong to two parts of speech, thus an option is given (e.g. N/V)

a) anticlimaxes [3.5]



b) confrontational [5.5]



6.

Consider the condition imposed on one-time pad: One-time pad - requires the use of a one-time pre-shared key the same size as, or longer than, the message being sent. Why can you not brute- force the pre-shared key for subsequent communications? [2]

a. Select in the table below whether it is true that the key given would be suitable to be used as a pre-shared key for the plaintext to be encrypted with one-time pad. *Draw the table in your answer booklet.* [3]

Plaintext size	Pre-shared key size	True/False
4000	**4005**	
150	**135**	
603	**603**	