



**NAMIBIA UNIVERSITY  
OF SCIENCE AND TECHNOLOGY**

**FACULTY OF COMPUTING AND INFORMATICS**

**DEPARTMENT OF COMPUTER SCIENCE**

<b>QUALIFICATION:</b> BACHELOR OF COMPUTER SCIENCE	
<b>QUALIFICATION CODE:</b> 08BHIF	<b>LEVEL:</b> 8
<b>COURSE:</b> APPLIED CRYPTOGRAPHY	<b>COURSE CODE:</b> APC811S
<b>DATE:</b> JUNE 2022	<b>SESSION:</b> 1
<b>DURATION:</b> 2 HOURS	<b>MARKS:</b> 60

<b>FIRST OPPORTUNITY EXAMINATION QUESTION PAPER</b>	
<b>EXAMINER(S)</b>	<b>DR MERCY CHITAURO</b>
<b>MODERATOR:</b>	<b>MS ESNA MANGUNDU</b>

**THIS QUESTION PAPER CONSISTS OF 3 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 presentable**.
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 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 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. [2]
  - 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.
  - a. Cryptography can be used to obtain security objective of authentication. Which other security property or objective can be achieved using cryptography? Mention 2 only. [1]
  - b. Suppose emails sent from Zenane will be authenticated using message authentication codes (MAC). Explain in detail how Adelino will ensure integrity of the message sent from Zenane to him using MAC. [10]
  - c. Explain how Adelino verifies that Zenane sent the email in "2b". [4]

3. Given the RSA algorithm shown in Figure 1

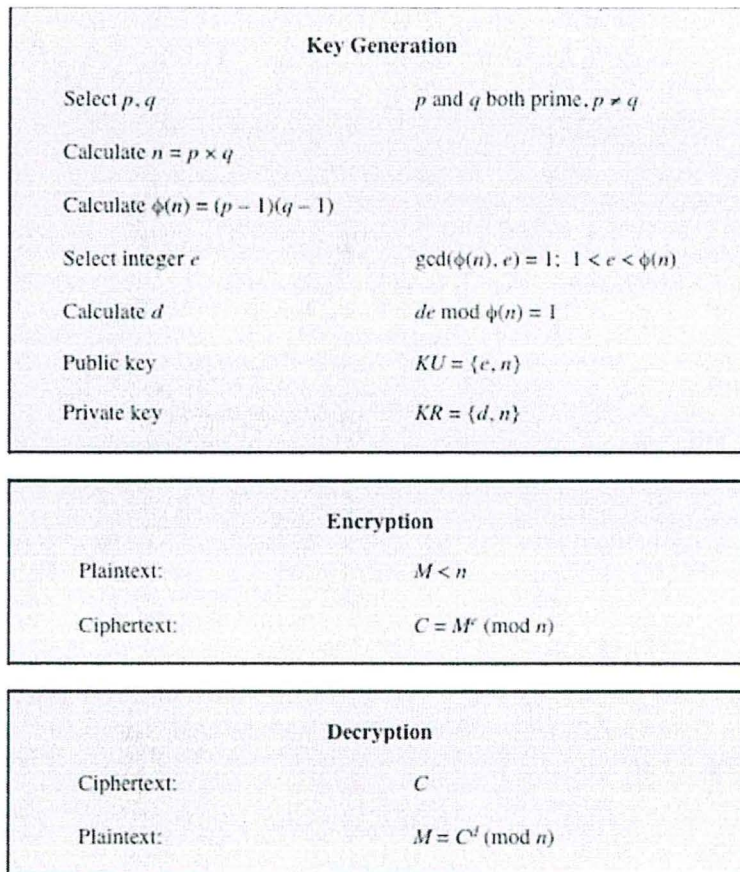


Figure 1: RSA Algorithm

- 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. The design of encryption schemes generally incorporates the use of large block and key sizes to enhance security. What is the drawback to this type of design?

- 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 hexadecimal 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)? [3]