NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

QUALIFICATION : BACHELOR OF COMPUTER SCIENCE IN (CYBER SECURITY)	
QUALIFICATION CODE: 07BCCS	**LEVEL: 6**
COURSE: NETWORK SECURITY	**COURSE CODE: NWS620S**
DATE: JULY 2019	**PAPER: THEORY**
DURATION: 2 hours	**MARKS: 60**

SUPPLEMENTARY/ SECOND OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**Mrs. Mercy Chitauro**
MODERATOR:	**Mr. Joel Eelu**

THIS EXAMINATION PAPER CONSISTS OF 2 PAGES

(Excluding this front page)

INSTRUCTIONS

1. Answer **all questions**.
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. Please, ensure that your writing is **legible, neat** and **presentable.**
4. When answering questions you should be led by the allocation of marks. Do not give too few or too many facts in your answers.
5. Number your answers clearly according to the question paper numbering.
6. Clearly mark rough work as such or cross it out unambiguously in ink.

PERMISSIBLE MATERIALS

1. Calculator.

1. Message Authentication
   a. What security measure is required when you need to protect against falsification of data? [1]
   b. What three things are verified to prove message authentication? [3]
   c. Why is encryption alone not suitable for data authentication? [2]
   d. Explain three uses for public key-systems [3]

2. Use Figure 1 to answer the following questions

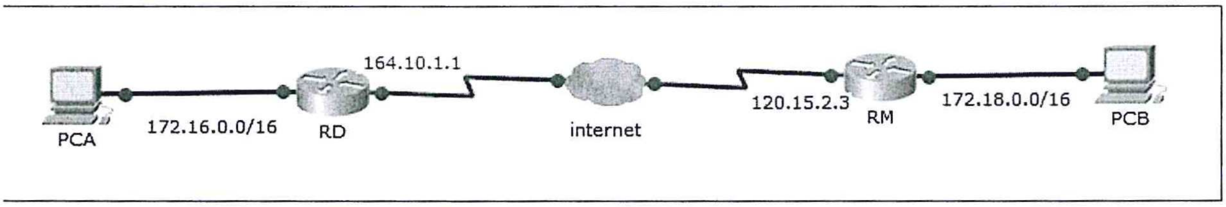

Figure 1: Bakers Fresh Branch Connection

   a. Highlight four Pretty Good Privacy (PGP) services that are availed to email users in the 172.16.0.0/16 and 172.18.0.0/16 networks. [2]
   b. Explain how PGP encrypts a message sent from user at 172.16.0.253 to user at 172.18.5.13 [2]
   c. Does the user at 172.18.5.13 have the key used for encryption before the message is transmitted? [1]
   d. Explain your answer in '4c'. [3]
   e. Secure/Multipurpose Internet Mail Extension (S/MIME) is another email security standard. S/MIME provides which security services for a MIME? [2]
   f. Worms are typically attached to electronic mails so that they access remote systems and replicate.
      i. What is a worm? [2]
      ii. Which other means do worms use to access remote sites besides attaching to emails? [2]
   g. In a worm's lifetime it goes through the same phases as that of a virus. Explain the difference between worm's propagation phase and a virus's propagation phase. [4]

3. The SSL Record Protocol provides confidentiality and message integrity security services for SSL connections.
   a. Which 2 services does the SSL Record Protocol provides for SSL connections? [2]
   b. Which method does SSL use to get message integrity? [1]
   c. Using your knowledge of SSL. Explain how SSL circumvents the attack given.

        i. Brute-force cryptanalytic attack: An exhaustive search of the key space for a conventional encryption algorithm. [2]

        ii. Man-in-the-middle attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client. [2]

        iii. Password sniffing: Passwords in HTTP or other application traffic are eavesdropped. [2]

   d. When Change Cipher spec protocol value is set to one; what happens? [2]

   e. One stage of SSL operation involves the use MAC. What is different at this stage compared with TLS? [2]

4. Kerberos

   a. Describe briefly how Kerberos works. [4]

   b. Why is the ticket granting ticket non-corruptible? [2]

   c. What is the use of a timestamp in a ticket granting ticket? [1]

   d. A public key certificate consists of a public key plus a user ID of the key owner, with the whole block signed by a trusted third party

        i. Explain *"trusted third party"*. [2]

        ii. How does a user obtain a public key certificate? [2]

5. 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. Viruses typically have 3 components. State and explain the three components of a virus [6]

   b. Give an example of each virus component in the context of Cryptolocker virus. [3]

Good luck!!