NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY OF COMPUTING AND INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

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

SUPPLEMENTARY / SECOND OPPORTUNITY EXAMINATION QUESTION PAPER	
EXAMINER(S)	Mrs. Mercy Chitauro
MODERATOR:	Mr. Attlee Gamundani

THIS EXAMINATION PAPER CONSISTS OF 4 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. For any given block x, it is computationally infeasible to find y ≠ x with H(y) =H(x), were H is a hash function. This is a hash function property that states that it is __________? [1]
    a. one-way resistant
    b. weak collision resistant
    c. strong collision resistant
    d. preimage resistant
    e. collision resistant

2. Data Origin Authentication is defined as: [1]
    a. Providing assurance that the source of received data is claimed in a connectionless transfer.
    b. Proof that the message was sent by the specified party.
    c. The assurance that the communicating entity is the one that it claims to be.
    d. Providing confidence in the identity of the entities connected.

3. Which of the following is not used by PGP for message encryption? [1]
    a. CAST-128
    b. 3DES
    c. IDEA
    d. RSA

4. Which IPSec documents is responsible for describing the key management schemes for use with IPSec? [1]
    a. Encapsulating Security Payload (ESP)
    b. Internet Key Exchange (IKE)
    c. Authentication Header (AH)
    d. Cryptographic algorithms
    e. Architecture

5. When does PGP compress a message? [1]
    a. After applying a signature and encryption
    b. After applying encryption before signing
    c. After applying a signature before encryption
    d. Before applying a signature and encryption

6. What are the two requirements for secure use of symmetric encryption? [2]

7. 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? [1]
   a. DES is an example of which type of encryption algorithm? [1]
   b. DES works by encrypting groups of 64 message bits. How many hexadecimal digits is this? [1]
   c. How many bits of the DES key are actually used and how are they selected? [1]

   e. 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.
      I. Which key is used on the sixth iteration? [1]
      II. Which key is used on the last iteration? [1]

8. Hash-based Message Authentication Code (HMAC) is a message authentication code that uses a cryptographic key in conjunction with a hash function.
   a. How many steps does it take HMAC to create a message digest? [1]
   b. The first two steps of HMAC are; *append padding bits* and *append length*. Describe briefly what happens at these two stages [4]
   c. What is the output of the last step? [1]

9.

a. What was the initial design purpose for SSH? [2]

b. SSH is a suite of protocols. Select from the table the correct use of each of the SSH protocols. (*Half mark each. Draw the table in your answer sheet).* [3]

Uses	**SSH User Authentication Protocol**	**SSH Connection Protocol**	**SSH transport Layer Protocol**
Optional compression			
Authenticates the user to the server			
server authentication			
Multiplexes multiple logical communications channels over a single, underlying SSH connection			
data confidentiality, and data integrity			
forward secrecy			

c. State and explain three SSH authentication methods. [7]

10. Write in the spaces provided which firewall technique to control access and enforce the site's security policy is described. (*1 mark each. Draw the table in your answer sheet).* [4]

Firewall technique	**Control**
Controls how particular services are used	
Determines the types of Internet services that can be accessed, inbound or outbound	
Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall	
Controls access to a service according to which user is attempting to access it	

11. A packet filter firewall is typically set up as a list of rules based on matches to fields in the IP or TCP header. If there is a match to one of the rules, that rule is invoked to determine whether to forward or discard the packet. If there is no match to any rule, then a default action is taken.

    a. Describe two default policies possible. [4]

    b. What type of devices or systems are kept in the demilitarized zone? [1]

12.

    a. Highlight four Pretty Good Privacy (PGP) services. [2]

    b. Explain how PGP encrypts a message. [2]

    c. Does the receiver have the key used for encryption before the message is transmitted? [1]

    d. Explain your answer in '12c'. [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. In S/MIME Terminology what does it mean to say, ***"When S/MIME creates a message digest to be used in forming a digital signature it MUST support SHA – 1 and it SHOULD support MD5"***? [2]

13. One function of an intrusion detection is to audit system configuration for vulnerabilities and misconfigurations.

a. What will be the result of such an audit? [2]

b. Which of pattern based or heuristic IDS would be able to carry out the audit in (13a)? [2]

c. Explain how an Intrusion Prevention System IPS extends the functionalities of an IDS. [2]

d. How would you protect an IDS from network attacks [2]

Good Luck!!!!!