THE PAPUA NEW GUINEA UNIVERSITY OF TECHNOLOGY

DEPARTMENT OF MATHEMATICS & COMPUTER SCIENCE

FIRST SEMESTER EXAMINATIONS – 2023

FOURTH YEAR BACHELOR OF SCIENCE IN COMPUTER SCIENCE

CS414 – ADVANCED TOPICS IN COMPUTER SCIENCE

TIME ALLOWED: 3 HOURS

INFORMATION FOR CANDIDATES:

1. Write your name and student number clearly on the front of the examination answer booklet/s.
2. You have 10 minutes to read this paper. You must not begin writing during this time.
3. This paper contains three (3) sections. Part A – Multiple Choice, Part B – Short Answers and Part C – Calculations. You should attempt all the questions.
4. All answers must be written in examination answer booklets provided. No other written materials will be accepted.
5. Start the answer for each question on a new page. Part A answers should be on one page.
6. Do not use red ink or pencil.
7. Notes, textbooks, mobile phones and other recording devices are not allowed in the examination room.
8. Scientific and business calculators are allowed in the examination room.

MARKING SCHEME

Marks are indicated at the beginning of each question. Total is 100 marks.

PART A – MULTIPLE CHOICE [20 MARKS]

Instructions: *Select the most appropriate answer and write your answer in the answer booklet.*

1. In terms of confidentiality, which of these college student records would have a high confidentiality rating?
   A. Student's admission information.
   B. Student's boarding status information.
   C. Student's scholarship information.
   D. Student's grade information.

2. A Denial of Service (DoS) attack disrupts ________________________.
   A. Accountability B. Availability C. Confidentiality D. Integrity

3. Matt posted graphical images of a crime scene he witnessed. In court the images were used as evidence to prosecute the offender. Matt could not refute that he posted the images on Facebook. This is an example of ______________________________.
   A. Confidentiality B. Integrity C. Availability D. Non-repudiation

4. An example of a passive attack is ____________________.
   A. Phishing B. Masquerading C. Traffic Analysis D. Denial of Service

5. Which list below gives hashing functions ONLY?
   A. MD2, MD5, SHA1, SHA256, Whirlpool and Tiger.
   B. MD2, MD5, SHA1, SHA256, AES and DES.
   C. MD2, MD4, MD5, MD6, SHA1 and Diffie-Hellman.
   D. SHA1, SHA256, SHA384, SHA512, Tiger and RSA.

6. The digest length of a SHA1 function is ________________.
   A. 64 bits B. 128 bits C. 160 bits D. 224 bits

7. How many rounds of hashing would a file of 256 bytes go through when the message blocks are 32 bits?
   A. 64 B. 32 C. 128 D. 16

8. Peter hashed a file using hashing function X before sending it to Rita. Rita then used hashing function X to hash the same file without opening it and found that the two digests did not match. What would be the most probable cause of this?
   A. Rita should have opened the file first and hash it.
   B. Peter must have done some changes to the file after hashing it.
   C. Rita must have used a different hashing function.
   D. Peter must have done some changes to the file before hashing it.

9. The digital signature scheme is based on __________________ cryptography.
   A. shared key B. private key C. public key D. modulus

10. When generating a digital signature, there are two inputs that goes into the signature algorithm. What are the two inputs?

    A. Signer's Private Key and Data.
    B. Signer's Public Key and Data.
    C. Signer's Data and Data's Hash.
    D. Signer's Private Key and Data's Hash.

11. Cisco Networking Academy runs a short course on Switching and Routing. After the course each participant is given a certificate. The certificate is digitally signed by Cisco. To verify the signature on the certificate, a potential employer needs to compare the hash of the data (certificate) and hash stored in the ______________________.

    A. digital verification B. digital signature C. public key D. private key

12. Alice uses her credentials (username and password) to log into system X. This is a form of ____________________.

    A. non-repudiation B. authentication C. availability D. confidentiality

13. Which of these is a widely used file format for digital signed documents?

    A. .txt B. .jpg C. .docx D. .pdf

14. Which of the listed organization is responsible for developing and maintaining the standards for digital signatures?

    A. IEEE B. ISO C. NIST D. IETF

15. Which of the following is NOT a benefit of using digital signatures?

    A. non-repudiation B. integrity C. encryption D. authentication

16. Which protocol is commonly used for securely transmitting digital certificates over a network?

    A. HTTP B. FTP C. SMTP D. HTTPS

17. What is the purpose of the Registration Authority (RA) in Public Key Infrastructure (PKI)?

    A. To verify the identity of the certificate requestor.
    B. To issue and sign digital certificates.
    C. To revoke digital certificates when necessary.
    D. To store and manage private keys on behalf of users.

18. Which of the following is NOT a symmetric cipher?

    A. AES B. DES C. RSA D. Blowfish

19. Data Encryption Standard is an implementation of a Feistel Cipher where DES uses ____________ round Feistel structure.

    A. 4 B. 8 C. 16 D. 32

20. The block size of a DES ciphertext is ____________________.

A. 8 bit B. 48 bit C. 56 bit D. 64 bit

PART B – SHORT ANSWERS [58 MARKS]

Question 21. [3 + 3 + 2 + 2 = 10 Marks]

A. What is the purpose of **salting** a password?

B. What is **Phishing** attack?

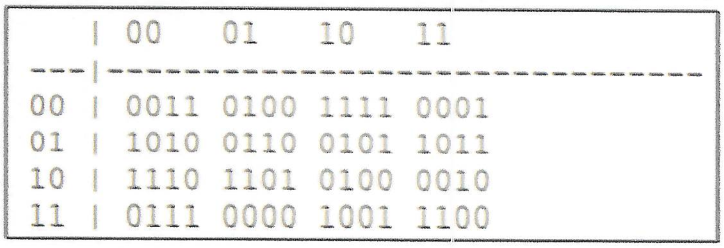
C. Give **two** examples of active attacks where modifications are done to a data stream or a false stream is created.

D. List **two** concepts/technology that provides service availability to a Banking System like BSP.

Question 22. [3 + (2 + 2) + 3 = 10 Marks]

A. During World War 2 the German Enigma machine was used to transmit encrypted messages to field agents. The Germans used a form of *steganography* to hide messages. With the increase in digital technology products, how can steganography be helpful in the digital music industry?

B. The following question refer to the Substitution Box (S-box) shown below.



```
   | 00   01   10   11
---|-----------------------------
00 | 0011 0100 1111 0001
01 | 1010 0110 0101 1011
10 | 1110 1101 0100 0010
11 | 0111 0000 1001 1100
```

What would be the substitutions for the two decimal numbers given?

i. 5

ii. 13

C. Explain why padding is done in Block Ciphers.

Question 23. [3 + 2 + 3 + 2 = 10 Marks]

A. The strength of the RSA cryptosystem relies on the values of p and q. Explain why the values of p and q are important.

B. Which of these two asymmetric algorithms (RSA and El Gamal) is more efficient in encrypting?

C. Why is the key size important in an Asymmetric Algorithm?

D. The RSA encryption formula is;

$$C = P^{e} \bmod n$$

What would be the decryption formula?

Question 24. **[(1 + 1) + 8 = 10 Marks]**

A. The following questions refer to using OpenSSL commands. The text file name is "*Assignment1.txt*"

i. Write the commands that generate a MD5 hash.

ii. Write the commands that generate a SHA256 hash.

B. List the **four** properties of a hashing function and briefly explain each.

Question 25. **[2 + 3 + 2 + 1 = 8 Marks]**

A. Give **two** examples of Certification Authorities (CA) that have clients in Papua New Guinea.

B. Explain what a fingerprint is on a Digital Certificate.

C. List **two** information that can be found in a digital certificate.

D. What feature of Computer Security is not addressed by cryptography?

Question 26. **[6 + 4 = 10 Marks]**

A. What are the three important elements of Digital Signatures? Briefly explain each.

B. In many digital communications, it is desirable to exchange an encrypted message than plaintext to achieve confidentiality. This can be achieved by combining digital signatures with encryption. Explain why **"encrypt-then-sign"** is preferred over **"sign-then-encrypt"**.

PART C – CALCULATIONS **[22 MARKS]**

Question 27. **[10 Marks]**

Use modular arithmetic to find the plaintext from the information provided below.

Information:
Vigenere Cipher was used to encrypt the plaintext.
Ciphertext: SUDVNM
Key: GUAVA
Letters should be converted to their numerical values A = 0, B = 1, C = 2, ... , Z = 25.

Question 28. **[1 + 1 + 8 + 2 = 12 Marks]**

This question refers to the generation of RSA Key Pair.

Given **p** = 7, **q** = 17 and **e** = 5.

A. Find the modulus (**n**).

B. What are the pair of numbers that form the public key?

C. Find the value of the unique number **d**.

D. What are the pair of numbers that form the private key?

END OF EXAMINATION.