GRIFFITH COLLEGE DUBLIN

QUALITY AND QUALIFICATIONS IRELAND
EXAMINATION

POSTGRADUATE DIPLOMA IN SCIENCE IN COMPUTING
INFORMATION SECURITY
Module code: PGDC-IS

MASTER OF SCIENCE IN COMPUTING
INFORMATION SECURITY
Module code: MSCC-IS

Lecturer(s):	**Dr Faheem Bukhatwa**
External Examiner(s):	**Dr Mubashir Husain Rehmani**
Date: 16th May 2023	**Time: 2.15-5.15**

THIS PAPER CONSISTS OF FIVE QUESTIONS
FOUR QUESTIONS TO BE ATTEMPTED
ALL QUESTIONS CARRY EQUAL MARKS

THE USE OF NON PROGRAMMABLE CALCULATORS IS PERMITTED DURING THIS EXAMINATION

QUESTION 1

Answer all parts.

(a) Analyse the reasons why DES encryption uses a set of eight transformation S-boxes?

(9 marks)

(b) Create an S-box and use it to calculate the correct output for each of the following binary sequence inputs: 011001 and 110000

(6 marks)

(c) Use the Playfair cipher with the password "**LEARN MORE**" to decrypt the following ciphered message:

"**UDGEE AOKAG BXBHO QKRRK EKDSU RGODK**".

(10 marks)

(Total 25 marks)

QUESTION 2

Answer all parts.

(a) With aid of a diagram, explain how hash functions are used in digital signatures.

(9 marks)

(b) Use the Euclidean Algorithm to find the greatest common divisor of: 216459 and 93582. Show your work.

(6 marks)

(c) Using the regular Column Transposition Cipher, use the keyword "**HARMING**" and show how to decipher the following ciphered message:

"**HIILG ELOML IXTDM AAMOE AISEW BGVAO RCSLT SESNL EG**"

(10 marks)

(Total 25 marks)

QUESTION 3

Answer all parts.

(a) Recommend six ways through which a conventional encryption system can be made harder to break.

(9 marks)

(b) State advantages of public key encryption systems over conventional encryption systems.

(6 marks)

(c) This ciphered messaged: "**HROF**" was produced after ciphering a plain text message with the Hill cipher and the given key matrix A.

$$A = \begin{pmatrix} 3 & 5 \\ 3 & 2 \end{pmatrix}$$

(i) Find the 26 modular inverse matrix A^{-1}

(6 marks)

(ii) Use A^{-1} to decipher the message "HROF". Show your work. Hint: the plaintext message relates to cars.

(4 marks)

(Total 25 marks)

QUESTION 4

Answer all parts.

(a) Describe the operation of a public key (asymmetric) cryptographic system. Use a diagram in your answer.

(6 marks)

(b) What is meant by the properties of Confusion and Diffusion in an encryption system?

(4 marks)

(c) Use Vigenère cipher with the password "**knowledge**" to decrypt the following ciphered message:

"GVGZZ QJUIC JWPSJ HCICG KKCGV"

(10 marks)

(d) Consider the Diffie-Hellman key exchange protocol; Alice and Bob choose a prime n=13 and g=2. Alice chooses a secret integer a=5 and Bob chooses b=3. What is the new secret key S that they both can use for their conventional encryption. Show your steps.

(5 marks)

(Total 25 marks)

QUESTION 5

Answer all parts.

(a) This number n = 117613 is known to be the product of two prime numbers. Use Fermat's factoring algorithm to find those two prime numbers.

(7 marks)

(b) Alice wishes to send Bob a confidential message m in an email using PGP. Explain the steps in detail.

(9 marks)

(c) Using RSA algorithm, and given the two prime numbers: p=3 and q=11, and a value chosen for private key e=7.

(i) Generate the pair of keys: (e, n) and (d, n)

(5 marks)

(ii) Use the encrypting part of the key (e,n) to encrypt the two numbers message m=5, 7.

(2 marks)

(iii) Use the decrypting part of the key (d,n) to decrypt the ciphered message m=22, 28.

(2 marks)

(Total 25 marks)