GRIFFITH COLLEGE DUBLIN

QUALITY AND QUALIFICATIONS IRELAND
EXAMINATION

MASTER OF SCIENCE IN COMPUTING

INFORMATION SECURITY
Module code: MSCC-IS

Lecturer(s):	**Dr Faheem Bukhatwa**
External Examiner(s):	**Dr Mubashir Husain Rehmani**

Date: 23rd May 2022 **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

(a) Use the Vigenère cipher with the password "ARTIFICIAL" to decrypt the ciphered message:

"MRVPN VGJES AMBWZ ZNAPC EUBKYI DTE"

(9 marks)

(b) This number n = 2173 is the product of two prime numbers. Use Fermat's factoring algorithm to find those two prime numbers.

(8 marks)

(c) PGP allows users to have more than one public/private key pair. In the cases of confidentiality and authenticity, explain how the receiver knows which set of keys the sender has used.

(8 marks)

Total (25 marks)

QUESTION 2

(a) Using the regular Column Transposition Cipher, use the keyword "GUITAR" and show how to decipher the ciphered message:

"**HWIXF TSUIM 8ETAN XGEMS LI8T"**

(10 marks)

(b) Explain in detail how a Public key authority can be used to distribute public keys for a public key encryption system without using public key certificates.

(8 marks)

(c) Explain the Diffie-Hellman key exchange protocol by giving an example of integers representing the numbers used and the secret key S generated by two end users A and B.

(7 marks)

Total (25 marks)

QUESTION 3

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

$$A = \begin{pmatrix} 5 & 4 \\ 3 & 1 \end{pmatrix}$$

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

(10 marks)

(ii) Use it to decipher the message "JPPT". Show your work.

(5 marks)

(b) Calculate the determinant of the following 3x3 matrix:

$$\begin{pmatrix} 5 & 2 & 1 \\ 0 & 6 & 3 \\ 8 & 4 & 7 \end{pmatrix}$$

(10 marks)

Total (25 marks)

QUESTION 4

(a) Encrypt the following number: 6, 8 using the RSA algorithm and the e, n key: 3, 11.

(8 marks)

(b) The DES encryption operation involves 16 loop steps operating on the right and left halves of the data where: Rn = Ln-1 + f(Rn-1,Kn). Explain in detail the function f(Rn-1,Kn) with particular attention to the sizes of data and sub-keys.

(10 marks)

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

(7 marks)

Total (25 marks)

QUESTION 5

(a) Use the Playfair cipher with the password "Computer Security" to decrypt the ciphered message:

"EROGZ FOYHD LPFSE TUHDP"

(10 marks)

(b) Explain digital signature of a document when using hash functions. Support your answer with a diagram.

(10 marks)

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

(5 marks)

Total (25 marks)