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: AUG 2022 P2	**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 “INTELLIGENCE” to decrypt the ciphered message:

“UNGAT WTGPJ CCAPH RECWR VBDSB F”

(9 marks)

(b) Use the Euclidean Algorithm to find the greatest common divisor of: 11214 and 8001. Show your work.

(8 marks)

(c) Suppose Alice wishes to send Bob an authentic message. Explain in detail how PGP provides authenticity.

(8 marks)

Total (25 marks)

QUESTION 2

(a) Using the regular Column Transposition Cipher, use the keyword “VERDICT” show how to decipher the ciphered message:

“**RACDX PEE2E EULDR EHX0S MRYSE AREEX TTDEG”**

(10 marks)

(b) Explain in detail how a Key distribution centre can be used to distribute keys for a conventional encryption system.

(8 marks)

(c) Consider the Diffie-Hellman key exchange protocol; Alice and Bob choose a prime n=11 and a g=2. Alice chooses a secret integer a=4 and Bob chooses b=6. What is the new secret key S that they both can use. Show your steps.

(7 marks)

Total (25 marks)

QUESTION 3

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

$$A = \begin{pmatrix} 4 & 7 \\ 3 & 1 \end{pmatrix}$$

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

(10 marks)

(ii) Use it to decipher the message “WIAN”. Show your work.

(5 marks)

(b) When a pair of RSA keys are to be produced, two primes are selected p, q. From p and q two other values are generated n, m. Two more values referred to e and d are extracted. What are the conditions for selecting a value for each of those two variables: e and d?

(6 marks)

(c) Define the following security services: Authentication, Non-Repudiation, Integrity and Confidentiality.

(4 marks)

Total (25 marks)

QUESTION 4

(a) Given (3, 9) represent (d, n) in a public key pair in RSA public key encryption system, and also given the ciphered message c represented by the following three numbers: = 5, 2, 3 calculate the numbers representing the plain message p.

(9 marks)

(b) An S-Box in the DES algorithm takes a 6-bit input and produces 4-bit output. Design a DES S-Box that will accept a 5-bit input and return a 3 bit output. Elaborate on your design.

(8 marks)

(c) Test the operation of the S-Box you designed in part (b) through an example by suggesting input values which target the first and last values on first row. Also, the first and last values on last row. Show clearly how output values are obtained.

(8 marks)

Total (25 marks)

QUESTION 5

(a) Use the Playfair cipher with the password “Polar Bears” to decrypt the ciphered message: “OTYTY FDZBL PLNCI YGAQW”. Write the steps you followed.

(10 marks)

(b) Write six statements describing hash functions and give two applications where hash functions are used.

(5 marks)

(c) Differentiate between passive attacks and active attacks and explain which of the two is more dangerous.

(10 marks)

Total (25 marks)