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: 10th of August 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) Explain the operation of a transformation S-box as used in DES encryption systems.

(9 marks)

(b) Which would you recommend for a client, an encryption system or a hashing function? Discuss six reasons when explaining your recommendation.

(6 marks)

(c) Use Playfair cipher with the password "**GROWING YOUNGER**" to decrypt the ciphered message:

"**NYXGY WTBUV FEFAA KEATV GWBGN ZPNFV**".

(10 marks)

Total (25 marks)

QUESTION 2

Answer all parts.

(a) (i) Explain three techniques used to distribute session keys between communicating parties.

(3 marks)

(ii) Write four reasons you would recommend in favour of using session keys.

(4 marks)

(b) Design a protocol by which Alice can send a message to Bob and only Bob can decrypt the message. Design a separate protocol by which Alice can send the message to anyone, and anyone receiving the message can be assured that the message is not a replay of a previously sent message and it is indeed from Alice.

(8 marks)

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

"OAITR NNWLE DEDEH EHEOA USLEB WHOED BARTF UVNTL WD"

(10 marks)

Total (25 marks)

QUESTION 3

Answer all parts.

(a) Using public key cryptography; show how a message can be sent while both confidential and authenticated.

(8 marks)

(b) Use the Euclidean Algorithm to find the greatest common divisor of: 7222363 and 9031441. Show your work.

(7 marks)

(c) Hill cipher was used with the 2X2 key matrix K below in order to encrypt a message and produce the ciphered text c = "A J B X". Using the Hill cipher show the calculations and the plain text when you decipher the same encrypted message c back into plain text.

$$K = \begin{pmatrix} 15 & 20 \\ 17 & 9 \end{pmatrix}$$

(10 Marks)

Total (25 marks)

QUESTION 4

Answer all parts.

(a) Describe the operation of a conventional (symmetric) cryptographic system. Use a diagram in your answer.

(6 marks)

(b) With reference to encryption systems, what is the difference between the properties of completeness and avalanche?

(4 marks)

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

"PWLGL TXGCB AIPRF MLROK ZVAO"

(10 marks)

(d) Consider the Diffie-Hellman key exchange protocol; Alice and Bob choose a prime n=17 and a g=2. Alice chooses a secret integer a=7 and Bob chooses b=2. 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) Describe in detail how a Certification Authority can be used to provide a secure communication through distribution of public keys. Use a diagram in your answer.

(9 marks)

(b) This number n = 126727 is known to be the product of two prime numbers. Use Fermat's factoring algorithm to find those two prime numbers.

(7 marks)

(c) Using RSA algorithm, and given the two prime numbers: p=11 and q=5, and a value chosen for private key e=7.

(i) Generate the par 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.

(4 marks)

Total (25 Marks)