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: 21st May 2024	**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
AN APPENDIX CAN BE FOUND AT THE END OF THE EXAM PAPER

QUESTION 1

(a) Create an S-box example table, which would accept 5-bit input and produce a 3-bit output. Use it to calculate the binary output for each of the following binary sequence inputs: 01001 and 10101

(8 marks)

(b) Use the Playfair cipher with the password "LIVING THE LIFE" to decrypt the following ciphered message. Show your works.

"VGURY OIVAF DEFQX KFZBP YLQZ".

(10 marks)

(c) This number n = 89951 is known to be the product of two prime numbers. Use Fermat's factoring algorithm to find those two prime numbers.

(7 marks)

Total (25 marks)

QUESTION 2

(a) Differentiate between digital signatures and Public key certificate in two points:

(i) What is the main purpose for each?

(5 marks)

(ii) How is each obtained?

(5 marks)

(b) This ciphered messaged: "A Q B W" was produced after ciphering a plain text message with Hill cipher with the following key matrix A. The plain text message relates to diamonds belonging to me. Must show your work. Producing result without steps earn you 0 mark.

$$A = \begin{pmatrix} 15 & 10 \\ 2 & 25 \end{pmatrix}$$

(i) Find the 26 modular inverse matrix A and prove it is the inverse.

(10 marks)

(ii) Use the 26 modular inverse matrix A to decipher the message "A Q B W".

(5 marks)

Total (25 marks)

QUESTION 3

(a) Use the Euclidean Algorithm to find the greatest common divisor of: 1591 and 1073. Show your work.

(7 marks)

(b) Use Vigenere cipher with the keyword: "**INFORMATION**" to decrypt this ciphered messaged: "**T B T Y W A R P I F Q B B X I D Y E K B W Z M"**. Explain the steps you take.

(8 marks)

(c) In order to engage into a secure communication both party A and party B need to obtain the public key of the other party. Both A and B use the same public key authority. Trace the sequence of actions used in public key distribution using a public key authority. Use a diagram to support your answer.

(10 marks)

Total (25 marks)

QUESTION 4

(a) Consider the Diffie-Hellman key exchange protocol; Alice and Bob choose a prime n=33 and a g=3. Alice chooses a secret integer a=5 and Bob chooses b=4. What is the new secret key S that they both can use for their conventional encryption. Show your steps.

(7 marks)

(b) PGP allows users to have more than one public/private key pair. How does the receiver know which set of keys the sender has used? Explain the cases of Encryption and Digital signatures.

(8 marks)

(c) Using the regular Column Transposition Cipher, use the keyword "DUSTED" and show steps involved in how to decipher the following ciphered message:

"TYISW UOLWI OONGN EMNYW NERDN NNHOU OKGOI HTSII KT"

(10 marks)

Total (25 marks)

QUESTION 5

(a)

(i) Discuss the weaknesses of Caesar's cipher

(5 marks)

(ii) The following ciphered message was intercepted. It was encrypted using Caesar's cipher. Use brute force to decipher the message. Show the approach you use and the work you do.

"Jajwd ifdhf sgjfr fpjtw fgwjf pifd"

(10 marks)

(b) Explain the steps in the process of generating the sub-keys in DES encryption system. Draw a diagram of the process.

(10 marks)

Total (25 marks)

APENDIX

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25