**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: 9th August 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) Analyse different reasons why DES was no longer suitable for evolving security requirements. Outline changes needed to be introduced in encryption systems.

**(6 marks)**

(b) Use Playfair cipher with the password "Going Strong" to decrypt the following ciphered message. Pleas show all the steps taken:

**"HOXGE ROQHO ALERR DTRNI IY"**

**(11 marks)**

(c) When a message is going to be sent four times, each time it will have one of the following services provided: confidentiality, integrity, authenticity or digitally signed. Each time the message is sent with each service, which would you recommend using: Public key encryption or Hashing? Give a reason for each recommendation.

**(8 marks)**

**Total (25 marks)**

**QUESTION 2**

(a) This number n = 131753 is known to be the product of two prime numbers. Use Fermat's factoring algorithm to find those two prime numbers.

**(7 marks)**

(b) Two parties A & B have a pair of private/public keys and they have already shared their public keys. Create a protocol for A and B in order for a fast exchange long messages between and the messages are both confidential and authentic.

**(8 marks)**

(c) This ciphered messaged: "**WOXZ**" was produced after ciphering a plain text message with the Hill cipher and the given key matrix A. We know the plain text message relates to the motor industry.

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

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

**(8 marks)**

(ii) Use inverse matrix $A^{-1}$ to decipher the message "**WOXZ**". Show your work.

**(2 marks)**

**Total (25 marks)**

**QUESTION 3**

(a) Outline the following security attacks:

(i) Denial of service attack

**(2 marks)**

(ii) Cryptanalysis attack

**(2 marks)**

(iii) Timing and power consumption attacks on RSA

**(2 marks)**

(b) Use the Euclidean Algorithm to find the greatest common divisor of: 4611 and 6786. Show your work.

**(8 marks)**

(c) Use Vigenere cipher with the keyword: "**FLORA**" to decrypt this ciphered messaged: "**DZISILRSJTGLFIIJCHFSZQVSXTGL"**. Sow all your work.

**(11 marks)**

**Total (25 marks)**

**QUESTION 4**

(a) Consider the Diffie-Hellman key exchange protocol; Alice and Bob choose a prime n=21 and a g=4. Alice chooses a secret integer a=3 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)**

(b) Differentiate between the two PGP services: authentication and segmentation.

**(10 marks)**

(c) Use the keyword "**SELLING**" with the regular Column Transposition Cipher and show how to decipher the ciphered message:

"**LOEIB LKUPL EWOBR WENLW NOEEY ACNRD UOYIV OANTT LA**"

Show your work. Giving a result only, without steps will earn 0 marks.

**(10 marks)**

**Total (25 marks)**

**QUESTION 5**

(a) Use brute force and Caesar's cipher to decrypt this ciphered message. Show your work.

"**Jvuzpkly mhzaly zlsm-kypcpun jhyz**"

**(7 marks)**

(b) Use the public key (d, n): 5, 34 to decrypt the following encrypted numerical values c1, c2, c3: 12, 8, 17. Use the RSA public key encryption system. Show your work.

**(6 marks)**

(c) What conditions are required when selecting the value for "***e***" when creating an RSA key pair?

**(6 marks)**

(d) Calculate the determinant of the following matrix (must show your work):

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

**(6 marks)**

**Total (25 marks)**

**APPENDIX**

| 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 |