

Reg No.:\_\_\_\_\_

Name:\_\_\_\_\_

**APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY**

Fifth Semester MCA Degree Supplementary Examination December 2022

**Course Code: RLMCA305****Course Name: CRYPTOGRAPHY AND CYBER SECURITY**

Max. Marks: 60

Duration: 3 Hours

**PART A***Answer all questions, each carries 3 marks.*

Marks

- |   |  |     |
|---|--|-----|
| 1 | Illustrate symmetric cipher model in cryptography.                               | (3) |
| 2 | Define Group and Ring with examples  | (3) |
| 3 | Differentiate block and a stream cipher  | (3) |
| 4 | How authenticity and confidentiality achieved in encryption by using public key? | (3) |
| 5 | Define HMAC. How it is used for security?  | (3) |
| 6 | List out the attacks on digital signature schemes                                | (3) |
| 7 | Explain security services for Email.   | (3) |
| 8 | Explain Authentication Header  | (3) |

**PART B***Answer six questions, one full question from each module and carries 6 marks.****Module I***

- |   |   |     |
|---|---|-----|
| 9 | Explain network security services and mechanisms with the help of a neat diagram? | (6) |
|---|---|-----|

***OR***

- |    |   |     |
|----|---|-----|
| 10 | Describe the working of Playfair cipher. Construct the Playfair matrix with the key ‘larkspur’, using this Playfair matrix encrypt the message “rocky mountain meadow”. | (6) |
|----|---|-----|

***Module II***

- |    |  |     |
|----|--|-----|
| 11 | Explain the Miller- Rabin algorithm for testing primality. | (6) |
|----|--|-----|

***OR***

- |    |  |     |
|----|--|-----|
| 12 | Describe Chinese Remainder theorem with an example | (6) |
|----|--|-----|

***Module III***

- |    |  |     |
|----|--|-----|
| 13 | Explain in detail Advanced Encryption Standard (AES) algorithm | (6) |
|----|--|-----|

***OR***

- |    |  |     |
|----|--|-----|
| 14 | Explain RSA algorithm with an example. | (6) |
|----|--|-----|

***Module IV***

- 15 Define hash function and explain it's properties? (6)

***OR***

- 16 Explain RSA digital signature scheme? (6)

***Module V***

- 17 Explain how bit coin achieves decentralization? (6)

***OR***

- 18 Explain how to store and use Bit coins? (6)

***Module VI***

- 19 Explain working of Transport mode ESP and Tunnel mode ESP with necessary diagrams. (6)

***OR***

- 20 Discuss the four protocols of SSL. (6)

\*\*\*\*\*