JAMIA HAMDARD
Department of Computer Science & Engineering
School of Engineering Sciences & Technology
New Delhi-110062

Examination: Odd Semester Examination 2024 (Backlog)

Paper Name: Cryptography and Network Security **Paper Code: MCA PE 333**

Time: 3 Hours **Maximum Marks: 75**

Note: This question paper has two sections : Section A and Section B. Assume missing data, if any.
Attempt (i) Section-A: All questions are compulsory.
(ii) Section-B: Attempt any FOUR QUESTIONS.

Section –A (All questions are compulsory) 7×5=35 Marks

1. Explain different types of Intrusion Prevention system?	CO2	BL3
2. Draw block diagram for Diffie Hellman algorithm?	CO1	BL2
3. What are the features of message digest because of which it is used in Hash algorithms?	CO3	BL2
4. Draw the block diagram of Cipher Feedback Mode?	CO2	BL3
5. Show how ESP header is added in IPv4 and IPv6 headers in Transport and Tunnel mode? Draw diagrams only.	CO4	BL3
6. Calculate GCD by recursive method for 50,12 ?	CO3	BL4
7. What are the important features of cryptography?	CO1	BL1

Section –B (Attempt any Four questions) 4×10=40 Marks

1. With the help of Extended Euclidean algorithm, find the multiplicative inverse of 11 mod 13? — CO2 — BL3

2. In DES, S-box takes values as : 61, 16, 30, 14, 48, 53, 28, 19 as input. What would be the output after the processing of S-box. Look up table is provided: — CO5 — BL5

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	4	14	12	3	4	5	12	10	5	2	13	15	11	9	7
1	15	5	7	7	9	4	11	3	5	12	6	6	8	13	3	7
2	12	7	5	9	8	12	14	12	12	11	13	13	3	6	13	5
3	6	13	4	6	7	9	10	1	0	4	12	6	14	14	12	14

3. Perform encryption and decryption using RSA, where p=3; q=11; e=7; Message=5? — CO3 — BL4

4. Draw the block diagram of various mode of operations by adding ESP header inIPv4 and IPv6? — CO1 — BL4

5. With the help of Columnar Cipher, show encryption and decryption for message = COLORFUL BALLOONS, where key is defined as PARTY. — CO4 — BL3

6. Factorise 3233 using Fermat's Factoring Algorithm? — CO3 — BL4