Aliah University

End-Semester Examination (Even Semester) - 2025

(CSE 4th Year 8th Semester)

Subject Name: Cryptography and Network Security **Full Marks: 80**

Subject Code: CSEUGPC26 **Time: 3hrs**

Group-A

(Answer all questions) **(5 × 2 = 10)**

1.

a) Define Cryptanalysis. [CO1, BL2]

b) If 40 people need to communicate using symmetric key cryptography, then find out the numbers of symmetric keys needed. [CO3, BL5]

c) Explain Transpositional cipher with example. [CO1, BL2]

d) Convert the Given Text "SUNDAY" into cipher text using monoalphabetic substitution with key=3. [CO3, BL5]

e) Define block cipher. [CO2, BL2]

Group-B

(Answer any five questions) **(5*6= 30)**

2. Explain Rail Fence Cipher and polyalphabetic ciphers with example. (3+3=6) [CO2, BL3]

3. Given the prime numbers p=11 and q=17.Try to find out N, e, d using RSA . (6) [CO3, BL5]

4. Explain various types of passive attacks in details. (6) [CO5, BL4]

5. Explain packet filter firewall and Proxy based firewall with diagram. (3+3=6) [CO5, BL4]

6. Explain the reason for using nonce. Differentiate between block cipher and stream cipher. (2+4=6) [CO2, BL2]

7. Prove that the result of G^{xy} mod N is same as the result of $(G^x \text{ mod } N)^y$ mod N, using G=5 ,x=2,y=3 and N=11. (6) [CO3, BL5]

Group-C

(Answer any four questions) **4 × 10 = 40**

8. Describe the IDEA algorithm with neat diagram and explain the steps. (10) [CO3, BL4]

9. Explain man in the middle attack with diagram. (10) [CO5, BL4]

10. What is Kerberos? Explain Kerberos protocol in details. (2+8=10) [CO5, BL2]

11. Write short note on Biometric Authentication, S/MIME and AH Protocol (3+3+4=10) [CO2, BL2]

12. Illustrate Digital Signature with neat diagram. (10) [CO4, BL4]