

Aliah University
End-Semester Examination (Even Semester) - 2024
(CSE 4th Year 8th Semester)

Subject Name: Cryptography and Network Security
Subject Code: CSEUGPC26

Full Marks: 80
Time: 3hrs

Group-A
(Answer all questions)

$5 \times 2 = 10$

1.

- ☒ a) What is Denial of Service Attack?
- ☒ b) If 40 people need to communicate using symmetric key cryptography, then find out the numbers of symmetric keys needed. *Ans: 1960*
- ☒ c) Differentiate between threats and attacks. *Threats are the danger, attacks are the action.*
- ☒ d) Convert the Given Text "EXAMINATION" into cipher text using monoalphabetic substitution with key=4.
- ☒ e) Define stream cipher.

$$P = 2^4 = 16$$
$$C = P - 4$$

Group-B

(Answer any five questions)

$5 \times 6 = 30$

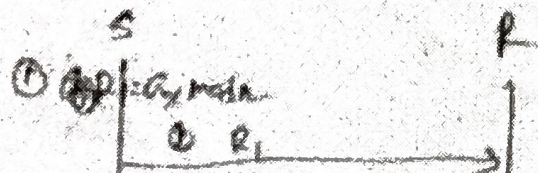
- ☒ 2. Differentiate between monoalphabetic and polyalphabetic ciphers with example. (6)
- ☒ 3. Explain the algorithm for generating keys in RSA algorithm. Perform encryption and decryption using RSA Alg. for the following. $P=7$; $q=11$; $e=13$; $M=8$. (6)
- ☒ 4. Draw and explain IPsec ESP Format. (6)
- ☒ 5. Explain DMZ network in details with diagram. (6)
- ☒ 6. Define Caesar cipher with example? Differentiate between block cipher and stream cipher. (3+3=6)
- ☒ 7. Prove that the result of $G^x \bmod N$ is same as the result of $(G^y \bmod N)^x \bmod N$, using $G=7$, $x=2$, $y=3$ and $N=11$. (6)

Group-C

(Answer any four questions)

$4 \times 10 = 40$

- ☒ 8. Describe the DES algorithm with neat diagram and explain the steps. (10)
- ☒ 9. Explain man in the middle attack with diagram. (10)
- ☒ 10. How TLS is different from SSL? Describe TLS protocol in details. (2+8=10)
- ☒ 11. Explain various types of active and passive attacks in details. (10)
- ☒ 12. Illustrate public key cryptography system with neat diagram. (10)



74869
40x39

24
24
25
18