Reg. No.																

Question Paper Code	14105

B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2025

Sixth Semester

Artificial Intelligence and Data Science

20AIEL605 - CRYPTOGRAPHY AND NETWORK SECURITY

Regulations - 2020

Duration: 3 Hours Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

Marks *K – Level* *CO*

1. Which of the following is a substitution technique? *1 K1 CO1*
   (a) Caesar cipher (b) Vigenère cipher
   (c) Transposition cipher (d) RSA encryption
2. Which of the following is NOT a classical encryption technique? *1 K1 CO1*
   (a) Substitution (b) Transposition (c) Steganography (d) AES
3. The Euclidean algorithm is used to________________. *1 K1 CO2*
   (a) Find Prime number (b) Find LCM (c) Find GCD (d) Find Key
4. Communication between end systems is encrypted using a key, known as ___________. *1 K1 CO2*
   (a) Temporary key (b) Line key (c) Section key (d) Session key
5. The Chinese Remainder Theorem is useful in_______________. *1 K1 CO3*
   (a)DSA (b)Diffie Hellman (c) AES (d) RSA
6. Which process in block cipers involves scrambling the plaintext using a secret key? *1 K1 CO3*
   (a)Key generation (b) Key expansion (c) Encryption (d) Decryption
7. Which is a message authentication code? *1 K1 CO4*
   (a)HMAC (b) SHA-12 (c) Hash function (d) DSS
8. In RSA, the public key is a pair of numbers ___________________. *1 K1 CO4*
   (a) (p,q) (b) (n,d) (c) (n,e) (d) (e,d)
9. Which protocol secures email communication? *1 K1 CO5*
   (a) Firewall (b) Hash function (c) S/MIME (d) PGP
10. Firewalls are primarily used to _______________. *1 K1 CO6*
    (a) Authorized access (b) Grant permission
    (c) Block unauthorized access (d) VPN devices only

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

11. Define Perfect Security. *2 K1 CO1*
12. List the different types of network security attacks. *2 K1 CO1*
13. State and explain Euler's Theorem. *2 K1 CO2*
14. Outline the concept of groups and rings. *2 K2 CO2*
15. Classify the types of block cipher mode of operations. *2 K2 CO3*
16. Differentiate between symmetric asymmetric cryptography. *2 K2 CO3*
17. What are the features of X.509 authentication service? *2 K1 CO4*
18. Explain why prime numbers are important in cryptography. *2 K2 CO4*
19. Write short notes on PGP. *2 K1 CO5*
20. Relate how digital signature ensures the security. *2 K2 CO5*
21. What is the role of an Intrusion Detection System? *2 K1 CO6*
22. List out the security threats in wireless networks. *2 K1 CO6*

K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyze; K5 – Evaluate; K6 – Create

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23. a) Using play fair cipher using the keyword MONARCHY. Consider plaintext as “SRISAIRAMINSTITUTION”. *11 K2 CO1*

OR

b) Explain the model for network security with a neat diagram. *11 K2 CO1*

24. a) Explain in detail about Groups, Rings and Fields. *11 K2 CO2*

OR

b) Show Modular Exponentiation and Modulo Arithmetic operations with its properties in detail with example. *11 K2 CO2*

25. a) Summarize the concept of AES algorithm with a neat diagram. *11 K2 CO3*

OR

b) Explain the key distribution and key management of public key encryption in detail. *11 K2 CO3*

26. a) Identify the possible threats for the RSA algorithm and list their counter measures. Perform encryption and decryption using the RSA algorithm for the following: p=7, q=11, e=7, M=9. *11 K3 CO4*

OR

b) Apply Diffie Hellman algorithm and find the secret key shared between user A and user B using Diffie Hellman algorithm for the following q=353; α (primitive root)=3,XA=45 and XB=50. *11 K3 CO4*

27. a) Identify the steps involved in Signature generation and Verification functions of DSS. *11 K3 CO5*

OR

b) Choose the various attacks on Kerberos and write the four requirements of Kerberos. *11 K3 CO5*

28. a) Experiment with how S/MIME is used to secure Email. *11 K3 CO6*

OR

b) Make use of firewall concepts to explain various types of firewalls. *11 K3 CO6*