Question Bank of Introduction to Cryptography for the Fourth Stage of the Second Semester:

1. What is the difference between encryption and decryption?
2. Define the terms plaintext and ciphertext.
3. Explain the concept of a key in cryptography.
4. What is a cryptosystem?
5. Define the term key length and its significance in cryptography.
6. What is the concept of a cryptographic algorithm?
7. What is the difference between a symmetric key and an asymmetric key?
8. Encrypt the word "HELLO" using the Caesar cipher with a key shift of 3.
9. Decrypt the ciphertext "WKLV LV D VHFUHW" using the Caesar cipher with a key shift of 3.
10. Encrypt the word "CRYPTOGRAPHY" using the Vigenère cipher with the keyword "KEY".
11. Decrypt the ciphertext "QWOMN GWSH" using the Vigenère cipher with the keyword "CRYPTO".
12. Encrypt the word "MESSAGE" using the Playfair cipher with the key matrix "CIPHER".
13. Decrypt the ciphertext "LBUOEI" using the Playfair cipher with the key matrix "MESSAGE".
14. Encrypt the word "SECRET" using a transposition cipher with a key (31425).
15. Decrypt the ciphertext "ESRTEC" using a transposition cipher with a key (24153).
16. Encrypt the word "CRYPTOGRAPHY" using the Rail Fence cipher with a rail count of 3.
17. Decrypt the ciphertext "CAPGOTHRYPYR" using the Rail Fence cipher with a rail count of 3.
18. Encrypt the word "HELLO" using a simple columnar transposition cipher with the key "CIPHER".
19. Decrypt the ciphertext "HOLLE" using a simple columnar transposition cipher with the key "CIPHER".

20. Encrypt the message "HELLO" using the Affine cipher with the key pair (a = 5, b = 8), where a is the multiplicative key and b is the additive key.

21. Decrypt the ciphertext "QHTTG" using the Affine cipher with the key pair (a = 7, b = 3).

22. Encrypt the message "HELLO" using the Hill cipher with the key matrix [2 3; 1 4].

23. Decrypt the ciphertext "JEPSU" using the Hill cipher with the key matrix [1 2; 3 5].

24. Define the concept of a super-increasing knapsack and its significance in the Knapsack cipher.

25. Encrypt the message "HELLO" using a super-increasing knapsack with the sequence [2, 7, 11, 21, 42] and a public key multiplier of 3.

26. Decrypt the ciphertext "125 335 583" using the corresponding private key for the above super-increasing knapsack.

27. Encrypt the plaintext "HELLO" using RSA with a public key (e, n) of (17, 3233). Demonstrate the step-by-step encryption process.

28. Decrypt the ciphertext "2561" using RSA with a private key (d, n) of (2753, 3233). Illustrate the step-by-step decryption process.

29. Given a specific RSA key pair with a public key (e, n) of (13, 2537), calculate the corresponding private key (d) using the extended Euclidean algorithm.

30. Encrypt the plaintext "OPENAI" using RSA with a public key (e, n) of (5, 2537). Show the resulting ciphertext using modular exponentiation.

31. Decrypt the ciphertext "2351" using RSA with a private key (d, n) of (937, 2537). Illustrate the modular exponentiation process to obtain the original plaintext.

32. Let $p = 7$ and $q = 11$ with $\mathrm{A} = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$ encrypt the plaintext "HELLO" using the Lu-Lee System cipher with a specific key and demonstrate the step-by-step encryption process.

33. Decrypt the ciphertext "5C8B3" using the Lu-Lee System cipher with a specific key and demonstrate the step-by-step decryption process. Choose $p = 11$, $q = 13$ and $\mathrm{A} = \begin{pmatrix} 2 & -1 \\ 3 & 5 \end{pmatrix}$.

34. Given a specific key schedule in the Lu-Lee System cipher, show the round keys generated for a 4-round encryption process.

35. Encrypt the plaintext "OPENAI" using the Lu-Lee System cipher with a specific key and illustrate the resulting ciphertext using a substitution-permutation network. Consider $p = 5,\ q = 7$ and A $= \begin{pmatrix} 1 & 4 \\ 3 & 2 \end{pmatrix}$.

36. Decrypt the ciphertext "2F7A6D" using the Lu-Lee System cipher with a specific key and illustrate the reverse substitution-permutation process to obtain the original plaintext. Choose $p = 11,\ q = 13$ and A $= \begin{pmatrix} 1 & 2 \\ 5 & -1 \end{pmatrix}$.

37. Encrypt the plaintext "HELLO" using the Rabin cryptosystem with the public key (n) of 2537 and demonstrate the step-by-step encryption process.

38. Decrypt the ciphertext "956" using the Rabin cryptosystem with the private key (p, q) of (37, 71) and illustrate the step-by-step decryption process.

39. Given a specific key generation process in the Rabin cryptosystem, calculate the public key (n) and private key (p, q) for a given modulus value.

40. Encrypt the plaintext "OPENAI" using the Rabin cryptosystem with the public key (n) of 5473 and illustrate the resulting ciphertext.

41. Decrypt the ciphertext "1441" using the Rabin cryptosystem with the private key (p, q) of (29, 59) and illustrate the step-by-step process to obtain the original plaintext.

42. Calculate the Lagrange symbol (a/p) for a = 7 and p = 11.

43. Evaluate the Jacobi symbol (a/n) for a = 3 and n = 15.

44. Determine the value of the Lagrange symbol (a/p) for a = 2 and p = 7.

45. Find the Jacobi symbol (a/n) for a = 5 and n = 13.

46. Let $p = 11, q = 43$ and $s = 5$. By using Williams System encrypt the message $M = 105$ and then decrypt your answer.

47. Calculate the result of adding two points, P = (2, 3) and Q = (-1, 5), on an elliptic curve with a specific equation.

48. Given an elliptic curve defined by the equation $y^2 \equiv x^3 + 2x - 2$, perform scalar multiplication of a point P = (2, 3) with a scalar value of 5, and determine the resulting point.

49. Determine the number of points on the elliptic curve $y^2 \equiv x^3 - 2x + 3 \pmod 5$.

50. Perform point addition on the elliptic curve $y^2 \equiv x^3 - x - 1 \pmod 7$ with P = (2, 3) and Q = (4, 5). Calculate the resulting point modulo 7.