«**CONFIRMED»**

**Head of the Department**

**“Cryptology”**

**\_\_\_\_\_\_\_\_\_\_\_\_ Khudoykulov Z.Т.**

**«\_\_\_\_»\_\_\_\_\_\_\_\_2024 year**

**Final control questions on Cryptography 1**

1. Euclidean and extended Euclidean algorithm rules and their examples.
2. Find the inverse of in the field .
3. Find the division and 75 in the area .
4. Modular Arithmetic, Its Properties, and Related Examples
5. Linear Congruences and Their Properties. Rules for Checking the Existence of Solutions and Determining the Number of Solutions of Linear Congruences
6. Solve the linear congruence
7. Solve the linear congruence .
8. **Solving Linear Diophantine Equations**
9. Solve the linear Diophantine equation
10. Solve linear diofant equation .
11. Calculate the value of the number .
12. Euler's function and theorems derived from it.
13. The concept of a primitive root is a rule for calculating the number and values ​​of primitive roots for a given modulus.
14. Calculate the value of the Euler function of the number p=24.
15. Calculate the value of the Euler function of the number p=11.
16. Еxplain the Chinese theorem on remainders.
17. va calculate this linear congruence using the Chinese theorem remainders.
18. va calculate this linear congruence using the Chinese theorem remainders.
19. Performing operations on the basis of parametric algebra (multiplication of numbers, exponentiation and finding the inverse by mmodule).
20. Multiply the numbers va by the parameter .
21. Multiply the numbers va by the parameter with module .
22. Increase the number a=4 to the power of 13 by the parameter R=2 when the module p=13.
23. Increase the number a=6 to the power of 9 by the parameter R=3 when the module p=11.
24. Find the inverse of the number a=3, modulo p=11, by parameter R=2.
25. Find the inverse of the number a=4, modulo p=13, by parameter R=2.
26. Solve quadratic congruence .
27. Solve quadratic congruence .
28. Solve quadratic congruence .
29. The Legendre symbol and its properties.
30. Method of calculation of Legendre's symbol by Gauss Lemma - theorem.
31. Use Gauss's Lemma to calculate all the values ​​for which the quadratic residues module p=13.
32. Method of calculating the Legendre symbol using Euler's criteria.
33. Calculate all values ​​for which p=13 is a quadratic residue by Euler's criteria.
34. A method of calculating the Legendre symbol by means of a primitive root.
35. Calculate all values ​​for which the quadratic residues module p=13 is given by the primitive root value.
36. Calculate all values ​​for which the quadratic residues module p=11 is given by the primitive root value.
37. Ferma's method of factoring numbers.
38. Factor 3053 using Ferma's method.
39. Describe Pollard's method of factoring numbers.
40. Factor 3053 using Pollard's method.
41. Fermat's test for primality testing of numbers.
42. Verify the number n=17 by Fermat's test (α>5) based on at least 3 witnesses.
43. Solovay-Strassen test for primality testing of numbers.
44. Check n=17 for depth by Solavey-Strassen test (α>5) based on at least 3 primality.
45. Rabin-Miller test for primality testing of numbers.
46. Test the primality of n=17n = 17 using the Rabin-Miller test with at least 3 witnesses where a>5.
47. Polyg-Hellman discrete logarithmization method.
48. Calculate the x – value from expression.
49. Calculate, . va , where .
50. Explain the rule for solving quadratic congruences a⋅x^2+b⋅x+c≡0(modp).
51. Verify that the quadratic similarities 2\*x^2+5x-9≡0 (mod 101) have a solution.
52. Verify that the quadratic similarities 3\*x^2+6x+5x+5≡0 (mod 89) have a solution.
53. Check that the quadratic similarities x^2+3x-2≡0 (mod 13) have a solution.
54. What conditions must be satisfied for the given set to be a group.
55. What conditions must be met for the given set to be a ring.
56. What conditions must be met for the given set to be a field.
57. Find the value of the Lejandre symbol (19/23).
58. Find the value of the Lejandre symbol (-23/59).
59. Find the value of the Lejandre symbol (18/43).
60. Perform factorizations of the numbers 3053 using Fermat's method.
61. Explain how the inverse of a number is calculated by a parameter.
62. Explain the methods of solving linear equations.
63. Explain the concepts of group, Abel's group, concepts of field in cryptography.
64. Concepts of field and polynomial, Galois field.
65. Explain the concepts of square subtraction, modular square root computation, Lejandre symbol, Jacobi symbol and its computation.
66. Give examples of ways to generate prime numbers.
67. Explain Fermat and Mersenne numbers, Carlmichael numbers.
68. Explain probability and truth tests prostate check.
69. Explain the Euler function in cryptography.
70. Give examples for methods of factorization of numbers.
71. Give examples for methods of discrete logarithmization.
72. Elliptic curve equations, methods for solving elliptic curve equations.
73. Explain performing operations on the points of an elliptic curve in a finite field.
74. Explain discrete logarithmization on elliptic curves and Pollard's algorithm, Pohlig-Hellman algorithm.
75. 14^x≡17 (mod 23) compute the values of x.
76. Find the inverse of 101 in the field GF(2^8)=x^8+x^4+x^3+x+1.
77. Find the product of the numbers 97 and 83 in the field GF(2^8)=x^8+x^4+x^3+x+1.
78. Find the inverse of the number 17 modulo p=23.
79. Find the inverse of the number 31 modulo p=23.
80. Solve the linear similarity of 5\*x≡2 (modulo 26).
81. Solve the linear similarity 51\*x=9 (modulo 4).
82. Find the value of x and y from the equation 44\*x-17\*y=9.
83. Find the value of x and y from the equation 5\*x-53\*y=17.
84. Calculate the value of 11^143 modulo 23 in an efficient way.
85. Calculate the value of 19^124 modulo 29 in an efficient way.
86. Calculate the value of the Euler function of the number p=28.
87. Calculate the value of the Euler function of the number p=32.
88. Calculate the value of the Euler function of the number p=42.
89. P=(5,25), Q=(1,30). Perform the operations R=P+Q and D=11Q on the points of an elliptic curve in a finite field E\_37 (2,9).
90. P=(21,32), Q=(1,30). Performing the operations R=P+Q and D=11Q over the points of an elliptic curve in a finite field E\_37 (2,9).
91. P=(5,25), Q=(35,16). Performing the operations R=P+Q and D=11Q over the points of an elliptic curve in the finite field E\_37 (2,9).
92. P=(16,20), Q=(1,30). Performing the operations R=P+Q and D=11Q over points on an elliptic curve in a finite field E\_37 (2,9).
93. P=(0,3), Q=(1,30). Perform the operations R=P+Q and D=11Q over the points of an elliptic curve in the finite field E\_37 (2,9).
94. Find the number and values of the primal roots of the number p=19.
95. Compute these linear congruences x≡2 (mod 3), x≡3 (mod 5) and x≡2 (mod 7) using the Chinese residue theorem.
96. Compute these linear congruences x≡3 (mod 11) and x≡2 (mod 7) using the Chinese residue theorem.
97. Multiply the numbers a=4 and b=7 by the parameter R=2 with modulo p=13.
98. Multiply the numbers a=5 and b=8 by the parameter R=3 modulo p=19.
99. Elevate to degree 11 the number a=7 with parameter R=5 modulo p=13.
100. Elevate to degree 5 the number a=6 with parameter R=3 modulo p=29.

**Compiled by:**

**Assistant teacher, department of Cryptology: Daminov A.A.**