**«ПОДТВЕРЖДАЮ»**

**Заведующей кафедрой**

**«Криптология»**

**\_\_\_\_\_\_\_\_\_\_\_\_ Худойкулов З.Т.**

**«\_\_\_\_» \_\_\_\_\_\_\_\_2024 год**

**Вопросы для итогового контроля**

**по дисциплине «Криптография 1»**

1. Приведите примеры правил алгоритма Евклида и расширенного Евклида.
2. Найдите обратное число в поле Гаула
3. Найдите произведение чисел и в поле
4. Приведите примеры модульной арифметики и ее свойств.
5. Объясните линейные сходства и их свойства. Правила проверки существования решения линейных сходства и определения количества решений.
6. Решите линейные сходства
7. Решите линейные сходства
8. Объясните линейные диофантовы уравнения.
9. Решите линейные диофантовы уравнения
10. Решите линейные диофантовы уравнения .
11. Вычислить значение .
12. Объясните функция Эйлера и выведенные из нее теоремы.
13. Объяснить понятие первообразный корней, правило вычисления количества и значений первообразный корень по заданному модулю.
14. Вычислите значение функции Эйлера числа p=24.
15. Найдите количество и значения первообразный корней числа p=11.
16. Объясните китайскую теорему об остатках.
17. Вычислите эти линейные сходства *x≡2 (mod 3), x≡3 (mod 5) и   
    x≡2 (mod 7)*, используя китайскую теорему об остатках.
18. Вычислите эти линейные сходства и , используя китайскую теорему об остатках.
19. Объясните выполнение операций на основе параметрической алгебры (умножение чисел, возведение в степень и нахождение обратного числа по модулю).
20. Умножьте числа a=4 и b=7 с параметром R=2 в модуле p=13.
21. Умножьте числа a=5 и b=8 с параметром R=3 в модуле p=19.
22. Возведите в степень 12 число a=4 с параметром R=2 в модуле p=13.
23. Возведите в степень 11 число a=6 с параметром R=3 в модуле p=13.
24. Найдите обратное число a=3 по модулю p=11 с параметром R=2.
25. Найдите обратное число a=4 по модулю p=13 с параметром R=3.
26. Проверите, что квадратные сходства *a\*x^2+b\*x+c≡0 (mod p)* имеют решение.
27. Проверите, что квадратные сходства *2\*x^2+5x-9≡0 (mod 101)* имеют решение.
28. Проверите, что квадратные сходства *3\*x^2+6x+5≡0 (mod 89)* имеют решение.
29. Объясните символ Лежандра и его свойства.
30. Объясните метод вычисления символа Лежандра, используя лемму-теорему Гаусса.
31. Используйте лемму Гаусса, чтобы вычислить все значения квадратный вычетов по модулю p=13.
32. Объясните метод расчета символа Лежандра по критерию Эйлера.
33. Вычислите все значения квадратный вычетов, по модулю *p=13* с критерию Эйлера.
34. Метод расчета символа Лежандра с помощью первообразный корен.
35. Вычислите все значения квадратный вычетов, по модулю *p=13* с помощью первообразный корен.
36. Вычислите все значения квадратный вычетов, по модулю *p=11*.
37. Объясните метод Ферма факторизации чисел.
38. Выполните факторизации чисел 3053 по методу Ферма.
39. Объясните метод Полларда факторизации чисел.
40. Выполните факторизации чисел 3053 по методу Полларда.
41. Объясните Тест Ферма проверка чисел на простоту.
42. Проверьте число n=17 на простоту с помощью теста Ферма (α>5) на основании как минимум 3-х свидетелей.
43. Объясните Тест Соловея — Штрассена проверка чисел на простоту.
44. Проверьте число n=17 на простоту с помощью Тест Соловея — Штрассена (α>5) на основании как минимум 3-х свидетелей.
45. Объясните Тест Миллера — Рабина проверка чисел на простоту.
46. Проверьте число n=17 на простоту с помощью Тест Миллера — Рабина (α>5) на основании как минимум 3-х свидетелей.
47. Объясните метод дискретное логарифмирование Полига-Хеллмана.
48. Рассчитайте значение *x* из выражения *14^x≡17 (mod 23).*
49. , . Выполнение операций и над точками эллиптической кривой в конечном поле .
50. Объяснить правило решения квадратичных сходства *a\*x^2+b\*x+c≡0 (mod p).*
51. Проверите, что квадратные сходства *2\*x^2+5x-9≡0 (mod 101)* имеют решение.
52. Проверите, что квадратные сходства *3\*x^2+6x+5≡0 (mod 89)* имеют решение.
53. Проверите, что квадратные сходства *x^2+3x-2≡0 (mod 13)* имеют решение.
54. Какие условия должны быть выполнены, чтобы данное множество было группой.
55. Какие условия должны быть выполнены, чтобы данное множество было кольцо.
56. Какие условия должны быть выполнены, чтобы данное множество было поля.
57. (19/23) Найдите значение символа Лежандра.
58. (-23/59) Найдите значение символа Лежандра.
59. (18/43) Найдите значение символа Лежандра.
60. Выполните факторизации чисел 3053 по методу Ферма.
61. Объясните как вычисляется обратные число по параметру.
62. Объясните методы решения линейных уравнений.
63. Объясните понятия группа, группа Абела, понятия поля в криптографии.
64. Понятия поля и полиномиал, поле Галуа.
65. Объясните понятия квадратное вычитание, модульное вычисление квадратного корня, символ Лежандра, символ Якоби и его вычисление.
66. Приведите примеры способы генерации простых чисел.
67. Объясните числа Ферма и Мерсенна, числа Карлмайкла.
68. Объясните вероятностные и истинные тесты проверка на простату.
69. Объясните функция Эйлера в криптографии.
70. Приведите примеры для методы факторизации чисел.
71. Приведите примеры для методы дискретная логарифмизация.
72. Уравнения эллиптических кривых, методы решения уравнений эллиптических кривых.
73. Объясните выполнение операций над точками эллиптической кривой в конечном поле.
74. Объясните дискретная логарифмизация на эллиптических кривых  и  алгоритм Полларда, алгоритм Поллига Хелмона.
75. вычислить значения *х.*
76. Найдите обратное число 101 в поле GF(2^8)=x^8+x^4+x^3+x+1.
77. Найдите произведение чисел 97 и 83 в поле GF(2^8)=x^8+x^4+x^3+x+1.
78. Найдите обратное число 17 по модулю p=23.
79. Найдите обратное числу 31 по модулю p=23.
80. Решите линейное сходство 5\*x≡2 (по модулю 26).
81. Решите линейную сходство 51\*x=9 (по модулю 4).
82. Найдите значение *х* и *y* из уравнения 44\*x-17\*y=9.
83. Найдите значение *х* и *y* из уравнения 5\*x-53\*y=17.
84. Вычислите значение 11^143 по модулю 23 с эффективном способом.
85. Вычислите значение 19^124 по модулю 29 с эффективном способом.
86. Вычислите значение функции Эйлера числа p=28.
87. Вычислите значение функции Эйлера числа p=32.
88. Вычислите значение функции Эйлера числа p=42.
89. , . Выполнение операций и над точками эллиптической кривой в конечном поле .
90. , . Выполнение операций и над точками эллиптической кривой в конечном поле .
91. , . Выполнение операций и над точками эллиптической кривой в конечном поле .
92. , . Выполнение операций и над точками эллиптической кривой в конечном поле .
93. , . Выполнение операций и над точками эллиптической кривой в конечном поле .
94. Найдите количество и значения первообразный корней числа p=19.
95. Вычислите эти линейные соответствия x≡2 (mod 3), x≡3 (mod 5) и x≡2 (mod 7), используя китайскую теорему об остатках.
96. Вычислите эти линейные соответствия x≡3 (mod 11) и x≡2 (mod 7), используя китайскую теорему об остатках.
97. Умножьте числа a=4 и b=7 на параметр R=2 с модулем p=13.
98. Умножьте числа a=5 и b=8 на параметр R=3 по модулю p=19.
99. Возведите в степень 11 число a=7 с параметром R=5 в модуле p=13.
100. Возведите в степень 5 число a=6 с параметром R=3 в модуле p=29.

**Составитель:**

**старший преподаватель**

**кафедры, «Криптология»: Турсунов О.О.**