|  |  |
| --- | --- |
|  |  |
| Институт (подразделение) | **ИНСТИТУТ КИБЕРБЕЗОПАСНОСТИ И ЦИФРОВЫХ ТЕХНОЛОГИЙ** |
| Кафедра | **КБ-8 «Информационное противоборство»** |
| Зав. кафедрой | **В.Р. Григорьев** |
| Дисциплина | **Криптографические методы защиты информации** |
| Курс | **3** |
| Семестр | **5** |
| № протокола заседания кафедры | **1** |
| Дата утверждения билетов | **31.08.2021** |
| Шифр направления подготовки | **10.03.01** |
| Направление подготовки | **Информационная безопасность** |
| Направленность (профиль) подготовки | **Организация и технологии защиты информации** |
| Форма обучения | **Очная** |
| Учебный год | **2021/2022** |
| Вид аттестации | **ЗАЧЕТНЫЙ БИЛЕТ №** |

Конторольные вопросы.

1.В чём суть симметричного шифрования?

2. Модульная арифметика. Сложение в Z7. Дано a=5, b =7. Вычислите значения суммы (a+b) mod 7.

3. Основная теорема арифметики.

4. Теорема Ферма.

5. Модульная арифметика. Сложение в Z7. Дано a=6, b =3. Вычислите значения суммы (a+b) mod 7.

6. Что такое криптография?

7. Теорема Эйлера-Ферма.

8. Модульная арифметика. Сложение в Z7. Дано a=5, b =4. Вычислите значения суммы (a+b) mod 7.

9. Что такое криптоанализ?

10. Что называется моноалфавитным шифром? Пример.

11. Модульная арифметика. Умножение в Z7. Дано a=3, b =6. Вычислите значения произведения (a\*b) mod 7.

12. Что такое криптология?

13. Что называется многоалфавитным шифром? Пример.

14. Модульная арифметика. Умножение в Z7. Дано a=2, b =6. Вычислите значения произведения (a\*b) mod 7.

15. Что такое стеганография? Пример.

16. В чём особенность использования квадрата Полибия при шифровании? Пример.

17. Модульная арифметика. Умножение в Z7. Дано a=4, b =6. Вычислите значения произведения (a\*b) mod 7.

18. Применяя шифр Цезаря – зашифруйте слово ЗАМЕНА. Алфавит записан ниже

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ?

19. В чём заключается принцип Керхоффса.(год 1883)

20. Модульная арифметика. Умножение в Z7. Дано a=6, b =6. Вычислите значения произведения (a\*b) mod 7.

21. Как записать слово «разведчик» в магический квадрат 3\*3 ?

22. Дано слово из 8 бит- 10011001 запишите соответствующий ему полином?

23. Свойства оператора mod?

24.В чём магия магического квадрата?

25. Дано слово из 8 бит- 00100110 запишите соответствующий ему полином?

26. Найти мультипликативную инверсию числа 8 в Z10**.**

27.Поясните принцип применения Сциталы.

28. Применить шифр-простая перестановка и зашифровать «место встречи изменить невозможно» применяя таблицу 5\*6 .

29. Найти мультипликативную инверсию числа 7 в Z10**.**

30. Поясните принцип применения диска Энея.

31. Применить простую перестановку с паролем «Привет» и зашифровать фразу «место встречи изменить невозможно», применяя таблицу 5\*6.

32. Найти мультипликативную инверсию числа 9 в Z10.

33. Модульная арифметика. Возведение в степень в Z7. Дано a=2, b =6. Вычислите значение (26) mod 7.

34. В чём суть пропорционального шифрования.

35. Найти мультипликативную инверсию числа 3 в Z10.

36. Модульная арифметика. Возведение в степень в Z7. Дано a=6, b =6. Вычислите значение (66) mod 7.

37.В чём суть применения в криптоанализе частотных характеристик английского и русского языков. Какие буквы чаще встречаются в английском и русском языках?

38. Какой шифр является многоалфавитным шифром? (Шифр Виженера, шифр Винера или шифр Цезаря)

39. Модульная арифметика. Возведение в степень в Z7. Дано a=3, b =6. Вычислите значение (36) mod 7.

40. Метод перестановки поблочный. Для блока длиной d=6 в качестве ключа перестановки взять 436215 и зашифровать такой текст:

ЭТО\_ТЕКСТ\_ДЛЯ\_ШИФРОВАНИЯ

41. Найти мультипликативную инверсию числа 3 в Z10.

42. Модульная арифметика. Возведение в степень в Z7. Дано a=2, b =6. Вычислите значение (46) mod 7.

43. Поясните гаммирование на примере чисел 14 и 12?

44. Найти мультипликативную инверсию числа 5 в Z11.

45. Модульная арифметика. Возведение в степень в Z7. Дано a=2, b =6. Вычислите значение (56) mod 7.

46.Теорема Эйлера- Ферма.

47. Найти мультипликативную инверсию числа 2 в Z11.

48. Модульная арифметика. Возведение в степень в Z7. Дано a=6, b =6. Вычислите значение (66) mod 7.

49.Аддитивная инверсия. Найдите все взаимно обратные пары по сложению в Z10.

50. Найти мультипликативную инверсию числа 9 в Z11.

51. Функция Эйлера. Вычислить функцию Эйлера для n=10, 12?

52. Мультипликативная инверсия чисел. Найти все мультипликативные инверсии в Z10.

53. Найти мультипликативную инверсию числа 3 в Z11.

54. Алгоритм Евклида. Найти НОД(161, 28).

55. Основная теорема арифметики?

56. Найти мультипликативную инверсию числа 10 в Z11.

3 9

57. Вычислите определитель матрицы 2-ого порядка 2 12 .

58. Мультипликативная инверсия чисел. Найти все мультипликативные инверсии в Z10.

59. Как можно применить теорему Ферма и Эйлера- Ферма для вычисления обратных значений?

60. Вычислите функцию Эйлера для простого числа- 13?

61. Есть система cравнений, найти x,y?

2x+3y=1 (mod26)

7x+8y=2(mod26)

62. Что называется криптологией?

63. Вычислить 13-1 mod 26?

64. Произвести сложение двух полиномов по модулю два x6 + x4 +1 и   x6 + x3 +1  в GF(28)?

65. Вычислить 3-1 mod 26?

66. Дано ax=b mod n. НОД(а,n) =d и d не делит b. Сколько существует решений?

67. Вычислить остаток от деления полинома x12 +x7+x2  на полином x8+x4 +x3+x+1?

68. Умножение матрицы на скаляр. Вычислить g\*A, где g – скаляр, А-матрица(n\*n).Результат на примере матрицы А третьего порядка. 69. Шифр Цезаря?

70. Произвести  умножение матриц- A (1\*L)на В(L\*1). Что получается в результате умножения?

71. Вычислить 15-1 mod 26?

72. Дано ax=b mod n. НОД(а,n) =d и d делит b. Сколько существует решений?

73. Произвести сложение двух полиномов по модулю два x7+ x4 +1 и   x6 + x4 +1  в GF(28)?

74. Вычислить 2-1 mod 33?

75. Китайская теорема об остатках. Какие требования предъявляются к ai , mi?

76. Модульная арифметика. Возведение в степень в Z7. Дано a=2, b =6. Вычислите значение (46) mod 7.

77. Умножение матрицы А-матрица(n\*n) на матрицу B(n\*1). Результат? 78. Пропорциональный шифр?

79. В чём отличие в операциях сложения и вычитания на полиномах? 80. Вычислить 9-1 mod 33?

81. Какой полином называется неприводимым?

82. Укажите какими свойствами обладают поля Галуа?

83. Умножение матрицы А-матрица(n\*n) на B(n\*q). Результат. 84. В чём суть метода гаммирования?

85. Шифр Вернама. 86. Вычислить 5-1 mod 33?

87. Какой полином называется неприводимым?

88.При применении шифра Хилла открытый текст разбивается на блоки по два или по три символа в каждом- какой размер имеет матрица шифрования?

89. В чём особенность симметричного шифрования?

90. Какой шифр называется моноалфавитным?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ №1** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1.В чём суть симметричного шифрования?

2. Модульная арифметика. Сложение в Z7. Дано a=5, b =7. Вычислите значения суммы (a+b) mod 7.

3. Основная теорема арифметики.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ №2** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Теорема Ферма.

2. Модульная арифметика. Сложение в Z7. Дано a=6, b =3. Вычислите значения суммы (a+b) mod 7.

3. Что такое криптография?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ №3** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Теорема Эйлера-Ферма.

2. Модульная арифметика. Сложение в Z7. Дано a=5, b =4. Вычислите значения суммы (a+b) mod 7.

3. Что такое криптоанализ?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ №4** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Что называется моноалфавитным шифром? Пример.

2. Модульная арифметика. Умножение в Z7. Дано a=3, b =6. Вычислите значения произведения (a\*b) mod 7.

3. Что такое криптология?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ №5** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Что называется многоалфавитным шифром? Пример.

2. Модульная арифметика. Умножение в Z7. Дано a=2, b =6. Вычислите значения произведения (a\*b) mod 7.

3. Что такое стеганография? Пример.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ №6** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. В чём особенность использования квадрата Полибия при шифровании? Пример.

2. Модульная арифметика. Умножение в Z7. Дано a=4, b =6. Вычислите значения произведения (a\*b) mod 7.

3. Применяя шифр Цезаря – зашифруйте слово ЗАМЕНА. Алфавит записан ниже

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ?

.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ №7** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. В чём заключается принцип Керхоффса.(год 1883)

2. Модульная арифметика. Умножение в Z7. Дано a=6, b =6. Вычислите значения произведения (a\*b) mod 7.

3. Как записать слово «разведчик» в магический квадрат 3\*3 ?

.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ №8** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Дано слово из 8 бит- 10011001 запишите соответствующий ему полином?

2. Свойства оператора mod?

3.В чём магия магического квадрата?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ №9** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Дано слово из 8 бит- 00100110 запишите соответствующий ему полином?

2. Найти мультипликативную инверсию числа 8 в Z10**.**

3.Поясните принцип применения Сциталы.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 10** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Применить шифр-простая перестановка и зашифровать «место встречи изменить невозможно» применяя таблицу 5\*6 .

2. Найти мультипликативную инверсию числа 7 в Z10**.**

3. Поясните принцип применения диска Энея.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ №11** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Применить простую перестановку с паролем «Привет» и зашифровать фразу «место встречи изменить невозможно», применяя таблицу 5\*6.

2. Найти мультипликативную инверсию числа 9 в Z10.

3. Модульная арифметика. Возведение в степень в Z7. Дано a=2, b =6. Вычислите значение (26) mod 7.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 12** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. В чём суть пропорционального шифрования.

2. Найти мультипликативную инверсию числа 3 в Z10.

3. Модульная арифметика. Возведение в степень в Z7. Дано a=6, b =6. Вычислите значение (66) mod 7.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 13** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1.В чём суть применения в криптоанализе частотных характеристик английского и русского языков. Какие буквы чаще встречаются в английском и русском языках?

2. Какой шифр является многоалфавитным шифром? (Шифр Виженера, шифр Винера или шифр Цезаря)

3. Модульная арифметика. Возведение в степень в Z7. Дано a=3, b =6. Вычислите значение (36) mod 7.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 14** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Метод перестановки поблочный. Для блока длиной d=6 в качестве ключа перестановки взять 436215 и зашифровать такой текст:

ЭТО\_ТЕКСТ\_ДЛЯ\_ШИФРОВАНИЯ

2. Найти мультипликативную инверсию числа 3 в Z10.

3. Модульная арифметика. Возведение в степень в Z7. Дано a=2, b =6. Вычислите значение (46) mod 7.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 15** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Поясните гаммирование на примере чисел 14 и 12?

2. Найти мультипликативную инверсию числа 5 в Z11.

3. Модульная арифметика. Возведение в степень в Z7. Дано a=2, b =6. Вычислите значение (56) mod 7.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 16** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1.Теорема Эйлера- Ферма.

2. Найти мультипликативную инверсию числа 2 в Z11.

3. Модульная арифметика. Возведение в степень в Z7. Дано a=6, b =6. Вычислите значение (66) mod 7.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 17** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1 Аддитивная инверсия. Найдите все взаимно обратные пары по сложению в Z10.

2. Найти мультипликативную инверсию числа 9 в Z11.

3. Функция Эйлера. Вычислить функцию Эйлера для n=10, 12?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 18** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Мультипликативная инверсия чисел. Найти все мультипликативные инверсии в Z10.

2. Найти мультипликативную инверсию числа 3 в Z11.

3. Алгоритм Евклида. Найти НОД(161, 28).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 19** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Основная теорема арифметики?

2. Найти мультипликативную инверсию числа 10 в Z11.

3 9

3. Вычислите определитель матрицы 2-ого порядка 2 12 .

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 20** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Мультипликативная инверсия чисел. Найти все мультипликативные инверсии в Z10.

2. Как можно применить теорему Ферма и Эйлера- Ферма для вычисления обратных значений?

3. Вычислите функцию Эйлера для простого числа- 13?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 21** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Есть система cравнений, найти x,y?

2x+3y=1 (mod26)

7x+8y=2(mod26)

2. Что называется криптологией?

3. Вычислить 13-1 mod 26?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 22** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Произвести сложение двух полиномов по модулю два x6 + x4 +1 и   x6 + x3 +1  в GF(28)?

2. Вычислить 3-1 mod 26?

3. Дано ax=b mod n. НОД(а,n) =d и d не делит b. Сколько существует решений?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 23** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Вычислить остаток от деления полинома x12 +x7+x2  на полином x8+x4 +x3+x+1?

2. Умножение матрицы на скаляр. Вычислить g\*A, где g – скаляр, А-матрица(n\*n).Результат на примере матрицы А третьего порядка. 3. Шифр Цезаря?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 24** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Произвести  умножение матриц- A (1\*L)на В(L\*1). Что получается в результате умножения?

2. Вычислить 15-1 mod 26?

3. Дано ax=b mod n. НОД(а,n) =d и d делит b. Сколько существует решений?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 25** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Произвести сложение двух полиномов по модулю два x7+ x4 +1 и   x6 + x4 +1  в GF(28)?

2. Вычислить 2-1 mod 33?

3. Китайская теорема об остатках. Какие требования предъявляются к ai , mi?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 26** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Модульная арифметика. Возведение в степень в Z7. Дано a=4, b =6. Вычислите значение (46) mod 7.

2. Умножение матрицы А-матрица(n\*n) на матрицу B(n\*1). Результат? 3. Пропорциональный шифр?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 27** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. В чём отличие в операциях сложения и вычитания на полиномах? 2. Вычислить 9-1 mod 33?

3. Какой полином называется неприводимым?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ №28** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Укажите какими свойствами обладают поля Галуа?

2. Умножение матрицы А-матрица(n\*n) на B(n\*q). Результат. 3. В чём суть метода гаммирования?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 29** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1. Шифр Вернама. 2. Вычислить 5-1 mod 33?

3. Какой полином называется неприводимым?

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | Утверждено | |
| МИНОБРНАУКИ РОССИИ | | | | **ЗАЧЕТНЫЙ БИЛЕТ № 30** | | | | на заседании кафедры | |
|  |  |  |  |  |  |  |  | (протокол №1 | |
| Федеральное государственное бюджетное | | | | Дисциплина: | | | | от «31» августа 2021 г.) | |
| образовательное учреждение | | | | **«Криптографические методы защиты информации»** | | | |  |  |
| высшего образования | | | | Заведующий кафедрой | |
| **«МИРЭА – Российский технологический** | | | |  |  |  |  |  |  |
| **университет»** | | | | **10.03.01 «Информационная безопасность»** | | | |  |  |
| Институт комплексной безопасности и специального приборостроения | | | | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| В.Р. Григорьев | |
| Кафедра КБ-8 «Информационное противоборство» | | | |  |  |  |  |  |  |
| Форма обучения: Очная | | | | 2021/2022 | |
|  |  |  |  |  | Курс 3 Семестр 5 | | | учебный год | |

1.При применении шифра Хилла открытый текст разбивается на блоки по два или по три символа в каждом- какой размер имеет матрица шифрования?

2. В чём особенность симметричного шифрования?

3. Какой шифр называется моноалфавитным?