Федеральное государственное бюджетное образовательное

учреждение высшего образования

Московский государственный университет имени М.В. Ломоносова

Факультет вычислительной математики и кибернетики

**УТВЕРЖДАЮ**

декан факультета вычислительной математики и кибернетики

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_/И.А. Соколов /**

**«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.**

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Наименование дисциплины:**

**Методы теории чисел в криптографии**

**Уровень высшего образования:**

**бакалавриат**

**Направление подготовки / специальность:**

**01.03.02 «Прикладная математика и информатика» (3++)**

**Направленность (профиль):**

**Математические методы обработки информации и принятия решений**

**Форма обучения:**

**очная**

**Москва 2023**

Рабочая программа дисциплины (модуля) разработана в соответствии с самостоятельно установленным МГУ образовательным стандартом (ОС МГУ) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.03.02, 01.04.02 "Прикладная математика и информатика" программы бакалавриата Утвержден приказом МГУ от 30 августа 2019 года № 1041 (в редакции приказов МГУ от 11 сентября 2019 года № 1109, от 10 июня 2021 года № 609, от 7 октября 2021 года № 1048, от 21 декабря 2021 года № 1404, от 2 ноября 2022 года № 1299)

**1.** Дисциплина относится к вариативной части ОПОП ВО.

**2.** Входные требования для освоения дисциплины (модуля): учащиеся должны владеть знаниями по математическому анализу, общей и линейной алгебре в объеме, соответствующем программе первых трех лет обучения основных образовательных программ бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

**3.** Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников*.*

Компетенции выпускников, частично формируемые при реализации дисциплины (модуля):

* **ОПК-1.Б** Способность применять и адаптировать существующие математические и компьютерные методы для разработки и реализации алгоритмов решения актуальных задач в области фундаментальной и прикладной математики
* **ОПК-2.Б** Способность применять и модифицировать математические модели, а также интерпретировать полученные математические результаты при решения задач в области профессиональной деятельности
* **ПК-2.Б** Способность понимать и применять в научно-исследовательской деятельности современный математический аппарат

Планируемые результаты обучения по дисциплине (модулю):

**Знать:**

1. историю возникновения задач криптографии, способы защиты информации древности и средневековья, политические задачи, решаемые при помощи криптографии:
2. методологию вывода и анализа основных моделей, приводящих к решению теоретико-числовых задач;
3. основные понятия, определения и факты теории чисел и криптографии;
4. строение конечных полей, колец и групп, используемых в криптографии;
5. основы теории распределения простых чисел, асимптотику, число и свойства простых чисел делителей натуральных чисел специального вида;
6. основы симметричной и асимметричной криптографии, односторонние функции;
7. методы решения линейных сравнений и систем, разрешимость и число решений сравнений второй степени;
8. основы теории стойкости криптографических алгоритмов, её связь с трудоемкостью решения теоретико-числовых задач;
9. основы теории делимости, её использование при решениии Диофантовых уравнений;
10. основные примеры и свойства логарифмических функций, их применение в криптографии:
11. основы теории арифметических функций:
12. основы теории цепных дробей, её связь с задачей построения рациональных приближений.

**Уметь:**

1. применять криптографические методы при решении социально-экономических задач:
2. применять на практике основные модели, приводящие к решению теоретико-числовых задач;
3. применять при решении социально-экономических задач основы симметричной и асимметричной криптографии, односторонние функции;
4. применять основные понятия, определения и факты теории чисел и криптографии;
5. использовать при решении криптографических и связанных с ними теоретико-числовых задач строение конечных полей, колец и групп, используемых в криптографии;
6. использовать на практике основы теории распределения простых чисел, асимптотику, число и свойства простых чисел делителей натуральных чисел специального вида;
7. использовать для построения схем и криптоанализа методы решения линейных сравнений и систем, разрешимость и число решений сравнений второй степени;
8. использовать на практике основы теории стойкости криптографических алгоритмов, её связь с трудоемкостью решения теоретико-числовых задач;
9. использовать для построения схем и криптоанализа основы теории делимости, её использование при решениии Диофантовых уравнений;
10. применять на практике основные примеры и свойства логарифмических функций, их применение в криптографии:
11. использовать для построения схем и криптоанализа основы теории арифметических функций:
12. использовать для построения схем и криптоанализа основы теории цепных дробей, её связь с задачей построения рациональных приближений.

**Владеть:**

1. навыками решения Диофантовых уравнений;
2. навыками применения теорем о распределении простых чисел;
3. навыками использования арифметических функций:
4. навыками использования алгоритмов с оракулом для исследования стойкости криптографических протоколов;
5. навыками использования логарифмических функций для построения и анализа криптопротоколов:
6. Навыками решения задач по элементарной теории чисел.

**4.** Формат обучения: занятия проводятся с использованием меловой или маркерной доски, интерактивные материалы демонстрируются с помощью ноутбука и проектора.

**5.** Объем дисциплины (модуля) составляет 5 з.е., в том числе 98 академических часа, отведенных на контактную работу обучающихся с преподавателем, 82 академических часа на самостоятельную работу обучающихся.

**6.** Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Наименование и краткое содержание разделов и тем дисциплины (модуля),**  **Форма промежуточной аттестации по дисциплине (модулю)** | **Всего**  **(часы**) | В том числе | | | |
| **Контактная работа  (работа во взаимодействии с преподавателем)**  **Виды контактной работы, часы** | | | **Самостоятельная работа обучающегося,**  **часы** |
| Занятия лекционного типа\* | Занятия семинарского типа\* | **Всего** |
| Криптографические протоколы древности и средневековья. Организационно правовые механизмы защиты и добывания информации (элементы истории и методы работы разведки, контрразведки, военно-промышленного шпионажа). | 10 | 4 | 4 | 8 | 2 |
| Принципиальные схемы шифрования и электронной подписи на основе односторонних функций. Функции, часто используемые в качестве односторонних. | 5 | 2 | 2 | 4 | 1 |
| Понятие стойкости криптопротокола. Вычислительная сложность арифметических операций в конечных полях. | 5 | 2 | 2 | 4 | 1 |
| Решение линейных сравнений и систем. Простота характеристики и структура конечных полей. Расширенный алгоритм Евклида и его связь с алгебраическими расширениями конечных полей. | 5 | 2 | 2 | 4 | 1 |
| Структура мультипликативной группы вычетов по произвольному модулю, свойства и методы поиска первообразных корней и их сложность. Нахождение элементов фиксированного порядка. Полная система образующих. Полная система индекосв. | 10 | 4 | 4 | 8 | 2 |
| Исследуются свойства простых и псевдопростых чисел. Возможности их построения. Некоторые свойства распределения простых чисел, связанные с принципом Дирихле, основной теоремой арифметики, тождеством Эйлера, обобщенными факториалами. Вводится преобразование Абеля. Исследуется возможность получения асимптотических оценок на суммы по простым числам, асимптотического закона распределения простых чисел, оценок на величину n-ого простого числа и произведения первых n простых чисел. Доказывается мультипликативность и оценки для φ(n). | 5 | 2 | 2 | 4 | 1 |
| Рассматриваются некоторые приемы решения Диофантовых уравнений. Пифагоровы тройки. Задачи на число, произведение и сумму простых делителей. Признаки делимости. Доказывается бесконечность множества просгых чисел в некоторых арифметических прогресиях. Вводится понятие вычета. Критерий Вильсона простоты. Другие примеры использования вычетов. Разложение n!, делимость, решение сравнений вида nk=n(m) | 5 | 2 | 2 | 4 | 1 |
| Текущий контроль успеваемости: контрольная работа № 1 | **2** | - | - | - | **2** |
| Устанавливаются теоремы о детерминированной и вероятностной сводимости задач вскрытия основных используемых криптопротоколов друг к другу и задачам факторизации и дискретного логарифмирования. | 10 | 4 | 4 | 8 | 2 |
| Теоремы о связи сложностей задач дискретного логарифмирования факторизации и задачи Диффи-Хеллмэна, целой факторизации и задачи вскрытия протокола RSA. | 10 | 4 | 4 | 8 | 2 |
| Вводится частное Ферма. Исследуется алгоритм подъема решений показательных сравнений. | 5 | 2 | 2 | 4 | 1 |
| Групповые характеры и характеры Дирихле. | 5 | 2 | 2 | 4 | 1 |
| Решение линейных систем в целых числах. | 3 | - | 2 | 2 | 1 |
| Подъем решений полиномиальных сравнений. | 5 | 2 | 2 | 4 | 1 |
| Исследуются арифметические функции, свертка Дирихле, ряды Дирихле. Доказываются свойства символов Лежандра и Якоби. Исследуется возможность применения их в решении теоретико-числовых задач. Разрешимость и число решений квадратичных сравнений. | 8 | 4 | 2 | 6 | 2 |
| Текущий контроль успеваемости: контрольная работа № 2 | **2** | - | - | **-** | **2** |
| Промежуточная аттестация: устный экзамен | **13** | - | - | **-** | **13** |
| Проводится криптоанализ схемы RSA. Исследуются некоторые атаки на RSA. | 4 | 2 | - | 2 | 2 |
| Исследуются логарифмические функции и их использование для сравнения стойкости схем и в протоколах шифрования. | 4 | 2 | - | 2 | 2 |
| Криптоанализ схемы открытого распределения ключей для конференц-связи, схемы Эль-Гамаля, схемы Шаума. | 8 | 4 | - | 4 | 4 |
| Доказывается связь задачи вскрытия схемы Эль-Гамаля с поиском неподвижных точек в задаче дискретного логарифмирования. Доказывается теорема о вероятностной сложности последней задачи (задача Бризолиса). | 8 | 4 | - | 4 | 4 |
| Рассматривается возможность использования в протоколе Диффи-Хеллмэна вместо мономов других полиномов и рациональных функций, а также линейных рекуррент и некоммутативных операций. Последовательности Люка. | 8 | 4 | - | 4 | 4 |
| Изучается возможность использования смешанной системы счисления для систем симметричного шифрования. | 4 | 2 | - | 2 | 2 |
| Доказательство существования неприводимого многочлена произвольной степени над произвольным конечным полем (круговой многочлен, конструктивное построение неприводимых многочленов и алгебраических расширений конечных полей) Неприводимость над Z. Критерий Эйзенштейна. (эквивалентность понятия неприводимости для многочленов над Q и над Z, признак неприводимости многочлена над Z). | 8 | 4 | - | 4 | 4 |
| Вводятся цепные дроби.  Периодические цепные дроби. Уравнение Пелля. Наилучшие приближения первого и второго рода. Теорема Лагранжа. Скорость рациональных приближений. | 8 | 4 | - | 4 | 4 |
| Промежуточная аттестация: устный экзамен | **20** | - | - | **-** | **20** |
| **Итого** | **180** | **62** | **36** | **98** | **82** |

**7. Фонд оценочных средств (ФОС) для оценивания результатов обучения по дисциплине (модулю)**

**7.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости.**

|  |  |
| --- | --- |
| Контрольная работа № 1 | |
| Вариант 1 | Вариант 2 |
| 1. Найти все первообразные корни по модулю 125.  2. Найти полную систему образующих в мультипликативной группе вычетов по модулю 70.  3. Найти полную систему индексов числа 3 в мультипликативной группе вычетов по модулю 140.  4. Найти элементы порядка 6 в мультипликативной группе вычетов по модулю 91.  5. Решить n!+5n+13=k2 | 1 Найти все первообразные корни по модулю 343.  2. Найти полную систему образующих в мультипликативной группе вычетов по модулю 80.  3. Найти полную систему индексов числа 3 в мультипликативной группе вычетов по модулю 80.  4. Найти элементы порядка 6 в мультипликативной группе вычетов по модулю 63.  5 Решить n!+7n-1=k2. |
| Контрольная работа № 2 | |
| Вариант 1 | Вариант 2 |
| 1. Найти все натуральные, оканчивающиеся на ноль и имеющие 15 натуральных делителей.  2. Решить n12=n (mod 91)  3.Решить в целых числах  4. Решить x3- x2+x+6=0 (mod 343)  5. Найти все вещественные характеры mod 100 | 1. Найти все натуральные, оканчивающиеся на ноль и имеющие 15 натуральных делителей.  2. Решить n16=n (mod 51)  3. Решить в целых числах  4. Решить x3- x2+x+4=0 (mod 125)  5. Найти все вещественные характеры mod 180 |

**7.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации.**

1. Найти индекс 7 по модулю 50 по основанию 2.
2. Получить рациональную параметризацию решений в целых числах уравнения x2 + y2 = z4 .
3. Найти главный член асимптотики суммы по простым числам ln2 p.
4. Оценить величину произведения первых n простых чисел.
5. Построить число Кармайкла вида 5·17·р, где р - простое.
6. Найти натуральное число, оканчивающееся на ноль и имеющее 15 натуральных делителей.
7. Найти натуральное число, имеющее 6 натуральных делителей, произведение которых равно 5832.
8. Найти натуральное число, делящееся на 19 и оканчивающееся на 1234567.
9. Решить в целых числах 7x+3y=2.
10. Найти все натуральные n, меньшие 20, такие, что n8 = n (mod 7).
11. Доказать взаимную простоту чисел Ферма.
12. Разрешимо ли сравнение: x2 = 2 (mod 113).
13. Найти число решений сравнения: x2 = 10 (mod 400).
14. Найти наименьшее натуральное решение x2 - 5y2 = 1.
15. Найти все наилучшие приближения первого рода квадратного корня из 10, со знаменателями меньше 50.
16. Найти полную систему образующих в группе Z\*100
17. Найти порядок элемента 5 в Z\*72
18. Найти все первообразные корни (mod 54)
19. Найти все элементы порядка 6 в Z\*27
20. Найти полную систему индексов числа 3 (mod 154)
21. Решить 5=3х(mod 216)
22. Решить 5=3х(mod 64)

**Вопросы к экзамену.**

1. Основные мировые цивилизации и их письменность, письменность монголов. Создание алфавтьного птсьма. Первое использование прототипа герба РФ.
2. Крупнейшие мировые войны, география шелкового пути, крестовых походов; войн, которые вела Россия.
3. Военное дело и денежное обращение в средневековой Европпе и России, Русская правда.
4. Классические шифры (исторический обзор).
5. Определение односторонней функции. Принципиальные схемы шифрования и электронной подписи. Примеры “односторонних” функций.
6. Первообразные корни.
7. Решение линейных сравнений и систем.
8. Структура Zm\*.
9. Криптоанализ RSA.
10. Атаки на RSA.
11. Частное Ферма и подъём решений.
12. Частное Ферма для случая основания отличного от первообразного корня.
13. Открытая генерация ключей. Схемы Диффи-Хеллмэна, полиномы Чебышева.
14. Открытая генерация ключей. Схемы Диффи-Хеллмана, функции Редея.
15. Открытая генерация ключей. Перестановки, некоммутативные группы.
16. Симметричное шифрование. Использование смешанной системы счисления.
17. Сравнительная стойкость некоторых схем. Теорема о полиномиальной сводимости за один шаг.
18. Теорема о полиномиальной вероятностной сводимости задач вскрытия схем.
19. Связь сложностей задач дискретного логарифмирования и Диффи-Хеллмана.
20. Связь сложностей задач целой факторизации и Диффи-Хеллмана.
21. Бесконечность множества простых в прогрессиях.
22. Свойства чисел Мерсенна и Ферма. Числа Кармайкла.
23. Оценка на число простых < 2n. Простота значений многочленов.
24. Разложение n!. Тождество Эйлера. Принцип Дирихле.
25. Преобразование Абеля. Суммы по простым числам. Асимптотический закон распределения простых чисел.
26. Задачи на делимость. Некоторые Диофантовы уравнения.
27. Пифагоровы тройки.
28. Арифметические функции.
29. Свёртка Дирихле.
30. Алгоритмы дискретного логарифмирования (Похлига-Хеллмэна, Гельфонда).
31. Решение линейных систем в целых числах.
32. Характеры.
33. Символ Лежандра.
34. Символ Якоби.
35. Разрешимость и число решений произвольного сравнения второй степени.
36. Решение квадратичных сравнений.
37. Подъём полиномиальных сравнений.
38. Решение полиномиальных сравнений.
39. Цепные дроби.
40. Уравнение Пелля.
41. Наилучшие приближения первого рода.
42. Наилучшие приближения второго рода.
43. Теорема Лагранжа. Рациональные приближения цепными дробями.

Экзаменационный билет состоит из двух вопросов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)** | | | | |
| Оценка  РО и соответствующие виды оценочных средств | 2 | 3 | 4 | 5 |
| **Знания**  *Коллоквиум,*  *Экзамен* | Отсутствие знаний | Фрагментарные знания | Общие, но не структурированные знания | Сформированные систематические знания |
| **Умения**  *Контрольная работа, зачет* | Отсутствие умений | В целом успешное, но не систематическое умение | В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера) | Успешное и систематическое умение |
| **Навыки (владения, опыт деятельности)**  *Экзамен* | Отсутствие навыков (владений, опыта) | Наличие отдельных навыков (наличие фрагментарного опыта) | В целом, сформированные навыки (владения), но используемые не в активной форме | Сформированные навыки, применяемые при решении задач |

|  |  |
| --- | --- |
| **Соответствие результатов обучения и компетенций, в развитии которых участвует дисциплина (модуль)** | |
| Результаты обучения | Компетенция, с частичным формированием которой связано достижение результата обучения |
| **Знать:**   1. строение конечных полей, колец и групп, используемых в криптографии; 2. основы теории распределения простых чисел, асимптотику, число и свойства простых чисел делителей натуральных чисел специального вида; 3. основы симметричной и асимметричной криптографии, односторонние функции; 4. методы решения линейных сравнений и систем, разрешимость и число решений сравнений второй степени; 5. основы теории стойкости криптографических алгоритмов, её связь с трудоемкостью решения теоретико-числовых задач; 6. основы теории делимости, её использование при решениии Диофантовых уравнений; 7. основные примеры и свойства логарифмических функций, их применение в криптографии:   **Уметь:**   1. использовать при решении криптографических и связанных с ними теоретико-числовых задач строение конечных полей, колец и групп, используемых в криптографии; 2. использовать на практике основы теории распределения простых чисел, асимптотику, число и свойства простых чисел делителей натуральных чисел специального вида; 3. использовать для построения схем и криптоанализа методы решения линейных сравнений и систем, разрешимость и число решений сравнений второй степени; 4. применять на практике основные примеры и свойства логарифмических функций, их применение в криптографии   **Владеть:**   1. навыками использования логарифмических функций для построения и анализа криптопротоколов: 2. Навыками решения задач по элементарной теории чисел. | ОПК-1.Б |
| **Знать:**   1. историю возникновения задач криптографии, способы защиты информации древности и средневековья, политические задачи, решаемые при помощи криптографии: 2. методологию вывода и анализа основных моделей, приводящих к решению теоретико-числовых задач; 3. основные понятия, определения и факты теории чисел и криптографии;   **Уметь:**   1. применять криптографические методы при решении социально-экономических задач: 2. применять на практике основные модели, приводящие к решению теоретико-числовых задач; 3. применять при решении социально-экономических задач основы симметричной и асимметричной криптографии, односторонние функции; 4. применять основные понятия, определения и факты теории чисел и криптографии; 5. использовать на практике основы теории стойкости криптографических алгоритмов, её связь с трудоемкостью решения теоретико-числовых задач; 6. использовать для построения схем и криптоанализа основы теории делимости, её использование при решениии Диофантовых уравнений;   **Владеть:**   1. навыками применения теорем о распределении простых чисел; 2. навыками использования алгоритмов с оракулом для исследования стойкости криптографических протоколов; | ОПК-2.Б |
| **Знать:**   1. основы теории арифметических функций: 2. основы теории цепных дробей, её связь с задачей построения рациональных приближений.   **Уметь:**   1. использовать для построения схем и криптоанализа основы теории арифметических функций: 2. использовать для построения схем и криптоанализа основы теории цепных дробей, её связь с задачей построения рациональных приближений.   **Владеть:**   1. навыками решения Диофантовых уравнений; 2. навыками использования арифметических функций: | ПК-2.Б |

8. Ресурсное обеспечение:

Основная литература:

1. С.Б.Гашков, Э.А.Применко, М.А.Черепнев Криптографические методы защиты информации.- Учебное пособие, М.: Академия, 2010, 298с.

2. Бабаш А.В., Шанкин Г.П. История криптографии. М.: Гелиос АРВ, 2002, 186с.

4. Виноградов И.М. Основы Теории чисел.- М.: Наука, 1972, 107с.

Дополнительная литература:

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии.-М.:МЦНМО,2006.-325с.
2. Бухштаб А.А. Теория чисел. М.: Просвещение, 1955, 385с.

Информационные справочные системы: https://numbertheory.org

Материально-техническое обеспечение: аудитория с партами, меловой или маркерной доской.

9. Язык преподавания - русский.

10. Преподаватели: профессор факультета ВМК МГУ Черепнев М.А.

11. Авторы программы: профессор факультета ВМК МГУ Черепнев М.А.