МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета

_____ Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Теоретико-числовые методы в криптографии

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 18 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целью освоения дисциплины является знакомство с теоретико-числовыми задачами, которые возникают в криптографии, а также изучение вычислительных алгоритмов для решения этих задач.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Теоретико-числовые методы в криптографии» относится к части, формируемой участниками образовательных отношений. Для освоения желательны базовые знания по курсам «Теории чисел» и «Теории алгоритмов». Полученные в курсе «Теоретико-числовые методы в криптографии» знания необходимы для изучения криптографических протоколов.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Универсальные компетенции		
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	**И-УК-1_1** Осуществляет системный анализ задачи, выделяя ее базовые составляющие **И_УК-1_2** Определяет, интерпретирует и ранжирует информацию, требуемую для решения поставленной задачи	**Знать:** основные понятия и методы математического аппарата дисциплины **Уметь:** применять математический аппарат для решения задач **Владеть навыками**: решения задач по дисциплине
Профессиональные компетенции		
ПК-1 Способен разрабатывать математические модели систем обеспечения информационной безопасности, математически доказывать их соответствие выбранным политикам безопасности	**И-ПК-1_3** Способен решать стандартные задачи по теории чисел	**Знать: о**сновные понятия и теоремы теории чисел, понятие делимости, свойства делимости, арифметику остатков, алгоритм Евклида, расширенный алгоритм Евклида, кольцо вычетов и его свойства, понятие сравнения, асимптотический закон распределения простых чисел **Уметь:** решать задачи на делимость целых чисел, применять алгоритм Евклида, расширенный алгоритм Евклида, проводить вычисления в кольце вычетов, решать некоторые типы сравнений и систем сравнений **Владеть навыками:** применения изученного математического аппарата для решения задач теории чисел

ПК-2 Способен анализировать математические модели систем обеспечения информационной безопасности, а также проводить тестирование средств защиты информации на соответствие этим моделям	**И-ПК-2_3** Способен применять теоретико-числовые алгоритмы для решения задач и программно реализовывать теоретико-числовые алгоритмы	**Знать:** Быстрые арифметические алгоритмы, алгоритмы распознающие простоту числа, алгоритмы разложения на множители, алгоритмы вычисления дискретных логарифмов, применение этих алгоритмов в криптографических протоколах. **Уметь:** применять теоретико-числовые алгоритмы для решения задач криптографии **Владеть навыками:** решения задач криптографии с помощью теоретико-числовых алгоритмов

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц, 108 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации *(по семестрам)* Формы ЭО и ДОТ *(при наличии)*
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Введение. Теоретико-числовые задачи, возникающие в криптографии	1	2					4	Задания для домашней работы
2	Основы теории чисел.		4	2				6	Задания для домашней работы
3	Простые числа. Основная теорема арифметики. Асимптотический закон распределения простых чисел		*2*	*2*				*4*	Задания для домашней работы
4	Кольца вычетов		4	2				6	Задания для домашней работы
5	Теория сравнений		2	2		2		6	Задания для домашней работы
6	Быстрые арифметические алгоритмы		4	2				6	Задания для домашней работы
7	Тесты на простоту		6	2		2		8	Задания для домашней работы
8	Алгоритмы разложения на множители		4	2				6	Задания для домашней работы
9	Алгоритмы вычисления дискретного логарифма		4	2		2		8	Задания для домашней работы
	ИТОГО	108	32	16		6		54	

Содержание разделов дисциплины:

1. Введение. Теоретико-числовые задачи, возникающие в криптографии. Криптографические системы и криптографические протоколы.

2. Основы теории чисел. Свойства делимости. Деление с остатком. Алгоритм Евклида. Расширенный алгоритм Евклида.

3. Простые числа. Основная теорема арифметики. Числовые мультипликативные функции. Асимптотический закон распределения простых чисел

4. Группы, кольца, поля. Кольца вычетов. Свойства. Обратимые элементы и делители нуля. Первообразные корни. Функция Эйлера и ее свойства.

5. Сравнения по модулю. Общие свойства сравнений. Решение линейных сравнений с одним неизвестным. Системы линейных сравнений. Китайская теорема об остатках. Квадратичные сравнения. Вычеты и невычеты. Символ Лежандра и символ Якоби.

6. Быстрые алгоритмы. Алгоритм Евклида. Символы Лежандра и Якоби. Быстрый алгоритм возведения в степень. Быстрые алгоритмы умножения чисел. Вероятностные алгоритмы.

7. Тесты на простоту. Решето Эратосфена. Тест на основе малой теоремы Ферма. Тесты на простоту для чисел специального вида. Числа Ферма и числа Мерсенна. Детерминированный алгоритм Миллера на простоту. Вероятностные алгоритмы на простоту. Тест Соловея-Штрассена.

8. Алгоритмы разложения на множители. Алгоритм пробных делений. Алгоритм Ферма. Метод Полларда.

9. Алгоритмы вычисления дискретного логарифма. Метод Гельфонда. Метод Полларда для вычисления дискретного логарифма.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция с элементами лекции-беседы – последовательное изло-жение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

В процессе обучения используются следующие технологии электронного обучения и дистанционные образовательные технологии:

Электронный учебный курс «Теоретико-числовые методы в криптографии» в LMS Электронный университет Moodle ЯрГУ.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- издательская система LaTex;

- Adobe Acrobat Reader.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

Автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Глухов, М. М., Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии [Электронный ресурс] : учеб. пособие / М. М. Глухов, И. А. Круглов, СПб., Лань, 2015, 176с
2. Введение в теоретико-числовые методы криптографии : учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург : Лань, 2021. — 400 с. — ISBN 978-5-8114-1116-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167921 (дата обращения: 25.01.2022). — Режим доступа: для авториз. пользователей.
3. Бухштаб, А. А. Теория чисел : учебное пособие для вузов / А. А. Бухштаб. — 6-е изд., стер. — Санкт-Петербург : Лань, 2022. — 384 с. — ISBN 978-5-8114-9228-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/189329 (дата обращения: 25.01.2022). — Режим доступа: для авториз. пользователей.

б) дополнительная литература

4. Василенко О.Н. Теоретико-числовые методы в криптографии. МЦНМО, 2003, с 328.
5.Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учеб. пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкуров, А. В. Черемушкин, СПб., Лань, 2011, 400с

в) ресурсы сети «Интернет» (при необходимости)

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;

- учебные аудитории для проведения практических занятий (семинаров);

- учебные аудитории для проведения групповых и индивидуальных консультаций;

- учебные аудитории для проведения текущего контроля и промежуточной аттестации;

- помещения для самостоятельной работы;

- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Доцент , к.ф.-м.н. М.А. Заводчиков

Приложение № 1 к рабочей программе дисциплины
«Теоретико-числовые методы в криптографии »
наименование дисциплины

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Задания для самостоятельной работы

1. Число n не делится на 3. Делится ли число 2n на 3?
2. Число n четно. Верно ли, что число 3n делится на 6?
3. Число 15n делится на 6. Верно ли, n делится на 6?
4. Целые числа m и n таковы, что m + 3n делится на 13. Докажите, что 11m + 7n делится на 13.
5. В ряд записаны числа 1, ..., n. Можно ли между ними поставить знаки плюс или минус так, чтобы значение выражения равнялось 0?
6. При каких n число (n-1)! делится нацело на n.
7. Докажите, что при любом натуральном n число 7n − 1 делится на 6.
8. Докажите, что при любом натуральном n число 5n + 3 делится на 4.
9. Докажите, что при любом четном натуральном n число 7n − 5n делится на 24.
10. Докажите, что 5n + 8n − 2n+1 делится на 3 при любом натуральном n.
11. Докажите, что 1n + 3n + 5n + 7n делится на 4 при любом натуральном n.
12. Докажите, что 13 + 23 + ... + 993 делится на 100.
13. Докажите, что если a3 + b3 + c3 делится на 7 (a, b, c ∈ Z), то abc делится на 7.
14. Докажите, что число, имеющее нечётное число делителей - точный квадрат.
15. Известно, что ab + cd делится на a + c. Докажите, что ad + bc делится на a + c.

.1. Найдите НОД и НОК чисел а) 29 · 33 · 54 и 23 · 32 · 72.
2. Найдите НОД(324,576). Найдите НОК. Найдите линейное представление.
3. Найдите НОД(1024,576). Найдите НОК. Найдите линейное представление.
4. Найдите НОД(5040,2184). Найдите НОК. Найдите линейное представление.
5. Найдите НОД(30030,34969). Найдите НОК. Найдите линейное представление.
6. Найдите НОД(324,576,144). Найдите НОК.
7. Найдите НОД(324,576,30030). Найдите НОК.
8. Найдите НОД(324,576,30030,34969). Найдите НОК.
9. Число a = 1775 + 30621 · 1733 − 1735, число b =
10. При каких натуральных n будут взаимно простыми числа 7n+6 и 2n+3?
11. Существует ли такая пара целых чисел x и y, что 6x + 8y = 1?
12. Докажите, что два нечетных последовательных числа взаимно просты.

13. Доказать, что если (a, b) = 1, то или (a+b, a−b) = 1, или (a+b, a−b) = 2.
14. Дробь ba несократима. Будет сократимой дробь aa+b?
15. Докажите, что (a, b) = (5a + 3b, 13a + 8b).
16. Докажите, что наименьшее общее кратное чисел 1, 2, ..., 2n равно наименьшему общему кратному чисел n + 1, n + 2, ..., 2n.

Найдите все простые числа, которые отличаются на 17.
2. Докажите, что любое простое число, большее 3, можно записать в одном из двух видов: 6n + 1 либо 6n–1, где n – натуральное число.
3. Является ли число 49 + 610 + 320 простым?
4. Докажите, что p2 − 1 делится на 24, если p – простое число и p > 3.
5. Найдите все простые числа, меньшие 150.
6. Найдите все простые числа от 150 до 250.
7. Укажите интервал длиной 100, в котором нет простых чисел.
8. Является ли число 1231 простым?
9. Является ли 1423 простым?
10. Существуют ли а) 5, б) 6 простых чисел, образующих арифметическую прогрессию?
11. Докажите, что 3, 5 и 7 являются единственной тройкой простых чисел-близнецов.
12. Существует ли такое число n, что n − 1996, n, n + 1996 – простые?
13. Верно ли, что многочлен f(n) = n2 + n + 41 принимает только простые значения.
14. Найдите все простые числа, которые нельзя записать в виде суммы двух составных.
15. Три простых числа p, q, r, большие 3, образуют арифметическую прогрессию.

1 . В кольце Z24 перечислите все обратимые элементы. Найдите все пары взаимно обратных элементов. Выпишите делители нуля.
2. В кольце Z45 найдите обратный элемент к элементу 17.
3. В кольце Z196 найдите обратный элемент к элементу 73.
4. В кольце Z841 найдите обратный элемент к элементу 91.
5. В кольце Z841 найдите обратный элемент к элементу 7.
6. Образует ли множество делителей нуля группу относительно сложения?
7. Образует ли множество делителей нуля группу относительно умножения?
8. Может ли произведение обратимого класса вычетов на необратимый класс вычетов быть обратимым?

1 . Решить сравнение 2x ≡ −5 (mod 3),
2. Решить сравнение 6x ≡ 39 (mod 51),
3. Решить сравнение 93x ≡ 2 (mod 17),
4. Решить сравнение 2x ≡ 3 (mod 6),
5. Решить сравнение 24x ≡ 18 (mod 36),
6. Решить сравнение 12x ≡ 7 (mod 16),
7. Решить сравнение 12x ≡ 5 (mod 13),
8. Решить сравнение 12x ≡ 8 (mod 16),
9. Решить сравнение x2 − 2x + 3 ≡ 0 (mod 4),
10. Решить сравнение x5 − 2x3 + 13x − 1 ≡ 0 (mod 4),
1 1 . Решить сравнение 5x2 + x + 4 ≡ 0 (mod 10),
12. Решить сравнение x2 ≡ 1 (mod 3),
13. Решить сравнение x3 ≡ 1 (mod 4),

14. Докажите теорему: сравнение $f(x) \equiv 0 \pmod p$ степени $n \geq p$ равносильно сравнению $r(x) \equiv 0 \pmod p$, где $r(x)$ остаток от деления $f(x)$ на $x^p - x$.
15. Примените предыдущую задачу для решения сравнений:
a) $x^5 + 2x^4 - 2x^3 - 2x^2 + 2x - 1 \equiv 0 \pmod 3$,
b) $x^7 - 3x^6 + x^5 - x^3 + 4x^2 - 4x + 2 \equiv 0 \pmod 5$,
c) $x^{14} - x^{13} - x^2 + 2x + 1 \equiv 0 \pmod{13}$.

Определите, будет ли составным число n1 с помощью теста на основе Малой теоремы Ферма.
2. С помощью детерминированного алгоритма Миллера определите, является ли число n2 простым?
3. С помощью вероятностного теста Соловея-Штрассена определите, является ли простым число n3?
4. С помощью алгоритма Ферма разложите на множители составное число n4.
5. Используя ρ−метод Полларда разложите на множители число n5.
6. Для заданных a, b и простого нечетного p вычислите с помощью метода Гельфонда дискретный логарифм Log_a(b) (mod p).
7. Для заданных a, b и простого нечетного p вычислите с помощью ρ-метода Полларда дискретный логарифм Log_a(b) (mod p).

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

На зачете проверяется сформированность компетенции.

Зачет выставляется по результатам контрольной работы по математическим основам и домашней контрольной работы по теоретико-числовым алгоритмам.

Самостоятельная работа 1

(проверка сформированности УК-1, индикатор ИД-УК-1_1)

1 . С помощью алгоритма Евклида найдите НОД(33264, 1320) . Найдите линейное представ-

ление НОД.

2. Найдите остаток от деления числа 21024 на 13.

3. Какие остатки при делении на 8 могут иметь числа вида n2?

Самостоятельная работа 2

(проверка сформированности УК-1, индикатор ИД-УК-1_2)

4. Выпишите все делители нуля в кольце Z36. Выпишите все обратимые элементы.

5. Найдите обратный элемент к 43 в кольце Z125.

6. Найдите порядок элемента 7 в мультипликативной группе обратимых элементов кольца

Z25.

Самостоятельная работа 3

(проверка сформированности УК-1, индикатор ИД-УК-1_3)

7. Вычислите значение функции Эйлера φ(1320).

8. Найдите последнюю цифру числа 131000, пользуясь функцией Эйлера. Найдите две последние цифры.

9. Проверить, будет ли простым число 1213?

Самостоятельная работа 4

(проверка сформированности УК-1, индикатор ИД-УК-1_2)

1 . Решить уравнение $7x + 2y = 5$,

2. Решить уравнение $10x + 4y = 12$,

3. Решить уравнение $12x + 9y = 5$,

4. Решить уравнение $17x + 19y = 23$,

5. Решить уравнение $73x + 61y = 97$.

Самостоятельная работа 5

(проверка сформированности ПК-1, индикатор ИД-ПК-1_3)

1 . Решить сравнение $2x \equiv -5 \pmod 3$,

2. Решить сравнение $6x \equiv 39 \pmod{51}$,

3. Решить сравнение $93x \equiv 2 \pmod{17}$,

4. Решить сравнение $2x \equiv 3 \pmod 6$,

5. Решить сравнение $24x \equiv 18 \pmod{36}$.

Самостоятельная работа 6

(проверка сформированности ПК-2, индикатор ИД-ПК-2_3)

1. Определите, будет ли составным число 111 с помощью теста на основе Малой теоремы Ферма.

2. С помощью детерминированного алгоритма Миллера определите, является ли число 97 простым?

3. С помощью вероятностного теста Соловея-Штрассена определите, является ли простым число 97?

Самостоятельная работа 7

(проверка сформированности ПК-2, индикатор ИД-ПК-2_3)

1. С помощью алгоритма Ферма разложите на множители составное число 136.
2. Используя ρ−метод Полларда разложите на множители число 136.
3. Для заданных 5, 21 и простого нечетного 47 вычислите с помощью метода Гельфонда дискретный логарифм Log_5(21) (mod 47).
4. Для заданных 5, 21 и простого нечетного 47 вычислите с помощью ρ-метода Полларда

Домашняя контрольная работа

Определите, будет ли составным число 123 с помощью теста на основе Малой теоремы Ферма.

2. С помощью детерминированного алгоритма Миллера определите, является ли число 103 простым?

3. С помощью вероятностного теста Соловея-Штрассена определите, является ли простым число 103?

4. С помощью алгоритма Ферма разложите на множители составное число 144.

5. Используя ρ−метод Полларда разложите на множители число 144.

6. Для заданных 7, 24 и простого нечетного 43 вычислите с помощью метода Гельфонда дискретный логарифм Log_7(24) (mod 43).

7. Для заданных 7, 24 и простого нечетного 43 вычислите с помощью ρ-метода Полларда дискретный логарифм Log_7(24) (mod 43).

Правила выставления оценки по результатам контрольной работы:

За контрольную работу выставляется оценка зачтено если правильно решено 70% задач.

Список вопросов к зачету

1. Задачи криптографии.
2. Примеры криптографических протоколов
3. Математические основы. Делимость. Свойства делимости.
4. Остатки. Алгоритм Евклида. Коэффициенты Безу.
5. Кольца вычетов.
6. Функция Эйлера. Малая теорема Ферма.
7. Сравнения. Общие свойства.
8. Линейные сравнения с одной неизвестной.
9. Системы линейных сравнений с одной неизвестной. Китайская теорема об остатках.
10. Квадратичные вычеты.
11. Символ Лежандра и Якоби.
12. Сложность алгоритма Евклида.
13. Сложность операций в кольце вычетов.
14. Быстрый алгоритм возведения в степень.
15. Решето Эратосфена
16. Тест на основе малой теоремы Ферма
17. Детерминированный алгоритм Миллера
18. Вероятностные алгоритмы проверки на простоту
19. Алгоритмы факторизации. Алгоритм Ферма.
20. ρ−метод Полларда факторизации
21. Дискретный логарифм. Метод Гельфонда.
22. Дискретный логарифм. ρ−метод Полларда.

Приложение № 2 к рабочей программе дисциплины
«_Теоретико-числовые методы в криптографии _»
наименование дисциплины

Методические указания для студентов по освоению дисциплины

В магистратуру студенты приходят с разной алгебраической подготовкой. Поэтому первая часть курса посвящена математическим основам. От студентов требуется качественно прорешивать задачи домашней работы. Все темы по теории чисел, включенные в курс, содержательно используются во второй части курса. Основной формой изложения являются лекции. На практических занятиях разбираются типовые задачи по соответствующей теме.