

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

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины
Теоретико-числовые методы в криптографии

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 12 апреля 2024 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2024 г.

1. Цели освоения дисциплины

Целями освоения дисциплины "Теоретико-числовые методы в криптографии" являются:

- приобретение знаний и умений в области криптографической защиты информации,
- формирование мировоззрения и математического подхода к основным теоретико-числовым методам, используемым в современной криптографии.

Целями курса являются:

- подготовка в области компьютерной безопасности;
- овладение методами решения основных задач в области современной криптографии;
- овладение современным математическим аппаратом, используемым в криптографии и теории кодирования для дальнейшего использования в приложениях.

2. Место дисциплины в структуре образовательной программы

Дисциплина "Теоретико - числовые методы в криптографии" относится к базовой части образовательной программы. Дисциплина "Теоретико-числовые методы в криптографии" является основополагающей в списке обучения методам криптографической защиты информации, базирующейся на результатах теории чисел. Изучение дисциплины основывается на курсах: "Алгебра", "Теория вероятностей и математическая статистика", "Математическая логика" и "Теория чисел".

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

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

Формируемая компетенция (код и формулировка)	Перечень планируемых результатов обучения
Общепрофессиональные компетенции	
ОПК-2 Обладает способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Знать: <ul style="list-style-type: none">- теоретические и эвристические соображения, лежащие в основе конструируемых теоретико-числовых алгоритмов;- теоретико-вероятностные и детерминистические схемы, используемые в теории чисел;- иметь представление о связи теории чисел с математической логикой;- основные понятия теории чисел, используемые в криптографии;- способы получения оценок сложности в используемых теоретико-числовых алгоритмах;- возможности применения теоретико-числовых методов в криптографии;- основные виды понятий и алгоритмов, используемых для защиты информации;- возможные сферы приложений теоретико-числовых

	<p>методов и алгоритмов для решения криптографических задач;</p> <ul style="list-style-type: none"> - возможности применения теоретико-числовых методов в криптографии; - основные виды понятий и алгоритмов курса; - возможные сферы приложений теоретико-числовых алгоритмов и методов для криптографических алгоритмов. <p>Уметь:</p> <ul style="list-style-type: none"> - использовать принципы построения основных теоретико-числовых алгоритмов, используемых в криптографии; - использовать принципы конструирования быстрых теоретико-числовых алгоритмов; - использовать системы модульной арифметики; - решать простейшие задачи дискретного логарифмирования; - разрабатывать машинные алгоритмы решения задач; - оценивать сложность основных теоретико-числовых алгоритмов; - использовать основные сведения о распределении простых чисел. - строить алгоритмы для решения алгебраических задач; - исследовать сложность используемых алгоритмов; - решать задачи теоретического и прикладного характера и разрабатывать машинные алгоритмы решения этих задач. <p>Владеть навыками:</p> <ul style="list-style-type: none"> - терминологией, используемой в теории чисел; - современной научной литературой в области теоретико-числовых алгоритмов - навыками использования основных теоретико-числовых алгоритмов, используемых в криптографии; - навыками моделирования и анализа теоретико-числовых алгоритмов; - применения математического аппарата алгебраической алгоритмики в программировании; - применения методов алгебраической алгоритмики в смежных дисциплинах; - применения математического аппарата и алгоритмов теоретико-числовых методов в программировании; - применения теоретико-числовых методов для построения больших простых чисел; - применения теоретико-числовых методов для проверки больших целых чисел на простоту; - применения теоретико-числовых методов факторизации больших простых чисел; - применения теоретико-числовых методов для решения задач дискретного логарифмирования.
--	---

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)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1.	Водная лекция	8	1						
2.	Элементы теории чисел	8	6	6				10	Самостоятельная работа. Контрольная работа № 1
3.	Сложность арифметических операций	8	1	1		1		2	Самостоятельная работа.
4.	Алгоритмы проверки чисел на простоту	8	6	2		1		9	Самостоятельная работа.
5.	Алгоритмы построения больших простых чисел	8	8	3		1		9	Самостоятельная работа.
6.	Алгоритмы факторизации целых чисел	8	6	2		1		9	Самостоятельная работа. Контр. раб. № 2
7.	Дискретное логарифмирование	8	4	2		1		7	Расчетно-графическая работа
							0,3	8,7	зачет
	Всего		32	16		5	0.3	54,7	

Содержание разделов дисциплины:

Тема 1: Вводная лекция

Применение теоретико-числовых методов в криптографии.

Тема 2: Элементы теории чисел

Непрерывные дроби и их свойства. Применение непрерывных дробей к решению сравнений. Квадратичные вычеты. Символы Лежандра и Якоби.

Квадратные корни: метод Цассенхауза- Кантора. Теорема Чебышева о распределении простых чисел. Классы вычетов, вычисления в кольцах вычетов. Китайская теорема об остатках и ее использование при решении теоретико-числовых задач. Строение мультипликативной группы кольца Z_m . Теорема Гаусса.

Тема 3: Сложность арифметических операций

Сложность операций в кольце вычетов. Сложность алгоритма Евклида. Модульная арифметика и ее использование. Вычисления с многочленами. Дискретное преобразование Фурье.

Тема 4: Алгоритмы проверки чисел на простоту

Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма. Псевдопростые числа и числа Кармайкла. Построение псевдопростых чисел и чисел Кармайкла. Эйлеровы псевдопростые числа. Тест Соловея -Штрассена. Сильно псевдопростые числа. Тест Рабина - Миллера. Полиномиальный тест простоты.

Тема 5: Алгоритмы построения больших простых чисел

Критерий Люка. Числа Ферма, критерий их простоты. Теорема Поклингтона. Теорема Диомитко. Метод Маурера. Метод Михалеску. Обзор $(n+1)$ -методов. Числа Мерсенна. Тест Лукаса - Лемера.

Тема 6: Алгоритмы факторизации целых чисел

Метод Полларда. Алгоритм Полларда-Штрассена. Факторизация Ферма. Алгоритм Диксона. Алгоритм Брилхарта - Моррисона. Метод квадратичного решета. $(p-1)$ - метод Полларда. Метод Шэнкса.

Тема 7: Дискретное логарифмирование

Криптографическая система RSA. Выбор параметров системы RSA. Детерминированные методы. p - метод Полларда. Дискретное логарифмирование в конечном поле. Частные Ферма в различных кольцах.

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 изложение 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.

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:

- программы Microsoft Office;
- 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

- Электронная библиотечная система «Лань» <https://e.lanbook.com>

- Электронная библиотечная система «Юрайт» <https://urait.ru>

- Электронная библиотечная система «Консультант студента»
<https://www.studentlibrary.ru>

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

а) основная литература

1. М. М. Глухов, И. А. Круглов, А. Б. Пичкуров, А. В. Черемушкин Введение в теоретико-числовые методы криптографии: учеб. пособие для вузов. - СПб.: Лань, 2011. <https://reader.lanbook.com/book/210746>

2. Яблокова С. И. Введение в быстрые алгоритмы цифровой обработки сигналов. Ярославль, ЯрГУ, 2009 <http://www.lib.uniyar.ac.ru/edocs/iuni/20090238.pdf>

б) дополнительная литература

1. Ноден П., Китте К. Алгебраическая алгоритмика. М.: "Мир", 1999 г. <https://matematika76.ru/fm/ноден.djvu>

2. О. Н. Герман, Ю. В. Нестеренко Теоретико-числовые методы в криптографии: учебник для вузов. - М.: Академия, 2012.

3. Маховенко Е. Б. Теоретико-числовые методы в криптографии. Учебное пособие. - М: "Гелиос АРВ", 2006.

4. Яблокова С.И. Основы алгебраической алгоритмики. Часть 1. - Ярославль, ЯрГУ, 2008. <http://www.lib.uniyar.ac.ru/edocs/iuni/20080290.pdf>

5. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/511700>

6. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2023. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/512423>

7. М. М. Глухов, И. А. Круглов Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии: учеб. пособие - СПб., Лань, 2015.

9. 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:

Доцент кафедры
алгебры и математической логики, к.ф.-м.н.

С. И. Яблокова

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

**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

*(данные задания выполняются студентом самостоятельно
и преподавателем в обязательном порядке не проверяются)*

Задания по темам № 2, 3.

Решать задачи, задаваемые на практических занятиях следующих типов:

1. С помощью разложения числа в цепную дробь, сократить данную дробь.
2. Свернуть конечную цепную дробь.
3. Свернуть периодическую цепную дробь, найти квадратичную иррациональность.
4. Разложить рациональное число в непрерывную дробь.
5. Разложить иррациональное число в непрерывную дробь.
6. Найти иррациональное число $\alpha = [a_1, a_2, \dots, a_k, \alpha_{k+1}]$, если дана k -я подходящая дробь $\frac{p_k}{q_k}$ и иррациональность α_{k+1} .
7. Решить уравнение Пелля: $x^2 - Ny^2 = 1$.
8. Используя непрерывные дроби, решить сравнение $ax \equiv b \pmod{n}$.
9. Решить систему сравнений:
$$\begin{cases} a_1x \equiv b_1 \pmod{m_1} \\ a_2x \equiv b_2 \pmod{m_2} \\ a_3x \equiv b_3 \pmod{m_3} \\ \dots \dots \dots \dots \dots \dots \dots \dots \\ a_nx \equiv b_n \pmod{m_n} \end{cases}$$
10. Выяснить, разрешимо ли сравнение $x^2 \equiv a \pmod{p}$. Если да, то найти решения.
11. При каких целых x функция $\frac{ax^2+bx+c}{p_1p_2\dots p_k}$ принимает целочисленные значения?
12. Решить сравнение $x^2 \equiv a \pmod{p}$ при $p = 4k + 3$, $p = 8k + 5$, $p = 2^h q$.
13. Какие из следующих групп изоморфны?
 $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, $\mathbb{Z}_{m_3} \times \mathbb{Z}_{m_4}$, $\mathbb{Z}_{m_5} \times \mathbb{Z}_{m_6}$.

Задания по темам № 4, 5.

Решать задачи, задаваемые на практических занятиях следующих типов:

1. Является ли $2^n - 1$ обратимым по модулю $2^m - 1$? Если да, то найти $(2^n - 1)^{-1} \pmod{2^m - 1}$.
2. Является ли число N по основанию a : а) псевдопростым? б) эйлеровым псевдопростым? в) сильно псевдопростым?
3. Найти все основания, по которым число n является псевдопростым.
4. Является ли a примитивным элементом по модулю n ? Найти порядок элемента a в группе \mathbb{Z}_n^* .
5. Найти все нечетные простые модули p , по которым имеет решение сравнения $x(x - a) \equiv b \pmod{p}$.

6. Не находя числа x , определить его знак, если относительно вектора оснований $\beta = \{p_1, p_2, \dots, p_k\}$ ему соответствует стандартный набор остатков $x = (a_1, a_2, \dots, a_k)$.
7. Является ли число N числом Кармайкла? Ответ обосновать.
8. Построить числа Кармайкла вида $n = p_1 p_2 p_3$, если дано одно из чисел p_i .
9. Построить псевдопростое число по основанию a .

Задания по темам № 6, 7.

Решать задачи, задаваемые на практических занятиях следующих типов:

1. Факторизовать число N , используя алгоритм
 - а) Полларда;
 - б) Полларда-Штрассена;
 - в) Ферма;
 - г) Диксона.
2. Найти дискретный логарифм, используя алгоритм
 - а) Гельфонда;
 - б) согласования;
 - в) встречи посередине;
 - г) Полига – Хеллмана;
 - д) метод базы разложения;
 - е) ρ – метод Полларда.

Для решения вычислительно трудоемких задач написать и использовать компьютерные программы на одном из языков программирования.

Контрольная работа № 1

1. С помощью разложения числа в цепную дробь, сократить дробь $\frac{3587}{2743}$.
2. Свернуть периодическую цепную дробь, найти квадратичную иррациональность: $[2, 3, (1, 4)]$.
3. Разложить число в цепную дробь, найти период: $\sqrt{47}$.
4. Найти иррациональное число $\alpha = [d_1, d_2, \dots, d_k, \alpha_{k+1}]$, если $\frac{p_k}{q_k} = \frac{17}{5}$,

$$\alpha_{k+1} = \frac{1 + \sqrt{5}}{2}.$$
5. Решить уравнение Пелля: $x^2 - 59y^2 = 1$.
6. Используя непрерывные дроби, решить сравнение $54x \equiv 36 \pmod{102}$.
7. Решить систему сравнений:

$$\begin{cases} 3x \equiv 1 \pmod{4} \\ 6x \equiv 2 \pmod{11} \\ x \equiv 1 \pmod{7} \end{cases}$$

Ответы к задачам:

1. $\frac{17}{13}$;
2. $\frac{13 + 2\sqrt{2}}{7}$;
3. $[6, (1, 5, 1, 12)]$;

4. $\frac{73 + \sqrt{5}}{22}$;
5. фундаментальное решение: $x = 530$, $y = 69$;
6. $x \equiv 12, 29, 46, 63, 80, 97 \pmod{102}$;
7. $x \equiv 15 \pmod{308}$.

Правила выставления оценки по результатам контрольной работы:

Оценка по результатам контрольной работы считается в баллах по каждому заданию по следующему принципу:

- правильно выполненное задание – 4 балла;
- при выполнении задания правильно найден оптимальный алгоритм решения, но имеются незначительные ошибки в численных расчетах – 3 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены не существенные ошибки в вычислениях – 2 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены существенные ошибки в вычислениях – 1 балл;
- при выполнении задания неправильно – 0 баллов.

Набранное количество баллов 26-28 соответствует оценке «отлично», 23-28 баллов – оценке «хорошо», 16-22 баллов – оценке «удовлетворительно», менее 22 баллов – оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

Контрольная работа № 2

1. Выяснить, разрешимо ли сравнение $x^2 \equiv 3 \pmod{13}$? Если да, то найти решения.
2. При каких целых x функция $\frac{x^2+4x-3}{21}$ принимает целочисленные значения?
3. Решить сравнение $x^2 \equiv 99 \pmod{227}$.
4. Решить сравнение $x^2 \equiv -10 \pmod{53}$.
5. Решить сравнение $x^2 \equiv -2 \pmod{97}$.
6. Какие из следующих групп изоморфны?
 $\mathbb{Z}_{140} \times \mathbb{Z}_{726}$, $\mathbb{Z}_{70} \times \mathbb{Z}_{1452}$, $\mathbb{Z}_{42} \times \mathbb{Z}_{2420}$.

Ответы к задачам:

1. $\left(\frac{3}{13}\right) = 1$, значит, сравнение разрешимо; $x \equiv \pm 4 \pmod{13}$;
2. $x \equiv 5, 12 \pmod{21}$;
3. $x \equiv \pm 120 \pmod{227}$;
4. $x \equiv \pm 34 \pmod{53}$;
5. $x \equiv \pm 17 \pmod{97}$;
6. все группы изоморфны группе $\mathbb{Z}_2 \times \mathbb{Z}_{50820}$.

Правила выставления оценки по результатам контрольной работы:

Оценка по результатам контрольной работы считается в баллах по каждому заданию по следующему принципу:

- правильно выполненное задание – 4 балла;
- при выполнении задания правильно найден оптимальный алгоритм решения, но имеются незначительные ошибки в численных расчетах – 3 балла;

- при выполнении задания не найден оптимальный алгоритм и допущены несущественные ошибки в вычислениях – 2 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены существенные ошибки в вычислениях – 1 балл;
- при выполнении задания неправильно – 0 баллов.

Набранное количество баллов 23-24 соответствует оценке «отлично», 20-22 балла – оценке «хорошо», 16-19 баллов – оценке «удовлетворительно», менее 16 баллов – оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

Расчетно-графическая работа

1. С помощью разложения числа в цепную дробь, сократить дробь $\frac{3587}{2743}$.
2. Свернуть периодическую цепную дробь, найти квадратичную иррациональность: $[2, 3, (1, 4)]$.
3. Разложить число в цепную дробь, найти период: $\sqrt{47}$.
4. Найти иррациональное число $\alpha = [d_1, d_2, \dots, d_k, \alpha_{k+1}]$, если $\frac{p_k}{q_k} = \frac{17}{5}$,

$$\alpha_{k+1} = \frac{1 + \sqrt{5}}{2}.$$
5. Решить уравнение Пелля: $x^2 - 59y^2 = 1$.
6. Используя непрерывные дроби, решить сравнение $54x \equiv 36 \pmod{102}$.
7. Выяснить, разрешимо ли сравнение $x^2 \equiv 3 \pmod{13}$? Если да, то найти решения.
8. При каких целых x функция $\frac{x^2 + 4x - 3}{21}$ принимает целочисленные значения?
9. Решить сравнение $x^2 \equiv 99 \pmod{227}$.
10. Решить сравнение $x^2 \equiv -10 \pmod{53}$.
11. Методом Кантора-Цассенхауза решить сравнение $x^2 \equiv -2 \pmod{97}$.
12. Какие из следующих групп изоморфны?
 $\mathbb{Z}_{140} \times \mathbb{Z}_{726}, \mathbb{Z}_{70} \times \mathbb{Z}_{1452}, \mathbb{Z}_{42} \times \mathbb{Z}_{2420}$.
13. Является ли $2^{17} - 1$ обратимым по модулю $2^{35} - 1$? Если да, то найти $(2^{17} - 1)^{-1} \pmod{2^{35} - 1}$.
14. Является ли число 2047 по основанию 2: а) псевдопростым? б) эйлеровым псевдопростым? в) сильно псевдопростым?
15. Найти все основания, по которым число 63 является псевдопростым.
16. Является ли 2 примитивным элементом по модулю 239? Найти порядок элемента 2 в группе \mathbb{Z}_{239}^* .
17. Найти все нечетные простые модули p , по которым имеет решение сравнения $x(x - 3) \equiv 1 \pmod{p}$.
18. Не находя числа x , определить его знак, если относительно вектора оснований $\vec{b} = \{5, 7, 11, 13, 2\}$ ему соответствует стандартный набор остатков $x = (3, 0, 4, 6, 1)$.
19. Является ли число 2465 числом Кармайкла? Ответ обосновать.
20. Решить систему сравнений:
$$\begin{cases} 3x \equiv 1 \pmod{4} \\ 6x \equiv 2 \pmod{11} \\ x \equiv 1 \pmod{7} \end{cases}$$
21. Решить уравнение $2^x \equiv 55 \pmod{79}$.

Правила выставления оценки по результатам расчетно-графической работы:

Оценка по результатам контрольной работы считается в баллах по каждому заданию по следующему принципу:

- правильно выполненное задание – 4 балла;
- при выполнении задания правильно найден оптимальный алгоритм решения, но имеются незначительные ошибки в численных расчетах – 3 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены не существенные ошибки в вычислениях – 2 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены существенные ошибки в вычислениях – 1 балл;
- при выполнении задания неправильно – 0 баллов.

Набранное количество баллов 100-104 соответствует оценке «отлично», 93-99 баллов – оценке «хорошо», 75-92 баллов – оценке «удовлетворительно», менее 75 баллов – оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

Задачи для самопроверки при подготовке к экзамену на примере темы 4.

За правильное решение задачи № 1 дается 1 балл, за правильное решение задач № 2 и № 4 – 2 балла, за правильное решение задач №3 и № 5 – 3 балла. Количество набранных баллов не менее 6 вместе с правильно решенными задачами по изученным темам соответствует уровню формирования в рамках данной дисциплины компетенций ОПК-2. В этом случае студенту выставляется оценка "зачтено".

Задача 1. Пусть $\text{НОД}(a, n) = 1$, $b, c > 0$ целые. Доказать: если

$a^b \equiv 1 \pmod{n}$ и $a^c \equiv 1 \pmod{n}$, а $d = \text{НОД}(b, c)$, то $a^d \equiv 1 \pmod{n}$.

(Указание: воспользоваться теоремой о представлении НОД с помощью коэффициентов Безу.)

Решение: По теореме о представлении НОД двух целых чисел b и c найдутся такие целые u и v такие, что $d = \text{НОД}(b, c) = bu + cv$.

Из $a^b \equiv 1 \pmod{n}$ следует $(a^b)^u \equiv 1^u \equiv 1 \pmod{n}$, из $a^c \equiv 1 \pmod{n}$ следует $(a^c)^v \equiv 1^v \equiv 1 \pmod{n}$. Тогда $a^d = a^{bu+cv} = (a^b)^u (a^c)^v \equiv 1 \pmod{n}$.

Задача 2. Найти все основания b , для которых число 15 является псевдопростым по основанию b .

(Указание: использовать структуру мультипликативной группы кольца вычетов \mathbb{Z}_{15}^* .)

Решение: По следствию из китайской теоремы об остатках для мультипликативных групп колец вычетов имеем $\mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^*$, где \mathbb{Z}_3^* -- циклическая группа порядка 2, \mathbb{Z}_5^* -- циклическая группа порядка 4, поэтому для любого элемента b группы \mathbb{Z}_{15}^* должно выполняться $b^4 \equiv 1 \pmod{15}$. По определению псевдопростоты требуется выполнение сравнения $b^{14} \equiv 1 \pmod{15}$. Отсюда получаем $1 \equiv b^{14} \equiv (b^4)^3 b^2 \equiv b^2 \pmod{15}$. Значит, нам нужны элементы группы \mathbb{Z}_{15}^* , имеющие порядок 2.

Сравнение $b^2 \equiv 1 \pmod{15}$ эквивалентно системе из двух сравнений

$$\begin{cases} b^2 \equiv 1 \pmod{3} \\ b^2 \equiv 1 \pmod{5} \end{cases}$$

Решая каждое, получаем $b \equiv \pm 1 \pmod{3}$, $b \equiv \pm 1 \pmod{5}$. Искомые основания являются решениями следующих 4 систем сравнений:

$$\begin{cases} b \equiv 1 \pmod{3} \\ b \equiv 1 \pmod{5} \end{cases}, \begin{cases} b \equiv 1 \pmod{3} \\ b \equiv -1 \pmod{5} \end{cases}, \begin{cases} b \equiv -1 \pmod{3} \\ b \equiv 1 \pmod{5} \end{cases}, \begin{cases} b \equiv -1 \pmod{3} \\ b \equiv -1 \pmod{5} \end{cases}.$$

Решив системы, находим $b \equiv 1, 4, 11, 14 \pmod{15}$.

Задача 3. Найти все основания b , для которых число 91 является псевдопростым по основанию b .

(Указание: использовать структуру мультипликативной группы кольца вычетов \mathbb{Z}_{91}^* .)

Решение: По следствию из китайской теоремы об остатках для мультипликативных групп колец вычетов имеем $\mathbb{Z}_{91}^* \cong \mathbb{Z}_7^* \times \mathbb{Z}_{13}^*$, где \mathbb{Z}_7^* -- циклическая группа порядка 6, \mathbb{Z}_{13}^* -- циклическая группа порядка 12, порядок группы \mathbb{Z}_{91}^* равен $6 \cdot 12 = 72$, для каждого элемента этой группы должно выполняться $b^{12} \equiv 1 \pmod{91}$. По определению псевдопростоты требуется выполнение сравнения $b^{90} \equiv 1 \pmod{91}$. Отсюда получаем $1 \equiv b^{90} \equiv (b^{12})^7 b^6 \equiv b^6 \pmod{91}$. Значит, нам нужны элементы группы \mathbb{Z}_{91}^* , имеющие порядок, делящий число 6, т. е. элементы порядков 1, 2, 3 и 6.

Сравнение $b^6 \equiv 1 \pmod{91}$ эквивалентно системе из двух сравнений

$$\begin{cases} b^6 \equiv 1 \pmod{7} \\ b^6 \equiv 1 \pmod{13} \end{cases}.$$

Заметим, что первое сравнение выполнено для любого основания из \mathbb{Z}_7^* (малая теорема Ферма), значит, оно имеет 6 решений: $1, 2, 3, 4, 5, 6 \pmod{7}$.

Чтобы решить второе сравнение, найдем образующую циклической группы \mathbb{Z}_{13}^* . Попробуем на роль образующей элемент 2. Поскольку простые делители числа 12 -- это 2 и 3, то вычислим $2^{\frac{12}{2}} \pmod{13}$ и $2^{\frac{12}{3}} \pmod{13}$:

$$2^4 \equiv 16 \equiv 3 \pmod{13},$$

$$2^6 \equiv 64 \equiv -1 \pmod{13},$$

отсюда заключаем, что 2 является элементом порядка 12, т.е. образующей группы \mathbb{Z}_{13}^* .

Тогда $2^2 \equiv 4 \pmod{13}$ имеет порядок 6, $2^4 \equiv 16 \equiv 3 \pmod{13}$ имеет порядок 3, $2^6 \equiv 12 \pmod{13}$ имеет порядок 2, $2^8 \equiv 9 \pmod{13}$ имеет порядок 3, $2^{10} \equiv 10 \pmod{13}$ имеет порядок 6, наконец, $2^{12} \equiv 1 \pmod{13}$ -- элемент порядка 1.

Таким образом, решениями сравнения $b^6 \equiv 1 \pmod{13}$ являются $b \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$.

Поскольку первое и второе сравнения нашей системы имеют по 6 решений, то система будет иметь 36 решений по модулю 91. Найдем общий вид этих решений, для чего решим систему

$$\begin{cases} b \equiv i \pmod{7} \\ b \equiv k \pmod{13} \end{cases}.$$

Из второго сравнения $b = k + 13t, t \in \mathbb{Z}$, подставляя это выражение в первое сравнение, получаем $k + 13t \equiv i \pmod{7}$ или $t \equiv k - i \pmod{7}$, откуда $b = k + 13((k - i) + 7s) = 14k - 13i + 91s$, т.е.

$$b \equiv 14k - 13i \pmod{91}, \text{ где } i = 1, 2, \dots, 6; k = 1, 3, 4, 9, 10, 12.$$

Перебирая значения i и k , получаем все 36 решений. Например, при $k = 1, i = 1, 2, \dots, 6$ получим $b \equiv 1, 89, 86, 83, 80, 77 \pmod{91}$.

Задача 4. Пусть p простое. Показать, что p^2 псевдопростое по основанию b тогда и только тогда, когда $b^{p-1} \equiv 1 \pmod{p^2}$.

(Указание: использовать теорему Эйлера и свойства сравнений.)

Решение. Пусть выполнено сравнение $b^{p-1} \equiv 1 \pmod{p^2}$. Возведем обе части сравнения в степень $p+1$: $(b^{p-1})^{p+1} \equiv 1 \pmod{p^2}$ или $b^{p^2-1} \equiv 1 \pmod{p^2}$, значит, p^2 является псевдопростым по основанию b .

Обратно, пусть p^2 является псевдопростым по основанию b , т. е. $b^{p^2-1} \equiv 1 \pmod{p^2}$. Согласно теореме Эйлера $b^{\varphi(p^2)} \equiv 1 \pmod{p^2}$, но $\varphi(p^2) = p(p-1)$, следовательно $b^{p^2-p} \equiv 1 \pmod{p^2}$. Имеем

$$\begin{cases} b^{p^2-1} \equiv 1 \pmod{p^2} \\ b^{p^2-p} \equiv 1 \pmod{p^2} \end{cases},$$

откуда

$$1 \equiv b^{p^2-1} = b^{(p^2-p)+(p-1)} \equiv b^{p-1} \pmod{p^2}.$$

Задача 5. Доказать: если n сильно псевдопростое по основанию b , то оно сильно псевдопростое по основанию b^k для любого целого $k > 0$.

(Указание: представить k в виде $2^i j$, где j нечетно.)

Решение. Так как n сильно псевдопростое по основанию b , то при $n-1 = 2^q t$, где t – нечетно, выполнено

либо 1) $b^t \equiv 1 \pmod{n}$,

либо 2) найдется $0 \leq r \leq q-1$ такое, что $b^{2^r t} \equiv -1 \pmod{n}$.

Пусть $k = 2^i j$, где j – нечетно, $i \geq 0$.

Если выполнено условие 1), то $(b^k)^t = (b^t)^k \equiv 1^k \equiv 1 \pmod{n}$.

Если выполнено условие 2), рассмотрим два случая: а) $i > r$ и б) $i \leq r$.

Если $i > r$, то $(b^k)^t = (b^{2^i j})^t = (b^{2^r t})^{2^{i-r} j} \equiv (-1)^{2^{i-r} j} \equiv 1 \pmod{n}$, поскольку $i-r > 0$, следовательно $2^{i-r} j$ – четное число.

Если $i \leq r$, то $(b^k)^{2^{r-i} t} = (b^{2^i j})^{2^{r-i} t} \equiv b^{2^r t j} \equiv (b^{2^r t})^j \equiv (-1)^j \equiv -1 \pmod{n}$, поскольку j – нечетное число. Итак, для основания b^k выполнено либо условие 1), либо условие 2), значит, n сильно псевдопростое по основанию b^k .

Вопросы для самопроверки при подготовке к зачету на примере темы 4.

Задачи №№ 1 – 3 оцениваются в 1 балл, задача № 4 – в 2 балла, задача № 5 – в 3 балла. Количество набранных баллов не менее 7 вместе с правильно решенными задачами по изученным темам соответствует уровню формирования в рамках данной дисциплины компетенций ОПК-2. В этом случае студенту выставляется оценка "зачтено".

Вопрос 1. Есть ли связь между понятиями псевдопростоты числа n по данному основанию a и сильной псевдопростоты числа n по тому же основанию?

Варианты ответов:

1. Связи между этими понятиями нет;
2. Из псевдопростоты числа n по основанию a следует сильная псевдопростота n по основанию a ;
3. Из сильной псевдопростоты числа n по основанию a следует псевдопростота n по основанию a .

Вопрос 2. Есть ли связь между понятиями эйлеровой псевдопростоты числа n по данному основанию a и псевдопростоты n по основанию a ?

Варианты ответов:

1. Связи между этими понятиями нет;
2. Из псевдопростоты числа n по основанию a следует эйлерова псевдопростота n по основанию a ;
3. Из эйлеровой псевдопростоты числа n по основанию a следует псевдопростота n по основанию a .

Вопрос 3. Есть ли связь между понятиями эйлеровой псевдопростоты числа n по данному основанию a и сильной псевдопростоты n по основанию a ?

Варианты ответов:

1. Связи между этими понятиями нет;
2. Из сильной псевдопростоты числа n по основанию a следует эйлерова псевдопростота n по основанию a ;
3. Из эйлеровой псевдопростоты числа n по основанию a следует сильная псевдопростота n по основанию a ;
4. Из сильной псевдопростоты числа n по основанию a следует эйлерова псевдопростота n по основанию a ; в случае

$$n \equiv 3 \pmod{4}$$

эйлерова псевдопростота влечет сильную псевдопростоту.

Вопрос 4. Является ли число 105 по основанию 8: а) псевдопростым? б) эйлеровым псевдопростым? в) сильно псевдопростым?

Варианты ответов:

1. Псевдопростое, не является эйлеровым псевдопростым, является сильно псевдопростым;
2. Псевдопростое, эйлерово псевдопростое, не является сильно псевдопростым;
3. Псевдопростое, не является эйлеровым псевдопростым, не является сильно псевдопростым.

Вопрос 5. Верно ли следующее утверждение:

пусть p и $2p-1$ простые числа и $n=p(2p-1)$, тогда n является псевдопростым для половины возможных оснований a таких, которые являются квадратичными вычетами по модулю $2p-1$? Если утверждение верно, дать обоснование.

Варианты ответов:

1. Утверждение не верно;
2. Утверждение верно.

Обоснование

В силу малой теоремы Ферма (p и $2p-1$ простые числа) имеем

$$\begin{cases} a^{p-1} \equiv 1 \pmod{p} \\ a^{2p-2} \equiv 1 \pmod{2p-1} \text{ или } a^{2(p-1)} \equiv 1 \pmod{2p-1}. \end{cases}$$

Значит, $a^{2(p-1)} \equiv 1 \pmod{p(2p-1)}$, откуда $a^{p-1} \equiv 1 \pmod{p(2p-1)}$, а, следовательно, по свойствам сравнений $a^{p-1} \equiv 1 \pmod{2p-1}$.

$$n-1 = p(2p-1)-1 = 2p^2-p-1 = (p-1)(2p+1), \text{ откуда } p-1 \mid n-1.$$

Тогда получаем

$$a^{n-1} \equiv (a^{p-1})^{2p+1} \equiv 1 \pmod{2p-1}, \text{ но } a^{p-1} = a^{\frac{(2p-1)-1}{2}} \equiv \left(\frac{a}{2p-1}\right) \pmod{2p-1}.$$

Итак, $1 \equiv a^{n-1} \equiv \left(\frac{a}{2p-1}\right) \pmod{2p-1}$, т. е. a квадратичный вычет по модулю $2p-1$, а квадратичных вычетов по любому простому модулю среди всех возможных оснований ровно половина.

3. Утверждение верно.

Обоснование

Очевидно,

$$n-1 = p(2p-1) - 1 = p(2p-2) + (p-1) = 2p(p-1) + (p-1),$$

откуда получаем $p-1 \mid n-1$ и $n-1 \equiv p-1 \pmod{2p-2}$.

В силу малой теоремы Ферма (p и $2p-1$ простые числа) имеем

$$\begin{cases} a^{p-1} \equiv 1 \pmod{p}, & \text{откуда } a^{n-1} \equiv 1 \pmod{p}, \\ a^{2p-2} \equiv 1 \pmod{2p-1}. \end{cases}$$

Значит, $a^{n-1} \equiv a^{p(2p-2)+(p-1)} \equiv (a^{2p-2})^p a^{p-1} \equiv a^{p-1} \pmod{2p-1}$.

Но $a^{p-1} = a^{\frac{(2p-1)-1}{2}} \equiv \left(\frac{a}{2p-1}\right) \pmod{2p-1}$, т. е. $a^{n-1} \equiv \left(\frac{a}{2p-1}\right) \pmod{2p-1}$.

Итак, $a^{n-1} \equiv 1 \pmod{2p-1}$ равносильно $\left(\frac{a}{2p-1}\right) = 1$, т. е. a квадратичный вычет по модулю $2p-1$, а квадратичных вычетов по любому простому модулю среди всех возможных оснований ровно половина.

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

Итоговая аттестация по дисциплине проводится в форме зачета. Зачет проводится в форме собеседования. Для допуска к собеседованию студент в течение семестра должен удовлетворительно написать контрольные №№ 1 - 2, т. е. в каждой контрольной работе правильно решить 75-80% предложенных задач. Если это условие не выполнено, студенту сначала предлагается решить задачи по тем темам, которые вызывали у него трудности в течение семестра. Задачи подбираются аналогичные тем, которые предлагались в контрольных работах.

Вопросы к зачету по курсу «теоретико-числовые методы в криптографии»

1. Квадратичные вычеты. Леммы о квадратичных вычетах. Критерий Эйлера.
2. Символ Лежандра и его свойства (квадратичный закон взаимности без доказательства).
3. Квадратичный закон взаимности для символа Лежандра. Вычисление символа Лежандра.
4. Символ Якоби и его свойства. Обобщение квадратичного закона взаимности. Вычисление символа Лежандра с использованием символа Якоби.
5. Квадратные корни по модулю простого числа. Частные случаи: $p \equiv 3 \pmod{4}$, $p \equiv 5 \pmod{8}$, $p \equiv 1 \pmod{8}$. Метод Кантора - Цассенхауза.
6. Непрерывные дроби и их свойства. Теорема единственности. Теорема о фундаментальном соответствии. Представление рациональных чисел непрерывными дробями.
7. Представление иррациональных чисел непрерывными дробями. Свойства последовательности подходящих дробей. Оценка близости подходящей дроби к представляемому непрерывной дробью числу. Теорема о единственности представления.

8. Периодические непрерывные дроби. Теорема Лагранжа.
9. Лемма о приближении рациональных чисел иррациональными. Лемма о числе решений неравенства $|x^2 - Ny^2| < c$.
10. Теорема о целочисленных решениях уравнения Пелля. Применение непрерывных дробей к решению уравнения Пелля.
11. Распределение простых чисел. Функция Чебышева. Верхняя оценка функции Чебышева.
12. Функция Чебышева. Нижняя оценка функции Чебышева.
13. Теорема Чебышева и следствия из нее.
14. Простейшие алгоритмы проверки целых чисел на простоту (решето Эратосфена, критерий Вильсона, теорема Ферма). Тест на основе малой теоремы Ферма, его недостатки.
15. Псевдопростые числа по данному основанию и их свойства (теорема). Примеры. Лемма о существовании бесконечного числа псевдопростых чисел по основанию 2.
16. Леммы о существовании бесконечного числа псевдопростых чисел по основанию a . Построение псевдопростых чисел по данному основанию. Примеры.
17. Числа Кармайкла и их свойство. Построение чисел Кармайкла.
18. Тест Соловья-Штрассена. Теорема. Эйлеровы псевдопростые числа по данному основанию и их свойства.
19. Сильно псевдопростые числа. Вероятностный тест простоты Рабина-Миллера. Его преимущества. Теорема о свойствах сильно псевдопростых чисел.
20. Леммы о значении символа Лежандра для целого числа, удовлетворяющего сравнению специального вида.
21. Теорема о связи сильной псевдопростоты и эйлеровой псевдопростоты.
22. Теорема Рабина. Следствие. Другие формулировки этой теоремы.
23. Полиномиальный тест распознавания простоты. основная теорема.
24. Критерий Люка. Тест простоты. Теорема Селфриджа.
25. Числа Ферма и их свойства. Теорема Пепина.
26. Теорема Поклингтона. Обобщение теоремы Люка. Теорема Прота.
27. Ослабленный вариант теоремы Поклингтона. Теорема Диemitко.
28. Свойства функции Эйлера. Три леммы.
29. Усиленный вариант теоремы Поклингтона. Лемма Коувера и Куискуотера.
30. Теорема Маурера. Следствие. Алгоритм Маурера.
31. $(n + 1)$ - методы. Лемма о представлении корня r уравнения $x^2 - px + q = 0$, где $p^2 - 4q$ не является квадратом по модулю n . Леммы о простоте n и представлении r^k . Формулировка основной теоремы.
32. Числа Мерсенна. Лемма 1 и доказательство достаточности условий Люка-Лемера.
33. Числа Мерсенна. Лемма 2 и доказательство необходимости условий Люка-Лемера.
34. Теорема Люка-Лемера (вторая формулировка и доказательство эквивалентности с первой).
35. Метод факторизации Полларда. Теорема о вероятности успеха алгоритма.
36. Алгоритм Полларда - Штрассена. Теорема.
37. Факторизация Ферма. Теорема. Алгоритм.
38. Алгоритм Диксона. Его сложность. Пути улучшения алгоритма.
39. Алгоритм Брилхарта - Моррисона. Теорема и следствие из нее. Исправление факторной базы.
40. Метод квадратичного решета (Померанц, Дэвис и Монтгомери).
41. $(p - 1)$ - метод Полларда. Выбор функции $M(k)$.
42. Дискретное логарифмирование в конечном поле. Метод Гельфонда. Теорема и алгоритм. Алгоритм согласования.

- 43. Метод встречи посередине дискретного логарифмирования. Вероятность успеха алгоритма.
- 44. Метод базы разложения дискретного логарифмирования.
- 45. Теорема Нечаева. Алгоритм Полига - Хеллмана.
- 46. ρ - метод Полларда дискретного логарифмирования. Два варианта алгоритма.
- 47. Индексный алгоритм дискретного логарифмирования в поле Галуа $GF(p^n)$.

3. Правила выставления зачета по курсу.

Оценка "зачтено" выставляется студенту, в течение семестра проявившему достаточно хорошие знания и навыки решения задач на контрольных работах и решившего не менее 80% задач из расчетно-графической работы. Зачет ставится, если:

- студент знает основные алгоритмы проверки чисел на простоту, построения больших простых чисел, факторизации больших целых чисел, решения задачи дискретного логарифмирования в рамках данного курса;
- студент может применить эти алгоритмы к решению практических задач;
- студент может дать математическую формулировку задачи и указать методы, которые могут быть применены для ее решения;
- студент владеет навыками проведения сложных вычислений под руководством преподавателя, может объяснить проведенные вычисления и логику хода решения, может самостоятельно выполнить простейшие вычисления, используя математический аппарат алгебры и теории чисел:

Студент может делать ошибки, но должен их исправлять самостоятельно после дополнительных (наводящих) вопросов преподавателя.

Оценка «не зачтено» выставляется студенту, проявившему на промежуточных аттестаций умения и навыки, не соответствующие требуемому выше уровню:

- студент не может выполнить постановку задачи, не может провести сравнительный анализ данной задачи с другими, не может определить метод ее решения и провести даже простейший анализ полученного результата;
- студент не может провести самостоятельно даже базовые вычисления с использованием математического аппарата алгебры и теории чисел, не может пояснить даже выполненные на практических занятиях вычисления и (или) логику решения.

Оценка «не зачтено» выставляется также студенту, получившему на зачете задание, но отказавшемуся отвечать.

Приложение № 2 к рабочей программе дисциплины «Теоретико-числовые методы в криптографии»

Методические указания для студентов по освоению дисциплины

Для успешного усвоения данного курса необходимо знание следующих вопросов из других математических дисциплин:

- сравнения по модулю целого числа, свойства сравнений;
- китайская теорема об остатках для чисел и для многочленов;
- функция Эйлера и ее основные свойства;
- теорема Эйлера и малая теорема Ферма;
- кольцо и поле вычетов по модулю натурального числа;
- мультипликативная группа кольца вычетов;
- строение мультипликативных групп колец вычетов по модулю простого числа, по модулю степени простого числа и по модулю степени двойки;
- квадратичные вычеты;
- символы Лежандра и Якоби и их свойства.