

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

Криптографические методы

Направление подготовки (специальности)
02.03.01 Математика и компьютерные науки

Направленность (профиль)
«Программирование, алгоритмы и анализ данных»

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 «Криптографические методы» являются: обеспечение подготовки в одной из важных областей приложения математики, знакомство с современными понятиями теории использующейся в защите информации.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, и является элективной дисциплиной. Данная дисциплина направлена на освоение алгоритмов, применяемых для анализа алгоритмов, применяемых в современной защите информации. Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения предшествующих математических дисциплин: теории чисел, линейной алгебры, аналитической геометрии.

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)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
Профессиональные компетенции		
ПК-3 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий и программирования и компьютерной техники	И-ПК-3.2 Умеет использовать методы проектирования и производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного продукта	Знать: основные методы и формулировки результатов, использующихся в защите информации Уметь: обосновывать алгоритмы защиты информации Владеть: навыками быстрых вычислений в основных алгебраических системах

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 акад. часов

№ п/п	Темы (разделы) дисциплины и их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в акад. часах)		Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа		

			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Основные понятия и задачи криптографии. Формальные модели шифров. Шифры гаммирования. Методы вскрытия шифров гаммирования	8	13	5		2		5	Задания для самостоятельной работы. Контрольная работа
2	Оценки качества криптографических преобразований. Поточные шифры и генерация псевдослучайных последовательностей. Блочные шифры.	8	13	5		2		5	Задания для самостоятельной работы
3	Асимметричное шифрование. Группа точек эллиптической кривой. Электронная подпись. Хэш функции. Управление ключами.	8	6	6		2		5	Задания для самостоятельной работы
							0,3	2,7	Зачет
	Всего		32	16		6	0,3	17,7	

Содержание разделов дисциплины:

Тема 1. Основные понятия и задачи криптографии. Формальные модели шифров. Модели открытых текстов. Шифры гаммирования. Методы вскрытия шифров гаммирования. Повторное использование гаммы.

Тема 2. Оценки качества криптографических преобразований. Поточные шифры и генерация псевдослучайных последовательностей. Блочные шифры. Алгоритмы DES, AES, "Кузнечик". Режимы использования блочных шифров.

Тема 3. Асимметричное шифрование. Группа точек эллиптической кривой. Электронная подпись. Хэш функции. Управление ключами. Схемы RSA, Эль Гамала, Рабина-Уильямса. Стандарт ГОСТ Р34.10-2012. Базовый протокол Диффи-Хэллмана. Разделение секрета

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:

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;
- MikTeX (свободно распространяемое ПО);
- GAP (GNU GPL).

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, необходимых для освоения дисциплины

а) основная литература

1. Лось А. Б., Нестеренко А. Ю., Рожков М. И., Криптографические методы защиты информации - Москва: Юрайт, 2023. <https://urait.ru/viewer/kriptograficheskie-metody-zaschity-informacii-dlya-izuchayuschih-kompyuternuyu-bezopasnost-511138>
2. Басалова Г. В. Основы криптографии - Москва: Национальный Открытый Университет "ИНТУИТ", 2016. https://www.studentlibrary.ru/ru/doc/intuit_184-SCN0000/000.html
3. Ноден П., Китте К. Алгебраическая алгоритмика - М.: Мир, 1999.
<https://matematika76.ru/fm/ноден.djvu>

б) дополнительная литература

1. Фомичев В. М. Сборник задач по криптологии. - Москва: Прометей, 2019.
<https://www.studentlibrary.ru/ru/doc/ISBN9785907100398-SCN0000/000.html>

2. Саломаа А. Криптография с открытым ключом, М.: Мир, 1996.
3. Никифоров С. Н. Методы защиты информации. Шифрование данных: учебное пособие — Санкт-Петербург: Лань, 2022. <https://reader.lanbook.com/book/206285>
4. А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин Основы криптографии: учеб. пособие для вузов - М.: Гелиос АРВ, 2005.

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(ы) :

Заведующий кафедрой алгебры и математической логики
профессор, д.ф.-м.н.

Казарин Л.С

**Приложение к №1 рабочей программе дисциплины
«Криптографические методы»**

**Оценочные средства
для проведения текущей и/или промежуточной аттестации аспирантов
по дисциплине**

**1. Типовые контрольные задания или иные материалы,
используемые в процессе текущей аттестации**

Задания для самостоятельной работы по теме 1

По книге Саломаа А. Криптография с открытым ключом

По книге . Лось А.Б., Нестеренко А.Ю., Рожков М.И, Криптографические методы защиты информации,

Задания для самостоятельной работы по теме 2

По книге Саломаа А. Криптография с открытым ключом

По книге . Лось А.Б., Нестеренко А.Ю., Рожков М.И, Криптографические методы защиты информации

Задания для самостоятельной работы по теме 3

По книге Ноден П., Китте К. «Алгебраическая алгоритмика», гл.V, упражнения 29 – 36

По книге Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии

Контрольная работа

1. Написать программу для вычисления частот встречаемости букв и биграмм русского языка.
2. По известному шифртексту восстановить неизвестный осмысленный открытый текст, зашифрованный шифром Хилла ($y_i = ax_i + b \pmod{33}$).
3. Найти группу инерции функции $f = x_1x_2 + x_2x_3 + x_1x_3 + x_1$ в группе S_3 .
4. Пусть H – подгруппа группы G индекса 2. Доказать, что она нормальна.
5. Найти период последовательности $x_j, j=0,1, \dots$ над кольцом Z_{17} вычетов по модулю 17, для которой $x_{j+1} = 2x_j + 3 \pmod{17}$.
6. Зашифровать с помощью алгоритма RSA, используя модуль $n=2773$, сообщение $w=275$.

Тест для самопроверки по результатам освоения дисциплины

Компетенция ПК-3

1. Группа порядка 36 действует на некотором множестве. Орбиты каких длин возможны?

А) 1,2,4,

Б) 1,3,9,

В) 1,2,3,4,6,9,12,18,36

Г) длин, не являющихся делителями 36.

2. Перечислите число и гомоморфизмы группы кватернионов Q_8

А) 5 гомоморфизмов с образами порядков 1,2, 2,2 и 8

Б) 2 с образами порядков 2 и 8

В) 3 с образами порядка 1,2 и 8

Г) 2 с образами порядка 1 и 8

3. Порядок подгруппы инерции функции $f=x_1+x_2+x_3+x_4$ в группе Жевонса.

А) равен 24

Б) равен 192

В) равен 16

Г) равен 36

4. Расшифровать слово над алфавитом {A, B}, зашифрованное словами над {C,D}, если ключ имеет вид: A-CCD, B-- C: CCDCCCCDC,

А) ABBBA,

Б) ABBAB

В) ABBBAB

Г) ABAVA

Вопрос №	Правильный ответ
1	В
2	А
3	Б
4	Б

Оценка сформированности компетенций

Компетенции	Номера вопросов	Уровень формирования	Количество правильных ответов, критерии
ПК-3	1-4	Пороговый	Не менее 2
		Продвинутый	Не менее 3
		Высокий	Не менее 4

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

Список вопросов к зачету:

1. Конфиденциальность. Дать определение.
2. Целостность информации. Как обеспечивается?.
3. Что такое аутентификация? По каким параметрам?
4. Как обеспечивается невозможность отказа от авторства?
5. Что такое шифрсистема?
6. Какие хэш-функции Вам известны? Их виды?
7. Описать модель шифра простой замены.
8. Описать вероятностную модель шифра.
9. Почему шифр Цезаря слабый?
10. Модель шифра перестановки. Сильные и слабые стороны.
11. Привести примеры шифров маршрутной перестановки..
12. Сколько существует решеток Кардано размера $n \times n$?
13. Дать описание поточного шифра. Привести примеры.
14. Модель композиции шифров..
15. Простейшая вероятностная модель открытого текста..
16. Критерий на открытый текст.
17. Определение и примеры шифра гаммирования. Вскрытие шифра гаммирования.

18. Книжная гамма. Использование
19. Что такое стойкость шифра? Как ее оценить?
20. Основные задачи и методы криптоанализа.
21. Совершенный шифр по Шеннону.
22. Расстояние единственности.
23. Имитостойкость.
24. Спектр Фурье булевой функции.
25. Преобразование Уолша-Адамара.
26. Расстояние между булевыми функциями.
27. Бент-функция.
28. Линейная рекуррентная последовательность. Оценка длины периода.
29. Линейный конгруэнтный генератор.
30. Генератор RSA.
31. Алгоритм RC4/
32. Формальное определение блочного шифра.
33. Сеть Файстеля.
34. Алгоритм DES.
35. ГОСТ 28147-89
36. AES.
37. "Кузнечик"
38. Режимы использования шифров.
39. Бесключевая функция хэширования.
40. Методы построения функций хэширования.
41. Ключевая функция хэширования.
42. Выработка имитовставки.
43. Шифрование RSA.
44. Случаи взлома RSA.
45. Шифрование Рабина-Уильямса.
46. Схема Эль-Гамала.
47. Электронная подпись Эль-Гамала.
48. Электронная подпись ГОСТ Р 34.10-2012
49. Протоколы выработки общего ключа.
50. Протоколы ключа для конференц-связи

**Приложение № 2 к рабочей программе дисциплины
«Криптографические методы»**

Методические указания для аспирантов по освоению дисциплины

**Учебно-методическое обеспечение
самостоятельной работы аспирантов по дисциплине**

В качестве учебно-методического обеспечения рекомендуется использовать литературу, указанную в разделе № 7 данной рабочей программы.