

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

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 18 апреля 2023 г., протокол № 8

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

Дисциплина «Криптографические методы» является дисциплиной по выбору вариативной части.Б1.В.ДВ.04.02 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 – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения программы и критерии их оценивания

- готовность к исследованию в области алгебраической геометрии, алгебраической и ана

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.	ПК-3,3 Умеет использовать методы проектирования и производства программного продукта, принципы построения структуры и приемы работы с инструментальными средствами, поддерживающими создание программного продукта	1. Знать: Основные методы и формулировки результатов, использующихся в защите информации 2. Уметь обосновывать алгоритмы защиты информации 3. Владеть навыками быстрых вычислений в основных алгебраических системах

4. Объем, структура и содержание дисциплины

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

Дисциплина изучается в течение первого семестра. Формой итоговой аттестации по дисциплине является зачет.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий и их трудоемкость (в академических часах)	Формы текущего контроля успеваемости
-------	--	---------	--	--------------------------------------

			лекции	практические	лабораторные	консультации	самостоятельная работа	Форма промежуточной аттестации (по семестрам)
1	Основные понятия и задачи криптографии. Формальные модели шифров. Шифры гаммирования. Методы вскрытия шифров гаммирования	8	13	5			5	Задания для самостоятельной работы. Контрольная работа
2	Оценки качества криптографических преобразований. Поточные шифры и генерация псевдослучайных последовательностей. Блочные шифры.	8	13	5		2.3	5	Задания для самостоятельной работы
3	Асимметричное шифрование. Группа точек эллиптической кривой. Электронная подпись. Хэш функции. Управление ключами.	8	6	6		2	7.7	Задания для самостоятельной работы
		8						Зачет
	Всего 72 часа		32	16		6.3	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-Хеллмана. Разделение секрета

5. Образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов. Академическая лекция, как правило, состоит из трех частей: вступления (введения), изложения и заключения:

- *вступление* (введение) определяет тему, план и цель лекции. Оно призвано заинтересовать и настроить аудиторию, сообщить, в чём заключается предмет лекции и (или) её актуальность, основная идея (проблема, центральный вопрос), связь с предыдущими и

последующими занятиями, поставить её основные вопросы. Введение должно быть кратким и целенаправленным.

- *изложение* является основной частью лекции, в которой реализуется научное содержание темы, ставятся все узловые вопросы, приводится вся система доказательств с использованием наиболее целесообразных методических приемов. Каждое теоретическое положение должно быть обосновано и доказано, приводимые формулировки и определения должны быть четкими, насыщенными глубоким содержанием.

- *заключение* обобщает в кратких формулировках основные идеи лекции, логически ее завершая. В заключении могут даваться рекомендации о порядке дальнейшего изучения основных вопросов лекции самостоятельно по указанной литературе.

Вводная лекция – дает первое целостное представление о дисциплине (или ее разделе) и ориентирует студента в системе изучения данной дисциплины. Обучающиеся знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки специалиста. 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 курса, а также дается анализ рекомендуемой учебно-методической литературы.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения и информационных справочных систем (при необходимости).

В процессе осуществления образовательного процесса используются:

-- программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов:

- Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery).
- Microsoft OfficeSTD 2013 RUS OLP NL Acdmc 021-10232 Microsoft Open License №0005279522
- 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)

-- для поиска учебной литературы библиотеки ЯрГУ -- Автоматизированная библиотечная информационная система "БУКИ - NEXT" (АБИС "БУКИ - NEXT""БУКИ - NEXT").

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, 2016, 474 с.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. - Гелиос АРВ, 2001 -- 480 с.

3. Ноден П., Китте К. Алгебраическая алгоритмика (под ред. Л.С.Казарина), М.:Мир, 1999.

б) дополнительная литература

1. Фомичев В.М. Дискретная математика и криптология.М: ДИАЛОГ-МИФИ, 2003 -- 400с.
2. Саломая А. Криптография с открытым ключом, М.:Мир, 1996, -- 318 с.

в) ресурсы сети «Интернет»

1. Электронная библиотека учебных материалов ЯрГУ
2. Электронная библиотека ЯрГУ: <http://www.lib.uniyar.ac.ru/>
3. <http://mech.math.msu.su/departement/>
(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).
4. Информационная система "Единое окно доступа к образовательным ресурсам" (<http://www.edu.ru> раздел Учебно-методическая библиотека) или по прямой ссылке (<http://www.edu.ru/library>).
5. Электронно-библиотечная система "Университетская библиотека online" (www.biblioclub.ru).
6. [http:// www.tc26.ru](http://www.tc26.ru)
7. [http:// www.nist.gov/manuscript-publicftion-search.cfm?pub_id=919061](http://www.nist.gov/manuscript-publicftion-search.cfm?pub_id=919061)
6. <http://habrahabr.ru/post/210684/>
8. http://www.nist.gov/customcf/get_pdf.cfm?pub_id=919061
9. <http://www.streebog.info/news/opredeleny-pobediteli-konkursa-po-issledovaniyu-khesh-funksii-stribog/>

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; групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания оборудования.

Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления информации большой аудитории.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы) :

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

Казарин Л.С

**Приложение к №1 рабочей программе дисциплины
«Теория представлений групп и ассоциативных алгебр»**

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

**1. Типовые контрольные задания или иные материалы,
необходимые для оценки знаний, умений, навыков и (или) опыта деятельности,
характеризующих этапы формирования компетенций**

1.1 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 шифр-система?
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

1.2 Контрольные задания и 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 Джевонса.

- 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) ABBVA,
- Б) ABBAB
- В) ABBVAB
- 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

**Приложение № 2 к рабочей программе дисциплины
«Теория представлений групп и ассоциативных алгебр»**

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.

**Перечень ресурсов информационно-телекоммуникационной сети «Интернет»,
рекомендованных к использованию при освоении дисциплины**

Электронные ресурсы ЯрГУ (<http://lib.uniyar.ac.ru>)

1. Библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках и поступивших позже 1995 года:

http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php (в открытом доступе)

2. Электронная библиотека учебных материалов ЯрГУ:

http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

3. Электронная картотека «Книгообеспеченность»:

http://www.lib.uniyar.ac.ru/opac/bk_bookreq_find.php

4. Электронно-библиотечная система «Университетская библиотека Online»:

www.biblioclub.ru

5. Проект MAPC: <http://mars.arbicon.ru>.

6. Электронно-библиотечная система «Лань»: <http://e.lanbook.com/>

7. Научная электронная библиотека eLIBRARY.ru: <http://elibrary.ru>

8. Англоязычные библиотеки в сети университета:

а) MathSciNet: <http://www.ams.org/snhtml/annser.csv> - с платформы издателя

<http://search.ebscohost.com/> - с платформы Ebscohost

б) Web of Science: <http://webofscience.com>

в) Scopus: <http://www.scopus.com>

г) Science The American Association for the Advancement of Science:

<http://www.sciencemag.org>

д) Ресурсы Springer

SpringerJournals: <http://link.springer.com/>

SpringerProtocols: <http://www.springerprotocols.com/>

SpringerMaterials: <http://materials.springer.com/>

SpringerReference: <http://link.springer.com>

zbMATH: <http://zbmath.org/>