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
Методы алгебраической геометрии 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 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 «Методы алгебраической геометрии в криптографии» является ознакомление студентов с основами теории эллиптических кривых и её приложениями к алгоритмам, используемым для защиты информации

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 обязательной части учебного плана (Б1.О.52). Она опирается на знания, полученные студентами в ходе изучения дисциплин «Алгебра», «Геометрия», «Избранные вопросы алгебры», «Алгебраическая алгоритмика».

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**
Общепрофессиональные компетенции		
ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;	**И-ОПК-3_4** знает основные понятия, результаты и методы современной математики и сценарии их применения в задачах профессиональной деятельности **И-ОПК-3_**8 умеет распознать математические структуры, возникающие в задачах профессиональной деятельности, конструировать, анализировать объекты и выполнять вычисления, формулировать требования к свойствам математических объектов, необходимым для решения профессиональной задачи	**Знает** основные понятия, результаты и методы из алгебры и алгебраической геометрии **Умеет** распознать математические структуры, исследовать их свойства **Имеет навыки** вычислений в группах, факторкольцах, конечных полях, на эллиптических кривых, в т.ч. над полями конечной характеристики
ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	**И-ОПК-10_7** знает основы теории эллиптических кривых и преимущества эллиптической криптографии в целом, а также основные алгоритмы на эллиптических кривых **И-ОПК-10_8** умеет организовывать и выполнять вычисления на эллиптических кривых	**Знает** основы теории эллиптических кривых и причины применения эллиптических алгоритмов в криптографии и требования стойкости эллиптическиой кривой **Умеет** умеет выполнять вычисления на эллиптических кривых

ОПК-2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	**И-ОПК-2.1_5** знает принципиальные закономерности применения математических методов и результатов в задачах защиты информации **И-ОПК-2.1_6** умеет понимать и анализировать работу вычислительного алгоритма, использующего современные математические методы	**Знает** принципиальные закономерности применения математических методов и результатов в задачах защиты информации **Умеет** понимать работу вычислительного алгоритма, использующего вычисления на эллиптических кривых

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет _4_ зачетных единицы, _144_ 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	**Полугруппы и моноиды**	9	2	2					
2	**Группы**	9	8	8				10	Задание для самостоятельной работы № 1
3	**Кольца и поля**	9	10	12		2		10	Задание для самостоятельной работы № 2
4	**Замкнутые аффинные и проективные множества и алгебраические кривые**	9	10	12				*10*	
5	**Эллиптическая кривая**	9	12	14		2		12	Задание для самостоятельной работы № 3 Контрольная работа
6	**Основные вычислительные алгоритмы, использующие эллиптические кривые**	9	8	2				1,7	
							0,3		зачёт
	ИТОГО	9	48	48		4	0,3	43,7	

4.Содержание разделов дисциплины

1. **Полугруппы и моноиды.** Множества, операции, арности. Полугруппы и моноиды. Определения, примеры. Гомоморфизмы и изоморфизмы полугрупп и моноидов. Свободные полугруппы и моноиды. Обобщенная ассоциативность в полугруппе. Операции над степенями элемента полугруппы. Конгруэнции в полугруппе. Теорема о гомоморфизме для полугрупп. Обратимые элементы и их основные свойства. Подполугруппы и подмоноиды. Задание полугрупп и моноидов образующими элементами и определяющими соотношениями. Проблемы равенства и изоморфизма для конечно определенных полугрупп и моноидов. Теоремы Маркова и Поста.
2. **Группы.** Свободные группы. Проблема изоморфизма для групп (проблема Дэна). Алгоритмические проблемы для конечно определенных групп. Теоремы Новикова и Адяна – Рабина. Задание группы образующими и определяющими соотношениями. Преобразования Титце. Группы кос и алгоритмические проблемы для них: результаты Артина, Маканина, Гарсайда. Подгруппы, пересечение подгрупп. Подгруппа, порожденная подмножеством элементов группы. Образующие элементы подгруппы. Теорема о гомоморфизме и две теоремы об изоморфизмах для групп. Сопряженные элементы. Разложение группы на классы сопряженных элементов. Нормализатор подмножества. Центр группы. Теоремы Силова. Строение конечных и конечно порожденных абелевых групп. Коммутант группы и его свойства.
3. **Кольца и поля.** Основные классы колец. Примеры колец. Кольца $Z[\sqrt{d}]$. Группа обратимых элементов кольца. Кольца вычетов и обратимые элементы в них. Матричные кольца и обратимые элементы в них. Обратимые элементы в кольце формальных степенных рядов от одной переменной над произвольным коммутативным кольцом с единицей. Сумма и пересечение подколец и идеалов. Идеал, порожденный подмножеством. Прямые суммы колец и идеалов. Поля и тела, их простейшие свойства. Тело кватернионов. Поля вычетов. Поле частных целостного кольца. Поле рациональных дробей. Подполя. Простое подполе и его связь с характеристикой поля. Гомоморфизм и изоморфизм полей. Изоморфизм $C \cong R[x]/(x^2+1)$. Расширения полей. Типы расширений: конечные, алгебраические, трансцендентные, конечно порожденные, простые. Нетеровы и артиновы кольца. Теорема Гильберта о базисе. Эквивалентность бесконечных систем алгебраических уравнений своим конечным подсистемам.
4. **Замкнутые аффинные и проективные множества и алгебраические кривые**. Современный подход к геометрии. Предмет алгебраической геометрии. Зачем специалисту по защите информации нужна алгебраическая геометрия? Проективное пространство над произвольным полем. Открытые и замкнутые подмножества аффинного и проективного пространств (топология Зарискoго). Аффинные карты на проективной плоскости и проективное замыкание плоской алгебраической кривой. Пример: проективные коники. Представление о групповом алгебраическом многообразии (сложение точек на конике). Кольцо регулярных и поле рациональных функций замкнутого алгебраического множества. Регулярное отображение (морфизм) и изоморфизм замкнутых алгебраических множеств. Представление о бирациональном изоморфизме. Проективное замыкание аффинного множества. Касательная к плоской алгебраической кривой над полем произвольной характеристики, не делящей степень кривой. Неособая плоская алгебраическая кривая. Кратность пересечения кривой и прямой в их общей точке. Точки перегиба плоской алгебраической кривой.
5. **Эллиптическая кривая**. Точки перегиба неособой кубической кривой. Канонические формы уравнений эллиптической кривой. Групповая структура на эллиптической кривой. Сложение точек эллиптической кривой в координатах. Нерациональность

эллиптической кривой. Дискриминант и j-инвариант кубической кривой. Случай нулевого дискриминанта. Сложение точек эллиптической кривой в координатах. Эллиптические функции. Функция Вейерштрасса. Параметризация комплексной эллиптической кривой. Сложение точек и сложение значений параметра.

6. **Основные вычислительные алгоритмы, использующие эллиптические кривые**. Преимущества криптографического применения эллиптических кривых. Факторизация целого числа с использованием эллиптической кривой: метод Ленстры. Дискретное логарифмирование на эллиптической кривой: метод Полларда.

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. 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.

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

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

а) основная литература

1. Зяблицева, Л. В. Алгебраические структуры и их приложения / Зяблицева Л. В. , Корабельщикова С. Ю. , Кузнецова И. В. , Тихомиров С. А. - Архангельск : ИД САФУ, 2015. - 169 с. - ISBN 978-5-261-01074-6. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785261010746.html (дата обращения: 01.02.2022). - Режим доступа : по подписке.

2. Тимофеева Н.В. Алгебраические структуры / Н. В. Тимофеева; Яросл. гос. ун-т им. П. Г. Демидова. - Ярославль: ЯрГУ, 2021. Ч. 1 [Электронный ресурс]: учебное пособие. - Б.м.: Б.и., 2021. - 79 с. http://www.lib.uniyar.ac.ru/edocs/iuni/20210203.pdf

3. Ростовцев, А. Г. Алгебраические основы криптографии. - СПб.: Мир и семья, 2000.-354с.

б) дополнительная литература

1. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие для вузов / Л. М. Мартынов. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 456 с. — ISBN 978-5-8114-9346-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/189446 (дата обращения: 01.02.2022). — Режим доступа: для авториз. пользователей.

2. Атья М. Введение в коммутативную алгебру / М. Атья, И.Макдональд. Пер. с англ. – М.: Мир, 1972. – 161 с.

3. Кокс Д., Литтл Дж., О’Ши Д. Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры / Д. Кокс; Пер. с англ. --- М. : Мир, 2000. http://www.bookre.org/reader?file=1221440

4. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел: учебное пособие / Ш.Т. Ишмухаметов. – Казань, Казанский ун-т, 2011. – 190 с.

7. Рид, М. Алгебраическая геометрия для всех / М. Рид. Пер. с англ. - М.: Мир, 1991.-149с

в) ресурсы сети «Интернет» (при необходимости)

6. Острик, В. В. Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые : учебное пособие / В. В. Острик, М. А. Цфасман. — Москва : МЦНМО, 2001. — 48 с. — ISBN 5-900916-71-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/9381 (дата обращения: 29.11.2021). — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/9381?category=908

9. Шафаревич, И. Р. Основы алгебраической геометрии : учебное пособие / И. Р. Шафаревич. — 3-е изд. — Москва : МЦНМО, 2007. — 589 с. — ISBN 978-5-94057-085-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/9441 (дата обращения: 29.11.2021). — Режим доступа: для авториз. пользователей. https://e.lanbook.com/book/9441?category=908

10. Cox D., Little J., O'Shea D. Using Algebraic Geometry, 2nd ed., Graduate texts in Math, vol.185, Springer, 2004. http://bookre.org/reader?file=741076

11. Gallian J. Contemporary Abstract Algebra. Cengage Learning, 2010. https://notendur.hi.is/mbh6/html/_downloads/Contemporary%20Abstract%20Algebra%20-%20Joseph%20Gallian%20(2012).pdf

12. Eisenbud D. Commutative Algebra with a View Towards Algebraic Geometry, Graduate texts in Math,vol.150. https://www.math.ens.psl.eu/~benoist/refs/Eisenbud.pdf

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):

Профессор кафедры АМЛ, д.ф.-м.н. Н.В. Тимофеева

Приложение № 1 к рабочей программе дисциплины
« Методы алгебраической геометрии 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

Задание для самостоятельной работы № 1 (И-ОПК-3_4, И-ОПК-3_8)

1. Перечислить все гомоморфизмы симметрической группы на n элементах в группу порядка 2
2. Найти все подгруппы в группе классов вычетов данного порядка
3. Перечислить все образующие в группе классов вычетов данного порядка
4. Перечислить все гомоморфизмы группы в группу (группы берутся из класса: группы классов вычетов и их конечные прямые произведения)
5. Выяснить, изоморфны ли две данные конечные группы (задача подразумевает сравнение порядков элементов)
6. Построить отношение эквивалентности в кольце целых чисел, не согласованное с операцией сложения
7. Найдите группу всех обратимых элементов кольца классов вычетов Z_{12}. Является ли она циклической?

Задание для самостоятельной работы № 2 (И-ОПК-3_4, И-ОПК-3_8)

1. Изоморфны ли кольца $Z_{10} \times Z_{12}$ и $Z_6 \times Z_{20}$? Обоснуйте ответ.
2. Перечислите все гомоморфизмы кольца Z_{12} в $Z_2 \oplus Z_3$
3. Докажите, что ядро гомоморфизма коммутативного кольца с единицей на поле является максимальным идеалом, а факторкольцо коммутативного кольца с единицей по максимальному идеалу является полем.
4. Опишите все подгруппы в группе Z_{12} и все подкольца в одноименном кольце.
5. Найдите группу всех обратимых элементов кольца классов вычетов Z_{12}. Является ли она циклической?
6. Перечислите все гомоморфизмы кольца Z_{12} в $Z_2 \oplus Z_3$

Задание для самостоятельной работы № 3 (И-ОПК-10_7)

1. Дана кривая, определенная над полем характеристики $\neq 2,3$: $y^2 + 2xy = x^3 - x^2$

А) Выясните любым известным вам способом, особа она или нет.
Б) Если кривая особа, определите координаты особой точки.

2. Дана кривая, определенная над полем характеристики 2: $y^2 + y = x^3 + x^2$

А) Выпишите явные формулы сложения точек на такой кривой.

Б) Вычислите координаты точки 2P, если P(1,1).

3. Охарактеризовать особые точки кубической кривой (характеристика произвольная)
$x^3 - y^2z - yz^2 - x^2z = 0$.

4. Вычислите координаты точек перегиба кривой (характеристика произвольная) $x^3 - y^2z - yz^2 = 0$.

5. Вычислите дискриминант и j-инвариант эллиптической кривой (в характеристике 0)

Вариант контрольной работы (И-ОПК-3_4, И-ОПК-3_8, И-ОПК-10_7, И-ОПК-10_8)

1. Дана кривая, определенная над полем характеристики $\neq 2,3$: $y^2 + 2xy = x^3 - x^2$
А) Выясните любым известным вам способом, особа она или нет.
Б) Если кривая особа, определите координаты особой точки и тип особенности.
2. Дана кривая, определенная над полем характеристики 2: $y^2 + y = x^3 + x^2$
А) Выпишите явные формулы сложения точек на такой кривой.
Б) Вычислите координаты точки 2P, если P(1,1).

Зачёт выставляется по итогам контрольной работы и короткого собеседования (И-**ОПК-3_4, И-ОПК-10_7, И-ОПК-2.1_5, И-ОПК-2.1_6**) по темам 5 и 6 (описание содержания тем – круг вопросов для собеседования)

Приложение № 2 к рабочей программе дисциплины
« Методы алгебраической геометрии в криптографии »
наименование дисциплины

Методические указания для студентов по освоению дисциплины

Дисциплина «Методы алгебраической геометрии в криптографии» имеет двустороннюю направленность. С одной стороны, в ходе ее освоения происходит знакомство студентов с одной из наиболее технически насыщенных и быстро развивающихся отраслей «чистой» математики, которое не может даться без усилий. С другой стороны, такое знакомство не является самоцелью, а лишь служит базой для изложения алгоритмов. Как правило, «прикладной» аспект воспринимается студентами с большей готовностью, несмотря на громоздкость самих алгоритмов. Основная трудность курса – обилие теоретического материала, поэтому разбор теории при самоподготовке необходим. Круг учебных задач, предлагаемых студентам, весьма узок; задачи в основном несложны и совершенно посильны при некотором усердии со стороны добросовестного студента. Курс готовит базу для разбора и применения алгоритмов, в него не вошедших, а быть может, приоткрывает возможность для разработки новых.