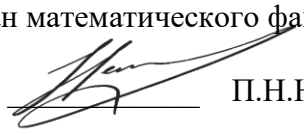
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



П.Н.Нестеров

«18» мая 2021 г.

Рабочая программа дисциплины
«Алгебраические и теоретико-числовые методы в криптографии»

Направление подготовки
01.06.01 Математика и механика

Направленность (профиль)
«Математическая логика, алгебра и теория чисел»

Форма обучения очная

Программа рассмотрена
на заседании кафедры алгебры и математической логики
от «16» апреля 2021 года, протокол № 8

Ярославль

1. Цели освоения дисциплины

Целью изучения дисциплины «Алгебраические и теоретико-числовые методы в криптографии» является

1) подготовка в области компьютерной безопасности;

2) овладение методами решения основных задач в области современной криптографии, основанных на теоретико-числовых и алгебраических алгоритмах;

3) овладение современным математическим аппаратом, используемым в криптографии и теории кодирования для дальнейшего использования в приложениях.

2. Место дисциплины в структуре программы аспирантуры

Дисциплина «Алгебраические и теоретико-числовые методы в криптографии» является дисциплиной по выбору вариативной части. Данная дисциплина направлена на освоение теоретико-числовых и алгебраических алгоритмов, применяемых в современных криптосистемах.

3. Планируемые результаты обучения по дисциплине – знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций и обеспечивающие достижение планируемых результатов освоения программы аспирантуры, и критерии их оценивания

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Профессиональные компетенции:

- способностью к разработке и совершенствованию теоретических и методологических подходов в теории представлений, теории категорий и функторов, теории моделей (изучение свойств семантических моделей для математических теорий), теории доказательств (в том числе неклассические логики), теории алгоритмов и вычислимых функций (в том числе алгоритмическая теория информации и теория сложности) **(ПК-3)**.

Код компетенции	**Планируемые результаты обучения**	**Критерии оценивания результатов обучения**		
		Пороговый уровень	**Продвинутый уровень**	**Высокий уровень**
ПК-3	ЗНАТЬ: Основные положения, касающиеся криптографической защиты информации. Основные алгоритмы, применяющиеся в криптографии, как симметричные, так и асимметричные. Положения теории секретных систем, основу применяемых алгебраических алгоритмов, эффективные алгоритмы вычислений в конечных полях	Основные понятия теории секретных систем Шеннона Алгоритмы, применяемые в криптографии как с секретным, так и с открытым ключом.. Методы работы с криптографическими примитивами. Основные идеи,обеспечивающие работу алгебраических алгоритмов, Однако не все знания достаточно детализированы.	Основные понятия, и алгоритмы, применяемые в защите информации, особенности их реализации и математические задачи, определяющие скорость и надежность применяемых алгоритмов. Теоретико-числовую и алгебраическую подоплеку основных алгоритмов	Алгоритмы и способы конструировании криптографических систем, эффективных алгоритмах, применяемых в криптографии, их теоретической сложности и возможности совершенствования в дальнейших исследованиях исследованиях
	УМЕТЬ: использовать положения теории для построения криптосистем с заданными	В целом успешное, но не систематическое использование теории для определения параметров	В целом успешное, но содержащее отдельные пробелы в использовании теории	Хорошее умение использовать положения и методы теории для получения

	свойствами. Оценивать сложность предлагаемых криптосистем. Сравнивать эффективность различных криптосистем	криптосистемы и оценки предлагаемых алгоритмов. Программировать (применять) готовые средства защиты информации в конкретной ситуации	для определения параметров криптосистемы и оценки предлагаемых алгоритмов.В частости не всегда оптимальное программирование	оптимальных параметров криптосистемы. Формулировать полезные предложения для ее усовершенствования.
	ВЛАДЕТЬ: навыками анализа криптосистем, конструирования криптосистем с заданными свойствами с помощью теоретико-числовых и алгебро-геометрических моделей, методами оценивания применяемых моделей.	В целом успешное, но не систематическое применение навыков анализа криптосистем. Освоены простейшие методы вычислений и не самые сложные модели защиты информации. Имеются пробелы в применении алгеброгеометрических моделей	Успешное, но содержащее отдельные пробелы в применении навыков анализа основных криптографических моделей и владение основными методами анализа криптографических систем и оценки их вычислительной сложности..	Успешное и систематическое применение навыков анализа криптосистем. Освоены основные методы вычи-слений в указан-ных структурах и приобретен опыт успешного использования теории в конкретных ситуациях

4. Объем, структура и содержание дисциплины

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

Дисциплина изучается в течение второго семестра. Формой итоговой промежуточной 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 Форма промежуточной аттестации *(по семестрам)*
			лекции	практические	лабораторные	консультации	самостоятельная работа	
1	Элементарная теория чисел и криптография. Делимость. Разложение на множители. Сравнения.. Конечные поля.	2	2	1			14	
2	Квадратичный закон взаимности. Символы Лежандра и Якоби. Некоторые простые криптосистемы. Открытый ключ.	2	2	1			14	
3	Криптосистема RSA, Дискретное логарифмирование. Задача о рюкзаке. Протоколы с нулевым разглашением и скрытая передача.	2	2	1			14	Контрольная работа № 1
4.	Простота и факторизация.	2	2	1			14	

	Факторизация Ферма и факторные базы. Метод цепных дробей. Метод квадратичного решета.6							
5	Эллиптические кривые. Группы точек эллиптических кривых. Эллиптические кривые над конечными полями. Арифметика в нормальных базисах. Протоколы на эллиптических кривых.	2	2	1			16	
6	Современные криптосистемы и стандарты. DES, AES и ГОСТ. Криптосистема Эль-Гамаля и варианты использования. Алгоритмы арифметики над конечными полями.	2	2	1			16	Контрольная работа № 2
		2				2		Зачет
	Всего		**12**	**6**		**2**	**88**	

Содержание разделов дисциплины:

1. Элементарная теория чисел и криптография. Делимость. Разложение на множители. Сравнения.. Конечные поля.
2. Квадратичный закон взаимности. Символы Лежандра и Якоби. Некоторые простые криптосистемы. Открытый ключ.
3. Криптосистема RSA, Дискретное логарифмирование. Задача о рюкзаке. Протоколы с нулевым разглашением и скрытая передача.
4. Простота и факторизация. Факторизация Ферма и факторные базы. Метод цепных дробей. Метод квадратичного решета
5. Эллиптические кривые. Группы точек эллиптических кривых. Эллиптические кривые над конечными полями. Арифметика в нормальных базисах. Протоколы на эллиптических кривых.
6. Современные криптосистемы и стандарты. DES, AES и ГОСТ. Криптосистема Эль-Гамаля и варианты использования. Алгоритмы арифметики над конечными полями.

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.

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

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).

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

7. Перечень основной и дополнительной учебной литературы, необходимых для освоения дисциплины

а) основная литература

1. Зубов, А. Ю., Криптографические методы защиты информации. Совершенные шифры : учеб. пособие для вузов / А. Ю. Зубов, М., Гелиос АРВ, 2005, 191с
2. Коблицт Н .Курс теории чисел и криптографии. М.: «Научное издательство ТВП», 260 с.
3. Осипян, В. О., Криптография в задачах и упражнениях : [учеб. пособие для вузов] / В. О. Осипян, К. В. Осипян, М., Гелиос АРВ, 2004, 143с

4. Болотов А.А., Гашков С.Б., Фролов А.Б. Часовских А.А., Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы. М.: «КомКнига», 2006, 324 с.

б) дополнительная литература

1. Столлингс В. Криптография и защита сетей. Принципы и практика.-- 2-е изд. М.: Гелиос АРВ, 2001.
2. Саломаа А. Криптография с открытым ключом. М: Мир, 1996.
3. Смарт Н. Криптография. М:Техносфера. 2003
4. Бабаш А.В., Шанкин Г.П. История криптографии. Учебное пособие. М.: “Гелиос АРВ”, 2002
5. Введение в криптографию : новые математические дисциплины / под ред. В. В. Ященко, СПб., Питер, 2001, 287с
6. Запечников, С. В., Криптографические протоколы и их применение в финансовой и коммерческой деятельности : учеб. пособие для вузов / С. В. Запечников, М., Горячая линия - Телеком, 2007, 319с
7. Ноден П., Китте К. Алгебраическая алгоритмика /под ред. Л.С. Казарина. М: Мир, 1999.

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/department/

(**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
7. 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/

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

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

-учебные аудитории для проведения занятий лекционного типа, практических занятий (семинаров); 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
«Алгебраические и теоретико-числовые методы в криптографии»

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. Проблемы защиты информации. Сведения, составляющие государственную тайну. Компьютерные преступления и противодействие им. Угрозы безопасности информации и их классификация. Государственная система защиты информации, обрабатываемой техническими средствами.
2. Правовое обеспечение защиты информации в России и за рубежом. Лицензирование, стандартизация и сертификация деятельности по защите информации. Правовое обеспечение защиты информации в России и за рубежом.
3. Требования к защите информации, оценка возможностей противоборствующей стороны. Методология разработки и анализа средств защиты. Криптографические и стеганографические методы защиты информации. Классические методы защиты информации.
4. Развитие криптографии. Основные этапы. Шифры Цезаря, Плйфейра, Хилла, квадрат Полибия, решетки и лабиринты, книжный шифр.
5. Криптоанализ шифра замены. Индекс совпадения Фридмана.
6. Криптоанализ шифра Виженера и шифра гаммирования с короткой гаммой.
7. Табличное и модульное гаммирование.
8. Роль Шеннона и отечественные достижения в области защиты информации.
9. Математические модели открытых сообщений. Критерии на открытый текст. Способы представления информации, подлежащей шифрованию. Особенности нетекстовых сообщений.
10. Определение шифра и его математические модели. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам.
11. Понятие криптосистемы. Симметричные и асимметричные системы шифрования.
12. Основные классы шифров и их свойства. Шифры перестановки. Разновидности шифров перестановки. Криптоанализ шифров перестановки.
13. Одноалфавитные и многоалфавитные шифры замены. Поточные и блочные шифры замены.
14. DES, ГОСТ 28147-89, AES. Режимы использования блочных шифров.
15. Надежность шифров и проблемы реализации криптосистемы.
16. Теоретико-информационный подход к оценке стойкости шифра. Ненадежность ключей и сообщений.
17. Совершенные шифры. Безусловно стойкие и практически стойкие шифры. Избыточность языка и расстояние единственности.

18. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость.
19. Регистры сдвига с обратной связью.
20. Блоки шифрования.
21. Теоретико-автоматная характеризация криптосистем и их блоков.
22. Методы шифрования с открытым ключом.
23. Односторонняя функция и односторонняя функция с «лазейкой»
24. Криптосистемы RSA и Эль-Гамаля
25. Проблемы факторизации целых чисел и логарифмирования в конечных полях.
26. Криптосистемы с открытым ключом, основанные на укладке рюкзака и линейных кодах.
27. Преимущества и недостатки асимметричных криптосистем.
28. Стандарты AES и серии ГОСТ
29. Понятие криптографического протокола. Основные примеры.
30. Переход о стандартного базиса конечного поля к нормальному.
31. Группа точек эллиптической кривой.
32. Тестирование неприводимости многочлена над конечным полем.
33. Алгоритмы умножения в конечном поле.
34. Быстрое возведение в степень в конечном поле.
35. Протоколы цифровой подписи.

1.2 Контрольные задания и иные материалы, используемые в процессе текущей аттестации

В течение семестра студенты решают задачи, указанные преподавателем, к каждому семинару. В семестре проводятся 2 контрольные работы.

Контрольная работа № 1 (один из 28 вариантов)

1. Определите наилучшее аффинное приближение функции f\in P_2(n). n=3, **f=x_1+x_2+x_3+x_1x_2x_3.**
2. Найти индекс совпадения Фридмана для текста задания
3. Описать известные Вам схемы получения псевдослучайной последовательности.
4. Зашифровать сообщение с помощью двойного шифра Хилла, использующего матрицы размеров 2 и 3.
5. Написать программу зашифрования с помощью шифра Плейфейра.
6. Прочитать сообщение, зашифрованное шифром Виженера (текст варьируется).

Контрольная работа № 2 (один из 28 вариантов)

1. Вычислить символ Лежандра (5/160465489).
2. Привести примеры использования ЭЦП Рабина.
3. Каковы основные этапы по вскрытию шифра Виженера?
4. Как определяются энтропия и избыточность языка?
5. Написать программу выработки имитовставки.
6. В чем заключаются достоинства и недостатки систем поточного шифрования по сравнению с блочными ?
7. Сравнить достоинства и недостатки шифров DES, AES и ГОСТ-28147-89
8. Для каких целей применяются хеш-функции? Как строятся криптографические хеш-функции?

Приложение № 2 к рабочей программе дисциплины
«Алгебраические и теоретико-числовые методы в криптографии»

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 МАРС: 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/