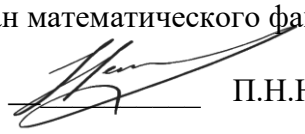
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета


П.Н.Нестеров

«18» мая 2021 г.

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

Направление подготовки
10.06.01 Информационная безопасность

Направленность (профиль)
«Методы и системы защиты информации,
информационная безопасность»

Форма обучения очная

Программа рассмотрена
на заседании кафедры компьютерной безопасности
и математических методов обработки информации
от «16» апреля 2021 года, протокол № 8

Ярославль

1. Цели освоения дисциплины

Дисциплина «Алгебраические и теоретико-числовые методы в криптографии» обеспечивает приобретение фундаментальных и профессиональных знаний, умений и навыков, содействует дальнейшей фундаментализации образования, развитию логического мышления и формированию математического и общенаучного мировоззрения. Целью изучения дисциплины является освоение фундаментальных понятий теории чисел, комбинаторной теории групп и алгебры, лежащих в основе современных подходов к построению криптоалгоритмов и криптопротоколов, математическому обоснованию их криптографической стойкости.

2. Место дисциплины в структуре программы аспирантуры

Дисциплина «Алгебраические и теоретико-числовые методы в криптографии» является дисциплиной по выбору вариативной части.

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:**
- способность выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах (ПК-1);

Результаты обучения выпускника формулируются в следующих категориях:
«знать» – означает способность выпускника воспроизводить учебный материал с требуемой степенью научной точности (формулировать определение, с достаточной полнотой описывать процесс и явление);
«уметь» – означает способность выпускника решать типовые (адаптированные) задачи на основе воспроизведения алгоритма решения и его применения в конкретных стандартных условиях;
«владеть» – означает способность выпускника решать усложненные, в том числе комплексные задачи. Задачи данного уровня решаются на основе ранее приобретенных знаний и умений, с их трансформацией и применением в новых нетиповых условиях.

Код компетенции	**Планируемые результаты обучения**	**Критерии оценивания результатов обучения**		
		Пороговый уровень	**Продвинутый уровень**	**Высокий Уровень**
способностью выявлять основные угрозы безопасности информации, строить и исследовать модели	**Знать:** основные угрозы безопасности информации и способы построения модели нарушителя.	**Знает:** основные угрозы безопасности информации и способы построения модели нарушителя.	**Знает:** основные угрозы безопасности информации и способы построения модели нарушителя.	**Знает:** основные угрозы безопасности информации и способы построения модели нарушителя.

нарушителя в компьютерных системах (ПК-1)	**Уметь:** строить модели нарушителя в компьютерных системах . **Владеть:** навыками исследования модели нарушителя в компьютерных системах.		**Умеет:** Строить модели нарушителя в компьютерных системах .	**Умеет:** Строить модели нарушителя в компьютерных системах . **Владеет:** Навыками исследования модели нарушителя в компьютерных системах.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные 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	Базовые понятия теории чисел, теории множеств и теории алгоритмов.	2	1				12	
2	Полугруппы, моноиды и группы.	2	1				12	
3	Кольца и многочлены.	2	1			0,5	12	
4	Поля и многочлены над ними.	2	1				12	
5	Конечные поля и многочлены над ними.	2	1			0,5	12	Собеседование на консультации
6	Элементы эллиптической криптографии.	2	1			0,5	12	Собеседование на консультации
7	Вычислительные алгоритмы в алгебре и	2	1				12	

	теории чисел.							
8	Методы теории чисел и комбинаторной теории групп в современной криптографии.	2	1			0,5	14	Собеседование на консультации
		2						Зачет
	Всего		**8**			**2**	**98**	

Содержание разделов дисциплины

Тема 1. Базовые понятия теории чисел, теории множеств и теории алгоритмов.

Отношение делимости для натуральных и целых чисел. Деление с остатком.

Простые и составные числа. Основная теорема арифметики.

НОД и НОК. Алгоритм Евклида, оценка его сложности. Коэффициенты Безу. Взаимно простые числа. Функция Л. Эйлера.

Распределение простых чисел в ряду натуральных чисел. Теорема Л. Эйлера. Асимптотический закон распределения простых чисел. Теоремы П.Л. Чебышева и Ж. Адамара - Ш.-Ж. Валле-Пуссена.

Сложность проблемы проверки числа на простоту. Тесты простоты и алгоритмы.

Сравнения по натуральному модулю. Квадратичные вычеты и невычеты. Квадратичный закон взаимности.

Цепные дроби, подходящие дроби. Теорема Ж.-Л. Лагранжа.

Диофантовы уравнения. 10-ая проблема Д. Гильберта. Уравнение Пелля и метод цепных дробей.

Математическое уточнение интуитивного понятия алгоритма - машины Тьюринга и частично рекурсивные функции.

Рекурсивные, рекурсивно перечислимые и диофантовы множества.

Временная и емкостная оценки сложности выполнения алгоритма.

Сложность описания (задания) алгоритма.

Теоретико-числовые функции. Мультипликативные функции.

Сумматорные функции. Функция Мебиуса и формула обращения.

Тема 2. Полугруппы, моноиды и группы.

Алгебраические операции. Группоиды. Гомоморфизмы и изоморфизмы группоидов.

Полугруппы. Нейтральные элементы, моноиды. Гомоморфизмы и изоморфизмы полугрупп и моноидов. Задание полугрупп и моноидов образующими и определяющими соотношениями. Алгоритмические проблемы для конечно определенных полугрупп и моноидов. Теорема А.А. Маркова - Э. Поста.

Обратимые элементы, группы. Задание групп образующими и определяющими соотношениями. Алгоритмические проблемы для конечно определенных групп, фундаментальные проблемы М. Дэна. Теоремы П.С. Новикова и С.И. Адяна.

Подгруппы, нормальные подгруппы и факторгруппы. Гомоморфизмы и изоморфизмы групп. Теоремы о гомоморфизмах.

Группы подстановок. Теорема Кэли.

Действие группы на множестве, орбиты элементов и стабилизаторы.

Фундаментальные группы топологических пространств.

Группы узлов и кос.

Прямое произведение групп. Теорема о строении конечно определенной абелевой группы.

Коммутаторы и коммутанты. Нильпотентные и разрешимые группы.

Свободные группы. Уравнения и системы уравнений в группах. Неразрешимые и NP-трудные алгоритмические проблемы для уравнений в группах.

Тема 3. Кольца и многочлены.

Понятие кольца. Ассоциативные и коммутативные кольца. Кольца Ли.
Гомоморфизмы колец.
Подкольца и идеалы. Факторкольца. Теорема о гомоморфизме для колец.
Кольца с единицей. Делители нуля. Области целостности.
Кольца главных идеалов.
Евклидовы кольца.
Прямое произведение колец.
Сумма и прямая сумма идеалов. Разложение кольца в прямую сумму идеалов.
Неразложимые и простые элементы колец. Факториальные кольца.
Кольца многочленов. Корни многочленов. Кратные и простые корни.
Производная многочлена.
Многочлена от нескольких переменных.
Нетеровы кольца. Теорема Д. Гильберта.

Тема 4. Поля и многочлены над ними.

Поле, подполе, простое подполе.
Характеристика поля. Связь с полями вычетов.
Расширения полей. Конечно порожденные и простые расширения.
Расширения конечной степени (конечные расширения).
Теорема о башне полей (конечные расширения).
Алгебраические над подполем элементы. Алгебраические расширения.
Теорема о башне полей (алгебраические расширения).
Алгебраически замкнутые поля. Алгебраическое замыкание поля.
Вложение областей целостности в поля (поля отношений).
Евклидовость кольца многочленов над полем, деление с остатком.
НОД и НОК многочленов.
Алгоритм Евклида для многочленов над полем.
Факториальность кольца многочленов над полем.
Многочлены над факториальным кольцом. Лемма Гаусса о произведении примитивных многочленов.
Многочлены над кольцом целых чисел и над полем рациональных чисел.
Корни многочленов над полями. Теорема о "символическом присоединении".
Неприводимые многочлены над полями комплексных и действительных чисел.

Тема 5. Конечные поля и многочлены над ними.

Существование и единственность поля с примарным числом элементов.
Теорема о цикличности мультипликативной группы конечного поля. Примитивные элементы, их число.
Существование над конечным полем неприводимого многочлена произвольной степени.
Формула обращения Мебиуса. Число унитарных неприводимых над конечным полем F многочленов степени n.
Примитивные многочлены и их число.
Использование в современной криптографии неприводимых и примитивных многочленов над конечными полями (Россия, США).

Тема 6. Элементы эллиптической криптографии.

Алгебраические кривые на евклидовой плоскости. Квадратичные кривые (квадрики, коники). Сложение точек, его свойства.

Кубические кривые, 2-местная операция сложения точек, ее свойства.

Понятие о проективном пространстве.

Проективная плоскость. Алгебраические кривые на проективной плоскости.

Особые и неособые кубические кривые. Форма Вейерштрасса.

Эллиптические кривые, свойства операции сложения точек на них.

Группа точек на эллиптической кривой.

Понятие об эллиптических функциях. Функция Вейерштрасса. Параметризация эллиптической кривой над полем комплексных чисел.

Эллиптические кривые над полем рациональных чисел, рациональные и целочисленные точки на них.

Эллиптические кривые над конечными полями.

Тема 7. Вычислительные алгоритмы в алгебре и теории чисел.

Проверка чисел и многочленов на простоту. Числа Мерсенна.

Факторизация П. Ферма и факторные базы.

Тест Рабина - Миллера.

Ро-метод Полларда.

Метод цепных дробей.

Метод квадратичного решета.

Тест простоты на базе эллиптических кривых.

Разложение натуральных чисел на множители с использованием эллиптических кривых.

Решение проблемы равенства и проблемы изоморфизма для конечно определенных абелевых групп.

Решение проблемы сопряженности для групп кос.

Алгоритмические проблемы для групп с условием малого налегания (сокращения).

Тема 8. Методы теории чисел и комбинаторной теории групп в современной криптографии.

"Рюкзачная" криптосистема.

Криптосистема RSA.

Дискретной логарифмирование.

Криптосистемы на эллиптических кривых.

Криптосистемы на базе групп, заданных образующими и определяющими соотношениями.

Протокол Anschel-Anschel-Goldfeld выработки общего секретного ключа на базе коммутаторов элементов групп.

Протокол Ko -- Lee -- Cheon -- Han -- Kang -- Park выработки общего секретного ключа на базе проблемы сопряженности для группы кос.

Протокол Wang -- Cao -- Okamoto -- Shao выработки общего секретного ключа на базе некоммутативного моноида.

Протокол Сидельникова В. М. -- Черепнева М. А. -- Ященко В. Ю на базе некоммутативных полугрупп.

Протокол Stickel на базе конечной (периодической) некоммутативной группы.

Протоколы, базирующиеся на групповых автоморфизмах и эндоморфизмах: протокол Mahalanobis, протокол Habeeb -- Kahrobaei -- Koupparis -- Shpilrain.

Протоколы аутентификации, основанные на некоторых "трудных" алгоритмических проблемах теории групп: протокол Романькова -- Григорьева -- Шпильрайна, протокол Шпильрайна -- Ушакова, протокол Мегрелишвили -- Джинджихадзе.

Криптосистема Росошека.

5. 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 (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.

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:

– для формирования текстов материалов для промежуточной и текущей аттестации – программы Microsoft Office, издательская система MikTex;

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

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

а) основная литература

1. Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2002. 480 с.
2. ГОСТ 34.12-2015. Информационная технология, Криптографическая защита информации. Блочные шифры. Москва. Стандартинформ. 2015.
3. ГОСТ 34.13-2015. Информационная технология, Криптографическая защита информации. Режимы работы блочных шифров. Москва. Стандартинформ. 2015.
4. ГОСТ 34.11-2012. Информационная технология, Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Москва. Стандартинформ. 2012.
5. ГОСТ 34.10-2012. Информационная технология, Криптографическая защита информации. Функция хэширования. Москва. Стандартинформ. 2012.
6. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. М.: Научное издательство "ТВП". 2001. 254 с.
7. Ноден П. Алгебраическая алгоритмика / П. Ноден, К. Китте. М.: Мир. 1999. 720 с.
8. Ростовцев А. Алгебраические основы криптографии / А. Ростовцев. СПб.: НПО "Мир и семья", ООО "Интерлайн". 2000. 354 с.

б) дополнительная литература

1. Романьков В.А. Введение в криптографию. Курс лекций / В.А. Романьков. - М.: ФОРУМ, 2012. - 240 с.
2. Кукина Е.Г. Сборник задач и упражнений по криптографии / Е.Г. Кукина, В.А. Романьков, Омск, Изд-во. ОГУ им. Ф.М. Достоевского, 2013. 148 с.
3. Введение в криптографию: новые математические дисциплины / под ред. В. В. Ященко, СПб., Питер, 2001, 287с.
4. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин. М.: Издательский дом "Академия", 2009.
5. Чмора А. Современная прикладная криптография / А.Л. Чмора. М.: Гелиос АРВ, 2002. 256 с.
6. Хенк К.А. ван Тилборг. Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2005. 465 с.
7. Зензин О.С. Стандарт криптографической защиты AES. Конечные поля / О.С. Зензин, М.А. Иванов. КУДИЦ-ОБРАЗ, 2003.
8. Столлингс В. Криптография и защита сетей. Принципы и практика.-- 2-е изд. М.: Гелиос АРВ, 2001.
9. Саломаа А. Криптография с открытым ключом. М: Мир, 1996.
10. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. М.: Высшая школа, 1999.
11. Ростовцев А.Г. Введение в криптографию с открытым ключом / А.Г. Ростовцев, Е.Б. Маховенко. Санкт-Петербург. НПО "Мир и семья". ООО "Интерлайн", 2001. 336 с.
12. Маховенко Е.Б. Теоретическая криптография / Е.Б. Маховенко, А.Г. Ростовцев. Санкт-Петербург. АНО НПО "Профессионал". ООО "Интерлайн", 2004.
13. Мао В. Современная криптография. Теория и практика / В. Мао. М.: Издательский дом "Вильямс", 2005. 768 с.
14. Харин Ю.С. Математические и компьютерные основы криптологии / Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Минск: ООО "Новое знание", 2003. 382 с.
15. Шнайер Б. Прикладная криптография / Б. Шнайер. М.: Триумф, 2002. 816 с.
16. Под ред. Погорелова Б.А., Сачкова В.Н. Словарь криптографических терминов. М.: МЦНМО, 2006.

в) ресурсы сети «Интернет»

1.Электронные каталоги НБ ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержат библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках.

2. Личный кабинет (http://lib.uniyar.ac.ru/opac/bk_login.php) возможность получения on-line доступа к списку выданной в автоматизированном режиме литературы, просмотра и копирования электронных версий изданий сотрудников университета (учеб. и метод. пособия, тексты лекций и т.д.) Для работы в «Личном кабинете» необходимо зайти на сайт Научной библиотеки ЯрГУ с любой точки, имеющей доступ в Internet, в пункт меню *«Электронный каталог»*; пройти процедуру авторизации, выбрав вкладку *«Авторизация»*, и заполнить представленные поля информации.

3.Электронная библиотека учебных материалов ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

4.Электронный архив ЯрГУ

(http://elar.uniyar.ac.ru/jspui/community-list) представляет собой коллекцию полнотекстовых электронных публикаций в области научных исследований. База данных предназначена для использования в учебных и научных целях, облегчая доступ к информации о научных работах и их содержанию.

5. Электронная картотека «Книгообеспеченность»

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

раскрывает учебный фонд научной библиотеки ЯрГУ, предоставляет оперативную информацию о состоянии книгообеспеченности дисциплин основной и дополнительной литературой, а также цикла дисциплин и специальностей. Электронная картотека «Книгообеспеченность» доступна в сети университета и через Личный кабинет.

Русскоязычные электронные ресурсы (внешние)

1. Научная электронная библиотека (НЭБ) (http://elibrary.ru) – это крупнейший российский информационный портал, содержащий рефераты и полные тексты более 12 млн. научных статей и публикаций. **ЯрГУ выписывает в электронном виде 66 журналов,** более 2 500 наименований журналов на английском и русском языках находятся в свободном доступе. Для работы с полными текстами необходимо зарегистрироваться. Доступ к полным текстам журналов в сети университета.

2. Электронная библиотека диссертаций Российской государственной библиотеки (http://diss.rsl.ru) содержит более 580 000 полных текстов диссертаций и авторефератов. Доступ осуществляется в сети университета.

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, 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) :

Зав. кафедрой компьютерной безопасности и математических методов обработки информации, д.ф.-м.н. Дурнев В.Г

Приложение №1 к 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

Вопросы к зачету (2 семестр)

Тема 1. Базовые понятия теории чисел, теории множеств и теории алгоритмов.

Отношение делимости для натуральных и целых чисел. Деление с остатком.

Простые и составные числа. Основная теорема арифметики.

НОД и НОК системы целых чисел. Алгоритм Евклида, оценка его сложности. Коэффициенты Безу. Взаимно простые числа. Функция Л. Эйлера.

Распределение простых чисел в ряду натуральных чисел. Теорема Л. Эйлера. Асимптотический закон распределения простых чисел. Теоремы П.Л. Чебышева и Ж. Адамара - Ш.-Ж. Валле-Пуссена.

Сложность проблемы проверки числа на простоту. Тесты простоты и алгоритмы.

Сравнения по натуральному модулю. Квадратичные вычеты и невычеты. Квадратичный закон взаимности.

Цепные дроби, подходящие дроби. Теорема Ж.-Л. Лагранжа.

Диофантовы уравнения. 10-ая проблема Д. Гильберта. Уравнение Пелля и метод цепных дробей.

Математическое уточнение интуитивного понятия алгоритма - машины Тьюринга и частично рекурсивные функции.

Рекурсивные, рекурсивно перечислимые и диофантовы множества.

Временная и емкостная оценки сложности выполнения алгоритма.

Сложность описания (задания) алгоритма.

Теоретико-числовые функции. Мультипликативные функции.

Сумматорные функции. Функция Мебиуса и формула обращения.

Тема 2. Полугруппы, моноиды и группы.

Алгебраические операции. Группоиды. Гомоморфизмы и изоморфизмы группоидов.

Полугруппы. Нейтральные элементы, моноиды. Гомоморфизмы и изоморфизмы полугрупп и моноидов. Задание полугрупп и моноидов образующими и определяющими соотношениями. Алгоритмические проблемы для конечно определенных полугрупп и моноидов. Теорема А.А. Маркова - Э. Поста.

Обратимые элементы, группы. Задание групп образующими и определяющими соотношениями. Алгоритмические проблемы для конечно определенных групп, фундаментальные проблемы М. Дэна. Теоремы П.С. Новикова и С.И. Адяна.

Подгруппы, нормальные подгруппы и факторгруппы. Гомоморфизмы и изоморфизмы групп. Теоремы о гомоморфизмах.

Группы подстановок. Теорема Кэли.

Действие группы на множестве, орбиты элементов и стабилизаторы.

Фундаментальные группы топологических пространств.

Группы узлов и кос.

Прямое произведение групп. Теорема о строении конечно определенной абелевой группы.

Коммутаторы и коммутанты. Нильпотентные и разрешимые группы.

Свободные группы. Уравнения и системы уравнений в группах. Неразрешимые и NP-трудные алгоритмические проблемы для уравнений в группах.

Тема 3. Кольца и многочлены.

Понятие кольца. Ассоциативные и коммутативные кольца. Кольца Ли.

Гомоморфизмы колец.

Подкольца и идеалы. Факторкольца. Теорема о гомоморфизме для колец.

Кольца с единицей. Делители нуля. Области целостности.

Кольца главных идеалов.

Евклидовы кольца.

Прямое произведение колец.

Прямая сумма идеалов. Разложение кольца в прямую сумму идеалов.

Неразложимые и простые элементы колец. Факториальные кольца.

Кольца многочленов. Корни многочленов. Кратные и простые корни.

Производная многочлена.

Многочлена от нескольких переменных.

Нетеровы кольца. Теорема Д. Гильберта.

Тема 4. Поля и многочлены над ними.

Поле, подполе, простое подполе.

Характеристика поля. Связь с полями вычетов.

Расширения полей. Конечно порожденные и простые расширения.

Расширения конечной степени (конечные расширения).

Теорема о башне полей (конечные расширения).

Алгебраические над подполем элементы. Алгебраические расширения.

Теорема о башне полей (алгебраические расширения).

Алгебраически замкнутые поля. Алгебраическое замыкание поля.

Вложение областей целостности в поля (поля отношений).

Евклидовость кольца многочленов над полем, деление с остатком.

НОД и НОК многочленов.

Алгоритм Евклида для многочленов над полем.

Факториальность кольца многочленов над полем.

Многочлены над кольцом целых чисел и полем рациональных чисел.

Лемма Гаусса о произведении примитивных многочленов.

Корни многочленов над полями. Теорема о "символическом присоединении".

Неприводимые многочлены над полями комплексных и действительных чисел.

Тема 5. Конечные поля и многочлены над ними.

Существование и единственность поля с примарным числом элементов.

Теорема о цикличности мультипликативной группы конечного поля. Примитивные элементы, их число.

Существование над конечным полем неприводимого многочлена произвольной степени.

Формула обращения Мебиуса. Число унитарных неприводимых над конечным полем F многочленов степени n.

Примитивные многочлены и их число.

Использование в современной криптографии неприводимых и примитивных многочленов над конечными полями (Россия, США).

Тема 6. Элементы эллиптической криптографии.

Алгебраические кривые на евклидовой плоскости. Квадратичные кривые (квадрики, коники). Сложение точек, его свойства.

Кубические кривые, 2-местная операция сложения точек, ее свойства.

Понятие о проективном пространстве.

Проективная плоскость. Алгебраические кривые на проективной плоскости.

Особые и неособые кубические кривые. Форма Вейерштрасса.

Эллиптические кривые, сложение точек на них. Группа точек эллиптической кривой.

Понятие об эллиптических функциях. Функция Вейерштрасса. Параметризация эллиптической кривой над полем комплексных чисел.

Эллиптические кривые над полем рациональных чисел, рациональные и целочисленные точки на них.

Эллиптические кривые над конечными полями.

Тема 7. Вычислительные алгоритмы в алгебре и теории чисел.

Проверка чисел и многочленов на простоту. Числа Мерсенна.

Факторизация П. Ферма и факторные базы.

Тест Рабина - Миллера.

Ро-метод Полларда.

Метод цепных дробей.

Метод квадратичного решета.

Тест простоты на базе эллиптических кривых.

Разложение натуральных чисел на множители с использованием эллиптических кривых.

Решение проблемы равенства и проблемы изоморфизма для конечно определенных абелевых групп.

Решение проблемы сопряженности для групп кос.

Алгоритмические проблемы для групп с условием малого налегания (сокращения).

Тема 8. Методы теории чисел и комбинаторной теории групп в современной криптографии.

"Рюкзачная" криптосистема.

Криптосистема RSA.

Дискретной логарифмирование.

Криптосистемы на эллиптических кривых.

Криптосистемы на базе групп, заданных образующими и определяющими соотношениями.

Протокол Anschel-Anschel-Goldfeld выработки общего секретного ключа на базе коммутаторов элементов групп.

Протокол Ko -- Lee -- Cheon -- Han -- Kang -- Park выработки общего секретного ключа на базе проблемы сопряженности для группы кос.

Протокол Wang -- Cao -- Okamoto -- Shao выработки общего секретного ключа на базе некоммутативного моноида.

Протокол Сидельникова В. М. -- Черепнева М. А. -- Ященко В. Ю на базе некоммутативных полугрупп.

Протокол Stickel на базе конечной (периодической) некоммутативной группы.

Протоколы, базирующиеся на групповых автоморфизмах и эндоморфизмах: протокол Mahalanobis, протокол Habeeb -- Kahrobaei -- Koupparis -- Shpilrain.

Протоколы аутентификации, основанные на некоторых "трудных" алгоритмических проблемах теории групп: протокол Романькова -- Григорьева -- Шпильрайна, протокол Шпильрайна -- Ушакова, протокол Мегрелишвили -- Джинджихадзе.

Криптосистема Росошека

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

Методические указания для аспирантов по освоению дисциплины

В связи с тем, что по дисциплине не предусмотрены практические занятия, а лекций лишь 8 часов, основным видом работы становится самостоятельное изучение теоретического материала. По наиболее трудным темам проводятся консультации. В процессе изучения дисциплины необходима регулярная работа с рекомендованной литературой, систематическое изучение теоретического материала.

Для проверки усвоения теоретического материала в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса-собеседования на лекциях и консультациях по теоретическому материалу.

Аспиранты сдают зачет во втором семестре. Зачет проводится в форме собеседования на основании списка вопросов к зачету, который охватывает полностью всю программу дисциплины.

Учебно-методическое обеспечение
самостоятельной работы аспирантов по дисциплине

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