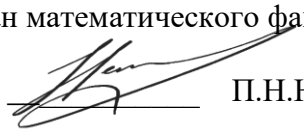
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета



П.Н.Нестеров

«18» мая 2021 г.

Рабочая программа дисциплины
«Диофантова криптография»

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 «Диофантова криптография» 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 овладение базовыми понятиями и методами теории диофантовых уравнений, ознакомление с их применениями в области обеспечения информационной безопасности, установление существования алгоритмически неразрешимых проблем в теории диофантовых уравнений и значение этого фундаментального факта для алгоритмической практики, компьютерных наук и защиты информации.

2. Место дисциплины в структуре программы аспирантуры

Дисциплина «Диофантова криптография» является дисциплиной по выбору вариативной части. Она играет важную роль для общематематической и общепрофессиональной подготовки специалиста. При ее изучении используются знания, полученные при изучении таких математических дисциплин, как “Алгебра”, "Теория чисел", "Дискретная математика", "Топология", "Математическая логика" и "Теория алгоритмов

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:

Общепрофессиональными компетенции

- способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1);
- способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности (ОПК-2);

Профессиональные компетенции:

- способностью разрабатывать защитные механизмы и средства обеспечения информационной безопасности, осуществлять их настройку, регулировку, восстановление работоспособности (ПК-2);

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 формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1)	**Знать:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3). **Уметь:** - обоснованно классифицировать защищаемую информацию по видам тайны и степени конфиденциальности (У-7.1); - обоснованно классифицировать и оценивать угрозы информационной безопасности компьютерных систем (У-7.2). **Владеть:** - специальной профессиональной терминологией в области	**Знает:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3).	**Знает:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3). **Умеет:** - обоснованно классифицировать защищаемую информацию по видам тайны и степени конфиденциальности (У-7.1); - обоснованно классифицировать и оценивать угрозы информационной безопасности компьютерных систем (У-7.2).	**Знает:** - методологию научного познания в области физико-математических и технических наук (З-7.1); - научные подходы к обеспечению информационной безопасности и характеристику ее составляющих (З-7.2); - научную классификацию источников и угроз информационной безопасности (З-7.3). **Умеет:** - обоснованно классифицировать защищаемую информацию по видам тайны и степени конфиденциальности (У-7.1); - обоснованно классифицировать и оценивать угрозы информационной безопасности компьютерных систем (У-7.2). **Владеет:** - специальной профессиональной терминологией в области

	информационной безопасности (В-7.1); - научно обоснованными методами обеспечения информационной безопасности и построения систем защиты информации от несанкционированного доступа (В-7.2).			информационной безопасности (В-7.1); - научно обоснованными методами обеспечения информационной безопасности и построения систем защиты информации от несанкционированного доступа (В-7.2).
способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности (ОПК-2)	**Знать:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3). **Уметь:** - применять философско-методологические принципы и установки для решения частных научных задач (У-8.1); - применять систему математических моделей и методов при осуществлении	**Знает:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3).	**Знает:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3). **Умеет:** - применять философско-методологические принципы и установки для решения частных научных задач (У-8.1); - применять систему	**Знает:** - принципы и инструментарий научно-исследовательской деятельности в области обеспечения информационной безопасности (З-8.1); - средства и методы научного исследования (З-8.2); - математический аппарат и инструментарий обработки результатов исследований (З-8.3). **Умеет:** - применять философско-методологические принципы и установки для решения частных научных задач (У-8.1); - применять систему математических моделей и методов при осуществлении

	научно-исследовательской деятельности (У-8.2); - оценивать достоверность результатов, полученных в ходе исследований (У-8.3). **Владеть:** - методами проведения теоретических исследований (В-8.1); - методами планирования и проведения экспериментов (В-8.2); - методами использования средств обработки результатов исследований (В-8.3).		математических моделей и методов при осуществлении научно-исследовательской деятельности (У-8.2); - оценивать достоверность результатов, полученных в ходе исследований (У-8.3).	научно-исследовательской деятельности (У-8.2); - оценивать достоверность результатов, полученных в ходе исследований (У-8.3). **Владеет:** - методами проведения теоретических исследований (В-8.1); - методами планирования и проведения экспериментов (В-8.2);- методами использования средств обработки результатов исследований (В-8.3).
Способностью разрабатывать защитные механизмы и средства обеспечения информационной безопасности, осуществлять их настройку, регулирование, восстановление работоспособности (ПК-2)	**Знать:** защитные механизмы и средства обеспечения информационной безопасности. **Уметь:** осуществлять настройку, регулирование и восстановление работоспособности защитных механизмов и средств обеспечения информационной безопасности. **Владеть:** навыками настройки, регулирования и	**Знает:** защитные механизмы и средства обеспечения информационной безопасности, основные понятия, результаты и методы теории диофантовых уравнений, их современные применения для построения криптографических протоколов.	**Знает:** защитные механизмы и средства обеспечения информационной безопасности, основные понятия, результаты и методы теории диофантовых уравнений, их современные применения для построения криптографических протоколов. **Умеет:** осуществлять настройку,	**Знает:** защитные механизмы и средства обеспечения информационной безопасности, основные понятия, результаты и методы теории диофантовых уравнений, их современные применения для построения криптографических протоколов. **Умеет:** осуществлять настройку, регулирование и восстановление

	восстановления работоспособности защитных механизмов и средств обеспечения информационной безопасности.		регулирование и восстановление работоспособности защитных механизмов и средств обеспечения информационной безопасности.	работоспособности защитных механизмов и средств обеспечения информационной безопасности. **Владеет:** навыками настройки, регулирования и восстановления работоспособности защитных механизмов и средств обеспечения информационной безопасности.

4. Объем, структура и содержание дисциплины

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

Дисциплина изучается в течение четвертого 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	Диофантовы уравнения. Десятая проблема Д. Гильберта.	4	1				5	
2	Частично рекурсивные, рекурсивные и примитивно рекурсивные функции.	4	1				5	
3	Примитивно рекурсивные и рекурсивные предикаты, отношения и множества, операции над ними.	4				0,5	5	Собеседование на консультации
4	Задание функций и предикатов.	4	1				5	

5	Нумерация.	4					5	
6	Рекурсивно перечислимые и диофантовы множества, отношения и предикаты.	4	1				5	
7	Теорема М. Дэвиса - Дж. Робинсон - Х. Путнам - Ю.В. Матиясевича о совпадении классов рекурсивно перечислимых и диофантовых множеств.	4	1				5	
8	Арифметизация теории диофантовых уравнений.	4				0,5	5	Собеседование на консультации
9	Диофантовы уравнения и криптография.	4	1				5	
10	Элементы теории групп - базовые сведений по теории групп.	4					5	
11	Задание групп образующими и определяющими соотношениями.	4	1				5	
12	Фундаментальные проблемы М. Дэна.	4				0,5	5	Собеседование на консультации
13	Свободные группы.	4					5	
14	Преобразования Тице.	4					5	
15	Фундаментальные группы топологических пространств.	4					5	
16	Задание факторгрупп и подгрупп.	4	1				5	
17	Факторгруппы по коммутанту.	4					5	
18	Свободное произведение групп и свободное произведение групп с объединенной подгруппой. HNN-расширения групп.	4				0,5	5	Собеседование на консультации
19	Некоторые криптографические протоколы на группах.	4	1				8	
		4						Зачет
	Всего		**8**			**2**	**98**	

Содержание разделов дисциплины.

Тема 1. Диофантовы уравнения. Десятая проблема Д. Гильберта.
Общее понятие диофантового уравнения, связь между решениями в целых числах и решениями в натуральных числах.
Линейные диофантовы уравнения и их системы.
Диофантовы уравнения второй степени с двумя неизвестными. Уравнение Пелля, существование натурального решения, общий вид его решения в натуральных и целых числах. Нахождение наименьшего натурального решения методом цепных дробей.
Теорема Лагранжа о разложении квадратичной иррациональности в цепную дробь.
Теорема Туэ.
Десятая проблема Д. Гильберта.
Проблемы Д. Гильберта и их историческое значение для развития математики в XX веке.

Тема 2. Частично рекурсивные, рекурсивные и примитивно рекурсивные функции.
Тезис Черча.
Примитивная рекурсивность теоретико-числовых функций.
Операции суммирования и мультиплицирования.

Тема 3. Примитивно рекурсивные и рекурсивные предикаты, отношения и множества, операции над ними.
Соотношения между классами примитивно рекурсивных, общерекурсивных и частично рекурсивных функций.

Тема 4. Задание функций и предикатов.
Задание функций кусочными схемами.
Ограниченный оператор минимизации.
Примитивная рекурсивность функций, связанных с каноническим представлением натуральных чисел и с делением с остатком.

Тема 5. Нумерация.
Канторовские нумерационные функции, их примитивная рекурсивность.
Примитивная рекурсивность функции Геделя.

Тема 6. Рекурсивно перечислимые и диофантовы множества, отношения и предикаты.
Рекурсивно перечислимые множества, отношения и предикаты, операции над ними.
Теорема о графике функции. Ее следствия.
Диофантовы множества, отношения и предикаты. Связь диофантовости с рекурсивной перечислимостью. Гипотеза М. Дэвиса.

Тема 7. Теорема М. Дэвиса - Дж. Робинсон - Х. Путнам - Ю.В. Матиясевича о совпадении классов рекурсивно перечислимых и диофантовых множеств.

Тема 8. Арифметизация теории диофантовых уравнений.
Нумерация уравнений. Построение универсального диофантового уравнения и множества.

Тема 9. Диофантовы уравнения и криптография.
Диофантовы функции с нерекурсивной областью значений как "претенденты" на роль односторонних функций (В.А. Романьков).

Тема 10. Элементы теории групп - базовые сведений по теории групп.

Двуместные алгебраические операции. Группоиды, гомоморфизмы и изоморфизмы группоидов. Ассоциативность, полугруппы. Обобщенная ассоциативность, натуральные степени элемента полугруппы. Нейтральные элементы, моноиды. Обратимые элементы, группы. Целочисленные степени элемента группы. Примеры групп: симметрические группы, фундаментальные группы многообразий, группы узлов, группы кос, группы движений метрических пространств, матричные группы, аддитивные и мультипликативные группы колец с единицей и полей, группы вычетов. Подгруппы, строение подгруппы, порожденной множеством элементов группы. Циклические подгруппы. Образующие элементы группы. Нормальные подгруппы, строение нормальной подгруппы, порожденной множеством элементов группы. Факторгруппы, теоремы о гомоморфизмах. Порядок элемента группы. Циклические группы. Сопряженные элементы. Коммутаторы, коммутант, ряды коммутантов. Абелевы, нильпотентные и разрешимые группы.

Тема 11. Задание групп образующими и определяющими соотношениями.
Групповые алфавиты, элементарные преобразования. Построение группы, заданной образующими и определяющими соотношениями. Представление (задание, генетический код) группы. Некоторые подходы к нахождению задания группы. Примеры заданий групп. Задания для групп узлов, групп кос, симметрических и знакопеременных групп.

Тема 12. Фундаментальные проблемы М. Дэна.
Конечно порожденные и конечно определенные задания групп. Проблема тождества для групп. Проблема сопряженности для групп. Проблема изоморфизма для групп. Массовые (алгоритмические) проблемы, их положительное и отрицательное решение. Общая проблема о распознавании групповых свойств по заданию группы. Понятие о фундаментальных результатах П.С. Новикова и С.И. Адяна.

Тема 13. Свободные группы.
Определение свободных групп, различные способы задания их элементов: классы эквивалентности и несократимые слова. Решение проблемы тождества для свободных групп. Решение проблемы сопряженности для свободных групп. Подгруппы свободных групп. Убывающие цепочки подгрупп свободных групп и теоремы об их пересечении. Хопфовость свободных групп. Финитная аппроксимируемость свободных групп.

Тема 14. Преобразования Тице.
Преобразования Тице T1, T2, T3 и T4. Изоморфность групп, задания которых получаются друг из друга преобразованиями Тице. Теорема, о возможности перейти с помощью преобразований Тице от одного задания группы к любому другому ее заданию. Построение инвариантов групп.
Граф Кэли группы. Построение графа Кэли по заданию группы образующими и определяющими соотношениями. Граф Кэли свободной группы, некоторых симметрических групп. Связь между группами и графами.

Тема 15. Фундаментальные группы топологических пространств.
Определение топологического пространства, примеры. Непрерывные отображения топологических пространств. Непрерывные пути и петли в топологическом пространстве. Умножение путей. Гомотопическая эквивалентность путей. Фундаментальная группа топологического пространства. Группы узлов. Группы кос. Связь между непрерывными отображениями топологических пространств и гомоморфизмами их фундаментальных групп. Гомеоморфизмы топологических пространств и изоморфизмы фундаментальных групп.

Тема 16. Задание факторгрупп и подгрупп.

Нахождение задания факторгруппы по заданию исходной группы и ее нормальной подгруппы. Вербальные подгруппы и приведенные свободные группы. Тождества в группах, многообразия групп. Абелевы, нильпотентные и разрешимые тождества и многообразия. Метод Рейдемейстера - Шрейера для нахождения задания подгруппы по заданию исходной группы. Система представителей правых смежных классов группы по подгруппе. Переписывающий процесс Рейдемейстера - Шрейера. Шрейеровская система представителей правых смежных классов группы по подгруппе.

Тема 17. Факторгруппы по коммутанту.

Специальные системы образующих для конечно порожденных подгрупп свободных абелевых групп конечного ранга. Прямое произведение групп. Теорема о строении конечно порожденных абелевых групп. Тест для изоморфизма групп. Факторгруппы групп узлов.

Свободное дифференциальное исчисление. Групповое кольцо. Свободное дифференциальное исчисление Фокса. Частные производные Фокса в свободной группе. Основная формула свободного дифференциального исчисления. Матрица Александера. Элементарные идеалы, их цепочки. Полиномы узлов.

Тема 18. Свободное произведение групп и свободное произведение групп с объединенной подгруппой. HNN-расширения групп.

Определение свободного произведения групп. Каноническая форма элементов свободного произведения групп. Подгруппы свободного произведения групп, понятие о теореме А.Г. Куроша. Решение алгоритмических проблем для свободного произведения групп. Определение свободного произведения групп с объединенной подгруппой, каноническая форма элементов. Понятие о теореме Зейферта - ван Кампена**.** HNN-расширение группы, каноническая форма элементов, лемма Британа.

Тема 19. Некоторые криптографические протоколы на группах.

Интерпретация диофантовых уравнений в свободных нильпотентных и свободных разрешимых группах.

Протокол аутентификации В.А. Романькова на базе свободной метабелевой группы ранга два.

Протокол Anschel-Anschel-Goldfeld: начальная установка - группа G (платформа протокола). Выбор Алисой и Бобом открытых наборов элементов группы G и секретных элементов. Выработка общего секретного ключа - коммутатора элементов.

Протокол Ko-Lee-Cheon-Han-Kang-Park: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) группу G - платформу протокола, два конечных подмножества попарно коммутирующих элементов и элемент g группы G.

Выработка материалов для создания общего секретного ключа: Алиса и Боб "случайным образом" выбирают секретные элементы.

Выработка общего секретного ключа.

Протокол Wang-Cao-Okamoto-Shao: начальная установка: корреспонденты Алиса и Боб выбирают (открыто) некоммутативный моноид G - платформу протокола, элемент g из G и обратимый элемент x в G.

Выработка материалов для создания общего секретного ключа.

Выработка общего секретного ключа.

Протокол Сидельников В.М.-Черепнев М.А.-Ященко В.Ю.: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) полугруппу (моноид, группу) G - платформу протокола, два конечных подмножества попарно коммутирующих элементов и элемент g в G.

Выработка материалов для создания общего секретного ключа.

Выработка общего секретного ключа.

Протокол Stickel: начальная установка - G - неабелева конечная группа и два ее коммутирующих элемента. Выработка материалов для создания общего секретного ключа. Выработка общего секретного ключа.

Протоколы базируются на групповых автоморфизмах и эндоморфизмах.
Протокол Mahalanobis: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) группу G - платформу протокола, два конечных подмножества попарно коммутирующих элементов группы автоморфизмов Aut (G) и элемент g в G.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.

Протокол Mahalanobis: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) группу G -- платформу протокола, два конечных подмножества попарно коммутирующих элементов группы автоморфизмов Aut (G) и элемент g в G.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.

Протокол Habeeb-Kahrobaei-Koupparis-Shpilrain: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) полугруппу или группу G - платформу протокола, ее автоморфизм и элемент. Выработка материалов для создания общего секретного ключа. Выработка общего секретного ключа.

Протоколы аутентификации, основанные на некоторых алгоритмических проблемах теории групп, которые можно отнести к сложным алгоритмическим проблемам.

Протокол Романькова-Григорьева-Шпильрайна: начальная установка - открыто выбирается бесконечная "эффективно заданная" группа G - платформа протокола с разрешимой проблемой равенства, но с алгоритмически неразрешимой проблемой эндоморфной сводимости.
Выбор "Системой" ("Доказывающим") открытого элемента g в G.
Выбор "Доказывающим" "Секретного" ключа - эндоморфизм группы G.
Построение "Открытого" ключа.
Раунд аутентификации.

Протокол Шпильрайна-Ушакова на базе проблемы скрученной сопряженности для групп.Начальная установка: открыто выбирается группа G - платформа протокола, два ее эндоморфизма и элемент w в G.
"Секретный"' ключ "Доказывающего" и "Открытый" ключ.
Раунд аутентификации.

Протокол Мегрелишвили-Джинджихадзе: начальная установка - корреспонденты Алиса и Боб выбирают (открыто) векторное пространство V над полем F - платформу протокола, квадратную матрицу A и вектор v в V.
Выработка материалов для создания общего секретного ключа.
Выработка общего секретного ключа.
Система Росошека: сообщения -- элементы группового (полугруппового) кольца K[G] группы (полугруппы) G с коэффициентами из кольца K.
Начальная установка: Алиса выбирает эндоморфизмы.
Открытый ключ Алисы - эндоморфизмы, обратимый элемент x группового кольца K[G] и элемент. Шифрование: зашифрование, расшифрование.

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

В процессе обучения используются следующие образовательные технологии:

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:

– 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. Адян С.И., Дурнев В.Г. Алгоритмические проблемы для групп и полугрупп //Успехи матем. наук. 2000. Том 55.С.3-94.

2. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи.М.: Мир, 1979.
3. Дурнев, В. Г., Элементы теории алгоритмов : учеб. пособие для вузов / В. Г. Дурнев ; Яросл. гос. ун-т, Ярославль, ЯрГУ, 2008, 247с
4. Катленд Н. Вычислимость. Введение в теорию рекурсивных функций. М.: Мир, 1983.
5. Линдон Р., Шупп П. Комбинаторная теория групп. М.: Мир. 1980.
6. Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп. М.: Наука. 1974.
7. Маканин Г.С. Уравнения в свободной группе // Изв. АН СССР. Сер. мат. 1982. Т. 46. № 6. С.1199-1273.
8. Матиясевич Ю.В. Диофантовость перечислимых множеств // ДАН СССР. - 1970. - Том 130, № 3. - С. 495-498.
9. Матиясевич Ю.В. Десятая проблема Гильберта. М.: Наука, 1993.
10. Мальцев, А.И. Алгоритмы и рекурсивные функции / А.И. Мальцев. М.: Наука, 1986.
11. Новиков П.С. Об алгоритмической неразрешимости проблемы тождества теории групп // Докл. АН СССР. 1952. Т. 85. № 4. С. 709-712.
12. Новиков П.С. Об алгоритмической неразрешимости проблемы тождества слов в теории групп // М.: Наука. 1955. Труды МИАН. Т. 44.
13. Разборов А.А. О системах уравнений в свободной группе // Изв. АН СССР. Сер. мат. 1984. Т. 48. № 4.
14. Репин Н.Н. Уравнения с одной неизвестной в нильпотентной группе // Мат. заметки. 1983. Т. 34. № 2. С.201-206.
15. Романьков В.А. О неразрешимости проблемы эндоморфной сводимости в свободных нильпотентных группах и в свободных кольцах // Алгебра и логика. 1977. Т. 16. № 4. С.457-471.
16. Романьков В.А. Об уравнениях в свободных метабелевых группах // Сиб. матем. журн. 1979. Т. 20. № 3. С.671-673.
17. Романьков В.А. Алгебраическая криптография. Омск. Изд-во. Ом. гос. ун-та., 2013. 136 с.
18. Сидельников В.М., Черепнев М.А., Ященко В.В. Системы открытого распределения ключей на основе некоммутативных полугрупп // Докл. РАН. 1993. Том 332. № 5. С. 566 -- 567.
19. Шпильрайн В.Э. Об уравнениях в группах вида F_n(R) // Алгоритмические проблемы теории групп и полугрупп. Тула. ТГПИ. 1990. С.164-183.
20. Diffie W., Hellman M.E. New directions in cryptography // IEEE Transaction Information Theory. 1976. Vol. 22. № 6. P. 644 - 654.
21. Ko K.H., Lee S.J., Cheon J.H. New public-key cryptosistem using braid groups // Advances in cryptology -- CRYPTO 2000 (Santa Barbara, CA). Lecture Notes in Comput. Sci. 1880. 2000. P. 166 - 183. Springer, Berlin.
22. Miller C.F. III. Some connection between Hilbert's 10th problem and the theory of groups // Word Probl. Decis. Probl. Group Theory. Amsterdam. London. P. 483-506.
23. Myasnikov A., Shpilrain V., Ushakov A. Group-based cryptography. Advances courses in Math. CRM, Barselona. Basel-Berlin-New York: Birkhauser Verlag, 2008. 183 p.
24. Myasnikov A., Shpilrain V., Ushakov A. Non-commutative cryptography and complexity of group-theoretic problems // Amer. Math. Soc. Surveys and Monographs. Providence R.I.: Amer. Math. Soc., 2001. 385 p.
25. Rivest R.L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosistems // Comm. ACM. 1978. Vol. 21. № 2. P. 120 - 126.

б) дополнительная литература

26. Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1983.
27. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. М.: Наука, 1982.
28. Коксетер Г.С.М., Мозер У.О.Дж. Порождающие элементы и определяющие соотношения дискретных групп. М.: Наука. 1980.
29. Курош А.Г. Теория групп. М.: Наука. 1967
30. Новиков П.С., Адян С.И. Определяющие соотношения и проблема тождества для свободных периодических групп нечетного порядка // Изв. АН СССР. Сер. матем. 1968. Т. 32. № 4. С. 971-979.
31. Churh A. An unsolvable problem of elementary number theory // Amer. J. Math. 1936. V. 58. № 2. P. 345-363.
32. Churh A. A note on the Entscheidungs-problem // J. Symbolic Logic. 1936. V. 1. № 1. P. 40-41.
33. Turing A.M. On computable numbers, with an application to the Entscheidugsproblem // Proceedings of London Mathematical Society. Ser. 2. 1936. V. 42. № 3,4. P. 230-265.

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 к №1 к рабочей программе дисциплины
«Диофантова криптографияи»

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

Домашние задания по теме № 2 "**Частично рекурсивные, рекурсивные и примитивно рекурсивные функции."**

Задания для самостоятельного решения № 1 - 15 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 3 "**Примитивно рекурсивные и рекурсивные предикаты, отношения и множества, операции над ними."**

Задания для самостоятельного решения № 16 - 30 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 4 "**Задание функций и предикатов."**

Задания для самостоятельного решения № 31 - 44 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с

Домашние задания по теме № 5 "**Нумерация."**

Задания для самостоятельного решения № 31 - 44 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с

Домашние задания по теме № **6. Рекурсивно перечислимые и диофантовы множества, отношения и предикаты.**

Задания для самостоятельного решения № 16 - 30 из параграфа 1 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Задания для самостоятельного решения № 1 - 48 из параграфа 3 части III сборника задач Лавров И.А. Задачи по теории множеств, математической логики и теории алгоритмов / И.А. Лавров, Л.Л. Максимова. М.: Наука. 1984. 287 с.

Домашние задания по теме № 10. "**Элементы теории групп - базовые сведений по теории групп."**

Задания для самостоятельного решения № 1.2.1 - 1.2.4 и № 1.2.6 - 1.2.12 из параграфа 1 главы I монографии Каргаполов М.И. Основы теории групп / М.И. Каргаполов, Ю.И. Мерзляков. М.: Наука. 1982. 288 с.

Задания для самостоятельного решения № 2.1.1 - 2.1.4 и №2.2.3 - 2.2.7 из параграфа 2 главы I монографии Каргаполов М.И. Основы теории групп / М.И. Каргаполов, Ю.И. Мерзляков. М.: Наука. 1982. 288 с.

Задания для самостоятельного решения № 2.4.1 - 2.4.10, №2.5.1 - 2.5.5 и №2.5.8 - 2.5.13 из параграфа 2 главы I монографии Каргаполов М.И. Основы теории групп / М.И. Каргаполов, Ю.И. Мерзляков. М.: Наука. 1982. 288 с.

Задания для самостоятельного решения № 3.1.2 - 3.1.7 и №3.2.4 - 3.2.11 из параграфа 3 главы I монографии Каргаполов М.И. Основы теории групп / М.И. Каргаполов, Ю.И. Мерзляков. М.: Наука. 1982. 288 с.

Домашние задания по теме № 11 **"Задание групп образующими и определяющими соотношениями."**

Задания для самостоятельного решения № 1 - 14 из параграфа 1.1 и № 1-21 параграфа 1.2 главы I монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № 12 **"Фундаментальные проблемы М. Дэна."**

Задания для самостоятельного решения № 1 - 16 из параграфа 1.3 главы I монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № 13 **"Свободные группы."**

Задания для самостоятельного решения № 1 - 31 из параграфа 1.4 главы I и № 1 - 37 из параграфа 2.4 главы II монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № 14 **"Преобразования Тице."**

Задания для самостоятельного решения № 1 - 16 из параграфа 1.5 главы I монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Задания для самостоятельного решения № 1 - 16 из параграфа 1.6 главы I монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № **16. "Задание факторгрупп и подгрупп."**

Задания для самостоятельного решения № 1 - 8 из параграфа 2.1 и № 1 - 40 из параграфа 2.2 № 1 - 26 из параграфа 2.4 главы II монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № **17. "Факторгруппы по коммутанту."**

Задания для самостоятельного решения № 1 - 21 из параграфа 3.3 главы III монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Задания для самостоятельного решения № 1 - 16 из параграфа 3.4 главы III монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № **18. "Свободное произведение групп и свободное произведение групп с объединенной подгруппой. HNN-расширения групп."**

Задания для самостоятельного решения № 1 - 34 из параграфа 4.1 и № 1 - 49 из параграфа 4.2 главы IV монографии Магнус В. Комбинаторная теория групп / В. Магнус, А. Каррас, Д. Солитэр. М.: Наука. 1974. 456 с.

Домашние задания по теме № **19. "Некоторые криптографические протоколы на группах."**

Выполнить программную реализацию одного из криптопротоколов.

1.1 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету по дисциплине
"Диофантова криптография "
(4 семестр)

Тема 1. Диофантовы уравнения. Десятая проблема Д. Гильберта.
1. Общее понятие диофантового уравнения, связь между решениями в целых числах и решениями в натуральных числах.
2. Линейные диофантовы уравнения и их системы.
3. Диофантовы уравнения второй степени с двумя неизвестными.
4. Уравнение Пелля, существование натурального решения, общий вид его решения в натуральных и целых числах. Нахождение наименьшего натурального решения методом цепных дробей.
5. Теорема Лагранжа о разложении квадратичной иррациональности в цепную дробь.
6. Теорема Туэ.
7. Десятая проблема Д. Гильберта.
8. Проблемы Д. Гильберта и их историческое значение для развития математики в XX веке.

Тема 2. Частично рекурсивные, рекурсивные и примитивно рекурсивные функции.
1. Тезис Черча.
2. Примитивная рекурсивность теоретико-числовых функций.
3. Операции суммирования и мультиплицирования.

Тема 3. Примитивно рекурсивные и рекурсивные предикаты, отношения и множества, операции над ними.
1. Соотношения между классами примитивно рекурсивных, общерекурсивных и частично рекурсивных функций.

Тема 4. Задание функций и предикатов.
1. Задание функций кусочными схемами.
2. Ограниченный оператор минимизации.
3. Примитивная рекурсивность функций, связанных с каноническим представлением натуральных чисел и с делением с остатком.

Тема 5. Нумерация.
1. Канторовские нумерационные функции, их примитивная рекурсивность.
2. Примитивная рекурсивность функции Геделя.

Тема 6. Рекурсивно перечислимые и диофантовы множества, отношения и предикаты.
1. Рекурсивно перечислимые множества, отношения и предикаты, операции над ними.
2. Теорема о графике функции. Ее следствия.
3. Диофантовы множества, отношения и предикаты. Связь диофантовости с рекурсивной перечислимостью. Гипотеза М. Дэвиса.

Тема 7. Теорема М. Дэвиса - Дж. Робинсон - Х. Путнам - Ю.В. Матиясевича о совпадении классов рекурсивно перечислимых и диофантовых множеств.
1. Теорема М. Дэвиса - Дж. Робинсон - Х. Путнам - Ю.В. Матиясевича о совпадении классов рекурсивно перечислимых и диофантовых множеств.

Тема 8. Арифметизация теории диофантовых уравнений.
1. Нумерация уравнений. Построение универсального диофантового уравнения и множества.

Тема 9. Диофантовы уравнения и криптография.
1. Диофантовы функции с нерекурсивной областью значений как "претенденты" на роль односторонних функций (В.А. Романьков).

Тема 10. Элементы теории групп - базовые сведений по теории групп.
1. Двуместные алгебраические операции. Группоиды, гомоморфизмы и изоморфизмы группоидов.
2. Ассоциативность, полугруппы. Обобщенная ассоциативность, натуральные степени элемента полугруппы.
3. Нейтральные элементы, моноиды. Обратимые элементы, группы. Целочисленные степени элемента группы.
4. Примеры групп: симметрические группы, фундаментальные группы многообразий, группы узлов, группы кос, группы движений метрических пространств, матричные группы, аддитивные и мультипликативные группы колец с единицей и полей, группы вычетов.
5. Подгруппы, строение подгруппы, порожденной множеством элементов группы. Циклические подгруппы. Образующие элементы группы.
6. Нормальные подгруппы, строение нормальной подгруппы, порожденной множеством элементов группы.
7. Факторгруппы, теоремы о гомоморфизмах.
8. Порядок элемента группы. Циклические группы.
9. Сопряженные элементы. Коммутаторы, коммутант, ряды коммутантов.
10. Абелевы, нильпотентные и разрешимые группы.

Тема 11. Задание групп образующими и определяющими соотношениями.
1. Групповые алфавиты, элементарные преобразования. Построение группы, заданной образующими и определяющими соотношениями.
2. Представление (задание, генетический код) группы. Некоторые подходы к нахождению задания группы.
3. Примеры заданий групп. Задания для групп узлов, групп кос, симметрических и знакопеременных групп.

Тема 12. Фундаментальные проблемы М. Дэна.
1. Конечно порожденные и конечно определенные задания групп.
2. Проблема тождества для групп.
3. Проблема сопряженности для групп.
4. Проблема изоморфизма для групп.
5. Массовые (алгоритмические) проблемы, их положительное и отрицательное решение.
6. Общая проблема о распознавании групповых свойств по заданию группы. Понятие о фундаментальных результатах П.С. Новикова и С.И. Адяна.

Тема 13. Свободные группы.
1. Определение свободных групп, различные способы задания их элементов: классы эквивалентности и несократимые слова.

2. Решение проблемы тождества для свободных групп.
3. Решение проблемы сопряженности для свободных групп.
4. Подгруппы свободных групп. Убывающие цепочки подгрупп свободных групп и теоремы об их пересечении.
5. Хопфовость свободных групп.
6. Финитная аппроксимируемость свободных групп.

Тема 14. Преобразования Тице.
1. Преобразования Тице T1, T2, T3 и T4. Изоморфность групп, задания которых получаются друг из друга преобразованиями Тице.
2. Теорема, о возможности перейти с помощью преобразований Тице от одного задания группы к любому другому ее заданию. Построение инвариантов групп.
3. Граф Кэли группы. Построение графа Кэли по заданию группы образующими и определяющими соотношениями.
4. Граф Кэли свободной группы, некоторых симметрических групп.
5. Связь между группами и графами.

Тема 15. Фундаментальные группы топологических пространств.
1. Определение топологического пространства, примеры. Непрерывные отображения топологических пространств.
2. Непрерывные пути и петли в топологическом пространстве. Умножение путей. Гомотопическая эквивалентность путей.
3. Фундаментальная группа топологического пространства. Группы узлов. Группы кос.
4. Связь между непрерывными отображениями топологических пространств и гомоморфизмами их фундаментальных групп. Гомеоморфизмы топологических пространств и изоморфизмы фундаментальных групп.

Тема 16. Задание факторгрупп и подгрупп.
1. Нахождение задания факторгруппы по заданию исходной группы и ее нормальной подгруппы.
2. Вербальные подгруппы и приведенные свободные группы.
3.Тождества в группах, многообразия групп. Абелевы, нильпотентные и разрешимые тождества и многообразия.
4. Метод Рейдемейстера - Шрейера для нахождения задания подгруппы по заданию исходной группы. Система представителей правых смежных классов группы по подгруппе.
5. Переписывающий процесс Рейдемейстера - Шрейера. Шрейеровская система представителей правых смежных классов группы по подгруппе.

Тема 17. Факторгруппы по коммутанту.
1. Специальные системы образующих для конечно порожденных подгрупп свободных абелевых групп конечного ранга.
2. Прямое произведение групп. Теорема о строении конечно порожденных абелевых групп.
3. Тест для изоморфизма групп. Факторгруппы групп узлов.
4. Свободное дифференциальное исчисление. Групповое кольцо. Свободное дифференциальное исчисление Фокса. Частные производные Фокса в свободной группе. Основная формула свободного дифференциального исчисления.
5. Матрица Александера. Элементарные идеалы, их цепочки. Полиномы узлов.

Тема 18. Свободное произведение групп и свободное произведение групп с объединенной подгруппой. HNN-расширения групп.

1. Определение свободного произведения групп. Каноническая форма элементов свободного произведения групп.
2. Подгруппы свободного произведения групп, понятие о теореме А.Г. Куроша.
3. Решение алгоритмических проблем для свободного произведения групп.
4. Определение свободного произведения групп с объединенной подгруппой, каноническая форма элементов.
5. Понятие о теореме Зейферта - ван Кампена**.**
6. HNN-расширение группы, каноническая форма элементов, лемма Британа.

Тема 19. Некоторые криптографические протоколы на группах.
1. Интерпретация диофантовых уравнений в свободных нильпотентных и свободных разрешимых группах.
2. Протокол аутентификации В.А. Романькова на базе свободной метабелевой группы ранга два.
3. Протокол Anschel-Anschel-Goldfeld: начальная установка, выработка общего секретного ключа - коммутатора элементов.
4. Протокол Ko-Lee-Cheon-Han-Kang-Park: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.
5. Протокол Wang-Cao-Okamoto-Shao: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.
6. Протокол Сидельников В.М.-Черепнев М.А.-Ященко В.Ю.: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.
7. Протокол Stickel: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.

8. Протоколы базируются на групповых автоморфизмах и эндоморфизмах.
9. Протокол Mahalanobis: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.
10. Протокол Mahalanobis: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.
11. Протокол Habeeb-Kahrobaei-Koupparis-Shpilrain: начальная установка, выработка материалов для создания общего секретного ключа, выработка общего секретного ключа.

12. Протоколы аутентификации, основанные на некоторых алгоритмических проблемах теории групп, которые можно отнести к сложным алгоритмическим проблемам.
13. Протокол Романькова-Григорьева-Шпильрайна: начальная установка, выбор "Системой" ("Доказывающим") открытого ключа, выбор "Доказывающим" "Секретного" ключа. Построение "Открытого" ключа. Раунд аутентификации.

14. Протокол Шпильрайна-Ушакова на базе проблемы скрученной сопряженности для групп. Начальная установка, "Секретный'" ключ "Доказывающего" и "Открытый" ключ. Раунд аутентификации.
15. Протокол Мегрелишвили-Джинджихадзе: начальная установка. Выработка материалов для создания общего секретного ключа. Выработка общего секретного ключа.
16. Система Росошека на базе группового (полугруппового) кольца K[G] группы (полугруппы) G с коэффициентами из кольца K. Начальная установка. Открытый ключ. Шифрование: зашифрование, расшифрование.

Приложение № 2 к рабочей программе дисциплины
«Диофантова криптография»

Методические указания для аспирантов по освоению дисциплины

Для успешного освоения дисциплины важно самостоятельное изучение теоретического материала, решение достаточно большого набора задач, прежде всего, самостоятельно в качестве домашних заданий, так как "Учебный план" из аудиторных занятий включает лишь 8 часов лекций. Примеры решения задач разбираются на лекциях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения задач – помочь усвоить фундаментальные понятия, методы и теоремы теории диофантовых уравнений, комбинаторной теории групп и диофантовой криптографии, научиться применять их в криптографии. Для решения задач необходимо не только знать, но и понимать теоретический материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с рекомендованной литературой.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями в течение обучения проводятся мероприятия текущей аттестации в виде устного опроса на занятиях и консультациях и разбору некоторых заданий для самостоятельной работы.

Аспиранты сдают зачет в четвертом семестре. Зачет проводится на основании выполнения домашних заданий и 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.