МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт математики и механики им. Н.И. Лобачевского

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
проф. Таюрский Д.А.
"___"_____20___ г.

Программа дисциплины

Дополнительные главы прикладной алгебры

Направление подготовки: 01.04.01 - Математика
Профиль подготовки: Анализ на многообразиях
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Тронин С.Н. (кафедра Интеллектуальные технологии поиска, Высшая школа информационных технологий и интеллектуальных систем), Serge.Tronin@kpfu.ru

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-1	способностью к интенсивной научно-исследовательской работе
ПК-9	способностью различным образом представлять и адаптировать математические знания с учетом уровня аудитории

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

Основы алгебраической техники, используемой в алгебраической криптографии как разделе прикладной алгебры.

Должен уметь:

Конструировать новые криптографические протоколы на алгебраических платформах, и анализировать уже известные.

Должен владеть:

Основами алгебры, применяемой в криптографии, и основами криптографии с открытым ключом.

Должен демонстрировать способность и готовность:

-применять методы абстрактной алгебры в приложениях (теории кодирования и криптографии).

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.5 Дисциплины (модули)" основной профессиональной образовательной программы 01.04.01 "Математика (Анализ на многообразиях)" и относится к дисциплинам по выбору.
Осваивается на 1 курсе в 2 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) на 144 часа(ов).

Контактная работа - 42 часа(ов), в том числе лекции - 14 часа(ов), практические занятия - 28 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 66 часа(ов).

Контроль (зачёт / экзамен) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен во 2 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Основные принципы криптографии с открытым ключом	2	3	3	0	12

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Криптография с открытым ключом на платформах коммутативных групп	2	4	10	0	12
3.	Тема 3. Криптография с открытым ключом на платформах некоммутативных групп	2	4	8	0	24
4.	Тема 4. Криптография на кольцевых платформах. Криптосистема NTRU и постквантовая криптография.	2	3	7	0	18
	Итого		14	28	0	66

4.2 Содержание дисциплины (модуля)

Тема 1. Основные принципы криптографии с открытым ключом

Криптография (в частности алгебраическая криптография) как раздел прикладной алгебры. Краткий обзор криптографии с открытым ключом. Основные принципы криптографии с открытым ключом. Секретный ключ и открытый ключ как функция открытого ключа. Шифры, подписи, протоколы формирования общего секретного ключа.

Тема 2. Криптография с открытым ключом на платформах коммутативных групп

Криптография с открытым ключом на платформах коммутативных групп. Задача о дискретном логарифме в коммутативной группе. Аналоги протоколов Эль-Гамаля и DSA на платформе коммутативных групп. Группы точек эллиптических кривых над конечными полями. Эллиптическая криптография. Подписи ECDSA и государственный стандарт цифровой подписи РФ.

Тема 3. Криптография с открытым ключом на платформах некоммутативных групп

Криптография с открытым ключом на платформах некоммутативных групп. Протоколы формирования общего секретного ключа. Протокол Anshel-Anshel-Goldfeld. Методы построения подходящих для криптографии групп. Задания групп образующими и соотношениями. Метод перечисления смежных классов. Группы кос как подходящая алгебраическая платформа. Задача о сопрягающем элементе в группах кос.

Тема 4. Криптография на кольцевых платформах. Криптосистема NTRU и постквантовая криптография.

Криптография на кольцевых платформах. Протоколы формирования общего секретного ключа. Решетки и способы их задания. Задача о нахождении кратчайшего вектора решетки как вычислительно сложная задача. Метод шифрования NTRU (Nth TRUncated polynomial ring) и постквантовая криптография. Обобщения NTRU, использующие кольца матриц и групповые кольца.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);
- критерии оценивания сформированности компетенций;
- механизм формирования оценки по дисциплине (модулю);
- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;
- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Заметки по теории кодирования - www.mccme.ru/~anromash/courses/coding-theory-05-2016.pdf

Курс лекций по дискретному анализу - http://vyalyy.narod.ru/da2-090419.pdf

Курс лекций по прикладной алгебре - http://www.machinelearning.ru/wiki/index.php?title=%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%B

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	Излагается раздел прикладной алгебры, имеющий непосредственное отношение к криптографии. В частности, речь идет о тех разделах криптографии, которые связаны с теорией групп, теорией колец и теорией решеток. У многих протоколов классической криптографии с открытым ключом существуют аналоги, использующие вместо чисел элементы групп или колец. Особое место занимают протоколы шифрования, основанные на сложных задачах из теории решеток. Эти задачи, по-видимому, невозможно эффективно решить с помощью ожидаемых квантовых компьютеров.
практические занятия	Чтобы понимать, как используется в криптографии теория групп (в частности, групп точек эллиптических кривых), необходимо частично повторить, а частично изучить ряд разделов алгебры. Для более качественного освоения материала необходимо потренироваться на конкретных примерах. Темы практических занятий - группы точек эллиптических кривых над конечными полями, и задание произвольных групп с помощью образующих и определяющих соотношений. Что позволяет лучше понять, что же такое группы кос, важне для приложений.

Вид работ	Методические рекомендации
самостоя-тельная работа	Чтобы понимать, как используется в криптографии теория групп (в частности, групп точек эллиптических кривых), необходимо частично повторить, а частично изучить ряд разделов алгебры. В частности, необходимо изучить (повторить) теорию свободных групп, и задание групп образующими и определяющими соотношениями. В частности, таким способом можно определить и исследовать группы кос. Этот материал частично выностися на самостоятельное изучение.
экзамен	1. Общая схема шифрования с открытым ключом. Односторонние функции. Общая схема цифровой подписи. 2. Пример криптосистемы с открытым ключом: RSA. 3. Пример: криптосистема Эль-Гамаля. 4. Пример: цифровая подпись DSA. 5. Аналоги Эль-Гамаля и DSA для коммутативных групп. 6. Группы точек эллиптических кривых над конечными полями. 7. Цифровая подпись ECDSA. 8. ГОСТ цифровой подписи РФ. 9. Криптография на некоммутативных группах. Протоколы формирования общего секретного ключа. Протокол Anshel-Anshel-Goldfeld. 10. Задание групп образующими и соотношениями. Метод перечисления смежных классов. 11. Группы кос. 12. Метод шифрования NTRU.

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

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

Компьютерный класс.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 01.04.01 "Математика" и магистерской программе "Анализ на многообразиях".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.5 Дополнительные главы прикладной алгебры

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 01.04.01 - Математика
Профиль подготовки: Анализ на многообразиях
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

Основная литература:

1. Чикрин Д.Е. Теория информации и кодирования: курс лекций / Д.Е. Чикрин. Казань: Казанский университет, 2013. 116 с http://dspace.kpfu.ru/xmlui/bitstream/handle/net/21172/50_000337.pdf

2. Основы информатики и защиты информации [Электронный ресурс] : Учеб.пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2013. - 183 с
http://znanium.com/bookread.php?book=415501

3.Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб.пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с http://znanium.com/bookread.php?book=441493

4. Применко, Эдуард Андреевич.
Алгебраические основы криптографии : учебное пособие для студентов высших учебных заведений, обучающихся по направлениям ВПО 010400 'Прикладная математика и информатика' и 010300 'Фундаментальная информатика и информационные технологии' / Э. А. Применко .? Москва : URSS : [ЛИБРОКОМ, 2013] .? 283 с. : ил. ; 21 .? (Основы защиты информации) .? Библиогр.: с. 282-283 (18 назв.) .? ISBN 978-5-382-01455-5 ((в обл.)) .

Дополнительная литература:

1. Практическая криптография: алгоритмы и их программирование [Электронный ресурс] / Аграновский А.В., Хади Р.А. - М. : СОЛОН-ПРЕСС, 2009. - http://www.studentlibrary.ru/book/ISBN5980030026.html

2. Теория кодирования. [Электронный ресурс] / Сидельников В.М. - М. : ФИЗМАТЛИТ, 2008. - http://www.studentlibrary.ru/book/ISBN9785922109437.html

3. Универсальное кодирование. Теория и алгоритмы [Электронный ресурс] / Штарьков Ю.М. - М. : ФИЗМАТЛИТ, 2013. - http://www.studentlibrary.ru/book/ISBN9785922115179.html

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.5 Дополнительные главы прикладной алгебры

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 01.04.01 - Математика
Профиль подготовки: Анализ на многообразиях
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2017

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.