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

Криптография

Направление подготовки: 02.03.01 - Математика и компьютерные науки
Профиль подготовки: Математическое и компьютерное моделирование
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2016

Содержание

Программу дисциплины разработал(а)(и) доцент, к.н. Насрутдинов М.Ф. (кафедра компьютерной математики и информатики, отделение педагогического образования), Marat.Nasrutdinov@kpfu.ru ; 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
ОПК-4	способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

Основные идеи, на которых основана современная криптография. Классические примеры шифров, цифровых подписей, и некоторых других криптографических протоколов. Основные идеи, на которых основана эллиптическая криптография. Примеры затемненных цифровых подписей. Первичные сведения о постквантовой криптографии.

Должен уметь:

Строить новые примеры шифров и цифровых подписей, исходя из общих конструкций, изложенных в лекционном курсе. Самостоятельно изучать новые сведения по криптографии, используя специальную литературу.

Должен владеть:

Методикой анализа корректности построения шифров и цифровых подписей, а также оценки их криптостойкости.

Должен демонстрировать способность и готовность:

Расширять область своих знаний в криптографии и криптоанализе.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.3 Дисциплины (модули)" основной профессиональной образовательной программы 02.03.01 "Математика и компьютерные науки (Математическое и компьютерное моделирование)" и относится к дисциплинам по выбору.
Осваивается на 4 курсе в 7 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 2 зачетных(ые) единиц(ы) на 72 часа(ов).

Контактная работа - 36 часа(ов), в том числе лекции - 18 часа(ов), практические занятия - 18 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 36 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 7 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. Введение. Общая					

характеристика криптографии и криптоанализа.

7	4	2	0	4	

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
2.	Тема 2. Криптогпрафия с открытым ключом. Криптосистема RSA.	7	4	4	0	6
3.	Тема 3. Криптосистемы, основанные на сложности проблемы дискретного логарифма.	7	4	4	0	10
4.	Тема 4. Затемненные цифровые подписи. Электронные деньги.	7	2	4	0	6
5.	Тема 5. Эллиптическая криптография.	7	2	2	0	6
6.	Тема 6. Постквантовая криптогафия. Криптосистема NTRU	7	2	2	0	4
	Итого		18	18	0	36

4.2 Содержание дисциплины (модуля)

Тема 1. Введение. Общая характеристика криптографии и криптоанализа.

Общая характеристика криптографии и криптоанализа. История возникновения. Способы дешифровки простейших шифров. Шифры и секретные ключи. Атаки на шифры. Примеры шифров. Потоковые и блочные шифры. DES и AES. Проблема распределения ключей. Режимы шифрования. Одноключевая криптография и криптография с открытым ключом.

Тема 2. Криптогпрафия с открытым ключом. Криптосистема RSA.

Криптография с открытым ключом. Односторонние функции. Криптографические хэш-функции. Криптосистема RSA, и ее криптостойкость. Алгоритм создания открытого и секретного ключей. Шифрование и расшифрование. Корректность схемы RSA. Примеры. Использование китайской теоремы об остатках для ускорения расшифрования. Общее определение цифровых подписей. Цифровая подпись RSA.

Тема 3. Криптосистемы, основанные на сложности проблемы дискретного логарифма.

Проблема дискретного логарифма. Протокол Диффи-Хеллмана, алгоритм шифрования и расшифрования. Применение для решения проблемы распределения ключей. Криптосистема Эль-Гамаля, и построенные по тому же принципу цифровые подписи, криптографическая стойкость криптосистемы. Цифровые подписи DSA и Шнорра.

Тема 4. Затемненные цифровые подписи. Электронные деньги.

Затемненные (слепые) цифровые подписи. Затемненные подписи RSA и Эль-Гамаля. Общая схема электронных денег, использующая трех участников: Банк, Покупатель, Продавец. Анализ транзакций. Требования, предъявляемые к электронным деньгам. Частично затемненные подписи. Финансовая криптография и электронное голосование.

Тема 5. Эллиптическая криптография.

Эллиптическая криптография. Эллиптические кривые. Группа точек эллиптической кривой. Свойства групп точек эллиптических кривых. Оценка порядка группы. Цифровая подпись ECDSA. Криптографическая стойкость.Государственный стандарт цифровых подписей. Простейшее шифрование: протокол Менезеса-Вэнстона.

Тема 6. Постквантовая криптогафия. Криптосистема NTRU

Проблемы криптостойкости и квантовые компьютеры. Криптографическая система с открытым ключом NTRU. Кольца усечённых многочленов. Генерация открытого ключа. Шифрование и расшифрование. Стойкость к атакам: полный перебор, встреча посередине, атака на основе множественной передачи сообщения, атака на основе решётки, атака на основе подобранного шифротекста. Криптография на кольцевых платформах.

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)

Лекториум - https://www.lektorium.tv

Математическая криптография - http://cryptography.ru

Национальный Открытый Университет "ИНТУИТ" - http://www.intuit.ru

Энциклопедия теоретической и прикладной криптографии - http://cryptowiki.net/index.php?title=Main_Page

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

Вид работ	Методические рекомендации
лекции	Студентам необходимо посещать лекции и вести конспект лекций вслед за изложением материала преподавателем. Рекомендуется прорабатывать конспект в течение дня после лекции и просматривать его вновь накануне следующей лекции. В случае обнаружения ошибок или возникновения вопросов по предыдущему материалу необходимо обратиться к преподавателю.
практические занятия	Подготовку к семинарам (практическим занятиям, лабораторным занятиям) следует начинать с изучения теоретической части (лекционного материала) с определениями основных понятий, выводом формул и доказательством теорем. Особое внимание следует обращать на определения основных понятий и формулировки основных теорем. Необходимо подробно разбирать примеры, которые поясняют определения и теоремы. При разборе теорем необходимо учитывать, что все предположения теоремы должны использоваться в доказательстве ее утверждения, при этом необходимо понимать, в каком месте доказательства используется то или иное предположение теоремы.
самостоя-тельная работа	Самостоятельная работа студентов состоит из двух основных частей - проработка лекционного материала и выполнения домашних заданий. Для освоения теоретического и практического материала, в случае, когда конспектов оказывается недостаточным, или для более детальной проработки отдельных тем рекомендуется использовать литературу, указанную в соответствующем разделе. Все возникающие вопросы рекомендуется заранее четко сформулировать и впоследствии обсудить с преподавателем.
зачет	Залогом успешной сдачи зачета является работа в течение всего семестра. Основным источником подготовки к зачету является конспект лекций. Правильно составленный конспект лекций содержит тот оптимальный объем информации, на основе которого студент сможет представить себе весь учебный материал. В ходе подготовки к зачету студентам необходимо обращать внимание не только на уровень запоминания, но и на степень понимания основных понятий.

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.

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 02.03.01 "Математика и компьютерные науки" и профилю подготовки "Математическое и компьютерное моделирование".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.3 Криптография

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 02.03.01 - Математика и компьютерные науки
Профиль подготовки: Математическое и компьютерное моделирование
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2016

Основная литература:

1. Чикрин Д.Е. Теория информации и кодирования [Текст: электронный ресурс] : курс лекций / Д. Е. Чикрин ; Казан. (Приволж.) федер. ун-т, Высш. шк. информ. технологий и информ. систем, Каф. автоном. робототехн. систем .- Электронные данные (1 файл: 4,46 Мб) .- (Казань : Казанский федеральный университет, 2013) .- Загл. с экрана .- Для 3-го семестра .- Режим доступа: открытый .- URL:http://libweb.kpfu.ru/ebooks/50-ITIS/50_000337.pdf

2. Баранова, Е. К. Основы информатики и защиты информации [Электронный ресурс] : Учеб. пособие / Е. К. Баранова. - М. : РИОР : ИНФРА-М, 2013. - 183 с. - (Высшее образование: Бакалавриат). - ISBN 978-5-369-01169-0 (РИОР), ISBN 978-5-16-006484-0 (ИНФРА-М). - Текст : электронный. - URL: http://znanium.com/catalog/product/415501

3. Кнауб, Л. В. 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. - ISBN 978-5-7638-2113-7. - Текст : электронный. - URL: http://znanium.com/catalog/product/441493

4. Аверченков В.И., Криптографические методы защиты информации / Аверченков В.И. - М. : ФЛИНТА, 2017. - 215 с. - ISBN 978-5-9765-2947-2 - Текст : электронный // ЭБС 'Консультант студента' : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785976529472.html

Дополнительная литература:

1. Аграновский А.В., Практическая криптография: алгоритмы и их программирование / Аграновский А.В., Хади Р.А. - М. : СОЛОН-ПРЕСС, 2009. - 256 с. - ISBN 5-98003-002-6 - Текст : электронный // ЭБС 'Консультант студента' : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN5980030026.html

2. Сидельников В.М., Теория кодирования. / Сидельников В.М. - М. : ФИЗМАТЛИТ, 2008. - 324 с. - ISBN 978-5-9221-0943-7 - Текст : электронный // ЭБС 'Консультант студента' : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785922109437.html

3. Штарьков Ю.М., Универсальное кодирование. Теория и алгоритмы / Штарьков Ю.М. - М. : ФИЗМАТЛИТ, 2013. - 288 с. - ISBN 978-5-9221-1517-9 - Текст : электронный // ЭБС 'Консультант студента' : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785922115179.html

4. Болелова Э.А., Информационный мир XXI века. Криптография - основа информационной безопасности / Болелова Э.А. - М. : Дашков и К, 2018. - 126 с. - ISBN 978-5-394-03031-4 - Текст : электронный // ЭБС 'Консультант студента' : [сайт]. - URL : http://www.studentlibrary.ru/book/ISBN9785394030314.html

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.ДВ.3 Криптография

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

Направление подготовки: 02.03.01 - Математика и компьютерные науки
Профиль подготовки: Математическое и компьютерное моделирование
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2016

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.