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

подписано электронно-цифровой подписью

Программа дисциплины

Криптография М1.ДВ.2

Направление подготовки: 010100.68 - Математика
Профиль подготовки: Алгебра
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Тронин С.Н.

Рецензент(ы):

Киндер М.И.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Арсланов М. М.
Протокол заседания кафедры No ___ от "____" _____ 201__г

Учебно-методическая комиссия Института математики и механики им. Н.И. Лобачевского :
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 81728715

Казань
2014

Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Тронин С.Н. Кафедра алгебры и математической логики отделение математики , Serge.Tronin@kpfu.ru

1. Цели освоения дисциплины

Необходимость в защите разнообразной информации возникает в современной жизни буквально на каждом шагу. В основе многих способов такой защиты лежат идеи и методы науки криптографии (или криптологии). Эта наука, крупнейшие достижения которой можно датировать серединой 20-го века, и особенно периодом после 1976 года, широко использует математические методы, в частности, методы современной теории чисел, алгебраической геометрии, теории сложности и т.д. Конечная цель курса - познакомить слушателей с самыми основами современной криптографии, и помочь им овладеть основными понятиями и принципами, лежащими в основе методов этой науки (не вдаваясь в излишние технические детали). Предполагается, что часть материала будет изучена слушателями самостоятельно, и по результатам этого изучения должны быть составлены подробные рефераты (или отчеты о проделанной работе).

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел " М1.ДВ.2 Общенаучный" основной образовательной программы 010100.68 Математика и относится к дисциплинам по выбору. Осваивается на 2 курсе, 3 семестр.

Данный курс предназначен для слушателей, которые имеют базовое математическое образование, в том числе прослушали курсы по элементарной теории чисел и вводный курс алгебры.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-10 (общекультурные компетенции)	умение находить, анализировать и контекстно обрабатывать информацию, в том числе относящуюся к новым областям знаний, непосредственно не связанным со сферой профессиональной деятельности
ПК-4 (профессиональные компетенции)	самостоятельный анализ физических аспектов в классических постановках математических задач
ПК-8 (профессиональные компетенции)	собственное видение прикладного аспекта в строгих математических формулировках

В результате освоения дисциплины студент:

1. должен знать:

Принципы, на которых основана современная математическая криптография. Важнейшие и типичные алгоритмы шифрования и цифровой подписи. Некоторое важные киптографические протоколы. Основы математического аппарата, используемого в современной криптографии.

2. должен уметь:

Студент должен уметь анализировать криптографические алгоритмы, и приспосабливать их к новым конкретным ситуациям, в которых они могут применяться. Студент должен уметь работать с литературой, и самсотоятельно находить и изучать новые криптографические алгоритмы и протоколы. Студент должен уметь проводить математические выкладки, необходимые для постоения и обоснования криптографических алгоритмов и протоколов.

3. должен владеть:

Студент должен владеть основами математических методов, используемых в современной криптографии.

4. должен демонстрировать способность и готовность:

основные идеи современной криптографии, прежде всего ? криптографии с открытым ключом, некоторые основные алгоритмы шифрования и генерации цифровых (электронных) подписей, а также некоторые важные криптографические протоколы.

4. должен демонстрировать способность и готовность:

применять полученные знания в конкретных ситуациях.

4. должен демонстрировать способность и готовность:

вычислительными навыками, необходимыми при решении простейших криптографических задач.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет зачетных(ые) единиц(ы) 72 часа(ов).

Форма промежуточного контроля дисциплины зачет в 3 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);

55-70 баллов - "удовлетворительно" (удов.);

54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. История криптографии. Исторические шифры.	3	1	2	0	0	устный опрос
2.	Тема 2. Блочные и потоковые шифры. Режимы шифрования.	3	2	2	0	0	устный опрос
3.	Тема 3. Математический аппарат: кольца вычетов, сравнения, и конечные поля.	3	3-5	2	4	0	контрольная работа домашнее задание

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
4.	Тема 4. Криптография с открытым ключом. Односторонние функции. Протокол Диффи-Хеллмана и идея цифровой подписи. Дискретный логарифм.	3	6-7	2	2	0	устный опрос
5.	Тема 5. Криптосистемы RSA, и Эль-Гамаля. Цифровые подписи Шнорра и DSA. Криптографические хэш-функции. Другие цифровые подписи.	3	8-10	2	4	0	реферат
6.	Тема 6. Слепые (затемненные) цифровые подписи. Электронные деньги.	3	11-12	2	2	0	устный опрос
7.	Тема 7. Эллиптическая криптография	3	13-14	2	2	0	домашнее задание
8.	Тема 8. Криптографические протоколы.	3	15-16	0	4	0	реферат
.	Тема . Итоговая форма контроля	3		0	0	0	зачет
	Итого			14	18	0	

4.2 Содержание дисциплины

Тема 1. История криптографии. Исторические шифры.

лекционное занятие (2 часа(ов)):

Шифры сдвига и шифры замены. Омофонические шифры. Частотный криптоанализ. Шифр Виженера. Клод Шеннон и абсолютно надежные шифры. Прицип Керкхоффа.

Тема 2. Блочные и потоковые шифры. Режимы шифрования.

лекционное занятие (2 часа(ов)):

Блоковые и потоковые шифры. Схема Фейстеля. Примеры блокоых шифров. Режимы шифрования.

Тема 3. Математический аппарат: кольца вычетов, сравнения, и конечные поля.

лекционное занятие (2 часа(ов)):

Кольца вычетов и конечные поля.

практическое занятие (4 часа(ов)):

Решение задач о сравнениях в кольцах вычетов, а также о конечных полях.

Тема 4. Криптография с открытым ключом. Односторонние функции. Протокол Диффи-Хеллмана и идея цифровой подписи. Дискретный логарифм.

лекционное занятие (2 часа(ов)):

Односторонние функции. Примеры односторонних функций. Протокол Диффи-Хеллмана и идея цифровой подписи.

практическое занятие (2 часа(ов)):

Дискретный логарифм. Метод: "Шаги младенца-шаги гиганта".

Тема 5. Криптосистемы RSA, и Эль-Гамаля. Цифровые подписи Шнорра и DSA. Криптографические хэш-функции. Другие цифровые подписи.

лекционное занятие (2 часа(ов)):

Криптосистемы RSA, и Эль-Гамаля. Цифровые подписи Шнорра и DSA. Криптографические хэш-функции.

практическое занятие (4 часа(ов)):

Обоснование RSA. Обоснование других цифровыхподписей. Самсотоятельный анализ некоторых других криптографических алгоритмов.

Тема 6. Слепые (затемненные) цифровые подписи. Электронные деньги.

лекционное занятие (2 часа(ов)):

Идея слепой цифровой подписи, основанной на RSA, и простейший протокол электронной платежной системы.

практическое занятие (2 часа(ов)):

Слепые подписи, основанные на других алгоритмах. Дальнейшая детализация протокола плтежной системы.

Тема 7. Эллиптическая криптография

лекционное занятие (2 часа(ов)):

Эллиптические кривые над конечными полями. Групповой закон на множестве точек элиптической кривой. Простейшие криптосистемы, использующие группы точек эллиптических кривых.

практическое занятие (2 часа(ов)):

Вычисление множеств точек конкретных эллиптических кривых, и группового закона на этих множествах.

Тема 8. Криптографические протоколы.

практическое занятие (4 часа(ов)):

Анализ протоколов обмена ключами, вручения бита, подбрасывания монеты по телефону, удаленного подписания контракта и т.п. Анализ некоторых протоколов доказательств с нулевым разглашением.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. История криптографии. Исторические шифры.	3	1	подготовка к устному опросу	2	устный опрос
2.	Тема 2. Блочные и потоковые шифры. Режимы шифрования.	3	2	подготовка к устному опросу	2	устный опрос
3.	Тема 3. Математический аппарат: кольца вычетов, сравнения, и конечные поля.	3	3-5	подготовка домашнего задания	5	домашнее задание
				подготовка к контрольной работе	5	контрольная работа

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
4.	Тема 4. Криптография с открытым ключом. Односторонние функции. Протокол Диффи-Хеллмана и идея цифровой подписи. Дискретный логарифм.	3	6-7	подготовка к устному опросу	2	устный опрос
5.	Тема 5. Криптосистемы RSA, и Эль-Гамаля. Цифровые подписи Шнорра и DSA. Криптографические хэш-функции. Другие цифровые подписи.	3	8-10	подготовка к реферату	10	реферат
6.	Тема 6. Слепые (затемненные) цифровые подписи. Электронные деньги.	3	11-12	подготовка к устному опросу	4	устный опрос
7.	Тема 7. Эллиптическая криптография	3	13-14	подготовка домашнего задания	5	домашнее задание
8.	Тема 8. Криптографические протоколы.	3	15-16	подготовка к реферату	5	реферат
	Итого				40	

5. Образовательные технологии, включая интерактивные формы обучения

Лекции, семинары, доклады на семинарах, рефераты, зачет. Самостоятельная работа с литературой, решение задач в процессе подготовки к докладам.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. История криптографии. Исторические шифры.

устный опрос , примерные вопросы:

Шифры сдвига и шифры замены. Омофонические шифры. Частотный криптоанализ. Шифр Виженера. Клод Шеннон и абсолютно надежные шифры. Прицип Керкхоффа.

Тема 2. Блочные и потоковые шифры. Режимы шифрования.

устный опрос , примерные вопросы:

Блоковые и потоковые шифры. Схема Фейстеля. Примеры блокоых шифров. Режимы шифрования.

Тема 3. Математический аппарат: кольца вычетов, сравнения, и конечные поля.

домашнее задание , примерные вопросы:

Кольца вычетов, необходимые сведения по теории чисел, и конечные поля

контрольная работа , примерные вопросы:

Решение сравнений, нахождение примитивных элементов и т.п.

Тема 4. Криптография с открытым ключом. Односторонние функции. Протокол Диффи-Хеллмана и идея цифровой подписи. Дискретный логарифм.

устный опрос , примерные вопросы:

Односторонние функции. Протокол Диффи-Хеллмана и идея цифровой подписи. Дискретный логарифм. Дискретный логарифм. Метод: "Шаги младенца-шаги гиганта".

Тема 5. Криптосистемы RSA, и Эль-Гамаля. Цифровые подписи Шнорра и DSA. Криптографические хэш-функции. Другие цифровые подписи.

реферат , примерные темы:

Криптосистемы RSA, и Эль-Гамаля. Цифровые подписи Шнорра и DSA. Криптографические хэш-функции. В качестве тем рефератов предлагаются конкретные цифровые подписи, не рассматиаемые на лекции.

Тема 6. Слепые (затемненные) цифровые подписи. Электронные деньги.

устный опрос , примерные вопросы:

Анализ протокола платжной системы.

Тема 7. Эллиптическая криптография

домашнее задание , примерные вопросы:

Основы теории эллиптических кривых над конечными полями. Простейшие криптосистемы на эллиптических кривых (ECDSA и т.п.)

Тема 8. Криптографические протоколы.

реферат , примерные темы:

Анализ протоколов обмена ключами, вручения бита, подбрасывания монеты по телефону, удаленного подписания контракта и т.п. Анализ некоторых протоколов доказательств с нулевым разглашением.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

Приложение 1. Билеты для зачета

Билет № 1

Одноключевая криптография. Поточные и блоковые (блочные) шифры. Абсолютно надежные шифры. Схема Фейстеля. Режимы шифрования. Принцип Керкхоффа.

Билет № 2

Односторонние функции. Односторонние функции с секретом (с ловушкой). Цифровая (электронная) подпись, использующая одностороннюю функцию. Примеры (гипотетические) односторонних функций.

Криптографические хэш-функции. Основные требования к криптографическим хэш-функциям.

Билет № 3

Протокол Диффи-Хеллмана для обмена ключами по открытому каналу связи. Аналог, использующий группу общего вида.

Билет № 4

Криптосистема RSA. Шифрование и цифровая подпись. Обоснование правильности дешифрования. Обоснование подписи.

Билет № 5

Криптосистема Эль-Гамаля. Шифрование и цифровая подпись. Обоснование подписи. Аналог криптосистемы Эль-Гамаля, использующий группу общего вида.

Билет № 6

Цифровая подпись DSA (DSS). Обоснование подписи. Аналог, использующий группу общего вида.

Билет № 7

Цифровая подпись Шнорра и ее модификация для смарт-карт. Обоснование подписи.

Билет № 8

Слепые (затемненные) подписи и электронные платежные системы.

Билет № 9

Группа точек эллиптической кривой над конечным полем.

Билет № 10

Криптография на эллиптических кривых. Цифровая подпись ECDSA. Шифрование по методу Менезеса-Вэнстона.

Билет № 11

Задача о дискретном логарифме. Метод "шаги младенца - шаги гиганта".

Билет № 12

Задача о дискретном логарифме. Исчисление индексов. Метод для мультипликативной группы конечного поля.

Билет № 13

Задача о дискретном логарифме. Исчисление индексов. Метод для достаточно общей аддитивной группы.

Билет № 14

Свойства простых чисел. Критерии простоты чисел. Теорема Лукаса (Люка). Тесты Соловея-Штрассена и Миллера-Рабина.

Билет № 15

Метод Ферма для разложения на множители, основанный на формуле для разности квадратов. Алгоритм Шенкса-Тоннелли.

Билет № 16

Криптографические протоколы. Требования к протоколам. Протоколы обмена ключами.

Билет № 17

Варианты протокола вручения бита. Подбрасывание монеты по телефону.

Билет № 18

Доказательства с нулевым разглашением. Пещера Алладина. Протокол доказательства знания изоморфизма графов. Протокол доказательства знания секретного ключа, основанный на подписи Шнорра.

7.1. Основная литература:

Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с.: http://znanium.com/bookread.php?book=432654

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. http://znanium.com/bookread.php?book=441493

Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. - М.: Физматлит, 2012. - 280с. http://e.lanbook.com/books/element.php?pl1_id=5300

7.2. Дополнительная литература:

Теоретическая информатика, Громкович, Юрай;Мельников, Б. Ф., 2010г.

Введение в теоретико-числовые методы криптографии : учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090101 "Криптография" / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин .- Санкт-Петерург [и др.] : Лань, 2011 .- 394 с. ; 21 см. - (Учебники для вузов, Специальная литература) .- Библиогр.: с. 382-389 .- ISBN 978-5-8114-1116-0 ((в пер.)) , 1000.

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.))

7.3. Интернет-ресурсы:

Аграновский А.В., Хади Р.А.Практическая криптография: алгоритмы и их программирование - http://www.bibliorossica.com/book.html?currBookId=10512

Алешников С.И., Болтнев Ю.Ф.Математические методы защиты информации. Ч. 4: Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых : практическое пособие - http://www.bibliorossica.com/book.html?currBookId=6793

Баранова Е.К., Бабаш А.В.Информационная безопасность и защита информации : учебное пособие - http://www.bibliorossica.com/book.html?currBookId=6182

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. - http://znanium.com/bookread.php?book=441493

Криптографические методы защиты информации. Том 3: Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. - http://znanium.com/bookread.php?book=432654

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Криптография" предполагает использование следующего материально-технического обеспечения:

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе " БиблиоРоссика", доступ к которой предоставлен студентам. В ЭБС " БиблиоРоссика " представлены коллекции актуальной научной и учебной литературы по гуманитарным наукам, включающие в себя публикации ведущих российских издательств гуманитарной литературы, издания на английском языке ведущих американских и европейских издательств, а также редкие и малотиражные издания российских региональных вузов. ЭБС "БиблиоРоссика" обеспечивает широкий законный доступ к необходимым для образовательного процесса изданиям с использованием инновационных технологий и соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. 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, УМК, 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 профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен студентам. 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.

учебные аудитории для проведения лекционных и семинарских занятий, библиотека, доступ студентов к Интернету. Студенты получаю DVD-диск, содержащий в электронном виде большое количество книг на русском и на английском языках, которые можно использовать при подготовке докладов и рефератов.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010100.68 "Математика" и магистерской программе Алгебра .

Автор(ы):
Тронин С.Н. _____
"__" _____ 201 __ г.

Рецензент(ы):
Киндер М.И. _____
"__" _____ 201 __ г.