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

УТВЕРЖДАЮ
Проректор
по образовательной деятельности КФУ
Проф. Минзарипов Р.Г.
_____
"___"_____20___ г.

Программа дисциплины

Криптография Б2.ДВ.1

Направление подготовки: 010200.62 - Математика и компьютерные науки
Профиль подготовки: Математическое и компьютерное моделирование
Квалификация выпускника: бакалавр
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

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 " Б2.ДВ.1 Общепрофессиональный" основной образовательной программы 010200.62 Математика и компьютерные науки и относится к дисциплинам по выбору. Осваивается на 2 курсе, 4 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.

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.

применять полученные знания в конкретных ситуациях.

вычислительными навыками, необходимыми при решении простейших криптографических задач.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) 108 часа(ов).

Форма промежуточного контроля дисциплины зачет в 4 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.	4	1	2	0	0	устный опрос
2.	Тема 2. Блочные и потоковые шифры. Режимы шифрования.	4	2	2	0	0	устный опрос
3.	Тема 3. Математический аппарат: кольца вычетов, сравнения, и конечные поля.	4	4-6	3	3	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.	4	7-8	2	2	0	устный опрос
5.	Тема 5. Криптосистемы RSA, и Эль-Гамаля. Цифровые подписи Шнорра и DSA. Криптографические хэш-функции. Другие цифровые подписи.	4	9-11	2	4	0	реферат
6.	Тема 6. Слепые (затемненные) цифровые подписи. Электронные деньги.	4	12-13	2	2	0	устный опрос
7.	Тема 7. Эллиптическая криптография	4	14-15	2	2	0	домашнее задание
8.	Тема 8. Криптографические протоколы.	4	16-17	2	4	0	реферат
.	Тема . Итоговая форма контроля	3		0	0	0	зачет
	Итого			17	17	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 (3 часа(ов)):

Кольца вычетов и конечные поля.

практическое занятие (3 часа(ов)):

Решение задач.

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)):

Классические криптосистемы и цифровые подписи двухключесвой криптографии

практическое занятие (4 часа(ов)):

Самостоятельный анализ некоторых цифровых подписей

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

лекционное занятие (2 часа(ов)):

Затемненая подпись, основанная на агоритме RSA, и использующий ее протокол, реализующий простую платежную систему

практическое занятие (2 часа(ов)):

Другие затемненные подписи.

Тема 7. Эллиптическая криптография

лекционное занятие (2 часа(ов)):

Группы точек элиптических кривых над конечными поями. Крипотграфыические алгоритмы (ECDSA и др.), использующие эти группы.

практическое занятие (2 часа(ов)):

Вычисление групп точек некотоых эллиптических кривых

Тема 8. Криптографические протоколы.

лекционное занятие (2 часа(ов)):

Протоколы обмена ключами. Протокол вручения бита. Протокол подбрасывания монеты по телефону. Протоколы доказательств с нулевым разглашением.

практическое занятие (4 часа(ов)):

Анализ некоторых протоколов.

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.	4	1	подготовка к устному опросу	4	устный опрос
2.	Тема 2. Блочные и потоковые шифры. Режимы шифрования.	4	2	подготовка к устному опросу	4	устный опрос
3.	Тема 3. Математический аппарат: кольца вычетов, сравнения, и конечные поля.	4	4-6	подготовка домашнего задания	8	домашнее задание
				подготовка к контрольной работе	10	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.	4	7-8	подготовка к устному опросу	6	устный опрос
5.	Тема 5. Криптосистемы RSA, и Эль-Гамаля. Цифровые подписи Шнорра и DSA. Криптографические хэш-функции. Другие цифровые подписи.	4	9-11	подготовка к реферату	18	реферат
6.	Тема 6. Слепые (затемненные) цифровые подписи. Электронные деньги.	4	12-13	подготовка к устному опросу	6	устный опрос
7.	Тема 7. Эллиптическая криптография	4	14-15	подготовка домашнего задания	8	домашнее задание
8.	Тема 8. Криптографические протоколы.	4	16-17	подготовка к реферату	10	реферат
	Итого				74	

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:

Тема 2. Блочные и потоковые шифры. Режимы шифрования.

устный опрос , примерные вопросы:

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

домашнее задание , примерные вопросы:

Решение задач

контрольная работа , примерные вопросы:

Решение сравнений. Вычисления в конечных полях

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

устный опрос , примерные вопросы:

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

реферат , примерные темы:

Некоторые цифровые подписи

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

устный опрос , примерные вопросы:

Тема 7. Эллиптическая криптография

домашнее задание , примерные вопросы:

Вычисление групп точек некоторых эллиптических кривых над конечными полями

Тема 8. Криптографические протоколы.

реферат , примерные темы:

Анализ некоторых криптографических протоколов

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

На практических занятиях контроль осуществляется при устном опросе и по результатам доклада на семинаре. Оцениваются также рефераты (отчеты о самостоятельной работе). Используется балльная система.

Приложение 1. Вопросы для зачета.

1. Потоковые шифры. Абсолютно надежные шифры.
2. Блочные шифры. Примеры. Схема Фейстеля. DES.
3. Режимы шифрования.
4. Односторонние функции. Шифрование и цифровая подпись.
5. Алгоритм RSA и его обоснование.
6. Цифровая подпись RSA. Криптографические хэш-функции.
7. Шифрование по методу Эль-Гамаля.
8. Цифровая подпись Эль-Гамаля.
9. Цифровая подпись DSA (DSS).
10. Цифровая подпись Шнорра и ее модификация для смарт-карт (банковских карт).
11. Группы точек эллиптических кривых.
12. Криптография на эллиптических кривых: ECDSA и алгоритм шифрования Менезеса-Вэнстона.
13. ГОСТ Р 34.10-2012 для цифровых подписей
14. Цифровые платежные системы. Электронные деньги. Затемненные (слепые) цифровые подписи.

Приложение 2. Дополнительные вопросы

15. Математический аппарат: кольца вычетов, функция Эйлера, теорема Эйлера, малая теорема Ферма, китайская теорема об остатках.
16. Математический аппарат: расширенный алгоритм Евклида и деление в кольцах вычетов.
17. Математический аппарат: строение конечных полей, характеристика поля, примитивные элементы (первообразные корни).
18. Математический аппарат: решение задачи о дискретном логарифме методом "Шаги младенца - шаги гиганта".
19. Математический аппарат: группы, циклические группы, порядок группы и порядок элемента.

7.1. Основная литература:

Методы факторизации натуральных чисел, Ишмухаметов, Шамиль Талгатович, 2011г.

Основы современной криптографии и стеганографии, Рябко, Борис Яковлевич;Фионов, Андрей Николаевич, 2010г.

Алгебраические основы криптографии, Применко, Эдуард Андреевич, 2013г.

Лекции по криптографии, Музыкантский, Александр Ильич;Фурин, Виктор Владимирович, 2011г.

Торстейнсон П., Ганеш Г.А.Криптография и безопасность в технологии .NET. - М.: БИНОМ. Лаборатория знаний, 2013. - 489 с. http://www.bibliorossica.com/book.html?currBookId=8242

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

Панин, В. В. Основы теории информации [Электронный ресурс] : учебное пособие для вузов / В. В. Панин. - 4-е изд. (эл.). - М. : БИНОМ. Лаборатория знаний, 2012. - 438 с.. http://znanium.com/bookread.php?book=366057

7.2. Дополнительная литература:

Теория чисел, Корешков, Николай Александрович, 2010г.

Вычислительно сложные задачи теории чисел, Гречников, Евгений Александрович;Михайлов, Сергей Владимирович;Нестеренко, Юрий Валентинович;Поповян, Илья Ардашесович, 2012г.

Коды и шифры, Черчхауз, Роберт Ф., 2005г.

Булевы функции в теории кодирования и криптологии, Логачев, О. А.;Сальников, А. А.;Ященко, В. В., 2004г.

Введение в теоретико-числовые методы криптографии, Глухов, Михаил Михайлович;Круглов, Игорь Александрович;Пичкур, Андрей Борисович;Черемушкин, Александр Васильевич, 2011г.

1. Смарт Н. Криптография. ? М.: Техносфера, 2006. ? 528 с.

2. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. ? М.: Научный мир, 2004. ? 173 с.

3. Введение в криптографию / Под общ. ред. В.В.Ященко. ? 3-е изд., доп. ? М.:МЦНМО:"ЧеРо", 2000. ? 288 с.

4. Земор Ж. Курс криптографии. ? М. - Ижевск: НИЦ "Регулярная и хаотическая динамика"; Ин-т компьютерных исследований, 2006. ? 256 с.

5. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. ? М.:"Мир", 1987. ? 416 с.

6. Бабаш А.В., Шанкин Г.П. Криптография. ? М.: СОЛОН-ПРЕСС, 2007. ? 512 с.

7. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. ? М.: КомКнига, 2006. ? 328 с.

8. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. ? М.: КомКнига, 2006. ? 280 с.

9. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. - М.: МЦНМО, 2003. - 328 с.

10. Ишмухаметов Ш.Т. Методы факторизации натуральных чисел. - Казань: Казанский ун-т., 2011. - 192 с.

11. Коблиц Н. Курс теории чисел и криптографии. ? М: Научн. изд-во ТВП, 2001. ? 254 с.

12. Латыпов Р.Х. Математические основы кодирования информации и криптографии. - Казанский гос. ун-т., 2005. - 60 с.

13. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. ? СПб.: БХВ-Петербург, 2005. ? 288 с.

14. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. ? СПб.: БХВ-Петербург, 2007. ? 304 с.

15. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. ? СПб.: БХВ-Петербург, 2009. ? 576 с.

16. Сингх С. Книга шифров: тайная история шифров и их расшифровки. ? М.: АСТ: Астрель, 2007. ? 447 с.

17. Черемушкин А.В. Криптографические протоколы. основные свойства и уязвимости. ? М.: Изд. центр "Академия", 2009. ? 272 с.

18. Чмора А.Л. Современная прикладная криптография. ? М.: Гелиос АРВ: 2001. ? 256 с.

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

Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2 - http://znanium.com/bookread.php?book=405000

Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. - (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5, 1000 экз. - http://znanium.com/bookread.php?book=423927

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

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.

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 010200.62 "Математика и компьютерные науки" и профилю подготовки Математическое и компьютерное моделирование .

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

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