МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

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

Программа дисциплины

Криптографические методы защиты информации Б1.В.ДВ.12

Направление подготовки: 02.03.02 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Системный анализ и информационные технологии
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):
Ишмухаметов Ш.Т. , Латыпов Р.Х.
Рецензент(ы):
Тагиров Р.Р.

СОГЛАСОВАНО:
Заведующий(ая) кафедрой: Латыпов Р. Х.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института вычислительной математики и информационных технологий:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No

Казань
2018

Содержание

Программу дисциплины разработал(а)(и) профессор, д.н. (доцент) Ишмухаметов Ш.Т. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Shamil.Ishmukhametov@kpfu.ru ; заведующий кафедрой, д.н. (профессор) Латыпов Р.Х. кафедра системного анализа и информационных технологий отделение фундаментальной информатики и информационных технологий , Roustam.Latypov@kpfu.ru

1. Цели освоения дисциплины

Курс должен преследовать следующие цели.

1. Ввести слушателей читателя в те области арифметики, как классические, так и самые современные, которые находятся в центре внимания приложений теории чисел, особенно криптографии. Предполагается, что знание высшей алгебры и теории чисел ограничено самым скромным знакомством с их основами; по этой причине излагаются также необходимые сведения из этих областей математики. Авторами избран алгоритмический подход, причем особое внимание уделяется оценкам эффективности методов, предлагаемых теорией.

2. Ознакомить студентов с основными достижениями теории помехоустойчивого кодирования: существующие ограничения и основные линейные коды: Хэмминга, БЧХ, Рида-Маллера, Рида-Соломона.

3. Значительное внимание уделяется изучению широко используемых криптографических алгоритмов симметричного и асимметричного шифрования, а также криптографических хэш-функций.

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

Данная учебная дисциплина включена в раздел " Б1.В.ДВ.12 Дисциплины (модули)" основной образовательной программы 02.03.02 Фундаментальная информатика и информационные технологии и относится к дисциплинам по выбору. Осваивается на 4 курсе, 8 семестр.

'Криптографические методы защиты информации' входит в состав профессиональных дисциплин. Читается на 4 курсе в 8 семестре.

Курс базируется как на общих дисциплинах - алгебра, теория вероятностей, так и на специальных дисциплинах ('Основы информационной безопасности', 'Теория кодирования и криптография'). Курс имеет важное значение с точки зрения математических основ защиты информации.

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-1 (профессиональные компетенции)	способностью использовать базовые знания естественных наук, математики и информатики, основные факты, концепции, принципы теорий, связанных с фундаментальной информатикой и информационными технологиями
ОПК-2 (профессиональные компетенции)	способностью применять в профессиональной деятельности современные языки программирования и языки баз данных, методологии системной инженерии, системы автоматизации проектирования, электронные библиотеки и коллекции, сетевые технологии, библиотеки и пакеты программ, современные профессиональные стандарты информационных технологий

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-3 (профессиональные компетенции)	способностью к разработке алгоритмических и программных решений в области системного и прикладного программирования, математических, информационных и имитационных моделей, созданию информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных, тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям
ОПК-4 (профессиональные компетенции)	способностью участвовать в разработке подсистемы управления информационной безопасностью
ПК-2 (профессиональные компетенции)	способностью понимать, совершенствовать и применять современный математический аппарат, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий

В результате освоения дисциплины студент:

1. должен знать:

- основные результаты теории чисел и алгебры, понимать проблемы сложности алгоритмов.

2. должен уметь:

- использовать на практике полученные знания.

3. должен владеть:

- знаниями по основным разделам теории кодирования и криптографии.

4. должен демонстрировать способность и готовность:

- знаниями по основным разделам теории кодирования и криптографии.

4. Структура и содержание дисциплины/ модуля

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

Форма промежуточного контроля дисциплины экзамен в 8 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. Сложность						

алгоритмов

					Письменное
8		2	0	1	

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	
2.	Тема 2. Сведения из теории чисел	8		2	0	1	Письменное домашнее задание
3.	Тема 3. Алгебраические структуры, конечные поля	8		2	0	1	Письменное домашнее задание
4.	Тема 4. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.	8		2	0	1	Письменное домашнее задание
5.	Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.	8		2	0	4	Контрольная работа Письменное домашнее задание
6.	Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.	8		2	0	4	Письменное домашнее задание
7.	Тема 7. Аспекты безопасности. Основные угрозы. Стандарты и законодательство в области безопасности.	8		4	0	4	Письменное домашнее задание
8.	Тема 8. Симметричное шифрование. Современные симметричные блочные шифры.	8		4	0	4	Письменное домашнее задание
9.	Тема 9. Обзор результатов Клода Шеннона	8		4	0	4	Письменное домашнее задание
10.	Тема 10. Симметричное шифрование: обзор современного состояния.	8		4	0	4	Контрольная работа Письменное домашнее задание
	Тема . Итоговая форма контроля	8		0	0	0	Экзамен
	Итого			28	0	28	

4.2 Содержание дисциплины

Тема 1. Сложность алгоритмов

лекционное занятие (2 часа(ов)):

Понятие сложности алгоритмов. Верхние и нижние оценки. Приемы построения оценок. Классы сложности. Классы P и NP. Полиномиальная сводимость. NP-полные проблемы.

лабораторная работа (1 часа(ов)):

Решение задач на оценку сложности алгоритмов. Выполнение учебных проектов.

Тема 2. Сведения из теории чисел

лекционное занятие (2 часа(ов)):

Кольцо вычетов Zn. Полная и приведенные системы вычетов. Функция Эйлера. Теорема Эйлера. Мультипликативность функции Эйлера. Решений сравнений 1 и 2-о порядка.

лабораторная работа (1 часа(ов)):

Решений сравнений в кольце Zn. Контрольная работа по теме.

Тема 3. Алгебраические структуры, конечные поля

лекционное занятие (2 часа(ов)):

Алгебраические структуры: группы, кольца, поля. Конечные поля простой характеристики. Расширений конечных полей. Вычисления в конечных полях.

лабораторная работа (1 часа(ов)):

Вычисления в конечных полях. Построения неприводимых многочленов. Нахождение примитивных элементов в конечном поле. Символ Лежандра и его вычисление.

Тема 4. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.

лекционное занятие (2 часа(ов)):

Общая задача построения кодов. Избыточные и неизбыточные коды. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.

лабораторная работа (1 часа(ов)):

Решение задач на построение кодов. Построение кодов Хемминга. Корректирующие коды.

Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.

лекционное занятие (2 часа(ов)):

Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ

лабораторная работа (4 часа(ов)):

Разработка программ,реализующих коды БЧХ. Оценка их сложности.

Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.

лекционное занятие (2 часа(ов)):

Ввендение в мажоритарное декодирование. Коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона. Использование кодов Рида-Маллера в криптографии.

лабораторная работа (4 часа(ов)):

Разработка программ, реализующих коды Рида-Соломона.

Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.

лекционное занятие (4 часа(ов)):

Аспекты безопасности, основные угрозы. Стандарты и законодательство в области информационной безопасности. Законы РФ об электронной подписи, о защите персональных данных, авторского права.

лабораторная работа (4 часа(ов)):

Разработка информационной системы с элементами аутентификации, авторизации и аудита. Использование электронной подписи для защиты данных.

Тема 8. Симметричное шифрование: докомпьютерные шифры.

лекционное занятие (4 часа(ов)):

Разработка алгоритмов симметричного шифрования. Хеш-функции. Блочные и потоковые методы. Примеры.

лабораторная работа (4 часа(ов)):

Блочные и потоковые методы. Разработка программ шифрования гна основе криптографических перестановок, подстановок и гаммирования.

Тема 9. Обзор результатов Клода Шеннона

лекционное занятие (4 часа(ов)):

Прямая и обратная теоремы Шеннона для источника общего вида ? о связи энтропии источника и средней длины сообщений.Прямая и обратная теоремы Шеннона для источника без памяти ? о связи энтропии источника и достижимой степени сжатия с помощью кодирования с потерями и последующего неоднозначного декодирования.

лабораторная работа (4 часа(ов)):

Решение задач по теме.

Тема 10. Симметричное шифрование: обзор современных шифров.

лекционное занятие (4 часа(ов)):

Симметричное шифрование: методы DES, AES, RC4. Их свойства и особенности применения.

лабораторная работа (4 часа(ов)):

Разработка системы шифрования на основе RC4.

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. Сложность алгоритмов	8		подготовка домашнего задания	6	домашнее задание
2.	Тема 2. Сведения из теории чисел	8		подготовка домашнего задания	6	домашнее задание
3.	Тема 3. Алгебраические структуры, конечные поля	8		подготовка домашнего задания	6	домашнее задание
4.	Тема 4. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.	8		подготовка домашнего задания	4	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
5.	Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.	8		подготовка домашнего задания	3	домашнее задание
				подготовка к контрольной работе	3	контрольная работа
6.	Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.	8		подготовка домашнего задания	6	домашнее задание
7.	Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.	8		подготовка домашнего задания	4	домашнее задание
8.	Тема 8. Симметричное шифрование: докомпьютерные шифры.	8		подготовка домашнего задания	4	домашнее задание
9.	Тема 9. Обзор результатов Клода Шеннона	8		подготовка домашнего задания	4	домашнее задание
10.	Тема 10. Симметричное шифрование: обзор современных шифров.	8		подготовка домашнего задания	3	домашнее задание
				подготовка к контрольной работе	3	контрольная работа
	Итого				52	

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лабораторных занятий и самостоятельной работы студентов.

Список литературы разделен на две категории: необходимый для сдачи экзамена минимум и дополнительная литература.

Изучение курса подразумевает не только овладение теоретическим материалом, но и получение практических навыков для более глубокого понимания разделов

на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности

самостоятельно доказывать утверждения.

Самостоятельная работа предполагает выполнение домашних работ. Практические задания, выполненные в аудитории, предназначены для указания общих

методов решения задач определенного типа. Закрепить навыки можно лишь в результате самостоятельной работы. Кроме того, самостоятельная работа включает

подготовку к экзамену. При подготовке к сдаче экзамену весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки

к экзамену, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда будет резерв времени.

Также рекомендуется писать небольшие программки для изучаемых алгоритмов и выполнять пошаговое тестирование выполняемых заданий.

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

Тема 1. Сложность алгоритмов

домашнее задание , примерные вопросы:

Оценить сложность следующих алгоритмов: умножение Карацубы, алгоритм быстрого возведения в степень, алгоритм Евклида.

Тема 2. Сведения из теории чисел

домашнее задание , примерные вопросы:

Найти наибольший общий делитель двух чисел. Найти обратный элемент по модулю. Вычислить функцию Эйлера.

Тема 3. Алгебраические структуры, конечные поля

домашнее задание , примерные вопросы:

Доказать, что множество полиномов степени, не превосходящей n, является кольцом. Показать, что множество целых чисел является кольцом, но не является мультипликативной группой.

Тема 4. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.

домашнее задание , примерные вопросы:

Программная реализация кода Хэмминга.

Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.

домашнее задание , примерные вопросы:

Программная реализация кодов БЧХ.

контрольная работа , примерные вопросы:

Реализовать расширенный алгоритм Евклида.

Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.

домашнее задание , примерные вопросы:

Программная реализация кодов Рида-Маллера.

Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.

домашнее задание , примерные вопросы:

Изучение государственных стандартов в области информационной безопасности.

Тема 8. Симметричное шифрование: докомпьютерные шифры.

домашнее задание , примерные вопросы:

Программная реализация шифра Виженера.

Тема 9. Обзор результатов Клода Шеннона

домашнее задание , примерные вопросы:

Написание программы, позволяющей оценить энтропию введенного текста.

Тема 10. Симметричное шифрование: обзор современных шифров.

домашнее задание , примерные вопросы:

Программная реализация алгоритма AES.

контрольная работа , примерные вопросы:

Программная реализация шифра RC4.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

1. Основные понятия сложность алгоритмов: временная и пространственная сложность, методы оценки, полиномиальные и экспоненциальные алгоритмы.

2. Сведения из теории чисел: кольцо вычетов по модулю целого числа, вычисление обратного элемента, расширенный алгоритм Евклида. Решение сравнений 1 порядка.

3. Теорема Лагранжа о порядке группы. Группа по умножению кольца вычетов Zn. Функция Эйлера и ее вычисление.

4. Алгебраические структуры, конечные поля. Структура конечных полей, поля по простому модулю. Вычисление степеней и дискретных логарифмов в конечных полях. Алгоритм Шенкса вычисления дискретного логарифма.

5. Метод шифрования Эль-Гамаля.

6. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.

7. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.

8. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.

9. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности. Закон об электронной подписи 2011 года. Виды электронной подписи. Понятие доверенннной подписи.

10. Симметричное шифрование: докомпьютерные шифры. Подстановки, перестановки, гнаммирование.

11. Обзор результатов Клода Шеннона

12. Симметричное шифрование: обзор современных шифров. Метод AES.

7.1. Основная литература:

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

2. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с. URL: http://znanium.com/bookread.php?book=420047

3. Чечёта, С.И. Введение в дискретную теорию информации и кодирования [Электронный ресурс] : учеб. пособие ? Электрон. дан. ? Москва : МЦНМО, 2011. - 224 с. - Режим доступа: https://e.lanbook.com/book/9437

4. Кельберт, М.Я. Вероятность и статистика в примерах и задачах. Т.3: Теория информации и кодирования [Электронный ресурс] / М.Я. Кельберт, Ю.М. Сухов. - Электрон. дан. - Москва : МЦНМО, 2016. - 567 с. ?- Режим доступа: https://e.lanbook.com/book/80125.

5. Штарьков, Ю.М. Универсальное кодирование. Теория и алгоритмы [Электронный ресурс] Электрон. дан. - М. : Физматлит, 2013. - 280 с. - Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=59667

7.2. Дополнительная литература:

1. Сидельников, В. М. Теория кодирования [Электронный ресурс] / В. М. Сидельников. - М.: ФИЗМАТЛИТ, 2008. - 324 с. URL:http://znanium.com/bookread2.php?book=544713

2.Масленников М. Е. Практическая криптография: Пособие / Масленников М.Е. СПб:БХВ-Петербург, 2015. - 465 с. URL: http://znanium.com/bookread2.php?book=944503

3. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=474838

4. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : Учебное пособие / Н. Г. Каратунова. - Краснодар: КСЭИ, 2014. - 188 с. - ЭБС 'Знаниум': http://znanium.com/bookread.php?book=503511

7.3. Интернет-ресурсы:

Интернет-портал образовательных ресурсов по ИТ - http://www.intuit.ru

Интернет--портал ресурсов по математическим наукам - http://www.math.ru/

Интернет--портал ресурсов по математическим наукам - http://www.mathnet.ru

Интернет--портал ресурсов по математическим наукам - http://www.allmath.com/

Интернет-портал со статьями по алгоритмике и программированию - http://algolist.manual.ru/

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Криптографические методы защиты информации" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

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.

практические занятия по дисциплине проводятся в аудитории, оснащенной доской и мелом(маркером).

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 02.03.02 "Фундаментальная информатика и информационные технологии" и профилю подготовки Системный анализ и информационные технологии .

Автор(ы):
Латыпов Р.Х. _____
Ишмухаметов Ш.Т. _____
"__" _____ 201 __ г.

Рецензент(ы):
Тагиров Р.Р. _____
"__" _____ 201 __ г.