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. Минзарипов Р.Г.
_____
"___"_____20___ г.

Программа дисциплины

Программирование криптографических алгоритмов М2.ДВ.6

Направление подготовки: 010300.68 - Фундаментальная информатика и информационные технологии
Профиль подготовки: Математические основы и программное обеспечение информационной безопасности и защиты информации
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Латыпов Р.Х.

Рецензент(ы):

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

2013

Содержание

Программу дисциплины разработал(а)(и) директор института вычислительной математики и информационных технологий Латыпов Р.Х. Директорат Института ВМ и ИТ Институт вычислительной математики 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 " М2.ДВ.6 Профессиональный" основной образовательной программы 010300.68 Фундаментальная информатика и информационные технологии и относится к дисциплинам по выбору. Осваивается на 2 курсе, 3 семестр.

"Программирование криптографических алгоритмов" входит в состав профессиональных дисциплин. Читается на 2 курсе в 3 семестре.

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-1 (профессиональные компетенции)	ПК1способность 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 (в соответствии с профилизацией)

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-2 (профессиональные компетенции)	способность профессионально решать задачи производственной и технологической деятельности с учетом современных достижений науки и техники, включая: разработку алгоритмических и программных решений в области системного и прикладного программирования; разработку математических, информационных и имитационных моделей по тематике выполняемых исследований; создание информационных ресурсов глобальных сетей, образовательного контента, прикладных баз данных; разработку тестов и средств тестирования систем и средств на соответствие стандартам и исходным требованиям; разработку эргономических человеко-машинных интерфейсов (в соответствии с профилизацией)
ПК-3 (профессиональные компетенции)	способность разрабатывать и реализовывать процессы жизненного цикла информационных систем, программного обеспечения, сервисов систем информационных технологий, а также методы и механизмы оценки и анализа функционирования средств и систем информационных технологий; способности разработки проектной и программной документации, удовлетворяющей нормативным требованиям
ПК-4 (профессиональные компетенции)	способность демонстрировать знания фундаментальных и смежных прикладных разделов специальных дисциплин магистерской программы, знания общеметодологического характера, знания истории развития информатики и информационных технологий
ПК-5 (профессиональные компетенции)	способность использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математики, фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий, а также знания, которые находятся на передовом рубеже науки

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.

- знаниями по основным разделам теории кодирования и криптографии.

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. Сложность алгоритмов	3		0	3	0	домашнее задание
2.	Тема 2. Сведения из теории чисел	3		0	3	0	домашнее задание
3.	Тема 3. Алгебраические структуры, конечные поля	3		0	3	0	домашнее задание
4.	Тема 4. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.	3		0	3	0	домашнее задание
5.	Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.	3		0	4	0	домашнее задание
6.	Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.	3		0	4	0	домашнее задание
7.	Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.	3		0	4	0	домашнее задание
8.	Тема 8. Симметричное шифрование: докомпьютерные шифры.	3		0	4	0	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	
9.	Тема 9. Обзор результатов Клода Шеннона	3		0	4	0	домашнее задание
10.	Тема 10. Симметричное шифрование: обзор современных шифров.	3		0	4	0	домашнее задание
.	Тема . Итоговая форма контроля	3		0	0	0	зачет
	Итого			0	36	0	

4.2 Содержание дисциплины

Тема 1. Сложность алгоритмов

практическое занятие (3 часа(ов)):

Сложность алгоритмов

Тема 2. Сведения из теории чисел

практическое занятие (3 часа(ов)):

Сведения из теории чисел

Тема 3. Алгебраические структуры, конечные поля

практическое занятие (3 часа(ов)):

Алгебраические структуры, конечные поля

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

практическое занятие (3 часа(ов)):

Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.

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

практическое занятие (4 часа(ов)):

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

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

практическое занятие (4 часа(ов)):

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

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

практическое занятие (4 часа(ов)):

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

Тема 8. Симметричное шифрование: докомпьютерные шифры.

практическое занятие (4 часа(ов)):

Симметричное шифрование: докомпьютерные шифры.

Тема 9. Обзор результатов Клода Шеннона

практическое занятие (4 часа(ов)):

Обзор результатов Клода Шеннона

Тема 10. Симметричное шифрование: обзор современных шифров.

практическое занятие (4 часа(ов)):

Симметричное шифрование: обзор современных шифров.

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	3		подготовка домашнего задания	3	домашнее задание
2.	Тема 2. Сведения из теории чисел	3		подготовка домашнего задания	3	домашнее задание
3.	Тема 3. Алгебраические структуры, конечные поля	3		подготовка домашнего задания	3	домашнее задание
4.	Тема 4. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.	3		подготовка домашнего задания	3	домашнее задание
5.	Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.	3		подготовка домашнего задания	4	домашнее задание
6.	Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.	3		подготовка домашнего задания	4	домашнее задание
7.	Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.	3		подготовка домашнего задания	4	домашнее задание
8.	Тема 8. Симметричное шифрование: докомпьютерные шифры.	3		подготовка домашнего задания	4	домашнее задание
9.	Тема 9. Обзор результатов Клода Шеннона	3		подготовка домашнего задания	4	домашнее задание
10.	Тема 10. Симметричное шифрование: обзор современных шифров.	3		подготовка домашнего задания	4	домашнее задание

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
	Итого				36	

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 зачета 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 зачету. При подготовке к сдаче зачета весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к зачету, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда будет резерв времени.

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:

Углубленное изучение литературы. Обсуждение.

Тема 2. Сведения из теории чисел

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение.

Тема 3. Алгебраические структуры, конечные поля

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение.

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

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение.

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

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение.

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

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение.

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

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение.

Тема 8. Симметричное шифрование: докомпьютерные шифры.

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение.

Тема 9. Обзор результатов Клода Шеннона

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение.

Тема 10. Симметричное шифрование: обзор современных шифров.

домашнее задание , примерные вопросы:

Углубленное изучение литературы. Обсуждение.

Тема . Итоговая форма контроля

Примерные вопросы к зачету:

По данной дисциплине предусмотрено проведение зачета. Примерные вопросы для зачета - Приложение1.

7.1. Основная литература:

1) Смарт Н. Криптография / Н. Смарт; пер. с англ. С.А. Кулешова; под ред. С.К. Ландо.?Москва: Техносфера, 2006.?525 с.: ил.; 25.?(Мир программирования).?Компьютерная криптография.

2) Масленников М. Практическая криптография. С.-П.: БХВ - Петербург, 2003.

7.2. Дополнительная литература:

1) Смит Р.Э. Аутентификация: от паролей до открытых ключей. М.: Издательский дом Вильямс, 2002.

2) Фролов А.В. Антивирусная защита. М.:МГУ, 2006..

3) Иванов М.А.Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ - ОБРАЗ, 2001.

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 согласно утвержденному учебному плану

Освоение дисциплины "Программирование криптографических алгоритмов" предполагает использование следующего материально-технического обеспечения:

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 010300.68 "Фундаментальная информатика и информационные технологии" и магистерской программе Математические основы и программное обеспечение информационной безопасности и защиты информации .

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

Рецензент(ы):
"__" _____ 201 __ г.

Лист согласования

N	ФИО	Согласование
1	Латыпов Р. Х.	
2	Латыпов Р. Х.	
3	Латыпов Р. Х.	
4	Чижанова Е. А.	
5	Соколова Е. А.	
6	Тимофеева О. А.	