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: 010400.68 - Прикладная математика и информатика
Профиль подготовки: Системный анализ и информационные технологии
Квалификация выпускника: магистр
Форма обучения: очное
Язык обучения: русский
Автор(ы):
Латыпов Р.Х.
Рецензент(ы):

СОГЛАСОВАНО:
Заведующий(ая) кафедрой:
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
2014

Содержание

Программу дисциплины разработал(а)(и) директор института вычислительной математики 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 010400.68 Прикладная математика и информатика и относится к дисциплинам по выбору. Осваивается на 2 курсе, 3 семестр.

Данная дисциплина относится к профессиональным дисциплинам.

Читается на 2 курсе в 3 семестре для студентов обучающихся в магистратуре по направлению "Прикладная математика и информатика".

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

В результате освоения дисциплины формируются следующие компетенции:

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.

- ориентироваться в вопросах стандартов безопасности и законодательства в области защиты информации.

4. Структура и содержание дисциплины/ модуля

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

Форма промежуточного контроля дисциплины экзамен 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	0	0	
2.	Тема 2. Сведения из теории чисел	3		0	0	0	
3.	Тема 3. Алгебраические структуры, конечные поля	3		0	0	0	
4.	Тема 4. Линейные блоковые коды, границы помехоустойчивого кодирования. Код Хэмминга.	3		0	0	0	
5.	Тема 5. Циклические коды. Аппаратная реализация кодирования и декодирования. Коды БЧХ.	3		0	0	0	
6.	Тема 6. Мажоритарное декодирование и коды Рида-Маллера. Недвоичные коды и коды Рида-Соломона.	3		0	0	0	
7.	Тема 7. Аспекты безопасности, основные угрозы. Стандарты и законодательство в области безопасности.	3		0	0	0	
8.	Тема 8. Симметричное шифрование: докомпьютерные шифры.	3		0	0	0	

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	0	0	
10.	Тема 10. Симметричное шифрование: обзор современных шифров.	3		0	0	0	
.	Тема . Итоговая форма контроля	3		0	0	0	экзамен
	Итого			0	0	0	

4.2 Содержание дисциплины

Тема 1. Сложность алгоритмов

Тема 2. Сведения из теории чисел

Тема 3. Алгебраические структуры, конечные поля

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

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

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

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

Тема 8. Симметричное шифрование: докомпьютерные шифры.

Тема 9. Обзор результатов Клода Шеннона

Тема 10. Симметричное шифрование: обзор современных шифров.

5. Образовательные технологии, включая интерактивные формы обучения

Обучение происходит в форме лекционных и практических занятий, а также самостоятельной работы студентов.

Теоретический материал излагается на лекциях. Причем конспект лекций, который остается у студента в результате прослушивания лекции не может заменить учебник. Его цель - формулировка основных утверждений и определений. Прослушав лекцию, полезно ознакомиться с более подробным изложением материала в учебнике. 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 дисциплины "Программирование криптографических алгоритмов" на основе решения задач и упражнений, иллюстрирующих доказываемые теоретические положения, а также развитие абстрактного мышления и способности самостоятельно доказывать частные 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 экзамена весь объем работы рекомендуется распределять равномерно по дням, отведенным для подготовки к экзамену, контролировать каждый день выполнения работы. Лучше, если можно перевыполнить план. Тогда всегда 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

Тема 2. Сведения из теории чисел

Тема 3. Алгебраические структуры, конечные поля

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

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

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

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

Тема 8. Симметричное шифрование: докомпьютерные шифры.

Тема 9. Обзор результатов Клода Шеннона

Тема 10. Симметричное шифрование: обзор современных шифров.

Тема . Итоговая форма контроля

Примерные вопросы к экзамену:

По данной дисциплине предусмотрено проведение экзамена. Примерные промежуточные и итоговые тесты - 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:

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 010400.68 "Прикладная математика и информатика" и магистерской программе Системный анализ и информационные технологии .

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

Рецензент(ы):
"__" _____ 201 __ г.