Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе
_____ А.Л. Толстик
“ 30 ” _____ 2015 г.
Регистрационный № УД- 1163 /уч.

АЛГОРИТМЫ В ТЕОРИИ ЧИСЕЛ И КРИПТОГРАФИИ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности
1-31 03 01 Математика (по направлениям)
Направление специальности 1-31 03 01-01
Математика (научно-производственная деятельность)

2015 г.

Учебная программа составлена на основе ОСВО 1-31 03 01-2013 (30.08.2013) и учебного плана № G31-140/уч. 2013 г. (30.05.2013) по специальности 1-31 03 01 Математика (по направлениям) (направление специальности 1-31 03 010-01 Математика (научно-производственная деятельность)

СОСТАВИТЕЛИ:
Васильев Денис Владимирович – доцент кафедры высшей алгебры и защиты информации механико-математического университета Белорусского государственного университета, кандидат физико-математических наук

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой высшей алгебры и защиты информации
(протокол № 11 от 22.05.2015)

Учебно-методической комиссией механико-математического факультета Белорусского государственного университета
(протокол № 6 от 29.06.2015)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

В настоящее время теоретико-числовые алгоритмы повсеместно используются в различных системах обеспечения безопасности информации, таких как системы шифрования, цифровой подписи и обмена ключами. Целью курса является знакомство учащихся с базовыми теоретико-числовыми алгоритмами, использующимися в современных асимметрических криптосистемах, а также рассмотрение ряда вспомогательных теоретических вопросов алгебры и теории чисел, необходимых для понимания работы алгоритмов защиты информации.

Дисциплина тесно связана с такими дисциплинами как «Алгебра и теория чисел».

Цель дисциплины «Алгоритмы в теории чисел и криптографии»: изложить базовые алгоритмы теории чисел в применении к задачам криптографии.

Образовательная цель: изучение теоретических основ современных методов защиты информации, знакомство с базовыми алгоритмами, использующихся в асимметрических криптосистемах.

Развивающая цель: формирование у студентов алгоритмического мышления и общей математической культуры, привитие студентам умения самостоятельно изучать учебную и научную литературу в области математики.

Основные задачи, решаемые в рамках изучения дисциплины «Алгоритмы в теории чисел и криптографии»:

- познакомить учащихся с базовыми теоретико-числовыми алгоритмами, использующимися в современных асимметрических криптосистемах;
- развить алгоритмическое мышление и общую математическую культуру;
- привить студентам умение самостоятельно изучать учебную и научную литературу в области математики.
- привить студентам умение самостоятельно изучать учебную и научную литературу в области математики и ее приложений.

В результате изучения учебной дисциплины студент должен

знать:

– основные математические методы, лежащие в основе построения современных криптосистем;

– базовые теоретико-числовые алгоритмы криптографии;

уметь:

– выполнять вычисления в конечных полях;

– уметь решать теоретико-числовые и алгоритмические задачи по курсу «Алгоритмы в теории чисел и криптографии»;

владеть:

– основными навыками решения задач теории чисел и криптографии;

– методами оценки сложности алгоритмов;

– навыками самообразования и способами использования аппарата алгебры и теории чисел для проведения математических и междисциплинарных исследований.

–

Учебная программа предназначена для студентов 2 и 3 курса (4,5 семестр) очной формы получения образования.

–

В соответствии с учебным планом специальности на изучение дисциплины отводится 99 часов, в том числе 52 часа аудиторных занятий. Распределение аудиторных часов по видам занятий: лекции – 38 часов, практические занятия-8 часов, УСР – 6 часов. Рекомендуемая форма отчетности – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Базовые теоретико-числовые алгоритмы

Полиномиальные, субэкспоненциальные и экспоненциальные алгоритмы. Алгоритм Евклида. Расширенный алгоритм Евклида, бинарный алгоритм Евклида

Тема 2. Эффективные алгоритмы арифметики

Эффективные методы выполнения арифметических операций над целыми числами. Метод Карацубы. Умножение с помощью системы остаточных классов.

Тема 3. Алгоритмы генерации больших простых чисел

Детерминированные алгоритмы тестирования чисел на простоту. Вероятностные алгоритмы тестирования чисел на простоту

Тема 4.Алгоритмы шифрования и распределения ключей.

Алгоритм шифрования RSA. Выбор криптостойких параметров для схемы RSA. Алгоритм Диффи-Хеллмана с аутентификацией сторон.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА

Номер раздела, темы, занятия	Название раздела, темы, занятия; перечень изучаемых вопросов	Количество аудиторных часов				Материальное обеспечение занятия (наглядные,	Форма контроля знаний
		Лекции	практические (семинарские) занятия	лабораторные занятия	контролируемая самостоятельная работа студента		
1	2	3	4	5	6	7	8
1	**Базовые теоретико-числовые алгоритмы**	**16**			**2**		
1.1	Полиномиальные, субэкспоненциальные и экспоненциальные алгоритмы.	2					Проверка индивидуальных заданий
1.2	Алгоритм Евклида. Расширенный алгоритм Евклида, бинарный алгоритм Евклида.	2					Проверка индивидуальных заданий
1.3	Оценка числа шагов и сравнение эффективности.	2					Проверка индивидуальных заданий
1.4	Алгоритмы решения систем линейных диофантовых уравнений. Китайская теорема об остатках.	2					Проверка индивидуальных заданий
1.5	Китайская теорема об остатках.	2			2		Контрольная работа
1.6	Алгоритмы решения квадратичных сравнений.	2					Проверка индивидуальных заданий
1.7	Алгоритмы решения полиномиальных уравнений в простом конечном поле.	2					Проверка индивидуальных заданий
1.8	Поднятие решений, лемма Гензеля.	2					Проверка индивидуальных заданий
2	**Эффективные алгоритмы арифметики**	**8**	**4**		**2**		
2.1	Эффективные методы выполнения арифметических операций над целыми числами.	2					Проверка индивидуальных заданий
2.2	Метод Карацубы. Умножение с помощью системы остаточных классов.		2				Проверка индивидуальных заданий Проверка индивидуальных заданий
2.3	Операция Монтгомери.	2			2		Контрольная работа
2.4	Редукция Баррета.		2				Проверка индивидуальных заданий
2.5	Бинарные алгоритмы возведения в степень в	2					Проверка индивидуальных

	алгебраических структурах.						заданий
2.6	Редукция по модулю специального вида	2					Проверка индивидуальных заданий
3	**Алгоритмы генерации больших простых чисел**	**8**	**2**				
3.1	Детерминированные алгоритмы тестирования чисел на простоту.	2					Проверка индивидуальных заданий
3.2	Тест простоты для чисел Мерсенна.		2				Проверка индивидуальных заданий
3.3	Вероятностные алгоритмы тестирования чисел на простоту.	2					Проверка индивидуальных заданий
3.4	Тест Миллера-Рабина. Оценка числа шагов.	2					Проверка индивидуальных заданий
3.5	Методы генерации простых чисел.						Проверка индивидуальных заданий
3.6	Методы ускорения алгоритмов генерации простых чисел.	2					Проверка индивидуальных заданий
4	**Алгоритмы шифрования и распределения ключей.**	**6**	**2**		**2**		
4.1	Алгоритм шифрования RSA.	2					Проверка индивидуальных заданий
4.2	Выбор криптостойких параметров для схемы RSA.		2				Проверка индивидуальных заданий
4.3	Алгоритм Диффи-Хеллмана для распределения ключей.	2			2		Контрольная работа
4.4	Алгоритм Диффи-Хеллмана с аутентификацией сторон.	2					Проверка индивидуальных заданий
	Итого	**38**	**8**		**6**		

ИНФОРМАЦИОННАЯ ЧАСТЬ

Основная литература

1. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии. – Мн., БГУ, 1999
2. Нестеренко Ю.В. Теория чисел. – М., 2008.
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М., 2003.

Дополнительная литература

1. Коблиц Н. Курс теории чисел и криптографии, Научное издательство ТВП, 2001, 254 с.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Алгебра и теория чисел	Кафедра высшей алгебры и теории чисел	нет	Вносить изменения не требуется (прот. № 11 от 22.05.2015)