Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе

_____ А.Л. Толстик

_____

Регистрационный № УД-1593 / уч.

АРИФМЕТИЧЕСКИЕ И АЛГЕБРАИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-98 01 01 Компьютерная безопасность (по направлениям)

2015 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-98 01 01-2013 и учебного плана Р 98-138/уч., 30.05.2013.

Составители:

Г. В. Матвеев, доцент кафедры высшей математики Белорусского государственного университета, кандидат физико-математических наук, доцент.

Рекомендована к утверждению:

Кафедрой математического моделирования и анализа данных Белорусского государственного университета (протокол № 19 от 07 апреля 2015 г.);

Учебно-методической комиссией факультета прикладной математики и информатики Белорусского государственного университета (протокол № 6 от 12 мая 2015 г.).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Большинство криптографических алгоритмов основаны на использовании операций в конкретных группах, кольцах и полях, не говоря уже о кольце целых чисел. Вот почему раздел под названием арифметические и алгебраические основы криптографии является необходимой составной частью любого учебника и учебного плана по криптографии.

Настоящий курс призван познакомить слушателя с рядом важнейших разделов теории чисел нашедших применения в криптографии. К их числу относятся: решение сравнений и систем сравнений первой степени, функция Эйлера, китайская теорема об остатках и некоторые другие вопросы.

На этой основе дается строгое описание математических моделей RSA-криптосистемы и электронной цифровой подписи на ее основе, а также хранения секрета в разделенном виде и CRT-пороговых схем.

Алгебраическая часть курса посвящена в основном изучению строения полей Галуа и дискретному логарифмированию в этих полях.

Это позволяет перейти к изучению линейных рекуррент и их связи с поточными шифрами. Для линейных рекуррентных последовательностей над конечными полями подробно изучаются их периоды, а также минимальный и характеристический многочлены.

Учебная дисциплина «Арифметические и алгебраические основы криптографии» относится к циклу дисциплин вузовского компонента и взаимосвязана с учебными дисциплинами «Геометрия и алгебра», «Вычислительные методы алгебры». Методы, излагаемые в дисциплине «Арифметические и алгебраические основы криптографии», могут быть использованы при изучении ряда других дисциплин по специальности «Компьютерная безопасность».

В результате изучения дисциплины студент должен

***знать*:**

- основные свойства делимости и теории сравнений в кольце целых чисел;
- основные свойства групп, колец и полей, расширений полей и полей Галуа;
- математическую модель RSA-криптосистемы и электронной цифровой подписи на ее основе, китайскую теорему об остатках и хранение секрета в разделенном виде, CRT-пороговые схемы;
- основные структурные свойства ЛРП над полями Галуа и их обоснование в рамках теории полей Галуа;
- использование ЛРП над полями Галуа в поточных криптосистемах;
- генерацию ЛРП с помощью регистров сдвига с обратной связью;
- использование ЛРП для генерации псевдослучайных последовательностей;

уметь:

– решать сравнения и системы сравнений первой степени и применять для этой цели функцию Эйлера и китайскую теорему об остатках;

– решать показательные и степенные сравнения путем индексирования;

– строить регистры сдвига для ЛРП, заданных в явном виде над различными полями;

– находить линейную сложность и рекуррентные уравнения по известным отрезкам периодической последовательности;

– решать базовые задачи теории ЛРП;

– оценивать частотные и периодические характеристики последовательностей;

– применять датчики на основе ЛРП для построения поточных криптосистем.

– ***владеть:***

– методами решения типовых задач по теории сравнений и теории конечных полей;

– навыками анализа математических моделей криптосистем с открытым ключом и схем цифровой подписи;

– навыками анализа кодов и их применения в криптографии;

– основными методами задач теории ЛРП над полями Галуа;

– методами построения усложненных ЛРП для последующего использования в качестве ключей поточных криптосистем.

В соответствии с образовательным стандартом специальности 1-98 01 01 «Компьютерная безопасность» учебная программа предусматривает для изучения дисциплины всего 82 часа, из них 34 аудиторных часов, в том числе лекций – 34 часа (3 курс, 5 семестр).

Форма текущей аттестации по учебной дисциплине – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Введение. Предмет курса и его цели и задачи, основные определения.

Раздел 1. Теория делимости

Тема 1.1. Простые числа. Простые числа. Каноническое разложение. Понятие о тестах на простоту и о проблеме факторизации. Применение алгоритма Евклида к проблеме факторизации.

Тема 1.2. Тесты на простоту. Понятие о тестах на простоту и о проблеме факторизации. Применение алгоритма Евклида к проблеме факторизации.

Раздел 2. Теория сравнений

Тема 2.1. Сравнения и системы сравнений. Решение сравнений и систем сравнений первой степени. Функция Эйлера.

Тема 2.2. RSA-криптосистема. RSA-криптосистема. Электронная цифровая подпись на основе RSA-криптосистемы.

Тема 2.3. Китайская теорема об остатках. Хранение секрета в разделенном виде. CRT-пороговые схемы.

Раздел 3. Показательные и степенные сравнения.

Тема 3.1. Решение показательных и степенных сравнений. Решение показательных и степенных сравнений путем индексирования.

Тема 3.2. Задача дискретного логарифмирования. Протокол Диффи-Хелмена.

Тема 3.3. Современные стандарты цифровой подписи. Примеры современных стандартов цифровой подписи.

Раздел 4. Кольца и поля.

Тема 4.1. Коды в криптографии. Коды и их применение в криптографии. Простые и максимальные идеалы.

Тема 4.2. Поля Галуа. Евклидовы кольца. Расширения полей Галуа. Строение полей Галуа.

Тема 4.3. Дискретное логарифмирование в полях Галуа. Поле разложения. Группы Галуа.

Тема 4.4. Коды и их применение в криптографии. Примеры применения кодов в криптографии.

Раздел 5. Линейные рекурренты.

Тема 5.1. Линейные рекурренты и поточные шифры. Линейные рекурренты. Связь линейных рекуррент с поточными шифрами.

Тема 5.2. Характеристические многочлены. Минимальный и характеристический многочлены.

Тема 5.3. Конечные поля и линейные рекурренты. Линейные рекуррентные последовательности над конечными полями.

Тема 5.4. Периоды ЛРП. Понятие периода ЛРП.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

№п/п	Название раздела, темы	Количество часов				Количество часов УСР	Форма контроля знаний
		Аудиторные					
		Лекции	Практ. и сем. занятия	Лаб. занятия	Иное		
	Введение.	**2**					
1	**Теория делимости**.	**4**					
1.1	Простые числа	2					
1.2	Тесты на простоту	2					
2	**Теория сравнений**	**6**					
2.1	Сравнения и системы сравнений	2					
2.2	RSA-криптосистема	2					
2.3	Китайская теорема об остатках.	2					
3	**Показательные и степенные сравнения**	**6**					
3.1	Решение показательных и степенных сравнений	2					
3.2	Задача дискретного логарифмирования	2					
3.3	Современные стандарты цифровой подписи	2					Коллоквиум
4	**Кольца и поля**	**8**					
4.1	Коды в криптографии	2					
4.2	Поля Галуа	2					
4.3	Дискретное логарифмирование в полях Галуа	2					
4.4	Коды и их применение в криптографии	2					
5	**Линейные рекурренты**	**8**					
5.1	Линейные рекурренты и поточные шифры	2					
5.2	Характеристические многочлены	2					
5.3	Конечные поля и линейные рекурренты	2					
5.4	Периоды ЛРП	2					Коллоквиум
ИТОГО		**34**					

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Рекомендуемая литература

Основная

1.Харин Ю.С.и др. Криптология учебник, Минск, БГУ, 2013
2.Бейкер А. Введение в теорию чисел. - Мн.: Высш. шк.,1995
3.Виноградов И. М. Основы теории чисел. - М.: Наука, 1991
4Лидл Р., Нидеррайтер Г. Конечные поля. – М.: Мир, Т.1,2. 1988
5.J. Hoffstein J. Pipher J. Silverman An Introduction to Mathematical Cryptography_ 2008, Springer, 2008

Дополнительная

1.Харин, Ю.С. Компьютерный практикум по математическим методам защиты информации / Ю.С. Харин, СВ. Агиевич. – Минск : БГУ, 2001.
2.Логачев, О.А. Булевы функции в криптологии / О.А. Логачев [и др.]. – М. : МЦНМО, 2012.
3.Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / М. : МЦНМО, 2003.
4.Stinson P. Cryptography: Theory and Practice. - CRS-Press,1995.

Рекомендации по контролю качества усвоения знаний и проведению аттестации

На лекционных занятиях по учебной дисциплине «Арифметические и алгебраические основы криптографии» рекомендуется использовать элементы проблемного обучения: проблемное изложение некоторых аспектов, использование частично-поискового метода.

Для аттестации обучающихся на соответствие их персональных достижений поэтапным и конечным требованиям образовательной программы создаются фонды оценочных средств, включающие типовые задания, контрольные работы и тесты. Оценочными средствами предусматривается оценка способности обучающихся к творческой деятельности, их готовность вести поиск решения новых задач, связанных с недостаточностью конкретных специальных знаний и отсутствием общепринятых алгоритмов.

Для диагностики компетенций в рамках учебной дисциплины рекомендуется использовать следующие формы:

– устная форма: собеседование, устный промежуточный зачет, итоговый зачет;

– письменная форма: тест, контрольный опрос, контрольная работа;

– устно-письменная форма: отчет по домашним практическим упражнениям с их устной защитой.

Контрольные мероприятия проводятся в соответствии с учебно-методической картой дисциплины. В случае неявки на контрольное мероприятие по уважительной причине студент вправе по согласованию с преподавателем выполнить его в дополнительное время. Для студентов, получивших неудовлетворительные оценки за контрольные мероприятия, либо не явившихся по неуважительной причине, по согласованию с преподавателем и с разрешения заведующего кафедрой мероприятие может быть проведено повторно.

Оценка текущей успеваемости рассчитывается как среднее оценок за каждую из письменных контрольных работ, оценки за отчеты по домашним практическим упражнениям и оценки за итоговый тест.

Итоговая аттестация предусматривает проведение зачета. При этом рекомендуется использовать оценивание успеваемости на основе модульно-рейтинговой системы.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Геометрия и алгебра	Кафедра математического моделирования и анализа данных	нет	Оставить содержание учебной дисциплины без изменения, протокол № 19 от 07 апреля 2015 г.
Вычислительные методы алгебры	Кафедра математического моделирования и анализа данных	нет	Оставить содержание учебной дисциплины без изменения, протокол № 19 от 07 апреля 2015 г.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ

на _____/_____ учебный год

№№ Пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры дискретной математики и алгоритмики (протокол № ____ от _____ 201_ г.)

Заведующий кафедрой

_____ _____ _____

(ученая степень, звание) (подпись) (И.О. Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ _____ _____

(ученая степень, звание) (подпись) (И.О.Фамилия)