Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и
образовательным инновациям
_____ С.М. Чуприс
“ 20 ” 06 2018 г.
Регистрационный № УД-_____/уч.

КРИПТОГРАФИЯ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Учебная программа учреждения высшего образования
второй ступени (магистратуры)
по учебной дисциплине специальной подготовки для специальностей:
1-31 80 03 Математика
1-31 81 06 Веб-программирование и интернет-технологии
1-31 81 07 Математическое и программное обеспечение мобильных устройств

2018 г.

Учебная программа составлена на основе ОСВО 1-31 80 03 – 2012 от 24.08.2012 №108, ОСВО 1-31 81 06 – 2013, ОСВО 1-31 81 07 – 2013 и учебных планов №G31-257/уч., №G31-258/уч. от 26.05.2017 по специальности 1-31 80-03 Математика, №G31-227/уч от 10.04.2017, №G31з-231/уч от 26.05.2017 по специальности 1-31 81 06 Веб-программирование и интернет-технологии, №G31-228/уч от 10.04.2017 и №G31з-230/уч от 26.05.2017 по специальности 1-31 81 07 Математическое и программное обеспечение мобильных устройств.

СОСТАВИТЕЛЬ:
Васильев Д. В.– доцент кафедры высшей алгебры и защиты информации механико-математического факультета Белорусского государственного университета, кандидат физико-математических наук.

РЕЦЕНЗЕНТЫ:
Берник В.И. – главный научный сотрудник Института математики НАН Беларуси, доктор физико-математических наук, профессор;
Калоша Н.И. – научный сотрудник Института математики НАН Беларуси, кандидат физико-математических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой высшей алгебры и защиты информации
(протокол № 9 от 18.04.2018)

Научно-методическим Советом Белорусского государственного университета
(протокол № 6 от 16.06.2018)

Зав.кафедрой ВАиЗИ /В.В. Беняш-Кривец/

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

За последние десятилетия такие направления научного исследования как криптография и компьютерная безопасность стали особенно актуальны для развития современного общества. Владение знаниями и навыками по этим специальностям, стало насущной необходимостью в работе любого специалиста естественнонаучного профиля. Эти дисциплины находятся на стыке нескольких научных и технических направлений, но особо важную роль в них играют математические методы и алгоритмы обеспечения информационной безопасности. Программа дисциплины «Криптография и компьютерная безопасность» охватывает ту часть этих дисциплин, которая непосредственно относится к математическим методам используемым при построении современных криптосистем.

Цель дисциплины «Криптография и компьютерная безопасность»: Обучить магистрантов математическим методам, лежащим в основе построения и работы современных криптосистем.

Образовательная цель: ознакомить магистрантов с методами обеспечения компьютерной и сетевой безопасности; дать математическое обоснование алгоритмов криптографии с открытым ключом; познакомить учащихся с некоторыми методами анализа криптосистем.

Развивающая цель: формирование у учащихся понимания принципов построения и работы современных систем защиты информации.

Основные задачи, решаемые в рамках изучения дисциплины специальной подготовки «Криптография и компьютерная безопасность»:

В результате изучения учебной дисциплины студент должен

знать:

– общие математические основы построения криптосистем с открытым ключом;
– протоколы работы широко используемых криптосистем.
– требования, налагаемые на параметры широко используемых криптосистем таких как шифрование с открытым ключом, цифровая подпись, распределение секретных ключей.

уметь:

– с помощью расширенного алгоритма Евклида решать линейные сравнения по произвольному модулю и находить обратные элементы в кольце вычетов;
– применять китайскую теорему об остатках для ускорения выполнения арифметических операций с большими числами;
– вычислять степени элементов группы с помощью различных версий бинарного алгоритма;
– уметь решать алгебраические уравнения над простым конечным полем;
– находить элементы заданного порядка в циклических группах;

владеть:

– методами оценки сложности алгоритмов
– умножением целых чисел по методу Карацубы;
– умножением в кольце вычетов по методам Монтгомери и Баррета;
– методами тестирования простоты чисел Миллера-Рабина и некоторыми детерминированные тестами, а также алгоритмами для построения больших простых чисел.
– методами выполнения операции в группе точек эллиптической кривой;

– алгоритмами генерации и проверки электронной цифровую подписи по схеме Эль-Гамаля, ECDSA, ГОСТ Р 34.10-2012, СТБ 34.101.45-2013.

Преподавание данной дисциплины должно строиться таким образом, чтобы обучающийся приобретал следующие компетенции:

академические

АК-1. Способность к самостоятельной научно-исследовательской деятельности (анализ, сопоставление, систематизация, абстрагирование, моделирование, проверка достоверности данных, принятое решений и др.), готовность генерировать и использовать новые идеи.

АК-3. Способность к постоянному самообразованию.

социально-личностные

СЛК-1. Совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования своей личности.

СЛК-2. Пользоваться одним из государственных языков Республики Беларусь и иным иностранным языком как средством делового общения.

СЛК-3. Формировать и аргументировать собственные суждения и профессиональную позицию.

профессиональные

ПК-1. Разрабатывать практические рекомендации по использованию научных исследований, планировать и проводить экспериментальные исследования, исследовать показатели технического уровня разработок программного обеспечения информационных систем.

ПК-2. Владеть основными методами, способами и средствами получения, хранения, переработки информации. Применять современные методы проектирования информационных систем, использовать веб-сервисы.

ПК-3. Применять методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности и в областях знаний, непосредственно не связанных со сферой деятельности.

ПК-4. Разрабатывать и тестировать информационные системы, осуществлять защиту приложений и данных.

ПК-5. Заниматься аналитической и научно-исследовательской деятельностью в области математики и информационных технологий.

ПК-6. Использовать и развивать современные информационные технологии и средства автоматизации управленческой деятельности.

ПК-7. Проводить исследования в области эффективности решения производственных задач.

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

Дисциплина «Криптография и компьютерная безопасность» относится к циклу дисциплин специальной подготовки (государственный компонент) и предназначена для магистрантов 1 курса (1 семестр) очной и заочной форм получения образования.

В соответствии с учебными планами специальностей на изучение учебной дисциплины отводится:

Очная форма обучения

Курс, семестр	Всего часов	Аудиторных	Лекции	Текущая аттестация
1-31 80 03 Математика УП рег. №G31-257/уч. (26.05.2017)				
1 курс 1 семестр	144	34	34	Экзамен
1-31 81 06 Веб-программирование и интернет-технологии УП рег. №G31-227/уч (10.04.2017) 1-31 81 07 Математическое и программное обеспечение мобильных устройств УП рег. №G31-228/уч (10.04.2017)				
1 курс 1 семестр	136	34	34	Экзамен

Заочная форма обучения

Курс, семестр	Всего часов	Аудиторных	Лекции	Текущая аттестация
1-31 80 03 Математика УП рег. №G31-258/уч. (26.05.2017)				
1 курс 1 семестр	144	10	10	Экзамен
1-31 81 06 Веб-программирование и интернет-технологии УП рег. №G31з-231/уч (26.05.2017) 1-31 81 07 Математическое и программное обеспечение мобильных устройств УП рег. №G31з-230/уч (26.05.2017)				
1 курс 1 семестр	136	10	10	Экзамен

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Теоретико-числовые основы

Делимость в кольце целых чисел. НОД, НОК, разрешимость линейного диофантового уравнения.

Закон распределения простых чисел, оценки расстояний между соседними простыми числами.

Алгоритм Евклида, расширенный алгоритм Евклида, оценка сложности алгоритма Евклида.

Сравнения, их свойства, решение линейного сравнения, китайская теорема об остатках, мультипликативные функции, функция Эйлера, теорема Эйлера, малая теорема Ферма.

Квадратичные вычеты. Символ Лежандра. Теорема Эйлера для квадратичных вычетов, Квадратичный закон взаимности. Символы Якоби. Вычисление символа Лежандра.

Первообразные корни. Структура мультипликативной группы кольца вычетов.

Тема 2. Базовые алгоритмы

Сложность алгоритмов: полиномиальные, субэкспоненциальные, экспоненциальные алгоритмы. Примеры.

Бинарные алгоритмы возведения в степень. Метод скользящего окна. Алгоритм решения квадратичных сравнений. Общий алгоритм решения полиномиальных сравнений.

Метод Карацубы для умножения целых чисел. Умножение целых чисел при помощи китайской теоремы об остатках. Операция Монтгомери и редукция Баррета.

Детерминированный тест на простоту. тест Миллера-Рабина. Алгоритм построения больших простых чисел. Алгоритм нахождения элемента циклической группы с заданным порядком.

Эллиптические кривые, группа точек эллиптической кривой. Вывод формул сложения. Алгоритм вычисления кратной точки.

Эффективные методы вычисления операции сложения точек эллиптической кривой. Кривые в форме Вейерштрасса, Монтгомери, Эдвардса.

Тема 3. Криптосистемы с открытым ключом

Криптосистема RSA. Алгоритм Диффи-Хеллмана распределения ключей. Схема цифровой подписи Эль-Гамаля.

Алгоритмы цифровой подписи на эллиптических кривых ECDSA, ГОСТ Р 34.10-2012, СТБ 34.101.45-2013.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА
(очная форма обучения)

Номер раздела, Темы	Название раздела, темы	Количество аудиторных часов				Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Иное		
1	2	3	4	5	6	7	8
1	**Теоретико-числовые основы**	**12**					
1.1	Делимость в кольце целых чисел. НОД, НОК, разрешимость линейного диофантового уравнения.	2					Экспресс-опрос
1.2	Закон распределения простых чисел, оценки расстояний между соседними простыми числами.	2					Экспресс-опрос
1.3	Алгоритм Евклида, расширенный алгоритм Евклида, оценка сложности алгоритма Евклида.	2					Собеседование
1.4	Сравнения, их свойства, решение линейного сравнения, китайская теорема об остатках, мультипликативные функции, функция Эйлера, теорема Эйлера, малая теорема Ферма.	2					Экспресс-опрос
1.5	Квадратичные вычеты. Символ Лежандра. Теорема Эйлера для квадратичных вычетов, Квадратичный закон взаимности. Символы Якоби. Вычисление символа Лежандра.	2					Экспресс-опрос
1.6	Первообразные корни. Структура мультипликативной группы кольца вычетов.	2					Тест
2	**Базовые алгоритмы**	**12**					
2.1	Сложность алгоритмов: полиномиальные, субэкспоненциальные, экспоненциальные алгоритмы. Примеры.	2					Экспресс-опрос
2.2	Бинарные алгоритмы возведения в степень. Метод скользящего окна. Алгоритм решения квадратичных сравнений. Общий алгоритм решения полиномиальных	2					Собеседование

	сравнений.						
2.3	Метод Карацубы для умножения целых чисел. Умножение целых чисел при помощи китайской теоремы об остатках. Операция Монтгомери и редукция Баррета.	2					Экспресс-опрос
2.4	Детерминированный тест на простоту. тест Миллера-Рабина. Алгоритм построения больших простых чисел. Алгоритм нахождения элемента циклической группы с заданным порядком.	2					Собеседование
2.5	Эллиптические кривые, группа точек эллиптической кривой. Вывод формул сложения. Алгоритм вычисления кратной точки.	2					Экспресс-опрос
2.6	Эффективные методы вычисления операции сложения точек эллиптической кривой. Кривые в форме Вейерштрасса, Монтгомери, Эдвардса.	2					Тест
3	**Криптосистемы с открытым ключом**	**10**					
3.1	Криптосистема RSA.	2					Экспресс-опрос
3.2	Алгоритм Диффи-Хеллмана распределения ключей.	2					Собеседование
3.3	Схема цифровой подписи Эль-Гамаля.	2					Экспресс-опрос
3.4	Алгоритмы цифровой подписи на эллиптических кривых ECDSA, ГОСТ Р 34.10-2012,	2					Собеседование
3.5	СТБ 34.101.45-2013.	2					Тест
	Итого	**34**					

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА
(заочная форма обучения)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов				Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Иное		
1	2	3	4	5	6	7	8
1	**Теоретико-числовые основы**	**2**					Экпресс-опрос
2	**Базовые алгоритмы**	**4**					Экспресс-опрос, тест
3	**Криптосистемы с открытым ключом**	**4**					Экспресс-опрос, контрольная работа
	Итого	**10**					

ИНФОРМАЦИОННАЯ ЧАСТЬ

ОСНОВНАЯ ЛИТЕРАТУРА

1. Виноградов И.М. «Основы теории чисел», м.-Л., Гостехиздат, 1952— 180 с.
2. Нестеренко Ю.В. «Теория чисел», М.: Академия, 2008. — 272 с.
3. Д.Кнут «Искусство программирования на ЭВМ» т.2, Москва: Издательский дом «Вильямс», 2001
4. Харин Ю.С., Агиевич С.В., Васильев Д.В., Матвеев Г.В. *Криптология*. (Учебник с грифом Минобразования). – Минск: БГУ, 2014. – 512 с

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

5. Василенко О.Н. «Теоретико-числовые алгоритмы в криптографии» — М.: МЦНМО, 2003. — 328 с.
6. Шнайер Б. «Прикладная криптография. Протоколы и алгоритмы на С» Вильямс, 2016, 1024 с.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СРЕДСТВ ДИАГНОСТИКИ РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

При чтении лекционного курса непосредственно в аудитории необходимо контролировать усвоение материала основной массой студентов путем проведения экспресс-опросов, тестирования и контрольной работы по конкретным темам. По итогам семестра проводится экзамен.

Методика формирования итоговой оценки

Итоговая оценка формируется на основе 3-ех документов:

1. Правила проведения аттестации (Постановление №53 от 29.05.2012 г.).
2. Положение о рейтинговой системе БГУ (ред. 2015 г.).
3. Критерии оценки студентов (10 баллов).

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

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)
Алгебра и теория чисел	Кафедра высшей алгебры и защиты информации	Нет	Вносить изменения не требуется(пр. №9 от 26.04.2018)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УВО
на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры высшей алгебры и защиты информации (протокол № ____ от _____ 20__ г.)

Заведующий кафедрой

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

УТВЕРЖДАЮ
Декан факультета

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

РЕЦЕНЗИЯ

на учебную программу дисциплины
«Криптография и компьютерная безопасность»

Программа курса «Криптография и компьютерная безопасность» для магистрантов 1 курса очной и заочной формы обучения предполагается изучение базовых математических понятий и алгоритмов, на которых основаны современные криптосистемы, а также методы обеспечения компьютерной безопасности, использующиеся при организации сетевого взаимодействия. В курсе рассматриваются основные понятия теории чисел, необходимые для построения криптосистем с открытым ключом, а также базовые алгоритмы, использующиеся при работе таких криптосистем. В третьей части курса рассмотрены основные криптосистемы для шифрования (RSA), цифровой подписи стандарты ECDSA и СТБ для формирования и проверки электронной цифровой подписи, а также алгоритм распределения секретного ключа Диффи-Хеллмана.

Материалы, включенные в курс, являются необходимым минимумом для понимания работы современных методов защиты информации и обеспечения компьютерной безопасности. Рецензируемая программа рекомендуется в качестве учебной программы учреждения высшего образования второй ступени (магистратуры) по учебной дисциплине специальностей: 1-31 80 03 «Математика», 1-31 81 06 «Веб-программирование и интернет-технологии», 1-31 81 07 «Математическое и программное обеспечение мобильных устройств»

Рецензент
Доктор физико-математических наук, профессор,
главный научный сотрудник Института математики
НАН Беларуси В.И. Берник

Подпись В.И. Берника заверяю:
Ведущий специалист
по кадрам
Института математики
НАН Беларуси Т.И. Лисовик

РЕЦЕНЗИЯ
на учебную программу дисциплины
«Криптография и компьютерная безопасность»

Курс «Криптография и компьютерная безопасность» читается в течение 1 семестра для магистрантов 1 курса механико-математического факультета БГУ. Цель данного курса – ознакомить магистрантов с методами обеспечения компьютерной и сетевой безопасности; дать математическое обоснование алгоритмов криптографии с открытым ключом; познакомить учащихся с некоторыми методами анализа криптосистем.

Преподавание дисциплины строится в форме лекций (34 часа).

Планируется рассмотреть следующие темы: теоретико-числовые основы криптографии с открытым ключом, базовые алгоритмы для реализации криптосистем, примеры некоторых криптосистем с открытым ключом (криптосистема RSA, алгоритмы распределения ключей и электронной цифровой подписи).

Отбор материалов для курса «Криптография и компьютерная безопасность» представляется вполне обоснованным. Объем планируемого к изложению материала соответствует часам, отводимым на изучение предмета. Рассматриваемый курс позволит магистрантам овладеть знаниями основ криптографии и компьютерной безопасности. Рецензируемая программа рекомендуется в качестве учебной программы учреждения высшего образования второй ступени (магистратуры) по учебной дисциплине специальностей: 1-31 80 03 «Математика», 1-31 81 06 «Веб-программирование и интернет-технологии», 1-31 81 07 «Математическое и программное обеспечение мобильных устройств»

Рецензент
Кандидат физико-математических наук,
Научный сотрудник Института математики
НАН Беларуси Н.И. Калоша

Подпись Н.И. Калоша заверяю:
Ведущий специалист по кадрам Института математики НАН Беларуси
Г.М. Хисамова