Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе
_____ А.Л. Толстик
"31" мая 2015 г.
Регистрационный № УД-1660/уч.

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Учебная программа учреждения высшего образования
по учебной дисциплине для специальности
1-31 03 01 Математика (по направлениям)
(направление 1-31 03 01-05 Математика (информационные технологии))

2015 г.

Учебная программа составлена на основе ОСВО 1-31 03 01-2008 (30.08.2008) и учебного плана № G31-019/уч. (24.09.2008) по специальности 1-31 03 01 Математика (по направлениям) (направление специальности 1-31 03 01-05 Математика (информационные технологии)).

СОСТАВИТЕЛИ:

Тихонов Сергей Викторович – доцент кафедры высшей алгебры и защиты информации механико-математического факультета Белорусского государственного университета, кандидат физико-математических наук, доцент.

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)

(Бенеш-Кривец В.В.)

(Тихонов С.В.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

В настоящее время теоретико-числовые и алгебраические методы повсеместно используются в различных системах обеспечения безопасности информации, таких как системы шифрования, цифровой подписи и обмена ключами. Предлагаемый курс посвящен рассмотрению базовых вопросов, связанных с разработкой и реализацией современных криптосистем с открытым ключом, использующих в своей работе методы теории чисел и алгебры.

В рамках курса предполагается рассмотреть ряд вспомогательных теоретических вопросов алгебры и теории чисел, необходимых для понимания основ работы алгоритмов защиты информации. Кроме того, изучаются эллиптические кривые, на преобразования в которых основаны современные методы криптографической защиты информации с открытым ключом. Аппарат теории эллиптических кривых оказывается полезным и при анализе криптографических алгоритмов, основанных на задачах факторизации целых чисел и дискретного логарифмирования в конечном поле.

Данный курс опирается и использует изученные ранее сведения из дисциплин «Web-программирование», «Методы программирования и информатика».

Цель дисциплины «Теоретико-числовые методы в криптографии»: изложить алгебраические и теоретико-числовые основы криптографии с открытым ключом.

Образовательная цель: знакомство с основными понятиями алгебры и теории чисел, а также теории эллиптических кривых, используемыми при построении криптосистем с открытым ключом, а также в алгоритмах факторизации и проверки числа на простоту.

Развивающая цель: формирование у студентов основ математического мышления, знакомство с методами математических доказательств, изучение алгоритмов решения конкретных математических задач, привитие студентам умения самостоятельно изучать учебную и научную литературу в области математики и защиты информации.

Основные задачи, решаемые в рамках изучения дисциплины «Теоретико-числовые методы в криптографии»:

- ознакомить студентов с фундаментальными понятиями алгебры и теории чисел, используемыми в криптографии с открытым ключом;
- изучить основы теории эллиптических кривых;
- ознакомить студентов с основными принципами построения криптосистем с открытым ключом;
- ознакомить студентов с некоторыми алгоритмами факторизации и проверки числа на простоту;

- развить у студентов аналитическое мышление и общую математическую культуру;
- привить студентам умение самостоятельно изучать учебную и научную литературу в области математики и ее приложений.

В результате изучения учебной дисциплины студент должен

знать:

– основные понятия алгебры, теории чисел и криптографии с открытым ключом;

– методы доказательств важнейших результатов, изучаемых в рамках учебной дисциплины «Теоретико-числовые методы в криптографии»;

– алгоритмы решения задач по дисциплине «Теоретико-числовые методы в криптографии»;

уметь:

– выполнять вычисления в конечных полях и группах точек эллиптических кривых над конечными полями;

– вычислять порядки групп точек специальных эллиптических кривых;

владеть:

– основными навыками решения задач, связанных с группами, полями и эллиптическими кривыми;

– методами доказательств основных теорем, встречающихся в курсе «Теоретико-числовые методы в криптографии»;

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

Учебная программа предназначена для студентов 5 курса (9 семестр) очной формы получения образования.

В соответствии с учебным планом специальности на изучение дисциплины отводится 128 часов, в том числе 68 часов аудиторных занятий. Из них лекции – 34 часа, семинарские занятия – 12 часов, лабораторные занятия – 20 часов, УСР – 2 часа. Форма отчетности – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Алгебраические основы

Группа. Подгруппа. Факторгруппа. Кольцо. Идеал. Простые и максимальные идеалы. Факторкольцо. Теорема о гомоморфизме колец. Поле. Характеристика поля. Степень расширения полей. Конечные поля. Число элементов в конечном поле. Мультипликативная группа конечного поля.

Тема 2. Теоретико-числовые основы

Квадратичные вычеты по модулю p. Символ Лежандра. Символ Якоби. Квадратичный закон взаимности. Китайская теорема об остатках. Первообразные корни.

Тема 3. Эллиптические кривые

Аффинное и проективное пространства. Уравнение Вейерштрасса над полями различной характеристики. Определение эллиптической кривой. Групповой закон на множестве точек эллиптической кривой. Формулы сложения точек в аффинных и проективных координатах. Вычисление кратной точки. Задача дискретного логарифмирования. Вычисление порядка группы точек эллиптической кривой над конечным полем. Дзета-функция эллиптической кривой. Теорема Вейля для эллиптической кривой. Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем.

Тема 4. Криптосистемы с открытым ключом

Понятие односторонней функции. Протокол обмена ключами Диффи–Хеллмана. Криптосистема RSA. Атаки на криптосистему RSA. Криптосистема Рабина. Криптосистема Эль-Гамаля. Электронная цифровая подпись. Схема электронной цифровой подписи Эль-Гамаля.

Тема 5. Алгоритмы факторизации и проверки числа на простоту

Факторизация целых чисел с помощью эллиптических кривых. Вероятностный тест Соловея-Штрассена на простоту.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов по УСР	Литература	Форма контроля знаний
		лекции	практические занятия	семинарские занятия	лабораторные занятия	Иное			
1	2	3		4	5	6	7	8	9
1	**Алгебраические основы**	**8**		**8**				[4,5]	
1.1	Группа. Подгруппа. Факторгруппа	2		2					
1.2	Кольцо. Идеал. Простые и максимальные идеалы. Факторкольцо. Теорема о гомоморфизме колец	2		2					
1.3	Поле. Характеристика поля. Степень расширения полей	2		2					
1.4	Конечные поля. Число элементов в конечном поле. Мультипликативная группа конечного поля	2		2					Проверка индивидуа-льных заданий
2	**Теоретико-числовые основы**	**6**		**4**	**2**			[3]	
2.1	Квадратичные вычеты по модулю p. Символ Лежандра. Символ Якоби. Квадратичный закон взаимности	4		2	2				
2.2	Китайская теорема об остатках. Первообразные корни	2		2					
3	**Эллиптические кривые**	**8**			**8**			[5]	
3.1	Аффинное и проективное пространства. Уравнение Вейерштрасса над полями различной характеристики. Определение эллиптической кривой	2			2				
3.2	Групповой закон на множестве точек эллиптической кривой. Формулы сложения точек в аффинных и проективных координатах. Вычисление кратной точки. Задача дискретного логарифмирования.	2			2				
3.3	Вычисление порядка группы точек эллиптической кривой над конечным полем. Дзета-функция	2			2				

	эллиптической кривой								
3.4	Теорема Вейля для эллиптической кривой. Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем	2			2				Проверка индивидуальных заданий
4	**Криптосистемы с открытым ключом**	**8**			**6**		**2**	[1, 5]	
4.1	Понятие односторонней функции. Протокол обмена ключами Диффи–Хеллмана	2			2				
4.2	Криптосистема RSA. Атаки на криптосистему RSA	2			2				
4.3	Криптосистема Рабина. Криптосистема Эль-Гамаля	2			2				
4.4	Электронная цифровая подпись. Схема электронной цифровой подписи Эль-Гамаля	2					2		Контрольная работа
5	**Алгоритмы факторизации и проверки числа на простоту**	**4**			**4**			[2]	
5.1	Факторизация целых чисел с помощью эллиптических кривых	2			2				Проверка индивидуальных заданий
5.2	Вероятностный тест Соловея-Штрассена на простоту	2			2				
	Итого по дисциплине	**34**		**12**	**20**		**2**		

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2001.
2. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. МЦНМО. 2003.
3. Виноградов И. М. Основы теории чисел. М.: Наука. 1981.
4. Ленг С. Алгебра. М.: Мир. 1968.
5. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. АНО НПО Профессионал. 1985.

Дополнительная литература

6. Коблиц Н. Введение в эллиптические кривые и модулярные формы. М.: Мир. 1988.
7. Koblitz N. Algebraic aspects of cryptography. Springer-Verlag. 1998.
8. Silverman J.H. The arithmetic of elliptic curves. Springer-Verlag. 1985.
9. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии. Учебное пособие. Новое знание, 2003.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ СРЕДСТВ ДИАГНОСТИКИ РЕЗУЛЬТАТОВ УЧЕБНОЙ ДЕЯТЕЛЬНОСТИ

Рекомендуются следующие формы диагностики компетенций.

Письменная форма
1.Контрольная работа

Устно-письменная форма
1.Проверка индивидуальных заданий.
2.Экзамен.

ПЕРЕЧЕНЬ ЗАДАНИЙ И КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Контрольные мероприятия СР по дисциплине «Теоретико-числовые методы в криптографии» проводятся преподавателем, как правило, во время аудиторных занятий.

Полученные студентом количественные результаты СР учитываются как составная часть итоговой оценки по дисциплине в рамках рейтинговой системы.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ЗАДАНИЙ

Индивидуальные задания для самостоятельной работы включают выполнение заданий, которые сдаются на проверку в письменном виде с последующей защитой.

(1) Является ли группой множество положительных целых чисел с обычной операцией умножения?
(2) Найти порядок группы (Z/121Z)*
(3) Содержит ли поле F_{27} поле F_9?
(4) Сколько корней в поле F_{81} имеет многочлен $x^3+ x$?
(5) Найдите символ Якоби (388/27).
(6) Найдите остаток от деления 19315 на 8.
(7) Пусть эллиптическая кривая E задана над полем F_3 уравнением $y^2 + y = x^3+x$. Найти $|E(F_9)|$.
(8) Найти такое натуральное n, что $n \equiv 4(\mathrm{mod}\ 7)$, $n \equiv 2(\mathrm{mod}\ 3)$ и $n \equiv 3(\mathrm{mod}\ 4)$.
(9) Является ли 43 первообразным корнем по модулю 12.
(10) Какой порядок точки P = (1, 0) в группе точек эллиптической кривой, заданной над полем рациональных чисел уравнением $y^2= x^3- 1$?
(11) Является ли группой множество четных целых чисел с обычной операцией сложения?
(12) Сколько элементов в мультипликативной группе поля F_{34}?
(13) Какая характеристика у расширения степени 2 поля F_{25}?
(14) Сколько корней в поле F_{125} имеет многочлен $x^3 - 2x?\neq$
(15) Найдите символ Лежандра (420/41).
(16) Найдите остаток от деления 20107 на 7.
(17) Пусть эллиптическая кривая E задана над полем F_2 уравнением $y^2 +xy = x^3+x+1$. Найти $|E(F_8)|$.
(18) Найти такое натуральное n, что $n \equiv 2(mod\ 8)$, $n \equiv 3(mod\ 5)$ и $n \equiv 1(mod\ 3)$.

(19) Является ли 32 первообразным корнем по модулю 15?
(20) Сколько элементов второго порядка в группе E(Q), где E — эллиптическая кривая, заданная над полем рациональных чисел уравнением $y^2=x^3-8$?
(21) Является ли группой множество нечетных целых чисел с обычной операцией сложения?
(22) Сколько элементов в группе (Z/56Z)*?
(23) Может ли поле характеристики 5 быть расширением поля характеристики 3?
(24) Сколько корней в поле F_{25} имеет многочлен $x3-x+1$?
(25) Найдите символ Якоби (573/35).
(26) Найдите остаток от деления 29^{297} на 5.
(27) Пусть эллиптическая кривая E задана над полем F_3 уравнением $y^2+y=x^3-x$. Найти $|E(F_9)|$.
(28) Найти такое натуральное n, что $n \equiv 2(mod\ 9)$, $n \equiv 1(mod\ 4)$ и $n \equiv 3(mod\ 5)$.
(29) Является ли 20 первообразным корнем по модулю 9?
(30) Является ли проективная кривая, заданная над полем рациональных чисел уравнением $zy^2=x^3-x^2z$, эллиптической кривой?
(31) Является ли группой множество нечетных целых чисел с обычной операцией умножения?
(32) Являются ли полями следующие множества с естественными операциями: $Z \cup \{1/m|m \in Z, m \neq 0\}$, Z/49Z, $M_2(C)$?
(33) Найдите $\phi(102)$.
(34) Какая характеристика у расширения степени три поля F_{16}?
(35) Сколько корней в поле F_{27} имеет многочлен x^3+2x+1?
(36) Является ли 63 квадратичным вычетом по модулю 23?
(37) Найдите остаток от деления 21^{351} на 8.
(38) Пусть эллиптическая кривая E задана над полем F^2 уравнением $y^2+y=x^3+x^2$. Найти $|E(F_8)|$.
(39) Найти такое натуральное n, что $n \equiv 3(mod\ 7)$, $n \equiv 4(mod\ 5)$ и $n \equiv 5(mod\ 6)$.
(40) Является ли 21 первообразным корнем по модулю 8?
(41) Является ли 3 квадратом в поле F_5?
(42) Является ли группой множество вещественных чисел с обычной операцией умножения?
(43) Являются ли полями следующие множества с естественными операциями: $\{1/m|m \in Z, m \neq 0\} \cup \{0\}$,Z/125Z, $\{A \in M_3(R)|det(A) \neq 0\}$?
(44) Сколько элементов в мультипликативной группе поля F_2^5.
(45) Какая характеристика у поля, состоящего из 81 элемента?
(46) Сколько корней в поле F_{27} имеет многочлен x^3+x-1?
(47) Найдите символ Лежандра (882/43).
(48) Найдите остаток от деления 29247 на 12.
(49) Пусть эллиптическая кривая E задана над полем F_2 уравнением $y^2-xy=x^3+x-1$. Найти $|E(F_{16})|$.
(50) Найти такое натуральное n, что $n \equiv 1(mod\ 6)$, $n \equiv 4(mod\ 5)$ и $n \equiv 5(mod\ 7)$.
(51) Является ли 13 первообразным корнем по модулю 10?
(52) Найдите в F_5 элемент, обратный к 3.
(53) Является ли проективная кривая, заданная над полем рациональных чисел уравнением $zy^2=x^3-xz^2$, эллиптической кривой?
(54) Какой порядок точки P = (1, 0) в группе точек эллиптической кривой, заданной над полем рациональных чисел уравнением $y^2=x^3-1$?

(55) Сколько элементов второго порядка в группе $E(\mathbb{Q})$, где E — эллиптическая кривая, заданная над полем рациональных чисел уравнением $y^2 = x^3 - 8$?
(56) Найдите порядок точки $P = (0, 4)$ эллиптической кривой, заданной уравнением $y^2 = x^3 + 16$ над полем рациональных чисел.
(57) Найдите порядок точки $P = (0, 1)$ эллиптической кривой, заданной уравнением $y^2 + xy = x^3 + 1$ над полем F_2.
(58) Найдите все F_4-точки эллиптической кривой, заданной уравнением $y^2 + y = x^3$.
(59) Найдите все точки порядка 2 на эллиптической кривой, заданной уравнением $y^2 = x^3 + x$ над полем F_5.
(60) Найдите координаты точки $-P$ для $P = (2, 1)$ на эллиптической кривой, заданной уравнением $y^2 = x^3 + x + 1$ над полем F_5.
(61) Пусть эллиптическая кривая E задана над полем F_3 уравнением $y^2 - y = x^3 + x$. Найти $|E(F_9)|$.
(62) Пусть эллиптическая кривая E задана над полем F_2 уравнением $y^2 - xy = x^3 + x^2 - x$. Найти $|E(F_{16})|$.
$y^2 - y = x^3 + 2x$. Найти $|E(F_9)|$.
(63) Пусть эллиптическая кривая E задана над полем F_2 уравнением $y^2 - xy = x^3 + x - 1$. Найти $|E(F_{16})|$.
(64) Пусть эллиптическая кривая E задана над полем F_3 уравнением $y^2 + y = x^3 + x$. Найти $|E(F_9)|$.
(65) Пусть эллиптическая кривая E задана над полем F_3 уравнением $y^2 + y = x^3 - x$. Найти $|E(F_9)|$.

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)
Web-программирование	Кафедра веб-технологий и моделирования	нет	Вносить изменения не требуется (прот. № 11 от 22.05.2015)
Методы программирования и информатика	Кафедра веб-технологий и моделирования	нет	Вносить изменения не требуется (прот. № 11 от 22.05.2015)

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ
на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
(протокол № ____ от _____ 20_ г.)

Заведующий кафедрой

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

УТВЕРЖДАЮ
Декан факультета

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