Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и
образовательным инновациям
_____ О.Г. Прохоренко
«05» июля 2023 г.

Регистрационный № УД – 12623/уч.

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В 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)

2023 г.

Учебная программа составлена на основе ОСВО 1-31 03 01-2021, типового учебного плана №G 31-1-011/пр.тип от 31.03.2021, и учебного плана № G-31-1-003/уч от 25.05.2021.

СОСТАВИТЕЛИ:

Беняш-Кривец Валерий Вацлавович – заведующий кафедрой высшей алгебры и защиты информации Белорусского государственного университета, доктор физико-математических наук, профессор;

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

РЕЦЕНЗЕНТЫ:

Васильев Денис Владимирович, заведующий отделом теории чисел и дискретной математики Института математики НАН Беларуси, кандидат физико-математических наук.

Кафедрой высшей алгебры и защиты информации
Белорусского государственного университета
(протокол № 11 от 08.06.2023);

Научно-методическим советом БГУ
(протокол № 9 от 29.06.2023)

Зав. кафедрой высшей алгебры
и защиты информации, профессор В.В. Беняш-Кривец

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

За последнее время компьютерная безопасность и криптография стали особенно актуальны для развития современного общества. Эти дисциплины находятся на стыке нескольких научных направлений, но особо важную роль в них играют математические методы и алгоритмы обеспечения информационной безопасности. Программа дисциплины “Теоретико-числовые методы в криптографии” непосредственно посвящена математическим методам, используемым при построении современных криптосистем. Целью учебной дисциплины является обучение студентов теоретико-числовым и алгебраическим методам, лежащим в основе построения и работы современных криптосистем.

Образовательная цель: ознакомить студентов с теоретико-числовыми и алгебраическими методами обеспечения компьютерной безопасности; дать математическое обоснование алгоритмов криптографии с открытым ключом.

Развивающая цель: формирование у обучающихся понимания принципов построения и работы современных систем 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 чисел 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.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина относится к **дисциплинам специализаций** компонента учреждения высшего образования.

Связи с другими учебными дисциплинами, включая учебные дисциплины компонента учреждения высшего образования, дисциплины специализации и др.

Данная дисциплина опирается и использует изученные ранее сведения из дисциплин «Алгебра и теория чисел», «Дополнительные главы алгебры».

Требования к компетенциям специалиста

Освоение учебной дисциплины «Теоретико-числовые методы в криптографии» должно обеспечить формирование следующих компетенций:

базовые профессиональные компетенции:

БПК-2. Использовать понятия и методы вещественного, комплексного и функционального анализа и применять их для изучения моделей окружающего мира.

БПК-5. Применять основные алгебраические и геометрические понятия, конструкции и методы при решении теоретических и прикладных математических задач.

Специализированные компетенции:

СК-2. Применять ключевые методы защиты информационных систем при реализации криптоприложений.

В результате изучения учебной дисциплины студент должен:

знать:

– общие математические основы построения криптосистем с открытым ключом;

– протоколы работы широко используемых криптосистем;

уметь:

– производить вычисления в конечных полях;

– находить символы Лежандра и Якоби;

– находить порядок группы точек специальных эллиптических кривых над конечными полями;

– строить конечные поля заданного порядка;

– строить расширения полей и выполнять вычисления в них;

владеть:

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

– методами доказательств основных теорем, встречающихся в дисциплине «Теоретико-числовые методы в криптографии».

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

Структура учебной дисциплины

Дисциплина изучается в 6 семестре. Всего на изучение учебной дисциплины «Теоретико-числовые методы в криптографии» отведено 120 часов, в том числе 68 аудиторных часов, из них: лекции – 62 часа, управляемая самостоятельная работа – 6 часов.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы. Формой текущей аттестации по учебной дисциплине является экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Алгебраические основы

Группа. Подгруппа. Факторгруппа. Алгоритмы возведения в степень. Задача дискретного логарифмирования. Кольцо. Идеал. Простые и максимальные идеалы. Факторкольцо. Теорема о гомоморфизме колец. Поле. Характеристика поля. Степень расширения полей. Алгебраические расширения.

Тема 2. Конечные поля

Число элементов в конечном поле. Мультипликативная группа конечного поля. Автоморфизм Фробениуса. Критерий неприводимости многочленов над конечным полем. Алгоритм Берлекэмпа. Построение неприводимых многочленов над конечным полем.

Тема 3. Теоретико-числовые основы

Алгоритм Евклида. Функция Эйлера. Теорема Эйлера. Квадратичные вычеты по модулю p. Символ Лежандра. Квадратичный закон взаимности. Символ Якоби. Вычисление символа Якоби. Китайская теорема об остатках. Первообразные корни. Существование первообразных корней.

Тема 4. 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. Эллиптические кривые над кольцами классов вычетов.

Тема 5. Вычисление порядка группы точек эллиптической кривой над конечным полем

Кольцо формальных степенных рядов. Дзета-функция эллиптической кривой. Теорема Вейля для эллиптической кривой. Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем.

Тема 6. Алгоритмы факторизации и проверки числа на простоту

Детерминированные тесты на простоту. Числа Мерсенна. Вероятностные тесты Соловея-Штрассена и Миллера-Рабина на простоту. Факторизация целых чисел с помощью эллиптических кривых. Тестирование чисел на простоту с помощью эллиптических кривых.

Тема 7. Криптосистемы с открытым ключом

Понятия односторонней функции и односторонней функции с секретом. Протокол обмена ключами Диффи–Хеллмана. Криптосистема Эль-Гамаля. Криптосистема RSA. Атаки на криптосистему RSA. Криптосистема Рабина.

Тема 8. Электронная цифровая подпись

Общая схема электронной цифровой подписи. Схема электронной цифровой подписи Эль-Гамаля. Схема электронной цифровой подписи на эллиптических кривых.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная форма получения высшего образования с применением дистанционных образовательных технологий (ДОТ)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Формы контроля знаний
		лекции	практические занятия	семинарские занятия	лабораторные занятия	Иное		
1.	**Алгебраические основы**	8						Устный опрос
2.	**Конечные поля**	8						Устный опрос
3.	**Теоретико-числовые основы**	8					2	Устный опрос, контрольная работа №1
4.	**Эллиптические кривые**	8						Устный опрос
5.	**Вычисление порядка группы точек эллиптической кривой над конечным полем**	8						Устный опрос
6.	**Алгоритмы факторизации и проверки числа на простоту**	8					2	Устный опрос, контрольная работа №2
7.	**Криптосистемы с открытым ключом**	8					2	Устный опрос, коллоквиум
8.	**Электронная цифровая подпись**	6						Устный опрос
	Итого	**62**					**6**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Глухов, М. М. Алгебра: учебник для вузов / М. М. Глухов, В. П. Елизаров, А. А. Нечаев. – 4-е изд., стер. – Санкт-Петербург: Лань, 2022. – 608 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/187793.
2. Мартынов, Л. М. Алгебра и теория чисел для криптографии: учебное пособие для вузов / Л. М. Мартынов. – 2-е изд., стер. – Санкт-Петербург: Лань, 2022. – 456 с. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/189446
3. Виноградов И. М. Основы теории чисел: учебное пособие [для вузов] / И. М. Виноградов. - Изд. 15-е, стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2023. - 176 с. URL: https://e.lanbook.com/book/298499
4. Харин, Ю.С. Криптология. / Ю.С. Харин, С.В. Агиевич, Д.В. Васильев, Г.В. Матвеев. – Минск: БГУ, 2013. – 512 с. URL: https://elib.bsu.by/handle/123456789/259637
5. Харин, Ю.С. Математические основы теории информации: учеб. пособие для студ. учреждений высш. образования по спец. "Компьютерная безопасность", "Прикладная криптография" / Ю. С. Харин, И. А. Бодягин, Е. В. Вечерко; БГУ. - Минск: БГУ, 2018.
6. Авдошин, С.М. Дискретная математика. Модулярная алгебра, криптография, кодирование / С. М. Авдошин, А. А. Набебин; [науч. ред. В. А. Захаров]. - Москва: ДМК Пресс, 2017.
7. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии. / О.Н. Василенко.– Москва: МЦНМО, 2003. – 326 с.

Перечень дополнительной литературы

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2001.
2. Черемушкин, А.В. Лекции по арифметическим алгоритмам в криптографии. / А.В. Черемушкин. – Москва: МЦНМО, 2002.
3. Коблиц, Н. Введение в эллиптические кривые и модулярные формы. / Н. Коблиц. – М.: Мир, 1988.
4. Коблиц, Н. Курс теории чисел и криптографии. / Н. Коблиц. – Москва: Научное изд-во ТВП, 2001. – 254 с.
5. Hankerson, D. Guide to elliptic curve cryptography. / D. Hankerson, A. Menezes, S. Vanstone – Springer-Verlag, 2004. – 332 p.
6. Koblitz, N. Algebraic aspects of cryptography. / N/ Koblitz. - Springer-Verlag, 1998.

7. Silverman, J.H. The arithmetic of elliptic curves. / J.H. Silverman. - Springer-Verlag, 1985.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Формой текущей аттестации по дисциплине «Теоретико-числовые методы в криптографии» учебным планом предусмотрен **экзамен.**

Контроль работы студента проходит в форме устного опроса, коллоквиума, выполнения контрольных, самостоятельных работ и практических упражнений в аудитории. Задания к самостоятельным работам составляются согласно содержанию учебного материала.

Итоговая отметка формируется на основе 3-х документов:

1. Правила проведения аттестации студентов, курсантов, слушателей при освоении содержания образовательных программ высшего образования (Постановление Министерства образования Республики Беларусь № 53 от 29.05.2012 г.).

2. ПОЛОЖЕНИЕ о рейтинговой системе оценки знаний обучающихся по учебной дисциплине в Белорусском государственном университете (Приказ ректора БГУ № 189-ОД от 31.03.2020).

3. Критериев оценки результатов учебной деятельности обучающихся в учреждениях высшего образования по десятибалльной шкале (Письмо Министерства образования Республики Беларусь от 28.05.2013 г. № 09-10/53-ПО).

При формировании итоговой отметки используется рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая система предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Формирование отметки за текущую успеваемость:

Отметка текущей успеваемости представляет собой среднеарифметическую величину отметок по всем формам (мероприятиям) текущего контроля знаний по учебной дисциплине.

Итоговая отметка по дисциплине рассчитывается на основе отметки текущей успеваемости и экзаменационной отметки с учетом их весовых коэффициентов. Вес отметки по текущей успеваемости составляет 40%, экзаменационной отметки – 60%.

Примерный перечень заданий для управляемой самостоятельной работы студентов

Тема 3. Теоретико-числовые основы. (2 ч.)

Примерный перечень заданий.

1. Методом математической индукции докажите, что для любого натурального n число a делится на число b: а) $a=6^{2n}-1,\ b=35$; б) $a=4^n+15n-1,\ b=9$; в) $a=n^3+5n+12,\ b=6$.
2. Найдите неполное частное и остаток от деления числа a на число b: а) $a=761, b=13$; б) $a=437, b=24$.
3. С помощью алгоритма Евклида вычислите $НОД(a,b)$ и выразите его через исходные числа. Используя связь НОД и НОК двух натуральных чисел, вычислите $НОК(a,b)$: а) $a=5544, b=7644$; б) $a=1188, b=3080$; в) $a=1296, b=6600$.
4. С помощью канонических разложений чисел a,b,c найдите $НОД(a,b,c)$ и $НОК(b,c)$: а) $a=6188, b=88, c=-320$; б) $a=1188, b=-132, c=-64$; в) $a=9100, b=92, c=-114$.
5. Решить в целых числах уравнение $1275x-3796y=1$.
6. Вычислите значение функции Эйлера для числа a: а) $a=142560$; б) $a=421200$.
7. Сколько элементов в поле, являющемся расширением степени 2 поля F_9?
8. Сколько корней в поле F_{125} имеет многочлен x^3+x+1?
9. Содержит ли поле F_{625} поле F_{16}?
10. Содержит ли поле F_{32} поле F_{16}?
11. Какая характеристика у расширения степени 3 поля F_{49}?
12. Сколько корней в поле F_{81} имеет многочлен x^3+2x+1?

Форма контроля – контрольная работа №1.

Тема 6. Алгоритмы факторизации и проверки числа на простоту. (2 ч.)

Примерный перечень заданий.

1. Найдите остаток от деления 23^{519} на 9.
2. Найдите символ Якоби $\left(\frac{136}{21}\right)$.
3. Сколько элементов второго порядка в группе E(Q), где E – эллиптическая кривая, заданная над полем рациональных чисел уравнением $y^2=x^3-8$?
4. Пусть эллиптическая кривая E задана над полем F_2 уравнением $y^2+y=x^3+x^2$. Найдите $|E(F_8)|$.

5. Найдите порядок точки P=(0,4) на эллиптической кривой, заданной над полем рациональных чисел уравнением $y^2=x^3+16$.

6. Найдите все точки второго порядка на эллиптической кривой, заданной над полем характеристики 5 уравнением $y^2=x^3+x$.

Форма контроля – контрольная работа №2.

Тема 7. Криптосистемы с открытым ключом. (2 ч.)

Примерный перечень заданий.

1. Объясните, как можно решить сравнение $x^e \equiv c(\mathrm{mod}\, N)$, если известно значение $\varphi(n)$.
2. Решите сравнения:

1) $x^{577} \equiv 60(\mathrm{mod}1463)$; 2) $x^{959} \equiv 1583(\mathrm{mod}1625)$; 3) $x^{133957} \equiv 224689(\mathrm{mod}\, 2134440)$.

3. Алиса опубликовала свои открытые ключи: $N = 2038667$ $e = 103$.

а) Боб хочет отправить Алисе сообщение $m = 892383$. Какое цифровое сообщение пошлет Боб Алисе?

б) Алиса знает, что ее модуль делится на простое число $p = 1301$. Найти секретную экспоненту d для Алисы.

в) Алиса получила зашифрованный текст $c = 317730$ от Боба. Расшифруйте сообщение.

4. Пусть выбраны 2 числа $p = 41$ и $q = 17$ в качестве параметров системы RSA. Какой из параметров $e_1 = 32$, $e_2 = 49$ можно взять в качестве экспоненты RSA? Вычислите соответствующие секретные ключи $K_{pr} = (p, q, d)$.
5. Пусть E, D – взаимно-обратные преобразования RSA-криптосистемы. Тогда выполняется $D(E(x)) = x$ для любого $x \in \mathbb{Z}_n^*$. Показать, что это равенство справедливо для любого x.

Форма контроля – коллоквиум.

Примерные варианты контрольных работ

Контрольная работа 1.

1. Сколько элементов в мультипликативной группе поля, являющегося расширением степени 5 поля F_9?
2. Пусть степень расширения $F(\alpha)/F$ нечетная. Докажите, что $F(\alpha^2)= F(\alpha)$.
3. Сколько корней в поле F_{125} имеет многочлен x^3+x+1?
4. Разложите многочлен x^4+x^3+x+2 на неприводимые множители над полем F_3.
5. Содержит ли поле F_{625} поле F_{125}?

Контрольная работа 2.

1. С помощью алгоритма Евклида вычислите *НОД* (554, 762) и выразите его через исходные числа.
2. Найдите символ Якоби $\left(\frac{136}{21}\right)$
3. Найдите остаток от деления 19^{315} на 8.
4. Сколько элементов второго порядка в группе E(Q), где E – эллиптическая кривая, заданная над полем рациональных чисел уравнением $y^2=x^3-8$?
5. Пусть эллиптическая кривая E задана над полем F_2 уравнением $y^2+y=x^3+x^2$. Найдите $|E(F_8)|$.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используется **практико-ориентированный подход**, который предполагает:

– освоение содержание образования через решения практических задач;

– приобретение навыков эффективного выполнения разных видов профессиональной деятельности;

– ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;

– использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

Методические рекомендации по организации самостоятельной работы обучающихся

Для организации самостоятельной работы студентов по учебной дисциплине «Теоретико-числовые методы в криптографии» используются современные информационные ресурсы: размещается на образовательном портале комплекс учебных и учебно-методических материалов (учебно-программные материалы, учебное издание для теоретического изучения дисциплины, материалы текущего контроля и текущей аттестации, позволяющие определить соответствие учебной деятельности обучающихся требованиям образовательного стандарта высшего образования и учебно-программной документации, в т.ч. вопросы для подготовки к экзамену,

задания, вопросы для самоконтроля и др., список рекомендуемой литературы, информационных ресурсов и др.).

При изучении дисциплины до сведения студентов вначале семестра доводится информация, которая включает: методы и формы контроля знаний и правила начисления баллов. Для активации работы студентов в семестре используется:

– организация непрерывного текущего контроля качества знаний студентов в течение всего срока изучения дисциплины;

– стимулирование работы студентов в течение семестра на основе использования накопительной рейтинговой системы;

– повышение значимости самостоятельной и индивидуальной работы путем разработки и выдачи студентам индивидуальных вариантов заданий, возможность получить консультацию и индивидуальную помощь при их выполнении;

– дифференцированный подход к оценке знаний студентов, стимулирование высокого рейтинга по дисциплине.

Примерный перечень вопросов к экзамену

1. Группа. Определение. Примеры.
2. Подгруппа. Факторгруппа.
3. Гомоморфизм групп. Теорема о гомоморфизме групп.
4. Порядок элемента группы. Циклическая группа. Примеры.
5. Кольца. Определение. Примеры.
6. Мультипликативная группа кольца.
7. Идеал. Факторкольцо.
8. Гомоморфизм колец. Теорема о гомоморфизме колец.
9. Простые и максимальные идеалы.
10. Идеалы в кольце целых чисел.
11. Идеалы в кольце многочленов.
12. Поле. Определение. Примеры.
13. Критерии простоты и максимальности идеалов.
14. Характеристика поля. Определение. Примеры.
15. Степень расширения полей.
16. Число элементов в конечном поле.
17. Существование конечного поля, состоящего из p^n элементов.
18. Мультипликативная группа конечного поля.
19. Автоморфизм Фробениуса.
20. Критерий неприводимости многочленов над конечными полями.
21. Алгоритм Берлекэмпа.
22. Построение неприводимых многочленов над конечным полем.
23. Алгоритм Евклида.
24. Функция Эйлера. Теорема Эйлера.

25. Квадратичные вычеты по модулю p.
26. Символ Лежандра. Определение. Критерий Эйлера.
27. Свойства символа Лежандра.
28. Символ Якоби. Определение и свойства.
29. Китайская теорема об остатках.
30. Первообразные корни. Существование первообразных корней по модулям p^n и $2p^n$.
31. Аффинное и проективное пространства.
32. Определение эллиптической кривой.
33. Групповой закон на множестве точек эллиптической кривой.
34. Формулы сложения точек эллиптической кривой. Аффинные и проективные координаты.
35. Бинарный метод вычисления кратной точки. Задача дискретного логарифмирования.
36. Дзета-функция эллиптической кривой. Теорема Вейля для эллиптической кривой.
37. Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем.
38. Детерминированные тесты на простоту. Числа Мерсенна.
39. Тест Соловея-Штрассена проверки числа на простоту.
40. Тест Миллера-Рабина проверки числа на простоту.
41. Факторизация целых чисел с помощью эллиптических кривых.
42. Тестирование чисел на простоту с помощью эллиптических кривых.
43. Протоколом обмена ключами Диффи-Хеллмана.
44. Понятие односторонней функции. Криптосистема Эль-Гамаля.
45. Криптосистема RSA.
46. Криптосистема Рабина.
47. Электронная цифровая подпись Эль-Гамаля.
48. Электронная цифровая подпись на эллиптических кривых.

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	высшей алгебры и защиты информации	Нет	Вносить изменения не требуется (протокол № 11 от 08.06.2023)
Дополнительные главы алгебры	высшей алгебры и защиты информации	Нет	Вносить изменения не требуется (протокол № 11 от 08.06.2023)

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 Высшей алгебры и защиты информации (протокол № ____ от _____ 20__ г.)

Заведующий кафедрой

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

УТВЕРЖДАЮ
Декан факультета

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