

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ

Ректор Белорусского
государственного университета

А.Д.Король

23 декабря 2024 г.

Регистрационный № УД- 13433/уч.



ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Учебная программа учреждения образования по учебной дисциплине для
специальности

1-31 03 01 Математика (по направлениям)

Направление специальности:

1-31 03 01-01 Математика (научно-производственная деятельность)

2024 г.

Учебная программа составлена на основе ОСВО 1-31 03 01-2021 и учебного плана № G-31-1-207/уч от 22.03.2022.

СОСТАВИТЕЛИ:

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

Беняш-Кривец Валерий Вацлавович, профессор кафедры высшей алгебры и защиты информации механико-математического факультета Белорусского государственного университета, доктор физико-математических наук, профессор.

РЕЦЕНЗЕНТЫ:

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

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой высшей алгебры и защиты информации БГУ
(протокол № 4 от 21.11.2024);

Научно-методическим советом БГУ
(протокол № 5 от 19.12.2024)

Заведующий кафедрой высшей алгебры
и защиты информации, доцент



С.В. Тихонов

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»:

1. Ознакомить студентов с фундаментальными понятиями алгебры и теории чисел, используемыми в криптографии с открытым ключом;
2. Изучить основы теории эллиптических кривых;
3. Ознакомить студентов с основными принципами построения криптосистем с открытым ключом;
4. Ознакомить студентов с некоторыми алгоритмами факторизации и проверки чисел на простоту;
5. Развить у студентов аналитическое мышление и общую математическую культуру;
6. 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.

Требования к компетенциям специалиста

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

Базовые профессиональные компетенции:

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

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

Специализированные компетенции:

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:

- навыком решения задач связанных с эллиптическими кривыми и конечными полями;
- навыком доказательства основных теорем, встречающихся в дисциплине «Теоретико-числовые методы в криптографии».
- навыком самообразования и 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:

- для очной формы получения высшего образования – 120 часов, в том числе аудиторных – 68 часов, из них: лекции — 62 часа, управляемая самостоятельная работа – 6 часов.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма промежуточной аттестации – 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 Берлекэмпса. 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. Индексы. Непрерывные дроби.

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. Числа Кармайкла. Детерминированные тесты на простоту. Факторизация целых чисел с помощью эллиптических кривых. Тестирование чисел на простоту с помощью эллиптических кривых. Построение больших простых чисел.

Тема 7. Криптосистемы с открытым ключом

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

Тема 8. Электронная цифровая подпись

Общая схема электронной цифровой подписи. Схема электронной цифровой подписи Эль-Гамала. 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	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	Контрольная работа №2
7	Криптосистемы с открытым ключом	8					2	Коллоквиум
8	Электронная цифровая подпись	6						Устный опрос
	Итого	62					6	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

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.

Дополнительная литература

1. Авдошин, С.М. Дискретная математика. Модулярная алгебра, криптография, кодирование / С. М. Авдошин, А. А. Набебин; [науч. ред. В. А. Захаров]. - Москва: ДМК Пресс, 2017.
2. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии. / О.Н. Василенко.– Москва: МЦНМО, 2003. – 326 с.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2001.
4. Черемушкин, А.В. Лекции по арифметическим алгоритмам в криптографии. / А.В. Черемушкин. – Москва: МЦНМО, 2002.
5. Коблиц, Н. Введение в эллиптические кривые и модулярные формы. / Н. Коблиц. – М.: Мир, 1988.
6. Коблиц, Н. Курс теории чисел и криптографии. / Н. Коблиц. – Москва: Научное изд-во ТВП, 2001. – 254 с.
7. Hankerson, D. Guide to elliptic curve cryptography. / D. Hankerson, A. Menezes, S. Vanstone – Springer-Verlag, 2004. – 332 p.
8. Koblitz, N. Algebraic aspects of cryptography. / N/ Koblitz. - Springer-Verlag, 1998.
9. Silverman, J.H. The arithmetic of elliptic curves. / J.H. Silverman. - Springer-Verlag, 1985.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

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

Контроль работы студента проходит в форме устного опроса, коллоквиума, выполнения контрольных работ. Задания к контрольным работам составляются согласно содержанию учебного материала.

Для формирования итоговой отметки по учебной дисциплине используется модульно-рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая система предусматривает использование весовых коэффициентов для текущей и промежуточной аттестации студентов по учебной дисциплине.

Формирование итоговой отметки в ходе проведения контрольных мероприятий текущей аттестации (примерные весовые коэффициенты, определяющие вклад текущей аттестации в отметку при прохождении промежуточной аттестации):

- устные опросы – 33%,
- коллоквиум – 33%,
- контрольные работы – 33%.

Итоговая отметка по дисциплине рассчитывается на основе итоговой отметки текущей аттестации (рейтинговой системы оценки знаний) 40% и 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 $\text{НОД}(a, b)$ и выразите его через исходные числа. Используя связь НОД и НОК двух натуральных чисел, вычислите $\text{НОК}(a, b)$: 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 $\text{НОД}(a, b, c)$ и $\text{НОК}(b, c)$: 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 $x^e \equiv c \pmod{N}$, если известно значение $\varphi(n)$.
2. Решите сравнения:
 - 1) $x^{577} \equiv 60 \pmod{1463}$; 2) $x^{959} \equiv 1583 \pmod{1625}$; 3) $x^{133957} \equiv 224689 \pmod{2134440}$.
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.

3. 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 $K_{pr}=(p,q,d)$.

4. 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 $\text{НОД}(554, 762)$ 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 содержания 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

При изучении учебной дисциплины рекомендуется использовать следующие формы самостоятельной работы:

- изучение литературы и материалов электронных источников по проблемам дисциплины;
- выполнение домашних заданий.

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 образовательных стандартов общего высшего образования и учебно-программной документации, в т.ч. вопросы для подготовки к зачету, экзамену, задания, вопросы для самоконтроля и др., список рекомендуемой литературы, информационных ресурсов и др.).

Примерный перечень вопросов к экзамену

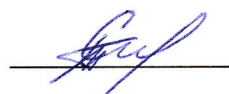
1. Группа. Определение. Примеры.
2. Подгруппа. Факторгруппа.
3. Гомоморфизм групп. Теорема о гомоморфизме групп.
4. Порядок элемента группы. Циклическая группа. Примеры.
5. Кольца. Определение. Примеры.
6. Мультипликативная группа кольца.
7. Идеал. Факторкольцо.
8. Гомоморфизм колец. Теорема о гомоморфизме 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. Протокол обмена ключами Диффи-Хеллмана.
44. Понятие односторонней функции. Криптосистема Эль-Гамала.
45. Криптосистема RSA.
46. Криптосистема Рабина.
47. Электронная цифровая подпись Эль-Гамала.
48. Электронная цифровая подпись на эллиптических кривых.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УО

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)
Учебная дисциплина не требует согласования			

Заведующий кафедрой
высшей алгебры и защиты
информации кандидат
физико-математических наук, доцент



С.В. Тихонов

21.11.2024

**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 _____ 202_ г.)
(название кафедры)

Заведующий кафедрой

(ученая степень, ученое звание)

(И.О.Фамилия)

УТВЕРЖДАЮ

Декан факультета

(ученая степень, ученое звание)

(И.О.Фамилия)