БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Ректор Белорусского
государственного университета
_____А.Д.Король
27 июня 2025 г.
Регистрационный № 4106/б.

ПРИКЛАДНАЯ АЛГЕБРА

Учебная программа учреждения образования по учебной дисциплине для специальности:

6-05-0533-07 Математика и компьютерные науки

Профилизация: Математика

2025 г.

Учебная программа составлена на основе ОСВО 6-05-0533-07-2023 и учебных планов БГУ: № 6-5.4-55/01 от 15.05.2023, № 6-5.4-55/11ин от 31.05.2023.

СОСТАВИТЕЛИ:

С.В.Тихонов, заведующий кафедрой высшей алгебры и защиты информации механико-математического факультета Белорусского государственного университета, кандидат физико-математических наук, доцент;
В.В.Беняш-Кривец, профессор кафедры высшей алгебры и защиты информации механико-математического факультета Белорусского государственного университета, доктор физико-математических наук, профессор

РЕЦЕНЗЕНТ:

Д.В.Васильев, 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 № 13 от 29.05.2025);

Научно-методическим советом БГУ
(протокол № 11 от 26.06.2025)

Заведующий кафедрой _____ С.В.Тихонов

Тихонов / С.В. Тихонов /

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

В настоящее время теоретико-числовые алгоритмы повсеместно используются в различных системах обеспечения безопасности информации, таких как системы шифрования, цифровой подписи и обмена ключами. Целью учебной дисциплины «Прикладная алгебра» является знакомство учащихся с базовыми теоретико-числовыми алгоритмами, использующимися в современных асимметрических криптосистемах, а также рассмотрение ряда вспомогательных теоретических вопросов алгебры и теории чисел, необходимых для понимания работы алгоритмов защиты информации.

Образовательная цель: изложить и строго обосновать большое число теоретико-числовых алгоритмов, возникающих при реализации, построении параметров и исследовании целого класса криптографических схем и протоколов.

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.

Основные задачи, решаемые в рамках изучения дисциплины «Прикладная алгебра»:

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 модулю** «Алгебра и геометрия 2» 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 «Прикладная алгебра» должно обеспечить формирование следующих компетенций:

Базовые профессиональные компетенции:

БПК. Применять основные алгебраические и геометрические понятия, конструкции и методы для решения теоретических и прикладных математических задач.

В результате изучения учебной дисциплины студент должен:

знать:

– основные понятия и результаты алгоритмической теории чисел;

– основные понятия и результаты, связанные с эллиптическими кривыми;

–общие математические основы построения криптосистем с открытым ключом;

уметь:

– производить вычисления в конечных полях и кольцах вычетов;

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

– строить конечные поля заданного порядка;

– строить расширения полей и выполнять вычисления в них;

– строить криптосистемы с открытым ключом;

владеть:

– навыком решения задач связанных с эллиптическими кривыми и конечными полями;

– навыком доказательства основных теорем, встречающихся в дисциплине «Прикладная алгебра».

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

Структура учебной дисциплины

Дисциплина изучается в 5 семестре. Всего на изучение учебной дисциплины «Прикладная алгебра» отведено:

– для очной формы получения высшего образования – 102 часа, в том числе аудиторных – 54 часа, из них: лекции — 28 часов, лабораторные занятия – 22 часа, управляемая самостоятельная работа – 4 часа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма промежуточной аттестации – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Теоретико-числовые основы

Алгоритм Евклида и его применения, теорема Ламе. Простые числа, основная теорема арифметики. Функция Эйлера, ее мультипликативность и вычисление. Теоремы Эйлера и Ферма. Сравнения. Классы вычетов. Решение сравнений первой степени. Китайская теорема об остатках. Операции над классами вычетов. Кольца и поля классов вычетов по модулю n.

Тема 2. Дальнейшие результаты по теории чисел

Первообразные корни. Существование первообразных корней. Индексы. Квадратичные вычеты по модулю p. Символ Лежандра и его свойства. Квадратичный закон взаимности. Символ Якоби и его свойства. Вычисление символов Лежандра и Якоби. Непрерывные дроби. Квадратичные иррациональности и периодические непрерывные дроби. Наилучшие приближения.

Тема 3. Алгоритмы факторизации и проверки числа на простоту

Числа Мерсенна. Вероятностный тест Миллера-Рабина на простоту. Числа Кармайкла. Детерминированные тесты на простоту. Построение больших простых чисел. Алгоритмы факторизации: метод пробного деления, метод Ферма, метод Полларда-Флойда.

Тема 4. Эллиптические кривые

Аффинное и проективное пространства. Определение эллиптической кривой. Уравнение Вейерштрасса над полями различной характеристики. 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. Криптосистемы с открытым ключом

Протокол обмена ключами Диффи–Хеллмана. Криптосистема Эль-Гамаля. Криптосистема RSA. Криптосистема на эллиптической кривой.

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.	**Теоретико-числовые основы**	4			4			Устный опрос
2	**Дальнейшие результаты по теории чисел**	6			2		2	Контрольная работа №1
3	**Алгоритмы факторизации и проверки числа на простоту**	6			4			Устный опрос
4	**Эллиптические кривые**	4			4			Контрольная работа №2
5	**Вычисление порядка группы точек эллиптической кривой над конечным полем**	4			4			Устный опрос.
6	**Криптосистемы с открытым ключом**	4			4		2	Контрольная работа №3
	Итого	**28**			**22**		**4**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Криптология: учебник / Ю. С. Харин, С. В. Агиевич, Д. В. Васильев, Г. В. Матвеев ; БГУ. – 2-е изд., пересмотр. – Минск : БГУ, 2023. – 511 с. – URL: https://elib.bsu.by/handle/123456789/309839
2. 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.
3. 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
4. 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
5. Деза, Е. И. Введение в криптографию. Теоретико-числовые основы защиты информации : [учеб. пособие] / Е. И. Деза, Л. В. Котова. – Изд. стер. – М. : URSS : ЛЕНАНД, 2022. – 368 с.

Дополнительная литература

1. Нестеренко А.Ю. Теоретико-числовые методы в криптографии / А.Ю. Нестеренко. – Москва: Московский государственный институт электроники и математики, 2012. – 224 с.
2. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии. / О.Н. Василенко.– Москва: МЦНМО, 2003. – 326 с.
3. Черемушкин, А.В. Лекции по арифметическим алгоритмам в криптографии. / А.В. Черемушкин. – Москва: МЦНМО, 2002.
4. Коблиц, Н. Введение в эллиптические кривые и модулярные формы. / Н. Коблиц. – М.: Мир, 1988.
5. Коблиц, Н. Курс теории чисел и криптографии. / Н. Коблиц. – Москва: Научное изд-во ТВП, 2001. – 254 с.
6. Hankerson, D. Guide to elliptic curve cryptography. / D. Hankerson, A. Menezes, S. Vanstone – Springer-Verlag, 2004. – 332 p.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

Контроль работы студента проходит в форме устных опросов и выполнения контрольных работ. Задания к контрольным работам составляются согласно содержанию учебного материала.

Формой промежуточной аттестации по дисциплине «Прикладная алгебра» учебным планом предусмотрен **экзамен**.

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 – 50%,
– контрольные работы – 50%.

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 2. Дальнейшие результаты по теории чисел. (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. 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) $a = 1296, b = 6600$.

3. Решить в целых числах уравнение $1275x - 3796y = 1$.

4. Вычислите значение функции Эйлера для числа a: а) $a = 142560$; б) $a = 421200$.

5. Найдите все первообразные корни по модулям 19, 27, 125.

7. Найдите остаток от деления 23^{519} на 9.

8. Решите предложенную систему сравнений первой степени.

8. Найдите символы Лежандра и Якоби $\left(\frac{151}{197}\right), \left(\frac{51}{97}\right), \left(\frac{136}{21}\right)$.

9. Разложите в непрерывную дробь $\sqrt{21}, \frac{85}{43}$.

Форма контроля – контрольная работа №1.

Тема 6. 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 – контрольная работа №3.

Примерные варианты контрольных работ

Контрольная работа № 1.

1. С помощью алгоритма Евклида вычислите *НОД* (554, 762) и выразите его через исходные числа.

2. Найдите символы Лежандра и Якоби $\left(\frac{151}{197}\right)$, $\left(\frac{51}{97}\right)$, $\left(\frac{136}{21}\right)$, $\left(\frac{5381}{6277}\right)$.

3. Найдите остаток от деления 19^{315} на 8.

4. Разложите в непрерывную дробь $\sqrt{27}, \frac{185}{143}$.

5. Решить систему сравнений $\begin{cases} x \equiv 12(\mathrm{mod}\, 31) \\ x \equiv 87(\mathrm{mod}\, 127) \\ x \equiv 91(\mathrm{mod}\, 255) \end{cases}$

Контрольная работа № 2.

1. Сколько элементов второго порядка в группе E(Q), где E – эллиптическая кривая, заданная над полем рациональных чисел уравнением $y^2=x^3-8$?

2. Пусть эллиптическая кривая E задана над полем F_2 уравнением $y^2+y=x^3+x^2$. Найдите $|E(F_8)|$.

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

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

Контрольная работа № 3.

1. Алиса опубликовала свои открытые ключи: $N = 2038667$ $e = 107$.

а) Боб хочет отправить Алисе сообщение $m = 892481$. 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.

2. Пусть выбраны 2 числа $p = 41$ и $q = 17$ в качестве параметров системы RSA. Какой из параметров $e_1 = 30$, $e_2 = 51$ можно взять в качестве экспоненты RSA? Вычислите соответствующие секретные ключи $K_{pr} = (p, q, d)$.

3. Объясните, как можно решить сравнение $x^e \equiv c (\mathrm{mod}\, N)$, если известно значение $\varphi(N)$.

Примерная тематика практических занятий

Лабораторное занятие 1. Делимость в кольце целых чисел. НОД, НОК, разрешимость линейного диофантового уравнения. Простые числа. Основная теорема арифметики. Расширенный алгоритм Евклида, бинарный алгоритм Евклида.

Лабораторное занятие 2. Сравнения и их свойства. Классы вычетов и операции над ними. Кольцо классов вычетов. Решение сравнений первой степени. Китайская теорема об остатках.

Лабораторное занятие 3. Функция Эйлера. Мультипликативность функции Эйлера, формула для вычисления функции Эйлера. Теорема Эйлера. Малая теорема Ферма.

Лабораторное занятие 4. Первообразные корни и индексы. Алгоритм нахождения первообразного корня.

Лабораторное занятие 5. Квадратичные вычеты. Символ Лежандра. Квадратичный закон взаимности Гаусса. Символы Якоби и их свойства. Вычисление символа Лежандра с помощью символа Якоби. Вычисление квадратного корня.

Лабораторное занятие 6. Конечные непрерывные дроби. Понятие подходящей дроби. Свойства подходящих дробей. Периодичность

непрерывных дробей, квадратичные иррациональности. Наилучшие приближения.

Лабораторное занятие 7. Тест на основе малой теоремы Ферма. Числа Кармайкла. Сильно псевдопростые числа. Тест Миллера-Рабина.

Лабораторное занятие 8. Алгоритмы построения больших простых чисел.

Лабораторное занятие 9. 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.

Лабораторное занятие 10. Кольцо формальных степенных рядов. Дзета-функция эллиптической кривой. Теорема Вейля для эллиптической кривой. Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем.

Лабораторное занятие 11. Протокол обмена ключами Диффи–Хеллмана. Криптосистема Эль-Гамаля. Криптосистема RSA. Криптосистема на эллиптической кривой.

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

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. Алгоритм Евклида.
2. Функция Эйлера. Теорема Эйлера.
3. Сравнения. Китайская теорема об остатках.
4. Кольцо классов вычетов.
5. Квадратичные вычеты по модулю p.
6. Символ Лежандра. Определение. Критерий Эйлера.
7. Свойства символа Лежандра.
8. Квадратичный закон взаимности.
9. Символ Якоби. Определение и свойства.
10. Первообразные корни. Существование первообразных корней по модулям $p, p^n, 2p^n$.
11. Детерминированные тесты на простоту. Числа Мерсенна.
12. Тест Миллера-Рабина проверки числа на простоту.
13. Построение больших простых чисел.
14. Алгоритмы факторизации: метод пробного деления, метод Ферма, метод Полларда-Флойда.
15. Определение эллиптической кривой. Уравнение Вейерштрасса над полями различной характеристики.
16. Групповой закон на множестве точек эллиптической кривой.
17. Бинарный метод вычисления кратной точки. Задача дискретного логарифмирования.
18. Дзета-функция эллиптической кривой. Теорема Вейля для эллиптической кривой.
19. Теорема Хассе о порядке группы точек эллиптической кривой над конечным полем.
20. Протоколом обмена ключами Диффи-Хеллмана.
21. Криптосистема RSA.
22. Криптосистема Эль-Гамаля.
23. Криптосистема на эллиптической кривой.

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

29.05.2025

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)