БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям
_____ О.Н. Здрок
«09» декабря 2020 г.
Регистрационный № УД-9467 /уч.

АЛГОРИТМЫ В ТЕОРИИ ЧИСЕЛ И 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)

2020 г.

Учебная программа составлена на основе образовательного стандарта ОСВО 1-31 03 01-2013, утвержденного 30.08.2013, и учебного плана G31-140/уч., утвержденного 30.05.2013.

СОСТАВИТЕЛИ:

Васильев Денис Владимирович – доцент кафедры высшей алгебры и защиты информации механико-математического университета Белорусского государственного университета, кандидат физико-математических наук.

РЕЦЕНЗЕНТ:

Берник Василий Иванович, главный научный сотрудник отдела теории чисел Института математики Национальной академии наук Республики Беларусь, доктор физико-математических наук, профессор.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой высшей алгебры и защиты информации
Белорусского государственного университета
(протокол №5 от 25.11.2020);

Научно-методическим советом
Белорусского государственного университета
(протокол № 2 от 07.12.2020).

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

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 «Алгоритмы в теории чисел и криптографии» 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: изучение теоретических основ современных методов защиты информации, знакомство с базовыми алгоритмами, использующихся в асимметрических криптосистемах.

Развивающая цель: формирование у студентов алгоритмического мышления и общей математической культуры, привитие студентам умения самостоятельно изучать учебную и научную литературу в области математики.

Основные задачи, решаемые в рамках изучения дисциплины «Алгоритмы в теории чисел и криптографии»:

- познакомить учащихся с базовыми теоретико-числовыми алгоритмами, использующимися в современных асимметрических криптосистемах;
- развить алгоритмическое мышление и общую математическую культуру;
- привить студентам умение самостоятельно изучать учебную и научную литературу в области математики.

В результате изучения учебной дисциплины студент должен

знать:

– основные математические методы, лежащие в основе построения современных криптосистем;

– базовые теоретико-числовые алгоритмы криптографии;

уметь:

– выполнять вычисления в конечных полях;

– уметь решать теоретико-числовые и алгоритмические задачи по курсу «Алгоритмы в теории чисел и криптографии»;

владеть:

– основными навыками решения задач теории чисел и

криптографии;

– методами оценки сложности алгоритмов;

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

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина относится **к циклу** дисциплин 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» и «Дополнительные главы алгебры».

Требования к компетенциям специалиста

В результате изучения дисциплины «Алгоритмы в теории чисел и криптографии» студент должен обладать следующими компетенциями:

Академические компетенции:

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

АК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-5. Быть способным вырабатывать новые идеи (обладать креативностью).

АК-6. Владеть междисциплинарным подходом при решении проблем.

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

АК-8. Обладать навыки устной и письменной коммуникаций.

АК-9. Уметь учиться, повышать свою квалификацию в течение всей жизни.

Социально-личностные компетенции:

СЛК-2. Быть способным к социальному взаимодействию.

СЛК-3. Обладать способностью к межличностным коммуникациям.

СЛК-5. Быть способным к критике и самокритике.

СЛК-6. Уметь работать в команде.

Профессиональные компетенции:

ПК-1. Разрабатывать практические рекомендации по использованию научных исследований, планировать и проводить экспериментальные исследования, исследовать патентоспособность и 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, оформлять техническую документацию.

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.

ПК-8. Работать с научной, нормативно-справочной и специальной литературой.

ПК-9. Осуществлять выбор оптимального варианта проведения научно-исследовательских работ.

ПК-13. Взаимодействовать со специалистами смежных профилей.

ПК-16. Готовить доклады, материалы к презентациям.

ПК-22. Работать с научной, технической и патентной литературой.

ПК-27. Реализовывать инновационные проекты в профессиональной деятельности.

Структура учебной дисциплины.

Дисциплина изучается в 4 и 5 семестре очной формы получения образования.

Всего на изучение учебной дисциплины «Алгоритмы в теории чисел и криптографии» отведено 100 часов, в том числе: 54 аудиторных часа, из них: лекции – 50 часов, управляемая самостоятельная работа – 4 часа, из них:

4 семестр – всего 28 часов, в том числе: 18 аудиторных часов, из них лекции 16 часов, управляемая самостоятельная работа – 2 часа;

5 семестр – всего 72 часа, в том числе: 36 аудиторных часов, из них лекции 34 часа, управляемая самостоятельная работа – 2 часа.

Трудоемкость учебной дисциплины составляет 2 зачетные единицы.

Форма текущей аттестации по учебной дисциплине – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Базовые теоретико-числовые алгоритмы

Полиномиальные, субэкспоненциальные и экспоненциальные алгоритмы. Алгоритм Евклида. Расширенный алгоритм Евклида, бинарный алгоритм Евклида

Тема 2. Эффективные алгоритмы арифметики

Эффективные методы выполнения арифметических операций над целыми числами. Метод Карацубы. Умножение с помощью системы остаточных классов.

Тема 3. Алгоритмы генерации больших простых чисел

Детерминированные алгоритмы тестирования чисел на простоту. Вероятностные алгоритмы тестирования чисел на простоту

Тема 4. Алгоритмы шифрования и распределения ключей

Алгоритм шифрования RSA. Выбор криптостойких параметров для схемы RSA. Алгоритм Диффи-Хеллмана с аутентификацией сторон.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения высшего образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов по УСР	Формы контроля знаний
		лекции	практические занятия	семинарские занятия	лабораторные	Иное		
	4 семестр							
1	Базовые теоретико-числовые алгоритмы	16					2	Контрольная работа
	Итого	**16**					**2**	
	5 семестр							
2.	Эффективные алгоритмы арифметики	12						Защита индивидуальных заданий
3	Алгоритмы генерации больших простых чисел	12						Защита индивидуальных заданий
4	Алгоритмы шифрования и распределения ключей	10					2	Контрольная работа
	Итого	**34**					**2**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Харин Ю.С., Агиевич СВ., Васильев Д.В., Матвеев Г.В. Криптология. (Учебник с грифом Минобразования). Минск: БГУ, 2014. 512 с.
2. Босс В. Лекции по математике: Теория чисел Т.14. URSS, 2019. 214 с.
3. Виноградов И.М. Основы теории чисел. Лань: Спб, 2019. 176 с.
4. Василенко ОН. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003. 328 с.

Перечень дополнительной литературы

1. Коблиц Н. Курс теории чисел и криптографии, Научное издательство ТВП, 2001, 254 с.
2. Нестеренко Ю.В. Теория чисел. М.: Академия, 2008. 272 с.
3. Применко А. Алгебраические основы криптографии. URSS, 2018. 288 с.
4. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации для изучающих компьютерную безопасность. URSS, 2019.473 с.

Перечень рекомендуемых средств диагностики и методика формирования итоговой оценки

Формой текущей аттестации по дисциплине «Алгоритмы в теории чисел и криптография» учебным планом предусмотрен зачет.

Контроль работы студента проходит в форме защиты индивидуальных заданий и выполнения контрольных работ и практических упражнений в аудитории, а также самостоятельной работы вне аудитории с предоставлением отчета с его устной защитой. Задания к самостоятельным работам составляются согласно содержанию учебного материала.

Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний и текущей аттестации в рейтинговую оценку:

– выполнение контрольной работы – 50 %;

– отчеты по индивидуальным заданиям с устной защитой– 50 %.

Зачет по дисциплине выставляется в случае сдачи всех контрольных работ и защиты всех индивидуальных заданий.

Итоговая оценка 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 студентов по дисциплине в Белорусском государственном университете (Приказ ректора БГУ № 189-ОД от 31.03.2020).

3. Критерии оценки знаний и компетенций студентов по 10-балльной шкале (Письмо Министерства образования Республики Беларусь от 22.12.2003 г. № 21-04-1/105).

Примерный перечень заданий для управляемой самостоятельной работы студентов

Тема 1. Базовые теоретико-числовые алгоритмы (2 часа)

Форма контроля – контрольная работа.

1. Решить сравнение $122x \equiv 182 (\mathrm{mod}\ 301)$.
2. Решить с помощью китайской теоремы об остатках

$$\begin{cases} x \equiv 3\ (\mathrm{mod}\ 11); \\ x \equiv 5\ (\mathrm{mod}\ 6); \\ x \equiv -3\ (\mathrm{mod}\ 5); \\ x \equiv -4\ (\mathrm{mod}\ 7). \end{cases}$$

3. Вычислить символ Лежандра, используя свойства символа Якоби: $\left(\frac{304}{409}\right)$.
4. Является ли 3 первообразным корнем по модулю 23?
5. Найти какой-нибудь первообразный корень по модулю 29.
6. Является ли 15 сильно псевдопростым по основанию 3.
7. 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) $a = n^3 + 5n + 12,\ b = 6$.
8. Найдите неполное частное и остаток от деления числа a на число b: а) $a = 761, b = 13$; б) $a = 437, b = 24$.
9. 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) $a = 1296, b = 6600$.
10. 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) $a = 9100, b = 92, c = -114$.
11. Решить в целых числах уравнение $1275x - 3796y = 1$.
12. Используя свойства сравнений, найти остаток от деления: а) $a = 178^{214}$ на $b = 22$; б) $a = 5^{50} + 13^{100}$ на $b = 18$.
13. Решите сравнение 1-й степени: а) $-3x \equiv 13 (\mathrm{mod}\, 4)$; б) $7x \equiv -12 (\mathrm{mod} 16)$.
14. Составьте таблицы сложения и умножения в кольце классов вычетов: а) $\mathbb{Z}_5$; б) $\mathbb{Z}_6$.

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

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

17. Для каждой приведенной ниже пары целых чисел a, b найдите наибольший общий делитель и такие числа u, v, что $НОД(a,b) = ua + vb$:

1) 14 и 25; 2) 252 и 180; 3) 6643 и 2873; 4) 272, 828, 282 и 3242 (обобщите предварительно все понятия на случай, когда чисел больше двух).

18. Пусть n – натуральное число, большее единицы. Покажите, что:

1) $НОД(n, 2n+1) = 1$; 2) $НОД(2n+1, 3n+1) = 1$;

3) $НОД(n!+1, (n+1)!+1) = 1$.

19. Пусть $n > m$ – натуральные числа, а r – остаток от деления n на m. Покажите, что остаток от деления $2^n - 1$ на $2^m - 1$ равен $2^r - 1$. Покажите, что если число r четное, то остаток от деления $2^n + 1$ на $2^m + 1$ равен $2^r + 1$.

20. $n > m$ – натуральные числа. С помощью упражнения 22 вычислите $НОД(2^{2^n} + 1, 2^{2^m} + 1)$.

21. Составить таблицы индексов: 1) по $\mathrm{mod}\, 29$ с основанием 2; 2) по $\mathrm{mod}\, 23$ с основанием 5.

22. Путем индексирования решить сравнения: 1) $52^x \equiv 38 (\mathrm{mod}\, 67)$; 2) $37x^{16} \equiv 62 (\mathrm{mod}\, 73)$; 3) $27x^5 \equiv 2 (\mathrm{mod}\, 31)$.

23. Пусть a принадлежит показателю δ, b – показателю \gamma, $(\delta, \gamma) = 1$. Показать, что ab принадлежит показателю $\delta\gamma$.

24. Вычислить символы Лежандра и Якоби: $\left(\frac{47}{25}\right), \left(\frac{131}{283}\right), \left(\frac{123}{917}\right)$.

25. Найти все квадратичные вычеты по модулю p: $p = 11$, $p = 13$, $p = 17$.

26. Пусть a принадлежит показателю δ. Какому показателю принадлежит a^γ?

Тема 4. Алгоритмы шифрования и распределения ключей (2 часа)

Форма контроля – контрольная работа.

1. Найти количество решений сравнения $x^m \equiv 1 (\mathrm{mod}\, N)$.

2. Сколько решений имеет сравнение $x^m \equiv -1 (\mathrm{mod}\, N)$ в случае его разрешимости?
3. Доказать, что всевозможные преобразования RSA-криптосистемы образуют группу относительно их композиции.
4. Зашифровано сообщение по правилу $y \equiv x^k (\mathrm{mod}\, p)$, где p – большое простое число, $1 \le x \le p-1$, k – целое число, $1 < k < p-1$. Показать, что если k выбрано взаимно простым с $p-1$, то алгоритм расшифрования $d(y) \equiv y^d (\mathrm{mod}\, p)$ является корректным с $d \equiv k^{-1} (\mathrm{mod}(p-1))$ и $d(y) = x$.
5. Что случится с криптосистемой в предыдущей задаче, если ошибочно взять целое число k, не ввзаимно простое с $p-1$?
6. Показать, что в схемах RSA и Рабина шифрование открытого текста длиной n битов в зашифрованный текст длиной N битов требует $O(n^3)$ операций.
7. Предположим, что пользователь RSA в качестве модуля N по ошибке выбрал большое простое число. Показать, что в этом случае расшифровать текст легко.
8. Рассмотрим RSA-систему с модулем N. Целое число x, $1 \le x \le N-1$, назовем неподвижной точкой, если оно и в зашифрованном виде тоже x. Показать, что если x – неподвижная точка, то и $N-x$ также есть неподвижная точка.
9. Показать, что в схеме RSA с параметрами p, q, e, d имеется $r+s+rs$ неподвижных точек $M, 1 \le M \le N-1$, где $r = (p-1, e-1)$, $s = (q-1, e-1)$. Задача показывает, что в схемах шифрования с большим количеством неподвижных точек уже заложен недостаток, поэтому желательно выбирать такие p и q, для которых r и s малы.
10. Предложите способ решения сравнения $x^2 \equiv 1 (\mathrm{mod}\, N)$. Найдите четыре решения сравнения $x^2 \equiv 1 (\mathrm{mod} 17 \cdot 91)$.
11. В системе аутентификации, основанной на схеме Рабина, A выбирает в качестве открытых ключей $B = 2, N = 200$. C посылает A число $R = 168$. Как должен ответить A, чтобы убедить C, что именно ему попало сообщение?
12. В схеме подписи, основанной на RSA, пользователи A и B имеют открытые ключи $e_A = 3, n_A = 15; e_B = 7, n_B = 77$ соответственно. A

хочет послать сообщение $M = 4$ как подпись к некоторому тексту. Какое целое число он посылает?

13. В схеме подписи Рабина A имеет открытый ключ N_A и желает подписать сообщения $m_1 = 9$ и $m_2 = 29$. Какими будут соответствующие подписи S_1 и S_2?

Описание инновационных подходов и методов к преподаванию учебной дисциплины (эвристический, проектный, практико-ориентированный)

При организации образовательного процесса используется ***эвристический подход,*** который предполагает**:**

– осуществление студентами личностно-значимых открытий окружающего мира;

– демонстрацию многообразия решений большинства профессиональных задач и жизненных проблем;

– творческую самореализацию обучающихся в процессе создания образовательных продуктов;

– индивидуализацию обучения через возможность самостоятельно ставить цели, осуществлять рефлексию собственной образовательной деятельности.

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.

При организации образовательного процесса ***используется метод проектного обучения,*** который предполагает***:***

– способ организации учебной деятельности студентов, развивающий актуальные для учебной и профессиональной деятельности навыки планирования, самоорганизации, сотрудничества и предполагающий создание собственного продукта;

– приобретение навыков для решения исследовательских, творческих, социальных, предпринимательских и коммуникационных задач.

Методические рекомендации по организации и выполнению самостоятельной работы студентов

Самостоятельная работа студентов - это любая деятельность, связанная с воспитанием мышления будущего профессионала. В широком смысле под самостоятельной работой следует понимать совокупность всей самостоятельной деятельности студентов как в учебной аудитории, так и вне её, в контакте с преподавателем и в его отсутствии.

Самостоятельная работа реализуется:

1. Непосредственно в процессе аудиторных занятий - на лекциях.
2. В контакте с преподавателем вне рамок расписания - на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.
3. В библиотеке, дома, в общежитии, на кафедре при выполнении студентом учебных и творческих задач.

При изучении дисциплины организация самостоятельной работы студентов должна представлять единство трех взаимосвязанных форм:

1. Внеаудиторная самостоятельная работа;
2. Аудиторная самостоятельная работа, которая осуществляется под непосредственным руководством преподавателя;
3. Творческая, в том числе научно-исследовательская работа.

Примерный перечень вопросов к зачету

1. Делимость в кольце целых чисел. НОД, НОК, разрешимость линейного диофантового уравнения.
2. Закон распределения простых чисел, оценки расстояний между соседними простыми числами.
3. Алгоритм Евклида, расширенный алгоритм Евклида, оценка сложности алгоритма Евклида.
4. Сравнения, их свойства, решение линейного сравнения.
5. Китайская теорема об остатках.
6. Мультипликативные функции, функция Эйлера.
7. Теорема Эйлера, малая теорема Ферма.
8. Квадратичные вычеты. Символ Лежандра. Теорема Эйлера для квадратичных вычетов.
9. Квадратичный закон взаимности. Символы Якоби. Вычисление символа

Лежандра.

10. Первообразные корни. Структура мультипликативной группы кольца вычетов.
11. Сложность алгоритмов: полиномиальные, субэкспоненциальные, экспоненциальные алгоритмы. Примеры.
12. Бинарные алгоритмы возведения в степень. Метод скользящего окна.
13. Алгоритм решения квадратичных сравнений. Общий алгоритм решения полиномиальных сравнений.
14. Метод Карацубы для умножения целых чисел. Умножение целых чисел при помощи китайской теоремы об остатках.
15. Операция Монтгомери и редукция Баррета.
16. Детерминированный тест на простоту.
17. Тест Миллера-Рабина.
18. Алгоритм построения больших простых чисел.
19. Алгоритм нахождения элемента циклической группы с заданным порядком.
20. Эллиптические кривые, группа точек эллиптической кривой.
21. Вывод формул сложения. Алгоритм вычисления кратной точки.
22. Эффективные методы вычисления операции сложения точек эллиптической кривой.
23. Кривые в форме Вейерштрасса, Монтгомери, Эдвардса.
24. Криптосистема RSA.
25. Алгоритм Диффи-Хеллмана распределения ключей.
26. Схема цифровой подписи Эль-Гамаля.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

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)
Дополнительные главы алгебры	Высшей алгебры и защиты информации	нет	Изменения не требуются (протокол № 5 от 25.11.2020)

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)