Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра фундаментальной математики

ОДОБРЕНО:
Руководитель ОП

_____ П.Г. Кононенко
(подпись)

«_1_» сентября_2022 г.

Рабочая программа дисциплины
Алгебраические основы криптографии

Уровень высшего образования:	бакалавриат
Квалификация выпускника:	бакалавр
Направление подготовки:	02.03.02 Фундаментальная информатика и информационные технологии
Направленность (профиль) образовательной программы:	Фундаментальная информатика и информационные технологии

Иваново

1. Цели освоения дисциплины

Целями освоения дисциплины «Алгебраические основы криптографии» являются:

1) получение базовых знаний в основополагающих разделах алгебры: элементы теории чисел, полей и колец;

2) знакомство с некоторыми ключевыми криптографическими алгоритмами и их использованием.

При освоении дисциплины развивается общематематическая культура, приобретаются навыки практических вычислений, качественного и численного исследования изучаемых проблем.

2. Место дисциплины в структуре ОП

Дисциплина «Алгебраические основы криптографии» (Б1.О.18) входит в обязательную часть учебного плана. Для ее успешного изучения необходимы «входные» знания и умения в области математики, полученные в процессе обучения по программе средней школы, а также знание основных сведений курса «Алгебра», читаемого в первом и втором семестрах.

Дисциплина является составной, призвана демонстрировать взаимодействие и взаимное проникновение алгебраических понятий и методов нескольких дисциплин. Кроме того, этот курс связан также с такими дисциплинами учебного плана как «Математический анализ», «Дискретная математика», «Практикум по элементарной математике». Эти дисциплины предоставляют материал для примеров и служат сферой ключевых приложений алгебраических теорий и алгоритмов. Взаимная зависимость алгебры, геометрии, анализа и дискретной математики является глубокой и прослеживается на всем протяжении изучения математики. Следующие дисциплины, изучаемые на втором-четвертом курсах, также используют материал данного курса: «Математическая логика и теория алгоритмов», «Дополнительные главы алгебры», «Методы и средства криптографической защиты информации», «Криптографические протоколы» и другие.

Для освоения данной дисциплины обучающийся должен:

Знать: содержание основных разделов школьного курса математики и курса «Алгебра» (1 и 2 семестры).

Уметь: преобразовывать алгебраические выражения, решать алгебраические уравнения и неравенства, свободно оперировать алгебраическими понятиями и использовать известные алгебраические результаты при решении теоретических задач.

Иметь: навыки математических рассуждений и доказательств.

3. Планируемые результаты обучения по дисциплине

3.1. Компетенции, формированию которых способствует дисциплина

При освоении дисциплины формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

Общекультурные (ОК): нет

общепрофессиональные (ОПК): нет

Профессиональные: ПК-1: способен применять в научно-исследовательской деятельности знания в области прикладной математики и (или) информационных технологий;

ПК-2: способен проводить работы по обработке и анализу научно-технической информации и результатов исследований по отдельным разделам темы.

3.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения формируемых компетенций

В результате освоения дисциплины обучающийся должен:

Знать:

- основы теории чисел, теории колец и полей, включая их приложения к криптографическому анализу (ПК-1, ПК-2);
- основные понятия и классические результаты алгебры, теории чисел, теории колец и полей; основные алгебраические алгоритмы и некоторые алгоритмы криптографии (ПК-1, ПК-2).

Уметь:

- воспроизводить доказательства основных классических результатов теории чисел, теории колец и полей, строить новые доказательства (ПК-1, ПК-2);
- корректно ставить математические задачи и решать их (ПК-1, ПК-2);
- решать задачи на основы теории делимости, теории сравнимости (ПК-1, ПК-2);
- решать задачи на шифрование с открытым ключом (ПК-1, ПК-2);

Иметь:

- высокий уровень математической и информационной культуры, навыки самостоятельной исследовательской работы (ПК-1, ПК-2);
- навыки владения методами и алгоритмами теории чисел, теории колец и полей, криптографии;
- навыки работы с алгебраическими объектами различной природы (ПК-1, ПК-2).

4. Объем и содержание дисциплины

Объем дисциплины составляет 7 зачетных единицы (252 академических часа).

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и трудоемкостью занятий лекционно-семинарского типа

Объем иной контактной работы и самостоятельной работы обучающегося по дисциплине указан в учебном плане образовательной программы.

№ п/п	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в ак.часах, по очной форме обучения)		Формы текущего контроля успеваемости (по очной форме обучения) Формы промежуточной аттестации
			Занятия лекцион-ного типа	Занятия семинар-ского типа	
1.	Кольцо целых чисел. Вопросы делимости целых чисел. НОД, алгоритм Евклида и его модификации. Простые числа. Основная теорема арифметики.	3	14	12	Контрольная работа №1
2.	Сравнения целых чисел по заданному модулю. Вычисление остатков. Установление признаков делимости. Кольцо классов вычетов по данному модулю. Функция Эйлера. Применение теорем Эйлера и Ферма.	3	12	8	
3.	Сравнение с неизвестной величиной	3	4	4	Контрольная работа №2
4.	Криптография с открытым ключом	3	4	4	
5.	Системы сравнений первой степени	3	2	4	Контрольная работа №3
	Итого за семестр:		36	32	Зачет с оценкой
6.	Сравнения высших степеней	4	2	1	
7.	Сравнения второй степени по простому модулю. Двучленные сравнения	4	2	3	
8.	Квадратичные вычеты и невычеты	4	2	2	Контрольная работа №4
9.	Степенные вычеты	4	2	4	
10.	Первообразные корни	4	2	4	
11.	Индексы	4	2	4	Контрольная работа №5
12	Алгебраические расширения полей	4	12	4	
13.	Элементы теории Галуа	4	6	6	
14.	Алгоритм дискретного логарифмирования	4	2	4	Контрольная работа №6
.					
Итого за семестр:			32	32	Экзамен
Итого по дисциплине:			68	64	

4.2. Развернутое описание содержания дисциплины по разделам (темам)

1. *Кольцо целых чисел.* Основные понятия. Принцип математиечской индукции и метод бесконечного спуска. Типы колец. Свойства кольца целых чисел. Делители нуля. Отсутствие делителей нуля в кольце целых чисел и возможность сокращения частей равенства на ненулевой множитель.

2. *Делимость целых чисел. Свойства отношения делимости.* Определение отношения делимости. Связь отношения делимости с операцией деления. Свойства отношения делимости. Некоторые алгоритмы решения типовых задач на применение свойств отношения делимости.

3. *НОД и НОК целых чисел.* Основные определения, свойства, представление НОД двух целых чисел в виде линейной комбинации с целочисленными коэффициентами этих чисел. Теорема о связи НОД и НОК. Алгоритм Евклида и его модификации (бинарный и расширенный алгоритмы Евклида).

4. *Простые числа Основная теорема арифметики.* Понятие и основные свойства простых чисел. Основная теорема арифметики и некоторые ее следствия. Применение этих результатов при решении задач.

5. *Сравнения целых чисел по натуральному модулю.* Определение отношения сравнения. Отношение сравнения как отношение эквивалентности. Классы вычетов. Системы вычетов по данному модулю. Свойства отношения сравнимости. Некоторые алгоритмы решения типовых задач.

6. *Вычисление остатков с помощью сравнений. Установление признаков делимости.* Существование системы счисления с произвольным натуральным основанием, большим единицы. Основная теорема о признаках делимости и ее следствия.

7. *Кольцо классов вычетов по заданному натуральному модулю. Модулярная арифметика.* Операции сложения и умножения на множестве классов вычетов по заданному натуральному модулю. Множество классов вычетов как кольцо. Свойства. Применение к решению задач.

8. *Функция Эйлера. Приведенная система вычетов.* Определение функции Эйлера. Вычисление функции Эйлера для простого значения аргумента, мультипликативность функции Эйлера, общая формула вычисления функции Эйлера в произвольной натуральной точке. Приведенная система вычетов. Ее свойства. Теоремы Эйлера и Ферма. Некоторые приложения этих теорем.

9. *Сравнение с неизвестной величиной.* Основные понятия. Теорема о числе решений сравнения произвольной натуральной степени. Линейное сравнение. Теорема о разрешимости и числе решений линейного сравнения. Решение неопределенного линейного уравнения с помощью сравнений.

10. *Криптография с открытым ключом.* Основные понятия. Теорема Эйлера в шифровании RSA. Алгоритм криптосистемы RSA. Цифровая подпись.

11. *Системы сравнений первой степени.* Основные определения. Китайская теорема об остатках. Алгоритмы решения систем линейных сравнений. Примеры.

12. *Системы сравнений высших степеней.* Основные понятия, алгоритмы.

13. *Сравнения второй степени по простому модулю. Двучленные сравнения.* Основные понятия. Теорема и приведении произвольного сравнения второй степени к двучленному. Число решений двучленного сравнения.

14. *Квадратичные вычеты и невычеты.* Основные определения. Свойства квадратичных вычетов и невычетов. Закон взаимности. Применение его к решению задач.

15. *Степенные вычеты.* Показатель натурального числа по натуральному модулю. Свойства. Решение степенного сравнения.

16. *Первообразные корни*. Определения, свойства. Решение задач.

17. *Индексы.* Определения, основные свойства. Применение к решению задач.

18. *Алгебраические расширения полей.* Определения. Расширение поля. Конечно порожденное расширение. Конечное расширение. Алгебраические расширения. Свойства.

19. *Конечные поля. Теория Галуа.*

20. *Алгоритм дискретного логарифмирования.* Определения. Алгоритм. Решение задач.

5. Образовательные технологии

Лекции с использованием компьютерных презентаций. Демонстрация проблемных ситуаций в развитии математического знания, связанных с разнообразными приложениями математики (в том числе, в области информационных технологий).

Практические занятия с использованием активных форм, в частности, - технологий *проблемного обучения* (не менее 30% занятий). Основной тип проблемных ситуаций - *решение учебных проблем,* чем обеспечивается сознательность, глубина и прочность знаний, повышение уровня самостоятельности обучающихся, выработка у них способности к актуализации ранее полученных и вновь приобретаемых знаний.

Важным аспектом организации учебного процесса является *параллельное* изучение алгебраических и геометрических разделов.

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: технологии смешанного обучения.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа студентов состоит в следующем: работа с конспектами лекций, изучение литературы, выполнение домашних заданий, подготовка к экзаменам.

Методический материал по обеспечению самостоятельной работы студентов приводится в Приложении 1 к рабочей программе.

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Предусмотрены:

- письменные контрольные работы;
- зачет с оценкой в третьем семестре и экзамен в четвертом семестре, программа которых включает как теоретические вопросы, так и практическую часть (задачи); оценка по практической части формируется по совокупности результатов контрольных работ (в данном семестре).

Фонд контрольных заданий по дисциплине является мобильным; критерии оценки вырабатываются оперативно; предусматривается своевременное ознакомление студентов с демонстрационными вариантами заданий, образцами их выполнения и критериями оценки.

***Критерии оценки контрольной работы студента*:**

Оценка «отлично» выставляется студенту, если**:**

1) работа выполнена полностью;

2) в логических рассуждениях и обосновании решения нет пробелов и ошибок;

3) в решении нет математических ошибок (возможна одна неточность, описка, не являющаяся следствием незнания или непонимания учебного материала).

Оценка «хорошо» выставляется студенту, если**:**

1) работа выполнена полностью, но обоснования шагов решения недостаточны (если умение обосновывать рассуждения не являлось специальным объектом проверки);

2) допущена одна ошибка или два-три недочета в выкладках, или чертежах (если эти виды работы не являлись специальным объектом проверки).

Оценка «удовлетворительно» выставляется, если**:**

допущены более одной ошибки или более двух-трех недочетов в выкладках или чертежах, но студент владеет обязательными умениями по проверяемой теме.

Оценка «неудовлетворительно» выставляется, если**:**

допущены существенные ошибки, показавшие, что студент не владеет обязательными умениями по данной теме в полной мере.

Типовые варианты контрольной работы представлены в фонде оценочных средств (Приложение 2).

Итоговой формой контроля является устный экзамен, который проводится 2 раза – по результатам каждого из двух семестров. Экзаменационный билет содержит 2 теоретических вопроса и задачу.

***Критерии оценки устного ответа студентов на экзамене*:**

Оценка «*отлично*» выставляется студенту, если:

1) полно раскрыто содержание учебного материала в объеме, предусмотренном программой, изложен материал грамотным языком в определенной логической последовательности, точно используя математическую терминологию и символику;

2) правильно выполнены рисунки и чертежи, сопутствующие ответу;

3) продемонстрировано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации при выполнении практического задания;

4) продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость используемых при отработке умений и навыков;

5) ответ самостоятельный без наводящих вопросов преподавателя. Возможны одна - две неточности при освещении второстепенных вопросов или в выкладках, которые студент легко исправил по замечанию преподавателя.

Оценка «*хорошо*» выставляется, если:

ответ удовлетворяет в основном требованиям на оценку «отлично», но при этом имеет один из недостатков:

1) в изложении допущены небольшие пробелы, не исказившие математическое содержание ответа;

2) допущены один–два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя;

3) допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию преподавателя.

Оценка «*удовлетворительно*» выставляется студенту, если:

1) неполно или непоследовательно раскрыто содержание учебного материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала;

2) имелись затруднения или допущены ошибки в определении понятий, использовании математической терминологии, чертежах, выкладках, исправленные после нескольких наводящих вопросов преподавателя;

3) студент не справился с применением теории в новой ситуации при выполнении практического задания, но выполнил задания обязательного уровня сложности по данной теме;

4) при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

Оценка «*неудовлетворительно*» выставляется, если:

1) не раскрыто основное содержание учебного материала;

2) обнаружено незнание или непонимание студентом большей или наиболее важной части учебного материала;

3) допущены ошибки в определении понятий, при использовании математической терминологии, в рисунках, чертежах или графиках, в выкладках, которые не исправлены после нескольких наводящих вопросов преподавателя.

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Винберг, Э.Б. Курс алгебры / Э.Б. Винберг. – Москва : МЦНМО, 2011. – 591 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=63299. – ISBN 978-5-94057-685-3. – Текст : электронный.

2. Кострикин, А.И. Введение в алгебру : учебник / А.И. Кострикин. - М. : МЦНМО, 2009. - Ч. 1. Основы алгебры. - 273 с. - ISBN 978-5-94057-453-8 ; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=63140

3. Кострикин, А.И. Введение в алгебру : учебник / А.И. Кострикин. - М. : МЦНМО, 2009. - Ч. 3. Основные структуры алгебры. - 272 с. - ISBN 978-5-94057-455-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=62951

4. Сборник задач по алгебре : задачник / под ред. А.И. Кострикин. - М. : МЦНМО, 2009. - 404 с. - ISBN 978-5-94057-413-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=63274

5. Яцкин Н. И. Алгебра: Теоремы и алгоритмы. Учеб. пособие. Иваново: Иван. гос. ун-т, 2006.

6. Яцкин Н. И. Линейная алгебра: Теоремы и алгоритмы. Учеб. пособие. Иваново: Иван. гос. ун-т, 2008.

Дополнительная литература:

7. Кострикин А. И. Введение в алгебру. М.: Наука, 1977.- 495 с. 108 экземпляров.

8. Курош А. Г. Курс высшей алгебры. 11-е изд, стереотип. – М.: Наука, 1975. 43 экземпляра.

9. Фаддеев Д. К. Сборник задач по высшей алгебре. - 11 –е изд., перераб. и доп. – М.: Наука, 1977. – 288 с. 120 экземпляров.

10. Яцкин Н. И. Алгебра: Теоремы и алгоритмы: Учеб. пособие. Иваново: ИвГУ, 2008. – 606 с. – 98 экз.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

Система электронной поддержки образовательного процесса «Мой университет» https://uni.ivanovo.ac.ru

Профессиональные базы данных и информационно-справочные системы:

ЭБС «Университетская библиотека онлайн» www.biblioclub.ru

Электронная библиотека ИвГУ http://lib.ivanovo.ac.ru

Электронный каталог НБ ИвГУ http://lib.ivanovo.ac.ru/index.php/ek

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ Microsoft Office и(или) LibreOffice, интернет-браузер Microsoft Edge и(или) Yandex Browser.

9. Материально-техническое обеспечение дисциплины

Учебные аудитории:

- для проведения занятий лекционного типа с комплектом специализированной учебной

мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;

- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими средствами обучения;

Помещение для самостоятельной работы, оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС.

Демонстрационное оборудование и учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации: демонстрационные устройства, электронные пособия (презентации), печатные пособия (таблицы, схемы).

Автор рабочей программы дисциплины: доцент кафедры фундаментальной математики, доцент кафедры фундаментальной математики, к. ф.-м.н Логинова Е.Д.

Программа рассмотрена и утверждена на заседании кафедры фундаментальной математики « 1 » сентября 2022 г., протокол № 1

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ /_____/
(подпись) (Фамилия И.О.)

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ /_____/
(подпись) (Фамилия И.О.)

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ /_____/
(подпись) (Фамилия И.О.)