АННОТАЦИЯ
дисциплины Б1. В.15

КОМПЬЮТЕРНАЯ АЛГЕБРА И КРИПТОГРАФИЯ

для направления 02.03.01 Математика и компьютерные науки

Объем трудоемкости: Общая трудоёмкость дисциплины составляет 4 зачетных единицы (82 часа, из них 58,3 часа контактной работы: лекционных 18 ч., лабораторных 34 ч., 2 ч. КСР, ИКР 0,3 час; 23,7ч. самостоятельной работы).

Цель освоения дисциплины.

Цель освоения дисциплины «Компьютерная алгебра и криптография» – получение базовых теоретических сведений по теории распределения простых чисел, разложения на простые множители, криптосистемы открытого ключа и реализации алгоритмов на подходящих языках программирования.

При освоении дисциплины вырабатывается общематематическая культура: умение логически мыслить, проводить доказательства основных утверждений, устанавливать логические связи между понятиями, применять полученные знания для решения задач криптографии. Получаемые знания лежат в основе математического образования и необходимы для понимания и освоения всех курсов математики, а также для продолжения обучения в магистратуре по соответствующему направлению подготовки.

Задачи дисциплины.

Дальнейшее формирование у студентов приобретенных на первых двух курсах знаний по фундаментальной, компьютерной алгебре и криптографии.

Место дисциплины в структуре образовательной программы.

Изучение дисциплины «Компьютерная алгебра и криптография» предусмотрено стандартом высшего профессионального образования специальности 020301 (федеральный компонент в цикле математических и естественных дисциплин). В рамках дисциплины ее изучение базируется на знаниях курса «Фундаментальная и компьютерная алгебра».

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	
ИПК-1.1. Способен решать актуальные и важные задачи фундаментальной и прикладной математики	Знает арифметику целых чисел: делимость, разложение на множители, основную теорему арифметики; структуру кольца многочленов: неприводимость, разложение на множители
	Умеет формировать понятия, взятые из кольца целых чисел и кольца многочленов, для создания криптосистем открытого ключа. Владеет способностью определения общих закономерностей разложения элементов кольца на неприводимые множители, владеть структурным анализом в теории колец вычетов и конечных полей

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
	Владеет способностью определения общих закономерностей разложения элементов кольца на неприводимые множители, владеть структурным анализом в теории колец.
ПК-5 Способен математически корректно ставить естественнонаучные задачи, знание постановок классических задач математически	
ИПК-5.1. Уметь применять , полученные теоретические знания по арифметике колец вычетов и конечных полей и их взаимосвязи с криптосистемами открытого ключа.	Знает определение основных понятий в данном курсе, формулировки основных теорем с примерами
	Умеет решать задачи по основным разделам курса : генерирование больших простых чисел, разложение на простые множители, создание криптосистем открытого ключа.
	Владеет необходимыми знаниями в программировании для реализации алгоритмов криптосистем открытого ключа.

Основные разделы дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 6 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Простые числа, их распределение, генерирование простых чисел.	8	2		4	2
2.	Алгоритмы разложения на простые множители.	9	2		4	3
3.	Дискретный логарифм.	9	2		4	3
4.	Криптосистема RSA и ее реализация.	9	2		4	3
5.	Криптосистема Рабина и ее реализация.	9	2		4	3
6.	El Gamel схема кодирования и ее реализация.	8,7	2		4	2,7
7.	Эллиптические кривые и групповая структура на них.	9	2		4	3
8.	Эллиптические кривые над конечными полями и схема кодирования с помощью эллиптических кривых.	14	4		6	4
	Итого по дисциплине:	75,7	18		34	23,7

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

Курсовые работы: *не предусмотрены*

Форма проведения аттестации по дисциплине: *экзамен*

Основная литература:

1. Кострикин, А.И. Введение в алгебру. Часть 3. Основные структуры [Электронный ресурс] : учеб. — Электрон. дан. — Москва : Физматлит, 2001. — 272 с. — Режим доступа: https://e.lanbook.com/book/59284.

2. Винберг, Э.Б. Курс алгебры : учебник / Э.Б. Винберг. - Москва : МЦНМО, 2011. - 591 с. - ISBN 978-5-94057-685-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=63299

б) дополнительная литература:

1. Нестеренко В. Основы теории чисел. М. МГУ. 2011.
2. Родосский К. Алгоритм Евклида. М. Наука. 1988.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах *«Лань» и «Юрайт».*

Автор (ы) РПД _____Любин В.А..