Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В.ЛОМОНОСОВА»
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ

УТВЕРЖДАЮ
Декан факультета ВМК МГУ
Академик _____ /*И.А. Соколов*/
«14» сентября 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Криптосистемы с открытым ключом
Public key cryptosystems

Программа (программы) подготовки научных и научно-педагогических кадров в аспирантуре

102.01.00.112-фмн-кфап, 102.01.00.122-фмн-кмф, 102.01.00.122-фмн- кски,
102.01.00.235-фмн- кски, 102.01.00.112-фмн-ком, 102.01.00.122-фмн-кани
102.01.00.112-фмн-кса, 102.01.00.122-фмн- кса, 102.01.00.112-фмн- кндсипу,
102.01.00.122-фмн- кндсипу, 102.01.00.114-фмн- кмс, 102.01.00.115-фмн- кммп
102.01.00.115-фмн- кмк, 102.01.00.123-фмн- кмк, 102.01.00.116-фмн- квтм,
102.01.00.122-фмн- квтм, 102.01.00.116-фмн- квм, 102.01.00.122-фмн- квм, 102.01.00.122-фмн- коу,
102.01.00.112-фмн- коу, 102.01.00.123-фмн- кио, 102.01.00.122-фмн- кио, 102.01.00.235-фмн- киит,
102.01.00.235-фмн-касвк, 102.01.00.235-фмн- ксп, 102.01.00.235-фмн- киб,
102.01.00.236-фмн-киб, 102.01.00.235-фмн-кая

Москва 2022

Рабочая программа дисциплины разработана в соответствии с Приказом Ректора МГУ №1216 от 24 ноября 2021 года «Об утверждении Требований к основным программам подготовки научных и научно-педагогических кадров в аспирантуре, самостоятельно устанавливаемых Московским государственным университетом имени М.В. Ломоносова»

1. Краткая аннотация:

Название дисциплины Криптосистемы с открытым ключом

Цель изучения дисциплины – Данный курс посвящен некоторым важным разделам криптографии, которые не затрагиваются в соответствующем стандартном курсе и которые важны как в теоретическом аспекте, так и для приложений. А именно, рассматриваются алгебраические основы теории делимости (кольца главных идеалов, евклидовы и факториальные кольца). Рассматриваются примеры использования этой теории для построения и анализа криптосхем. Рассматриваются протоколы цифровой подписи, обладающие дополнительными свойствами (интерактивность, стираемость, нулевое разглашение, неотслеживаемость, коллективная подпись, пороговые схемы, достоверность, законность и некоторые другие). Рассматриваются протоколы открытого распределения ключа, отличные от схемы Диффи-Хеллмэна, а также атаки на такие схемы отличные от использования дискретного логарифмирования. Рассматривается задача безопасного создания и хранения базы данных. Анализируются положительные и отрицательные стороны технологии «блокчейн». Вводится понятие децентрализованного протокола. Ро метод Полларда для логарифмов малого веса. Ро метод Полларда с оракулом Диффи-Хеллмэна. Вскрытие Шамиром рюкзака Меркла.

2. Уровень высшего образования –аспирантура

3. Научная специальность 2.3.6 «Методы и системы защиты информации, информационная безопасность», область науки**:** Физико-математические науки.

4. Место дисциплины (модуля) в структуре Программы аспирантуры- элективный курс.

5. *Объем дисциплины (модуля) составляет 2 зачетные единицы, всего 108 часов, из которых 28 часа составляет контактная работа студента с преподавателем (**24** часов занятия лекционного типа, 4 часов мероприятия текущего контроля успеваемости и промежуточной аттестации),80 часа составляет самостоятельная работа учащегося.*

6. Входные требования для освоения дисциплины (модуля), предварительные условия.

На предыдущих уровнях высшего образования должны быть освоены общие курсы:

1. Общая алгебра

2. Элементарная теория чисел

3. Введение в криптографию

4. Теоретико-числовые алгоритмы

7. Содержание дисциплины (модуля), структурированное по темам

Наименование и краткое содержание разделов и тем дисциплины (модуля), **форма промежуточной аттестации по дисциплине (модулю)**	**Всего** **(часы)**	В томчисле								
		Контактная работа (работа во взаимодействии с преподавателем), часы изних						**Самостоятельная работа обучающегося, часы** из них		
		Занятиялекционного типа	Занятиясеминарского типа	Групповыеконсультации	Индивидуальныеконсультации	Учебные занятия, направленные на проведение текущего контроля успеваемости, промежуточной аттестации	**Всего**	Выполнениедомашнихзаданий	Подготовка к коллоквиумам	**Всего**
Тема 1.Алгебраические основы теории делимости. Основные понятия и термины. Понятие евклидова кольца, простого элемента в произвольном кольце, единицы и ассоциированных элементов, факториального кольца.	16	6	2	-	-		8	8	-	8

Доказательство теоремы об однозначности разложения в кольце целых чисел, в произвольном евклидовом кольце. Теоремы о кольцах главных идеалов и о существовании единицы в евклидовом кольце. Разбираются примеры факториальных и нефакториальных колец из целых алгебраических чисел второй степени. Разбираются некоторые задачи на делимость в кольце целых чисел. В том числе решаемые с помощью локазаннойфакториальности некоторых колец целых алгебраических.										
Тема 2. Асимметричные протоколы. Вводятся понятия:	8	4	-	-	-	-	4	4	-	4

интерактивность, стираемость, нулевое разглашение, неотслеживаемость, коллективная подпись, пороговые схемы, достоверность, законность. Разбирается протокол Сидельникова открытого распределения ключа. Доказывается его нестойкость в кольце матриц. Разбираются протоколы протоколы аутентификации Антверпена и Шаума, BBSгенератор, протоколы с числами Блюма и последовательностями Лукаша. Разбираются протоколы цифровой подписи Шаума, Имаи-Матсумото-Патарина.										
Тема 3. Задача безопасного создания и хранения базы данных	12	6	-	-	-	-	6	6	-	6

Разбираются слабости централизованных схем. Вводится понятие децентрализации. Разбираются протоколы децентрализованных аутентификации, цифровой подписи и шифрования. Рассматриваются свойства схем, построенных при помощи технологии «блокчейн».										
Тема 4. Комплексные атаки на асимметричные протоколы Ро метод полларда для дискретных логарифмов малого веса. Ро метод Полларда с оракулом Диффи-Хеллмэна. Атака на схему Диффи-Хеллмэна на эллиптических кривых с использованием спариваний.	18	8	2	-	-		8	8	-	8

Вскрытие схемы «рюкзака» Меркла сведением к решению системы уравнений в целых числах.										
Промежуточная аттестация: *зачет (экзамен)*	22									56
Итого	108									

8. Образовательные технологии.

При проведении лекционных занятий предусматривается возможность использования информационных технологий, включающих пакеты математических программ: Pari, MATHEMATICA и др. Использование информационных технологий осуществляется, в частности, в процессе реализации активных и интерактивных форм проведения занятий. При чтении лекций в качестве материала, иллюстрирующего возможности математического моделирования в различных ситуациях, активно используются примеры из практики обработки данных в процессе работы криптографических протоколов. Информационные и интерактивные технологии используются при обсуждении проблемных и неоднозначных вопросов, требующих выработки решения в ситуации неопределенности.

9. Учебно-методические материалы для самостоятельной работы по дисциплине (модулю):

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к текущему контролю и промежуточной аттестации.

Литература для самостоятельной работы студентов в соответствии с тематическим планом .

Тема 1

- ✓ Ван дер Варден Б.Л. Алгебра М: Наука 1976.
- ✓ Р.Лиддл, Г.Нидеррайтер. Конечные поля. Т.1, М.: Мир, 1988.

Тема 2

- ✓ Черепнев М.А. Криптографические протоколы: Учебное пособие. Центр прикладных исследований при механико-математическом факультете, 2006.
- ✓ Василенко О.Н. Теоретико-числовые алгоритмы в криптографии: МЦНМО, 2003.

Тема 3

- ✓ Черепнев М.А.Децентрализованная схема защищенного создания и хранения баз данных. INJOIT, т.8, №7 (2020), с. 109-115
- ✓ ЧерепневМ.А. Estimates of Fork-attack effectiveness on blockchain protocol INJOIT, v.7 (2019), n.4, p.25-29
- ✓ ЧерепневМ.А. Blockchain and the common signature protocol INJOIT, v.7 (2019), n.6, p.17-23

Тема 4

- ✓ Черепнев М.А., Грачева С.П. Ро-метод Полларда для нахождения дискретного логарифма в случае его малого веса. Информационные технологии, т.28, 2022, №1, с.26-32. DOI: 10.17587/it.28.26-32
- ✓ A. Shamir, A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem, Proc. 23rd Annual Symposium on Foundations of Computer Science,1982, pp. 145-152.

10. Ресурсное обеспечение:

- Перечень основной и вспомогательной учебной литературы ко всему курсу

Основная литература:

- ✓ Ван дер Варден Б.Л. Алгебра М: Наука 1976.
- ✓ Р.Лиддл, Г.Нидеррайтер. Конечные поля. Т.1, М.: Мир, 1988.
- ✓ Черепнев М.А. Криптографические протоколы: Учебное пособие. Центр прикладных исследований при механико-математическом факультете, 2006.
- ✓ Василенко О.Н. Теоретико-числовые алгоритмы в криптографии: МЦНМО, 2003.
- ✓ Черепнев М.А.Децентрализованная схема защищенного создания и хранения баз данных. INJOIT, т.8, №7 (2020), с. 109-115
- ✓ ЧерепневМ.А. Estimates of Fork-attack effectiveness on blockchain protocol INJOIT, v.7 (2019), n.4, p.25-29
- ✓ ЧерепневМ.А. Blockchain and the common signature protocol INJOIT, v.7 (2019), n.6, p.17-23
- ✓ Черепнев М.А., Грачева С.П. Ро-метод Полларда для нахождения дискретного логарифма в случае его малого веса. Информационные технологии, т.28, 2022, №1, с.26-32. DOI: 10.17587/it.28.26-32
- ✓ A. Shamir, A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem, Proc. 23rd Annual Symposium on Foundations of Computer Science,1982, pp. 145-152.
- ✓ Черепнев М.А., Шалимов Ю.П.Ро-метод Полларда для нахождения дискретного логарифма в случае, когда его биты можно угадывать, Дискретная математика, (в печати).
- ✓

1. Дополнительнаялитература:

1. З.И.Боревич, И.Р.Шафаревич. Теория чисел М.: Наука, 1972.
2. Криптографические методы защиты информации.совм. с С.Б.Гашковым, Э.А.Применко. Учебное пособие, «Академия», 2010, 298 с.

- Перечень используемых информационных технологий, используемых при осуществлении образовательного процесса, включая программное обеспечение, информационные справочные системы (при необходимости):

http://elibrary.ru
www.scopus.com

- Описаниематериально-техническойбазы.
  Занятия проводятся в аудитории, оснащенной мультимедийным экраном

11. Язык преподавания – русский

12. Преподаватели:

Степень, должность ФИО., e-mail, тел.: д.ф.-м.н., профессорЧерепнев Михаил Алексеевич,cherepniov@gmail.com, 8-916-1579745

Фонды оценочных средств, необходимые для оценки результатов обучения

Образцы домашних заданий:

1. Докажите факториальность кольца целых Гауссовых чисел.
2. Решить в целых числахx^2+2=y^3
3. Разложить на простые множители 6+2i
4. Докажите нулевое разглашение в схеме стираемой подписи Шаума.
5. Кроме того в качестве домашнего задания подразумевается изучение рекомендуемой литературы.

Вопросы для промежуточной аттестации – **зачета (экзамена)**:

1. Слабости централизованных схем. Слабости элементарной схемы цифровой подписи. Схемы стираемой подписи в общем виде.

2. Схема Шаума. Интерактивность, стираемость, нулевое разглашение.

3. Факториальность колец целых алгебраических второй степени. Решение диофантовых уравнений с использованием факториальности.

4. Евклидовы кольца, кольца главных идеалов, факториальные кольца

5. Приводимость многочленов над Z и над Q. Критерий Эйзенштейна.

7. Схема Имаи-Матсумото-Патарина

9. Технология Блокчейн и протокол коллективной подписи

10. Вскрытие схемы рюкзака Шамиром.

10. Схема с последовательностями Люка

11. Ро метод Полларда для логарифмов малого веса.

Методические материалы для проведения процедур оценивания результатов обучения

Зачет (экзамен) проходит по билетам, включающем 2 вопроса. Уровень знаний аспиранта по каждому вопросу на «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». В случае если на все вопросы был дан ответ, оцененный не ниже чем «удовлетворительно», аспирант получает общую оценку «зачтено».