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

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:

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), примеры использования этой теории для построения и анализа криптосхем, протоколы цифровой подписи, обладающие дополнительными свойствами (интерактивность, стираемость, нулевое разглашение, неотслеживаемость, коллективная подпись, пороговые схемы, достоверность, законность и некоторые другие). 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.

Одна из задач курса заключается в развитии способности к критическому анализу современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях.

2. Уровень высшего образования - подготовка кадров высшей квалификации.

3. Научная специальность: в отрасли физико-математических наук - 1.2.1., 1.2.2., 1.2.3., 1.1.2., 1.1.4., 1.1.5., 1.1.6., 2.3.5., 2.3.6., а также в отрасли технических наук - 1.2.2.

4. Место дисциплины (модуля) в структуре Программы аспирантуры: Обязательные Дисциплины (модули) - Факультетская дисциплина (обязательная дисциплина по выбору).

5. Объем дисциплины (модуля) составляет 2 зачетные единицы, всего 72 часа, из которых 28 часов составляет контактная работа аспиранта с преподавателем, 44 часа составляет самостоятельная работа аспиранта.

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 том числе								
		Контактная работа (работа во взаимодействии с преподавателем), часы из них						**Самостоятельная работа обучающегося, часы** из них		
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные консультации	Учебные занятия, направленные на проведение текущего контроля успеваемости, промежуточной аттестации	**Всего**	Выполнение домашних заданий	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. 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.	**16**	6	2	-	-		**8**	8	-	**8**

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: 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.	**8**	4	-	-	-	-	**4**	4	-	**4**
Тема 3. Задача безопасного создания и хранения базы данных Разбираются слабости централизованных схем. Вводится понятие децентрализации. Разбираются протоколы децентрализованных аутентификации, цифровой подписи и шифрования. Рассматриваются свойства схем, построенных при	**12**	6	-	-	-	-	**6**	6	-	**6**

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. Вскрытие схемы «рюкзака» Меркла сведением к решению системы уравнений в целых числах.	**16**	8	-	-	-		**8**	8	-	**8**
Промежуточная аттестация: экзамен	**20**	-	-	-	-	2	**2**	18	-	**18**
Итого	**72**	**24**	**2**	**-**	**-**	**2**	**28**	**44**	**-**	**44**

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 аспиранта состоит в изучении лекционного материала, учебно-методической литературы, подготовки к текущему контролю и промежуточной аттестации. Литература для самостоятельной работы аспирантов в соответствии с тематическим планом.

Тема 1

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

Тема 2

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

Тема 3

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

Тема 4

1. 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
2. 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

Основная литература:

1. Ван дер Варден Б.Л. Алгебра М: Наука 1976.
2. Р.Лиддл, Г.Нидеррайтер. Конечные поля. Т.1, М.: Мир, 1988.
3. Черепнев М.А. Криптографические протоколы: Учебное пособие. Центр прикладных исследований при механико-математическом факультете, 2006.
4. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии: МЦНМО, 2003.
5. Черепнев М.А.Децентрализованная схема защищенного создания и хранения баз данных. INJOIT, т.8, №7 (2020), с. 109-115
6. ЧерепневМ.А. Estimates of Fork-attack effectiveness on blockchain protocol INJOIT, v.7 (2019), n.4, p.25-29
7. ЧерепневМ.А. Blockchain and the common signature protocol INJOIT, v.7 (2019), n.6, p.17-23
8. 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
9. 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. Черепнев М.А., Шалимов Ю.П.Ро-метод Полларда для нахождения дискретного логарифма в случае, когда его биты можно угадывать, Дискретная математика, (в печати).

Дополнительная литература:

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.

Информационные справочные системы:

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

Материально-техническая база:

- Занятия проводятся в аудитории, оснащенной мультимедийным экраном

11. Язык преподавания – русский

12. Преподаватели:

- профессор Черепнев Михаил Алексеевич

Фонды оценочных средств,
необходимые для оценки результатов обучения

Образцы домашних заданий:

1. Докажите факториальность кольца целых Гауссовых чисел.
2. Решить в целых числах $x^2+2=y^3$
3. Разложить на простые множители 6+2i
4. Докажите нулевое разглашение в схеме стираемой подписи Шаума.

Кроме того, в качестве домашнего задания подразумевается изучение рекомендуемой литературы.

Вопросы для промежуточной аттестации –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

8. Технология Блокчейн и протокол коллективной подписи

9. 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

Экзамен проходит по билетам, включающим 2 вопроса. Уровень знаний аспиранта оценивается на «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии и показатели оценивания ответа на экзамене			
2	3	4	5
Неудовлетворительно	**Удовлетворительно**	**Хорошо**	**Отлично**
Фрагментарные знания актуальных проблем и тенденций в области криптосистем и криптографии.	Неполные знания актуальных проблем и тенденций в области криптосистем и криптографии.	Сформированные, но содержащие отдельные пробелы знания актуальных проблем и тенденций в области криптосистем и криптографии. .	Сформированные и систематические знания актуальных проблем и тенденций в области криптосистем и криптографии.