Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям
_____ О.И. Чуприс
«17» 04 2019 г.

Регистрационный № УД-7134/уч.

КРИПТОГРАФИЯ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-98 80 02 Математическое и программное обеспечение информационной безопасности

2019 г.

Учебная программа составлена на основе ОСВО 1-98 80 02-2012 и учебного плана Р98-253/уч. от 26.05.2017

СОСТАВИТЕЛИ:

С.В.Агиевич – доцент кафедры математического моделирования и анализа данных факультета прикладной математики и информатики Белорусского государственного университета, кандидат физико-математических наук
В.Ю.Палуха – ассистент кафедры математического моделирования и анализа данных факультета прикладной математики и информатики Белорусского государственного университета

РЕЦЕНЗЕНТЫ:
А.И.Трубей – заведующий НИЛ прикладной информатики Учреждения БГУ "Научно-исследовательский институт прикладный проблем математики и информатики";

В.И.Берник – главный научный сотрудник отдела теории чисел Государственного научного учреждения «Институт математики Национальной академии наук Беларуси», доктор физико-математических наук, профессор.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математического моделирования и анализа данных
(протокол № 18 от 18 июня 2019 года);

Научно-методическим Советом БГУ

(протокол № 5 от 28 июня 2019 года).

Заведующий кафедрой
математического моделирования и анализа данных _____И.А. Бодягин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Учебная дисциплина «Криптография на эллиптических кривых»посвящена таким важным вопросам современной криптографии, как криптосистемы на основе эллиптических кривых, эффективная реализация криптографических преобразований, управление открытыми ключами,

Цель учебной дисциплины – изучение теоретических основ алгебры на эллиптических кривых, необходимых для разработки, анализа и эксплуатации современных средств криптографической защиты информации.

Задачи учебной дисциплины:

1. Приобретение практических навыков для эффективной реализации криптосистем на основе эллиптических кривых.
2. Изучить стандартные криптосистемы на основе эллиптических кривых для эффективного их использования на практике.
3. Изучить современные методы управления криптографическими ключами.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием (магистра).

Учебная дисциплина «Криптография на эллиптических кривых» относится к циклу дисциплин специальной подготовки (дисциплина по выбору студента) компоненты учреждения высшего образования.

Программа составлена с учетом **межпредметных связей** с учебными дисциплинами. Основой для изучения учебной дисциплины являются учебные дисциплины I ступени высшего образования «Геометрия и алгебра», «Криптографические методы». Знания, полученные в учебной дисциплине, используются при изучении дисциплины II ступени высшего образования «Квантовая криптография», а также способствовать успешному прохождению производственной практики по специальности и подготовки магистерской диссертации.

Требования к компетенциям

Освоение учебной дисциплины «Криптография на эллиптических кривых» должно обеспечить формирование следующих академических, социально-личностных и профессиональных компетенций:

академические компетенции**:**

АК-1. Способность к самостоятельной научно-исследовательской деятельности (анализ, сопоставление, систематизация, абстрагирование, моделирование, проверка достоверности данных, принятие решений и др.), готовность генерировать и использовать новые идеи.

социально-личностные компетенции:

СЛК-5. Формировать и аргументировать собственные суждения и профессиональную позицию.

профессиональные компетенции:

ПК-4. Разрабатывать новые методы и технологии защиты информации.

В результате освоения учебной дисциплины студент магистратуры должен:

знать:

- способы эффективной реализации криптосистем на основе эллиптических кривых;
- стандартные криптосистемы на основе эллиптических кривых и их использование на практике;
- методы управления открытыми ключами и принципы построения систем именного шифрования

уметь:

- применять полученные знания для создания надежных систем защиты информации;

владеть:

- основными методами построения надежных криптографических систем на основе эллиптических кривых;

Структура учебной дисциплины

Дисциплина изучается в 3-ем семестре. Всего на изучение учебной дисциплины «Комбинаторный анализ» отведено:

– для очной формы получения высшего образования – 104 часа, в том числе 40 аудиторных часов, из них: лекции – 20 часов, лабораторные занятия – 20 часов.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма текущей аттестации по учебной дисциплине – зачёт.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. Эллиптические кривые в криптографии

Тема 1.1. Группа точек эллиптической кривой

Квадратичный вычет. Символ Лежандра. Эллиптические кривые. Группа точек эллиптической кривой.

Тема 1.2. Операции над точками эллиптической кривой

Сложение и удвоение точек. Проблема дискретного логарифмирования в группе точек эллиптической кривой.

Раздел 2. Реализация арифметики эллиптических кривых

Тема 2.1.Критерии выбора параметров эллиптической кривой.

Вычисление кратной точки. Алгоритм Крэндалла. Оконный метод Брауэра. Специальные простые. Умножение Карацубы.

Тема 2.2. Проективные координаты.

Переход к проективным координатам.

Тема 2.3. Знаковое представление.

Аддитивные цепочки. Аддитивно-субтрактивные цепочки. Простое знаковое представление. Простая и оптимальная знаковые формы.

Тема 2.4. Эффективная реализация арифметики эллиптических кривых

Трюк Шамира. Лестница Монтгомери.

Раздел 3. Электронная цифровая подпись на основе эллиптических кривых

Тема 3.1. Схема Шнорра построения электронной цифровой подписи.

ЭЦП Шнорра. Стойкость. Модель ROM. Сведение задаче «единичная подделка» для ЭЦП Шнорра к задаче дискретного логарифмирования. Лемма о разветвлении.

Тема 3.2. Белорусский стандарт электронной цифровой подписи на основе эллиптических кривых.

Основные положения СТБ 34.101.45-2013.

Раздел 4. Протоколы формирования общего ключа на основе эллиптических кривых

Тема 4.1. Протокол Диффи – Хеллмана.

Протокол Диффи – Хеллмана. Протокол с сертификатами. Управление сертификатами открытых ключей. Протоколы MTI. Защита при раскрытии долговременных ключей. Атака «малые подгруппы». Аутентификация. Протокол MQV.

Тема 4.2 Современные стандартные протоколы формирования общего ключа.

Протокол STS. Протокол TLS.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов						Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное	Количество часов УСР	
1	2	3	4	5	6	7	8	9
1.	**Группа точек эллиптической кривой**	**4**			**2**			
1.1	Группа точек эллиптической кривой	2			0			Устный опрос.
1.2	Операции над точками эллиптической кривой	2			2			Отчет о выполнении домашних практических упражнений с их устной защитой.
2.	**Реализация арифметики эллиптических кривых**	**10**			**12**			
2.1	Критерии выбора параметров эллиптической кривой.	4			2			Устный опрос. Отчет о выполнении домашних практических упражнений с их устной защитой.
2.2	Проективные координаты	2			4			Отчет о выполнении домашних практических упражнений с их устной защитой.
2.3	Знаковое представление	2			4			Отчет о выполнении домашних практических упражнений с их устной защитой. Коллоквиум
2.4	Эффективная реализация арифметики эллиптических кривых	2			2			Отчет о выполнении домашних практических упражнений с их устной защитой. Контрольная работа

3	**Электронная цифровая подпись на основе эллиптических кривых**	**2**			**2**			
3.1	Схема Шнорра построения электронной цифровой подписи.				2			Отчет о выполнении домашних практических упражнений с их устной защитой.
3.2	Белорусский стандарт электронной цифровой подписи на основе эллиптических кривых.	2						Устный опрос
4	**Протоколы формирования общего ключа на основе эллиптических кривых**	**4**			**4**			
4.1	Протокол Диффи – Хеллмана	2			2			Отчет о выполнении домашних практических упражнений с их устной защитой.
4.2	Современные стандартные протоколы формирования общего ключа.	2			2			Отчет о выполнении домашних практических упражнений с их устной защитой. Контрольная работа.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. – М.: Диалектика, 2017. – 1040 с.

2. Харин Ю.С.[и др.] Криптология: учебник. — Минск: БГУ, 2013. – 511 с.

2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. — Москва: Гелиос АРВ, 2001.

3. Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим методам защиты информации. — Минск, БГУ, 2001.

4. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. — Москва: КомКнига, 2006. — 328 с.

Перечень дополнительной литературы

1. Menezes A.J., van Oorschot P. C., Vanstone S.A. Handbook of Applied Cryptography. — CRCPress, 1996.

2. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source code in C. — John Wiley & Sons, 1996.

3. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. N. Y.: Springer, 2004.

Переченьрекомендуемыхсредствдиагностикииметодикаформированияи тоговойоценки

Длядиагностикикомпетенций врамкахучебной дисциплины рекомендуется использовать следующие формы:

1. Устная форма: выборочный устный опрос, коллоквиум.
2. Письменная форма:контрольные работы, отчеты по домашним практическим упражнений.
3. Устно-письменная форма: отчеты попрактическим упражнениям с их устной защитой.

Формой текущей аттестации по дисциплине «Криптография на эллиптических кривых» учебным планом предусмотрен экзамен.

При формировании итоговой оценки используется рейтинговая оценка знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знанийстудентов по дисциплине.

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

- отчёты о выполнении домашних практических упражнений (с их устной защитой) – 40 %;
- контрольные работы – 30%;
- коллоквиум – 30%.

Рейтинговая оценка по дисциплине рассчитывается на основе оценки текущей успеваемости и зачетной оценки с учетом их весовых коэффициентов Вес оценка по текущей успеваемости составляет 30 %, зачетная оценка – 70 %.

Примерная тематика лабораторных занятий

Занятие № 1. Операции сложения и удвоения точек эллиптической кривой.

Занятие № 2.Вычисление кратной точки. Алгоритм Крэндалла. Оконный метод Брауэра.

Занятие № 3.Переход к проективным координатам.

Занятие № 4. Сложение и удвоение точек эллиптической кривой с использованием проективных координат

Занятие № 5.Построение аддитивных и аддитивно-субтрактивных цепочек.

Занятие № 6.Простое и оптимальное знаковое представление.

Занятие № 7. Изучение метода "трюк Шамира".

Занятие № 8. Реализация схемы Шнорра построения электронной цифровой подписи.

Занятие № 9.Реализация протокола Диффи-Хэллмана на основе эллиптических кривых.

Занятие № 10.Изучение протоколов STS и TLS и их применения на практике.

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

При организации образовательного процесса большинства практических занятий используется практико-ориентированный подход, который предполагает освоение содержания учебного материала через решение практических задач, а также приобретение навыков эффективного выполнения разных видов профессиональной деятельности.

Кроме этого, при организации образовательного процесса используется комбинация методов группового обучения, проектного обучения и учебной дискуссии. Комбинация методов предполагает: ориентацию на генерирование идей, приобретение навыков для решения исследовательских, творческих и коммуникационных задач, появление нового уровня понимания изучаемой темы, применение знаний (теорий, концепций) при решении проблем, определение способов их решения.

Методические рекомендации

по организации самостоятельной работы обучающихся, подготовка к экзамену

Для организации самостоятельной работы студентов магистратуры по учебной дисциплине следует использовать современные информационные технологии: разместить в сетевом доступе комплекс учебных и учебно-методических материалов (учебно-программные материалы, учебное издание для теоретического изучения дисциплины, презентации лекций, методические указания к практическим занятиям, электронные версии домашних заданий, материалы текущего контроля и текущей аттестации, позволяющие определить соответствие учебной деятельности обучающихся требованиям образовательных стандартов высшего образования и учебно-программной документации, в том числе вопросы для подготовки к экзамену, задания, вопросы для самоконтроля, список рекомендуемой литературы, информационных ресурсов и др.).

Примерный перечень вопросов к зачёту

1. Арифметика на ЭК: сложение и удвоение точек.
2. Арифметика на ЭК: кратная точка.
3. Арифметика на ЭК: специальные простые, алгоритм Крэндалла.
4. Арифметика на ЭК: проективные координаты, сложение и удвоение.
5. Арифметика на ЭК: аддитивные цепочки.
6. Арифметика на ЭК: аддитивно-субтрактивные цепочки, простое знаковое представление.
7. Арифметика на ЭК: оптимальное знаковое представление (NAF).
8. Арифметика на ЭК: трюк Шамира.
9. Арифметика на ЭК: лестница Монтгомери.
10. Умножение Карацубы.
11. ЭЦП Шнорра на ЭК: долговременные параметры.
12. ЭЦП Шнорра на ЭК: алгоритмы.
13. Протокол Диффи-Хеллмана на ЭК: базовый протокол, протокол с сертификатами.
14. Протоколы MTI.
15. Защита при раскрытии долговременных ключей (на примере протоколов MTI).
16. Атака «малые подгруппы» (на примере протоколов MTI).
17. Аутентификация на основе протокола Диффи-Хеллмана.
18. Протокол MQV.
19. Односторонний MQV.
20. Протокол STS.
21. Протоколы TLS.

Рекомендуемая тематика контрольных работ и коллоквиума:

1. Контрольная работа № 1 «Арифметика точек эллиптической кривой».
2. Контрольная работа № 2«Протоколы формирования общего ключа и электронная цифровая подпись на основе эллиптических кривых».
3. Коллоквиум «Арифметика точек эллиптической кривой и ее эффективная реализация».

Текущий контроль знаний проводится в соответствии с учебно-методической картой дисциплины.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Квантовая криптография	Математического моделирования и анализа данных	Нет	Изменений в содержании учебной программы не требуется, протокол № 15 от 02 апреля 2019 г.

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
_____ (протокол № ____ от _____ 201_ г.)

Заведующий кафедрой
_____ _____ _____

УТВЕРЖДАЮ
Декан факультета
_____ _____ _____