БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Ректор Белорусского
государственного университета
_____А.Д.Король
15 июля 2024 г.
Регистрационный №УД-13786/уч.

СОВРЕМЕННЫЕ ГЛАВЫ КРИПТОГРАФИИ

Учебная программа учреждения образования по учебной дисциплине для специальности:

1-98 01 01 Компьютерная безопасность (по направлениям)

Направление специальности:
1-98 01 01-01 Компьютерная безопасность (математические методы и программные системы)

2024 г.

Учебная программа составлена на основе ОСВО 1-98 01 01-2021, учебных планов БГУ: № Р98-1-005/уч. от 23.07.2021, № Р98-1-206/уч. от 22.03.2022.

СОСТАВИТЕЛЬ:

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

РЕЦЕНЗЕНТ:

Д.В. Васильев, заведующий отделом теории чисел и дискретной математики ГНУ «Институт математики НАН Беларуси», кандидат физико-математических наук.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математического моделирования и анализа данных БГУ (протокол № 14 от 28.05.2024);

Научно-методическим советом БГУ (протокол № 9 от 28.06.2024).

Заведующий кафедрой _____ В.И. Малюгин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

С помощью криптографических методов решаются все более трудные прикладные задачи, строятся все более сложные криптографические системы. Учебная дисциплина «Современные главы криптографии» знакомит студентов с современными криптографическими алгоритмами и протоколами и их комбинированием для построения сложных криптографических систем. Дисциплина дает представление о криптографии на эллиптических кривых, доказательствах с нулевым разглашением, протоколах формирования общего ключа, идентификационном шифровании, протоколах консенсуса, системах электронного голосования.

Изучаемые криптографические методы основываются на использовании объектов и применении методов широкого набора математических дисциплин: алгебры, теории чисел, теории вероятностей, математической статистики, теории информации, теории сложности вычислений.

Цели учебной дисциплины:

– изучение актуальных направлений развития криптографии;

– формирование навыков использования криптографических алгоритмов и протоколов для построения сложных криптографических протоколов и систем.

При изложении материала учебной дисциплины важно показать возможности использования конкретных криптографических методов при решении прикладных задач защиты информации.

Задачи учебной дисциплины:

1. Изучение криптографических решений на основе эллиптических кривых.
2. Изучение доказательств с нулевым разглашением;
3. Изучение систем электронного голосования;
4. Изучение протоколов формирования общего ключа;
5. Изучение протокола TLS;
6. Изучение систем идентификационного шифрования;
7. Изучение протоколов консенсуса.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина «Современные главы криптографии» относится к модулю «Криптография» компонента учреждения высшего образования.

Требования к компетенциям

Освоение учебной дисциплины «Современные главы криптографии» должно обеспечить формирование следующей **специализированной** компетенции:

СК. Разрабатывать и анализировать надежность блочных и поточных криптосистем, функций хэширования, криптосистем с открытым ключом и систем электронной цифровой подписи.

В результате освоения учебной дисциплины студент должен:

знать:

– основные инструменты криптографии на эллиптических кривых;

– требования к доказательствам с нулевым разглашением;

– принципы построения систем электронного голосования;

– стандартные протоколы аутентификации и формирования общего ключа;

– основы идентификационного шифрования и протоколов консенсуса.

уметь:

– применять полученные знания для создания надежных систем защиты информации;

иметь навык:

– применение правил комбинирования базовых криптографических примитивов для построения сложных протоколов и систем.

Структура учебной дисциплины

Дисциплина изучается в 7 семестре. В соответствии с учебным планом всего на изучение учебной дисциплины «Современные главы криптографии» отведено для очной формы получения высшего образования – 108 часов, в том числе 68 аудиторных часов, лекции – 34 часа, лабораторные занятия – 34 часа.

Лекции – 34 часа, лабораторные занятия – 30 часов, управляемая самостоятельная работа (УСР) – 4 часа.

Трудоемкость учебной дисциплины составляет 3 зачетные единицы.

Форма промежуточной аттестации – экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Эллиптические кривые в криптографии.

Эллиптические кривые. Дискриминант. Сложение точек. Группа точек. Задача дискретного логарифмирования.

Тема 2. Доказательства с нулевым разглашением.

Протокол Шнорра. Неинтерактивный протокол Шнорра. AND- и OR-композиции. Шифрование Эль-Гамаля и доказательства, с ним связанные. Свойства протоколов ZKP.

Тема 3. Электронное голосование.

Концепция и требования. Схемы построения. Слепая подпись. Криптографическое перемешивание. Гомоморфное шифрование и криптосистема Пэйе.

Тема 4. Модификации протокола Диффи–Хеллмана.

Протокол Диффи–Хеллмана на эллиптических кривых. Протокол с сертификатами. Протоколы MTI. Защита от «чтения назад». Атака «малая подгруппа». Аутентификация. Протокол MQV. Протокол STS. Протоколы PAKE.

Тема 5. Протокол TLS.

Схема протокола. Формирование общего ключа. Атака «Тройное рукопожатие». TLS 1.3.

Тема 6. Идентификационное шифрование.

Концепция. Спаривания на эллиптических кривых. Криптосистема Боне – Франклина.

Тема 7. Протоколы консенсуса.

Византийское соглашение. Блокчейн-системы.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Очная (дневная) форма получения высшего образования с применением дистанционных образовательных технологий (ДОТ)

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1	Эллиптические кривые в криптографии	6			2		4	Решение задач. Отчет по заданию с устной защитой
2	Доказательства с нулевым разглашением	6			6			Контрольная работа
3	Электронное голосование	4			4			Отчет по заданию с устной защитой
4	Модификации протокола Диффи – Хеллмана	6			6			Отчет по заданию с устной защитой
5	Протокол TLS	4			4			Тест
6	Идентификационное шифрование	4			4			Контрольная работа
7	Протоколы консенсуса	4			4			Опрос
ИТОГО		**34**			**30**		**4**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Введение в теоретико-числовые методы криптографии: учебное пособие для вузов / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. – 2-е изд., стер. – Санкт-Петербург: Лань, 2024. – 394 с. – URL: https://e.lanbook.com/book/397286.

2. Криптология: учебник для студентов учреждений высшего образования по математическим и техническим специальностям / [Ю. С. Харин и др.]; БГУ. – 2-е изд., пересмотр. – Минск: БГУ, 2023. – 511 с. – URL: https://elib.bsu.by/handle/123456789/309839.

Дополнительная литература

1. Основы криптографии / Алферов А. П. [и др.]. – Москва : Гелиос АРБ, 2001. – 480 с.

2. Столлингс В. Криптография и защита сетей: принципы и практика (2 изд.) / В. Столлингс – М: Вильямс, 2001. – 669 с.

3. Харин, Ю. С. Компьютерный практикум по математическим методам защиты информации / Ю. С. Харин, С. В Агиевич – Минск, БГУ, 2001. – 190 с.

4. Menezes, A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone – CRC Press, 1996. – 816 p.

5. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source code in C / B. Schneier – John Wiley & Sons, 1996. – 675 p.

6. Stinson, D. Cryptography. Theory and Practice / D. Stinson – N.Y. CRC, 1995 – 434 p.

Информационно-методическое обеспечение дисциплины доступно студентам в виде онлайн-курса, размещенного в интернете по адресу https://apmi.bsu.by/resources/cm.

Перечень рекомендуемых средств диагностики и методика формирования итоговой отметки

На лекционных занятиях по дисциплине «Современные главы криптографии» рекомендуется особое внимание обращать на создание связей между теоретическим темами дисциплины и использованием изучаемых методов и алгоритмов для решения практических задач защиты информации.

Контрольные мероприятия проводятся в соответствии с учебно-методической картой дисциплины.

Для диагностики компетенций в рамках учебной дисциплины рекомендуется использовать следующие формы:

1. устная форма: устные опросы по текущим темам;

2. письменная форма: контрольная работа, тест по нескольким теоретическим темам дисциплины, решение задач;

3. устно-письменная форма: отчёты по домашним практическим упражнениям и лабораторным работам с их устной защитой.

Формой промежуточной аттестации по дисциплине «Современные главы криптографии» учебным планом предусмотрен **экзамен** в седьмом семестре.

Для формирования итоговой отметки по учебной дисциплине используется модульно-рейтинговая система оценки знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая система предусматривает использование весовых коэффициентов для текущей и промежуточной аттестации студентов по учебной дисциплине.

Формирование итоговой отметки в ходе проведения контрольных мероприятий текущей аттестации (примерные весовые коэффициенты, определяющие вклад текущей аттестации в отметку при прохождении промежуточной аттестации):

– отчёты по заданиям с устной защитой – 50 %;

– контрольная работа № 1 – 25 %;

– контрольная работа № 2 – 25 %.

Итоговая отметка по дисциплине рассчитывается на основе итоговой отметки текущей аттестации (рейтинговой системы оценки знаний) 40 % и экзаменационной отметки 60 %.

Примерный перечень заданий для управляемой самостоятельной работы

Тема 1. Криптография на эллиптических кривых (4 ч)

Перечень вопросов для углубленного самостоятельного изучения**:**

– реализация арифметики эллиптических кривых;

– способы ускорения вычисления кратной точки.

Рекомендуемая литература: [2].

Форма контроля – отчет по заданию с устной защитой.

Примерный перечень лабораторных занятий

1. Дополнительные свойства протоколов ZKP.
2. Практические системы электронного голосования.
3. Криптосистема Кокса.
4. Виды доказательств в блокчейн-системах.
5. Программная реализация криптосистем и протоколов.

Примерный перечень тем для коллоквиумов

1) Расширения протокола TLS.

Рекомендуемая тематика контрольных работ

1) Контрольная работа №1. *Эллиптические кривые в криптографии. Доказательства с нулевым разглашением*.
2) Контрольная работа №2. *Протоколы аутентификации и формирования общего ключа.*

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используется практико-ориентированный подход.

Практико-ориентированный подход предполагает:

– освоение содержание образования через решения практических задач;

– приобретение навыков эффективного выполнения разных видов профессиональной деятельности;

– ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;

– использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

Методические рекомендации по организации самостоятельной работы

Студенты самостоятельно выполняют следующую работу:

– осуществляют углубленное изучение темы 1 с использованием рекомендуемой литературы;

– выполняют лабораторные задания с использованием различных языков программирования;

– готовят отчёт с результатами проведённых исследований в соответствии с установленными требования;

– работают над устранением указанных при проверке отчётов недостатков.

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются наличием и полной доступностью электронных (и бумажных) курсов лекций, учебно-методических материалов по основным темам дисциплины. Материалы размещены по адресу https://apmi.bsu.by/resources/cm.

Примерный перечень вопросов к экзамену

1. Эллиптические кривые: определения.
2. Дискриминант эллиптической кривой.
3. Сложение точек эллиптической кривой.
4. Группа точек эллиптической кривой.
5. Задача дискретного логарифмирования на эллиптической кривой.
6. Протокол Шнорра.
7. Неинтерактивный протокол Шнорра.
8. Протокол Шнорра на гомоморфизмах.

9. Шифрование Эль-Гамаля.
10. Свойства протоколов ZKP.
11. Электронное голосование: концепция и требования.
12. Схемы построения систем электронного голосования.
13. Слепая подпись.
14. Криптографическое перемешивание.
15. Криптосистема Пэйе.
16. Протокол Диффи—Хеллмана на эллиптических кривых.
17. Протокол Диффи—Хеллмана с сертификатами.
18. Протоколы MTI.
19. Защита от «чтения назад».
20. Атака «малая подгруппа».
21. Аутентификация в протоколах формирования общего ключа.
22. Протокол MQV.
23. Протокол STS.
24. Протоколы PAKE.
25. Схема протокола TLS 1.2.
26. Формирование общего ключа в TLS.
27. Атака «тройное рукопожатие»
28. Протокол TLS 1.3.
29. Идентификационное шифрование: концепция.
30. Спаривания на эллиптических кривых.
31. Криптосистема Боне – Франклина.
32. Византийское соглашение.
33. Блокчейн-системы.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УО

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)
Учебная дисциплина не требует согласования			

Заведующий кафедрой математического моделирования и анализа данных, доктор экономических наук, доцент _____ В.И.Малюгин

28.05.2024

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ УО

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____(протокол № ____ от _____ 202_ г.)
(название кафедры)

Заведующий кафедрой

_____ _____
(ученая степень, ученое звание) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета

_____ _____
(ученая степень, ученое звание) (И.О.Фамилия)