ГОУ ВПО РОССИЙСКО-АРМЯНСКИЙ УНИВЕРСИТЕТ

Составлен в соответствии с государственными требованиями к минимуму содержания и уровню подготовки выпускников по направлению 01.04.02 Прикладная математика и информатика и Положением «Об УМКД РАУ».

УТВЕРЖДАЮ:
Директор института
математики и информатики
к.ф.-м.н.,
Дарбинян Арман Араикович
"19" 07 2023г.

Институт Математики и информатики

Кафедра: Математической кибернетики

Автор(ы): ***д.ф.-м.н., профессор*** **Арутюнян Мариам Евгеньевна**

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

Дисциплина: Б1.О.09 «Ассиметричные алгоритмы кодирования»

Направление: «Прикладная математика и информатика» 01.04.02

Основная образовательная программа магистратуры:
01.04.02 «Математическое и программное обеспечение защиты информации»

ЕРЕВАН

1. **Аннотация** Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), в SSH. Также используется в PGP, S/MIME. Вообще, в основу известных асимметричных криптосистем кладётся одна из сложных математических проблем, которая позволяет строить односторонние функции и функции-лазейки. Алгоритмы криптосистемы с открытым ключом можно использовать как самостоятельное средство для защиты передаваемой и хранимой информации, как средство распределения ключей (обычно с помощью алгоритмов криптосистем с открытым ключом распределяют ключи, малые по объёму, а саму передачу больших информационных потоков осуществляют с помощью других алгоритмов), как средство аутентификации пользователей.
2. **Целью дисциплины** является ознакомление студентов с современными методами ассиметричного шифрования, которые широко используются в различных областях защиты информации. Программа составлена на основе классических и современных учебников, а также результатов последних исследований. В содержание курса входит изучение различных видов ассиметричного шифрования, в частности, на основе элиптических кривых.

Трудоемкость дисциплины и виды учебной работы по учебному плану

Виды учебной работы	Всего часов	Распределение по семестрам			
		1 сем.	2 сем.	3 сем.	4 сем.
1	2	3		5	6
1. Общая трудоемкость изучения дисциплины по семестрам, в т. ч.:	**144**	**144**			
1.1. Аудиторные занятия, в т. ч.:	**36**	**36**			
1.1.1. Лекции	**36**				
1.1.2. Лабораторные занятия					
1.1.3. Практические занятия					
3. Самостоятельная работа, в т. ч.:	**81**	**81**			
1. Контроль	**27**	**27**			
5. Кредиты	**4**	**4**			
6. Форма итогового контроля: Экзамен/Зачет	**экз.**	**экз.**			

1.1. Распределение весов по модулям и формам контроля

2. Формы контролей	Веса форм текущих контролей в результирующих оценках текущих контролей			Веса форм промежуточных контролей в оценках промежуточных контролей			Веса оценок промежуточных контролей и результирующих оценок текущих контролей в итоговых оценках промежуточных контролей			Веса итоговых оценок промежуточных контролей в результирующей оценке промежуточных контролей	Веса результирующей оценки промежуточных контролей и оценки итогового контроля в результирующей оценке итогового контроля
Вид учебной работы/контроля	**М1** [1]	**М 2**	**М 3**	**М 1**	**М 2**	**М 3**	**М 1**	**М2**	**М3**		
Контрольная работа						1					
Тест											
Курсовая работа											
Лабораторные работы											
Письменные домашние задания			1								
Реферат											
Эссе											
Другие формы (Указать)											
Другие формы (Указать)											
Веса результирующих оценок текущих контролей в итоговых оценках промежуточных контролей									0.4		
Веса оценок промежуточных контролей в итоговых оценках промежуточных контролей									0.6		
Вес итоговой оценки 1-го промежуточного контроля в результирующей оценке промежуточных контролей											
Вес итоговой оценки 2-го промежуточного контроля в результирующей оценке промежуточных контролей											
Вес итоговой оценки 3-го промежуточного контроля в результирующей оценке промежуточных контролей										1	
Вес результирующей оценки промежуточных контролей в результирующей оценке итогового контроля											0.4
Экзамен/зачет (оценка итогового контроля)											0.6 (Экзамен/Зачет)
	∑ = 1	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**	**∑ = 1**

[1] Учебный Модуль

2.3.2. Распределение объема дисциплины по темам и видам учебной работы

Разделы и темы дисциплины	**Всего (ак. часов)**	**Лекции(ак. часов)**	**Практ. занятия (ак. часов)**	**Семина-ры (ак. часов)**	**Лабор. (ак. часов)**	**Другие виды занятий (ак. часов)**
1	**2=3+4+5+6+7**	**3**	**4**	**5**	**6**	**7**
Ассиметричные алгоритмы кодирования						
Раздел 1. Введение						
Тема 1. Математическая модель ассиметричной системы	**2**	**2**				
Тема 2. Методы теории чисел применяемые в криптографии	**2**	**2**				
Тема 3. Модулярная арифметика в применении	**2**		**2**			
Тема 4. Сравнения первой степени	**2**	**2**				
Раздел 2. Классические ассиметричные шифры						
Тема 5. Экспоненциальные шифры	**2**	**2**				
Тема 6. RSA	**2**		**2**			
Тема 7. DSA	**2**	**2**				
Решение прикладных задач	**2**		**2**			
Раздел 3. Теория конечных полей						
Тема 8. Группы, кольца, поля	**2**	**2**				
Тема 9. Поля Галуа	**2**		**2**			
Тема 10. Модулярная арифметика многочленов	**2**	**2**				

Решение прикладных задач	**2**		**2**			
Раздел 4. Элиптические кривые						
Тема 11. Элиптические кривые на Zp	**2**	**2**				
Тема 12. Элиптические кривые на GF(2^m)	**2**		**2**			
Тема 13. Ассиметричное шифрование с помощью элиптических кривых	**2**	**2**				
Тема 14. Обмен ключами с помощью элиптических кривых	**2**		**2**			
Тема 15. ECDSA	**2**		**2**			
Решение прикладных задач	**2**		**2**			
ИТОГО	**36**	**18**	**18**			

2.3.3 Содержание разделов и тем дисциплины

Ассиметричные алгоритмы кодирования

Раздел 1. **Введение**

Тема 1. Математическая модель ассиметричной системы

Определение, виды, преимущества и недостатки ассиметричных алгоритмов; описание основных компонентов математической модели; схемы шифрования и электронной подписи; односторонние функции и функции с секретом.

Тема 2. Методы теории чисел применяемые в криптографии

Алгоритм Эвклида, расширенный алгоритм Эвклида.

Тема 3. Модулярная арифметика в применении

Сравнимость чисел, свойства отношения сравнимости, класс вычетов по модулю, полная система вычетов.

Тема 4. Сравнения первой степени

Задача поиска решений сравнения первойстепени, Китайская теорема, алгоритм решения системы сравнений.

Раздел 2. **Классические ассиметричные шифры**

Тема 5. Экспоненциальные шифры

Функция Эйлера, теорема Эйлера, малая теорема Ферма, экспоненциальный шифр, обмен ключами.

Тема 6. RSA

Вычислительная сложность задачи факторизации больших целых чисел, алгоритм шифрования, алгоритм дешифрования, алгоритм шифрования сеансового ключа, цифровая подпись, использование китайской теоремы об остатках для ускорения расшифрования.

Тема 7. DSA

Алгоритм цифровой подписи с использованием оркрытого ключа, DSS стандарт цифровой подписи, криптографическая хеш функция.

Раздел 3. **Теория конечных полей**

Тема 8. Группы, кольца, поля

Определение алгебраической группы, периодической, абелевой группы, кольца, кольцо с единицей, область целостности, поля.

Тема 9. Поля Галуа

Определение, арифметика многочленов, неприводимые многочлены.

Тема 10. Модулярная арифметика многочленов

Наибольший общий делитель многочленов, классы вычетов по неприводимому многочлену, алгоритм Эвклида для многочленов.

Раздел 4**. Элиптические кривые**

Тема 11. Элиптические кривые на Zp

Определение, свойства, геометрические кривые, сложение точек, кривые на Zp, сложение, умножение точек.

Тема 12. Элиптические кривые на GF(2^m)

Определение, свойства, сложение, умножение точек.

Тема 13. Ассиметричное шифрование с помощью элиптических кривых

Проблема дискретного логарифма для элиптических кривых, схема шифрования.

Тема 14. Обмен ключами с помощью элиптических кривых

Система обмена ключами на основе элиптических кривых

Тема 15. ECDSA

Алгоритм с открытым ключом для создания цифровой подписи, аналогичный по своему строению DSA, но определённый, в отличие от него, не над кольцом целых чисел, а в группе точек эллиптической кривой, алгоритмы генерирование ключей, вычисления цифровой подписи.

Рекомендуемая литература:

1. W. Stallings, Cryptography and Network Security, Principles and Practice. 5th edition, Prentice Hall, USA, 2011.