ЦЕНТРАЛЬНЫЙ УНИВЕРСИТЕТ

УТВЕРЖДЕНА

Решением Ученого совета
АНО ВО «Центральный университет»
«25» мая 2026 г.
Протокол №2

Рабочая программа дисциплины (модуля)
«Введение в теорию чисел и криптографию»

Направление подготовки: *38.03.05 Бизнес-информатика*

Направленность (профиль) подготовки: *Бизнес и аналитика*

Квалификация (степень) выпускника: *бакалавр*

Форма обучения: *очная*

Срок освоения программы: *4 года*

Год набора: *2026*

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0215B0C000D1B3FEB44A37EE631E0C27D4
Владелец: Ивашкевич Евгений Васильевич
Действителен: с 13.01.2026 до 13.04.2027

Электронный документ

Москва
2026

Содержание

1. Краткая характеристика дисциплины (модуля)

Рабочая программа дисциплины (модуля) «Введение в теорию чисел и криптографию» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования – бакалавриат по специальности 38.03.05 Бизнес-информатика, профиль Бизнес и аналитика, утвержденный приказом Министерства науки и высшего образования Российской Федерации № 838 от 29.07.2020 года.

Изучение дисциплины (модуля) «Введение в теорию чисел и криптографию» обеспечивает глубокое понимание фундаментальных числовых структур — целых чисел, остаточных классов, простых чисел и их взаимосвязей — которые лежат в основе современных криптографических схем. Дисциплина способствует развитию навыков алгоритмической реализации теоретико-числовых методов в Python, анализа их вычислительной сложности и построения прототипов криптографических протоколов (RSA, Диффи-Хеллман).

Место дисциплины (модуля) в структуре образовательной программы

Настоящая дисциплина (модуль) включена в учебный план по программе подготовки бакалавриата по направлению 38.03.05 Бизнес-информатика, профиль Бизнес и аналитика и входит в часть, формируемую участниками образовательных отношений, Блока 1.

Дисциплина (модуль) является выборной и доступна для изучения на 3 или 4 курсе в 6, 7, 8 семестрах на выбор после успешного освоения дисциплин «Основы математического анализа и линейной алгебры» или «Математический анализ» и «Линейная алгебра и геометрия» или «Математический анализ. Продвинутый уровень» + «Линейная алгебра и геометрия. Продвинутый уровень».

Цель изучения дисциплины (модуля): сформировать у студентов фундаментальные знания теории чисел и практические навыки их алгоритмической реализации, необходимые для построения, понимания и критического анализа базовых криптографических примитивов (RSA, Diffie-Hellman) и дальнейшего профессионального развития в ИБ.

Задачи изучения дисциплины (модуля):

— научиться выполнять арифметические операции с целыми числами, остатками и сравнениями по модулю;

— освоить алгоритм Евклида и расширенный алгоритм Евклида для нахождения НОД и обратного элемента;

— реализовать на Python быстрые методы: возведение в степень (mod), тест простоты, китайскую теорему об остатках, поиск обратного элемента; оценить их сложность;

— написать учебные версии RSA и протокола Диффи-Хеллмана (генерация ключей, шифрование/расшифрование, обмен);

— проанализировать реализованные схемы: корректность, ограничения, потенциальные атаки (факторизация, перебор, chosen-plaintext, MITM) и отличить учебные примеры от реально стойких решений.

В результате освоения дисциплины (модуля) обучающийся должен:

знать:

— выполнять вычисления с целыми числами, остатками и сравнениями по модулю;

— использовать алгоритм Евклида и расширенный алгоритм Евклида для решения задач теории чисел;

— реализовывать на Python базовые алгоритмы: быстрое возведение в степень по модулю, проверку простоты, китайскую теорему об остатках и поиск обратного элемента;

— реализовывать учебные версии криптографических алгоритмов, включая RSA и протокол Диффи — Хеллмана;

— анализировать простейшие криптографические схемы с точки зрения корректности, ограничений и возможных атак;

уметь:

— выполнять вычисления с целыми числами, остатками и сравнениями по модулю;

— использовать алгоритм Евклида и расширенный алгоритм Евклида для решения задач теории чисел;

— реализовывать на Python базовые алгоритмы: быстрое возведение в степень по модулю, проверку простоты, китайскую теорему об остатках и поиск обратного элемента;

— реализовывать учебные версии криптографических алгоритмов, включая RSA и протокол Диффи — Хеллмана;

— анализировать простейшие криптографические схемы с точки зрения корректности, ограничений и возможных атак;

владеть:

— навыками решения задач элементарной теории чисел, связанных с делимостью, сравнениями и простыми числами;

— приёмами алгоритмической реализации теоретико-числовых методов в Python;

— навыками анализа вычислительной сложности базовых алгоритмов теории чисел и криптографии;

— навыками построения и тестирования учебных криптографических протоколов;

— навыками критической оценки криптографических методов, различения учебных примеров и practically secure решений.

2. Перечень планируемых результатов обучения

Компетенции, формируемые в результате освоения дисциплины (модуля) при проведении учебных занятий в форме контактной работы обучающихся с педагогическими работниками Университета и в форме самостоятельной работы обучающихся:

Компетенция	Содержание компетенции	Индикатор компетенции	Перечень планируемых результатов обучения по дисциплине (модулю)
УК-1.	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1.	Знает методы поиска и анализа информации в области аналитики, основные принципы критической оценки источников информации и их релевантности.
		УК-1.2.	Умеет критически оценивать источники информации и синтезировать данные из различных источников для решения задач, применять системный подход к анализу и решению комплексных проблем
		УК-1.3.	Имеет практический опыт работы с современными инструментами и технологиями для обработки информации, формулировании и структурировании задач на основе полученной информации
ОПК-4.	Способен понимать принципы работы информационных технологий; использовать информацию, методы и программные средства ее сбора, обработки и анализа для информационно-аналитической поддержки принятия управленческих решений	ОПК-4.1.	Знает основные принципы работы информационных технологий и их влияние на бизнес-процессы
		ОПК-4.2.	Умеет использовать методы и программные средства для сбора, обработки и анализа информации, обеспечивая качественную информационно-аналитическую поддержку
		ОПК-4.3.	Имеет практический опыт в применении аналитических инструментов для поддержки принятия управленческих решений в организациях
ПК-2.	Способен использовать соответствующий математический аппарат и инструментальные средства для обработки, анализа и систематизации	ПК-2.1.	Знает основные математические методы и инструментальные средства, применяемые для обработки и анализа информации
		ПК-2.2.	Умеет эффективно использовать математический аппарат для систематизации данных и решения профессиональных задач

	информации по теме исследования для решения задач профессиональной деятельности	ПК-2.3.	Имеет практический опыт работы с инструментами анализа информации в рамках исследовательских проектов

3. Тематический план

№п/п	Наименование раздела дисциплины (модуля)	Трудоемкость, академические часы				ТКУ (текущий контроль успеваемости)
		Очная форма				
		Аудиторная работа		Контроль	Самостоятельная работа	
		Лекции	Семинары			
1	Введение в теорию чисел	6	6		24	Домашнее задание, аудиторная работа
2	Сравнения и арифметика по модулю	6	6	2	24	Домашнее задание, аудиторная работа, контрольная работа
3	Системы сравнений и введение в криптографию	6	6		24	Домашнее задание, аудиторная работа
4	Классическая криптография	6	6	2	24	Домашнее задание, аудиторная работа
5	Хеш-функции, подписи и итоговая систематизация	6	6	2	24	Домашнее задание, аудиторная работа, контрольная работа
	Зачет с оценкой			4		Коллоквиум
	Итого:	***30***	***30***	***10***	***120***	
Объем дисциплины (модуля) (в ак. ч.)		***190***				
Объем дисциплины (модуля) (в зач. ед.)		***5***				

4. Содержание дисциплины (модуля)

№п/п	Наименование раздела дисциплины (модуля)	Содержание дисциплины (модуля) по темам
1	Введение в теорию чисел	Основы делимости и алгоритмы теории чисел Наибольший общий делитель и алгоритм Евклида Простые числа и факторизация
2	Сравнения и арифметика по модулю	Сравнения по модулю Обратимые элементы и линейные сравнения. Теоремы Ферма и Эйлера
3	Системы сравнений и введение в криптографию	Китайская теорема об остатках Вероятностные тесты простоты
4	Классическая криптография	Понятие шифра, открытого текста, шифртекста, ключа. Шифр Цезаря, аффинный шифр, шифр Виженера. Уязвимости классических шифров. Симметричная криптография Асимметричная криптография. Протокол Диффи — Хеллмана Криптографический алгоритм с открытым ключом Стойкость и п криптографического протокола с открытым ключом и практические ограничения
5	Хеш-функции, подписи и итоговая систематизация	Хеш-функции, подписи и итоговая систематизация Идея цифровой подписи. Связь подписи с хешированием.

5. Учебно-методическое обеспечение

Университет располагает полным набором лицензионного и свободно распространяемого программного обеспечения, включая продукты отечественного производства.

Каждый студент в течение всего периода обучения получает индивидуальный неограниченный доступ к электронно-библиотечной системе и электронной информационно-образовательной среде университета. Эти системы предоставляют возможность доступа к ресурсам из любой точки, где есть подключение к сети Интернет, как на территории университета, так и за его пределами.

Студентам обеспечен удаленный доступ к современным профессиональным базам данных и информационным справочным системам.

Основная литература:

1. Теория чисел в криптографии : учебное пособие / В. А. Орлов, Н. В. Медведев, Н. А. Шимко, А. Б. Домрачева. - Москва : МГТУ им. Баумана, 2011. - 224 с. - ISBN 978-5-7038-3520-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/2017285

2. Манин, Ю. И. Введение в современную теорию чисел: Научное / Манин Ю.И., Панчишкин А.А. - Москва :МЦНМО, 2014. - 552 с.: ISBN 978-5-4439-2027-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/969551

Дополнительная литература:

1. Добрица, В. П. Практикум по алгебре, теории чисел, элементам криптографии : учебное пособие / В. П. Добрица, Е. А. Кулешова, Ю. А. Халин. – Москва ; Вологда : Инфра-Инженерия, 2025. - 136 с. – ISBN 978-5-9729-2476-9. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2226768

6. Материально-техническое обеспечение

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Изучение дисциплины (модуля) обеспечивается в учебных аудиториях, оснащенных:

- столами и стульями;
- компьютерной техникой;
- механическими калькуляторами;
- специализированным оборудованием, включая демонстрационное оборудование.

Помещения для самостоятельной работы обучающихся, в том числе приспособленные для использования инвалидами и лицами с ограниченными возможностями здоровья, оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

Обучающимся предоставляется доступ (в том числе удаленный) к ресурсам информационно-телекоммуникационной сети «Интернет», электронным ресурсам (в том

числе электронным библиотечным системам, современным профессиональным базам данных и информационным справочным системам):

№	Наименование портала (издания, курса, документа)	Ссылка
1.	Научная электронная библиотека elibrary.ru библиотека	https://elibrary.ru/defaultx.asp
2.	База данных для IT-специалистов	https://habr.com
3.	База данных ScienceDirect	https://www.sciencedirect.com
4.	Официальный сайт Министерства науки и высшего образования Российской Федерации	https://minobrnauki.gov.ru/
5.	Федеральный портал «Российское образование"	https://www.edu.ru/
6.	Информационная система "Единое окно доступа к образовательным ресурсам"	http://window.edu.ru/
7.	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru/
8.	Федеральный центр информационно - образовательных ресурсов	http://fcior.edu.ru/

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модуле), в том числе комплект лицензионного программного обеспечения, современные профессиональные базы данных и информационные справочные системы:

Наименование ПО	Производство	Лицензионное / свободно распространяемое
Операционные системы:		
Microsoft Imagine (Windows Client, Server)	зарубежное	лицензионное
Браузеры:		
Яндекс.Браузер	отечественное	свободно распространяемое
Google Chrome	зарубежное	свободно распространяемое
Офисные приложения:		
Microsoft Imagine (Visio, OneNote)	зарубежное	лицензионное
TeXstudio	зарубежное	свободно распространяемое
Adobe Acrobat Reader	зарубежное	свободно распространяемое
Программное обеспечение для планирования и учета времени:		
Toggle app	зарубежное	свободно распространяемое
Системы управления проектами:		
Microsoft Imagine (Project)	зарубежное	лицензионное
Системы управления базами данных:		
Microsoft Imagine (SQL Server)	зарубежное	лицензионное
Системы резервного копирования (backup):		
Acronis Backup Advanced for HyperV	зарубежное	лицензионное
Справочно-правовые системы:		
КонсультантПлюс: справочно-правовая система	отечественное	лицензионное
Средства антивирусной защиты:		
Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition	отечественное	лицензионное
Среды разработки:		
Visual Studio Code	зарубежное	свободно распространяемое

Электронный документ

Bash (Unix shell)	зарубежное	свободно распространяемое
Anaconda	зарубежное	свободно распространяемое
Robotic Operating System	зарубежное	свободно распространяемое
CopelliaSim	зарубежное	свободно распространяемое
Google Colaboratory	зарубежное	свободно распространяемое
Пакеты программных средств и библиотек:		
AutoPsy	зарубежное	свободно распространяемое
Interactive Disassembler (IDA)	зарубежное	свободно распространяемое
Системы управления библиографической информацией:		
Zotero	зарубежное	свободно распространяемое
Сервисы и службы:		
Bind	зарубежное	свободно распространяемое
Docker	зарубежное	свободно распространяемое

7. Методические и оценочные материалы

Методические указания для обучающихся по освоению дисциплины (модуля)

В процессе изучения дисциплины (модуля) «Введение в теорию чисел и криптографию» в рамках текущего контроля успеваемости используются такие виды учебной работы, как лекции, семинары, домашние задания, аудиторная работа, контрольная работа, коллоквиум, а также различные виды самостоятельной работы обучающихся по заданию преподавателя, направленные на развитие навыков профессиональной лексики, закрепление практических профессиональных компетенций, поощрение инициатив.

Лекция – систематическое, последовательное, монологическое изложение преподавателем учебного материала, как правило, теоретического характера.

В процессе лекций рекомендуется вести конспект лекций: кратко и схематично фиксировать основные идеи, выводы и обобщения лекции; выделять важные мысли, ключевые слова и термины. Необходимо отметить вопросы или материалы, которые вызывают затруднения, и попытаться найти ответы в рекомендованной литературе. Если разобраться в материале не удается, следует сформулировать вопрос и задать его преподавателю на консультации или во время семинарского (практического) занятия.

Семинар – это форма учебной деятельности, проводимая в учебном заведении под руководством преподавателя, где студенты активно участвуют в обсуждениях, практических заданиях и других формах взаимодействия.

Для успешной подготовки к семинару рекомендуется заранее ознакомиться с темой занятия и основными материалами, чтобы иметь возможность активно участвовать в обсуждении. Также полезно подготовить вопросы и идеи для обсуждения, что поможет глубже понять материал и продемонстрировать заинтересованность.

Домашнее задание – набор задач по темам недели.

При работе над домашними заданиями важно внимательно ознакомиться с требованиями и сроками выполнения. Рекомендуется разбивать задания на этапы, чтобы избежать перегрузки и лучше усвоить материал. Использовать различные источники информации, включая учебники и онлайн-ресурсы, для более глубокого понимания темы.

Аудиторная работа – активная работа студента на семинаре или лекции, его ответы на вопросы преподавателя и участие в дискуссии.

Для успешного участия в аудиторной работе студентам рекомендуется заранее ознакомиться с темой обсуждения, прочитать необходимые материалы и подготовить вопросы. Важно активно слушать и вовлекаться в дискуссию, высказывая свои мнения,

аргументируя их. При ответах на вопросы преподавателя стоит быть уверенным, четким и логичным, опираясь на изученный материал. Также полезно поддерживать диалог с однокурсниками, чтобы обогатить обсуждение и расширить свои знания.

Контрольная работа – письменная работа с набором задач, которые нужно решить за ограниченное время.

Цель контрольной работы – получить специальные знания по одной или нескольким темам дисциплины и продемонстрировать навыки их практического применения.

Коллоквиум – устные ответы на вопросы, список которых известен студенту заранее.

В процессе подготовки к коллоквиуму необходимо проанализировать учебные материалы, ознакомившись с лекциями, учебниками и дополнительными источниками, акцентируя внимание на ключевых темах. Рекомендуется создать структурированные конспекты, выделяя основные идеи, термины и формулы.

Самостоятельная работа – работа студентов, направленная на углубленное изучение отдельных тем и вопросов учебной дисциплины (модуля).

В процессе самостоятельной работы студенты взаимодействуют с рекомендованными материалами при минимальном участии преподавателя. Задачи студента включают работу с конспектами лекций (обработка текста), повторное изучение учебных материалов планов и тезисов ответов, изучение дополнительных тем, выполнение учебно-исследовательских заданий и другое.

Система оценивания результатов обучения по дисциплине (модулю)

Критерии получения уровня и оценивания сформированности компетенций по дисциплине (модуле) «Введение в теорию чисел и криптографию»

Оценивание уровня учебных достижений, обучающихся по дисциплине (модулю), осуществляется в виде текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация по дисциплине (модулю) осуществляется в форме ***зачета с оценкой***, при этом проводится оценка компетенций, сформированных по дисциплине.

Для оценивания текущего контроля успеваемости и промежуточной аттестации используется десятибалльная шкала оценивания, которая соотносится с традиционной пятибалльной шкалой следующим образом, если иное не указано в силлабусе дисциплины:

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
10	Отлично	Зачтено	Студент полностью владеет знаниями, изложенными в рабочей программе, и глубоко осмысляет дисциплину. Он самостоятельно и логически последовательно отвечает на все вопросы, акцентируя внимание на наиболее важном. Умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя ключевые моменты и устанавливая причинно-следственные связи. Четко формулирует ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные задачи. Студент хорошо знаком с
9	Отлично	Зачтено	
8	Отлично	Зачтено	

Десятибалльная оценка	Пятибалльная оценка	Оценка за зачет	Общая характеристика результата обучения по дисциплине (модулю)
			методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты дисциплины (модуля) с практическими задачами.
7	Хорошо	Зачтено	Студент обладает знаниями предмета почти в полном объеме рабочей программы и самостоятельно, логически последовательно и всесторонне отвечает на все вопросы, акцентируя внимание на наиболее значимых моментах. Он умеет анализировать, сравнивать, классифицировать, обобщать, конкретизировать и систематизировать изученный материал, выделяя его ключевые аспекты и устанавливая причинно-следственные связи. Формулирует свои ответы, уверенно интерпретирует результаты анализов и других исследований, а также решает сложные ситуационные задачи. Студент хорошо знаком с методами исследования, необходимыми для практической деятельности, и умеет связывать теоретические аспекты предмета с практическими задачами.
6	Хорошо	Зачтено	
5	Удовлетворительно	Зачтено	Студент обладает базовыми знаниями по дисциплине (модулю), но испытывает трудности при самостоятельных ответах и использует неточные формулировки. В ходе ответов он допускает ошибки, касающиеся сути вопросов. Студент способен решать только самые простые задачи и владеет лишь минимальным набором методов исследования.
4	Удовлетворительно	Зачтено	
3	Не сдан	Не зачтено	Студент не овладел обязательным минимумом знаний по предмету и не может ответить на вопросы, даже если преподаватель задает дополнительные наводящие вопросы.
2	Не сдан	Не зачтено	
1	Не сдан	Не зачтено	

Дисциплина (модуль) «Введение в теорию чисел и криптографию» оценивается следующим образом:

Активность	Вес	Количество	Описание
Домашние задания	25%	10	Набор задач по темам недели
Аудиторная работа	15%	15	Активная работа студента на семинаре или лекции
Контрольная работа	35%	2	Письменная работа с набором задач, которые нужно решить за ограниченное время
Зачет с оценкой	25%	1	Коллоквиум - устные ответы на вопросы, список которых известен студенту заранее

Электронный документ

Формула расчёта итоговой оценки по дисциплине (модулю) «Введение в теорию чисел и криптографию»: «0,25 × среднее за домашние задания + 0,15 × среднее за аудиторную работу + 0,35 × контрольная работа + 0,25 × зачет с оценкой».

Текущий контроль успеваемости обучающихся по дисциплине (модуле)

Примерные домашние задания

1. Доказать, что из $a|bc$ и $\gcd(a,b)=1$ следует $a|c$. Оформить результат в виде короткого отчёта.
2. Реализовать функцию **is_divisible(a,b) → True/False** и протестировать её на 10 случайных парах целых чисел.
3. Написать собственную функцию **gcd(a,b)** по классическому алгоритму Евклида; сравнить её время работы с **math.gcd** на 1000 пар больших чисел (от 1012 до 1013).
4. Реализовать расширенный алгоритм Евклида, возвращающий кортеж (g,x,y) такой, что $g=x\cdot a+y\cdot b$. Использовать полученный x для вычисления обратного элемента по модулю m.
5. Составить таблицу простых чисел от 2 до 200, реализовать решето Эратосфена и продемонстрировать его работу.
6. Написать простой факторизатор (по пробным делителям) и применить его к 5 случайным 8-–10-значным числам; оценить среднее число делений.
7. Реализовать функцию, проверяющую малую теорему Ферма для всех простых $p<100$ перебором.
8. Написать функцию **mod_inverse(a,m)** с использованием расширенного алгоритма Евклида; проверить её на 20 случайных парах, где $\gcd(a,m)=1$.
9. Реализовать функцию **crt(remainders, moduli)**, решающую систему сравнения по КТЭ; продемонстрировать работу на системе

   $x\equiv 2 \pmod 3, x\equiv 3 \pmod 5, x\equiv 2 \pmod 7$.
10. Написать упрощённый тест Миллера-Рабина (3 раунда) и сравнить результаты с **sympy.isprime** на 100 случайных числах до 1012.
11. Шифровать слово «КРИПТОГРАФИЯ» аффинным шифром с параметрами $a=5, b=8$; затем расшифровать, найдя мультипликативный обратный.
12. Реализовать упрощённый протокол Диффи-Хеллмана: сгенерировать простое p (пример 1024 бит) и базу g; выполнить обмен ключами между двумя участниками и вывести общий секрет.
13. Сгенерировать два 512-битных простых числа, построить открытый/закрытый ключи RSA, зашифровать и расшифровать короткое сообщение; измерить время работы.
14. Вычислить SHA-256-хеш строки «OpenAI».
15. Симулировать простую цифровую подпись: взять SHA-256-хеш сообщения, зашифровать его закрытым RSA-ключом отправителя, затем проверить подпись, расшифровав её.

Примерные задания для контрольной работы

1. **Теоретический блок**

— Сформулировать и доказать расширенную формулу Евклида.

— Перечислить условия существования обратного элемента в Z_m.

2. **Алгоритмический блок**

— Записать псевдокод бинарного возведения в степень; оценить его временную сложность.

3. **Практический блок (Python)**

— Дана функция **solve_crt(rem, mod)**. Исправить ошибку, чтобы корректно решать систему из четырёх сравнениий.

Электронный документ

— Реализовать простой RSA-крипт (генерация ключей, шифрование, расшифрование) и продемонстрировать работу на числе 12345.

4. **Аналитический блок**

— Описать две основные атаки на протокол обмена ключами и указать, какие параметры (размер модуля, выбор генератора) позволяют их предотвратить.

Примерные задания для семинаров

1. Доказать теорему Ферма для произвольного простого p и любого $\gcd(a,p)=1$ (построить доказательство на доске).
2. На примере шифра Виженера показать, как метод Касиски восстанавливает ключ, используя известный открытый текст; продемонстрировать процесс в пару человек.
3. В парах разработать генератор параметров для обмена ключами: выбрать безопасное простое число, найти примитивный корень, измерить время работы; сравнить с готовой реализацией из библиотеки **cryptography**.
4. Обсудить недостатки использования хеш-функций без соли для хранения паролей; сформулировать рекомендации по применению PBKDF2, bcrypt и Argon2.

Примерные задания для коллоквиума

1. Что такое делимость? Привести определение и пример числа, делящегося на 9.
2. Выполнить вручную шаги расширенного алгоритма Евклида для $a=252, b=198$; указать полученный обратный элемент по модулю 198.
3. Почему проверка делимости только до n достаточна для определения простоты числа?
4. Найти все решения уравнения $7x \equiv 3 \pmod{20}$.
5. Дать формальное условие совместимости системы сравнения; привести пример несовместимой системы.
6. Сколько раундов Миллера-Рабина обычно требуется, чтобы вероятность ошибки была $<2^{-80}$ при проверке 64-битных чисел?
7. Почему шифр Цезаря легко ломается частотным анализом?
8. Чем режим ECB отличается от CBC в блочном шифре?
9. Как протокол обмена ключами обеспечивает условную секретность?
10. Почему открытый экспонент e в RSA выбирают взаимно простым с $\phi(n)$?

Задания для промежуточной аттестации по дисциплине (модулю)

№ п/п	Задание	Ответ	Компетенция
1	Найдите наибольший общий делитель чисел 462 и 1071 с помощью алгоритма Евклида.	33	УК-1
2	Вычислите обратный элемент к 17 по модулю 3120 (расширенный алгоритм Евклида).	2753	ПК-2
3	Быстрое возведение в степень: найдите $5117 \pmod{23}$ (бинарное возведение).	7	ПК-2
4	Выполните расширенный алгоритм Евклида для $a=1234, b=567$. Укажите (g,x,y) – $g=\gcd(a,b)=x\cdot a+y\cdot b$.	(1, -53, 115)	УК-1
5	Решите систему сравнений (Китайская теорема об остатках): $x \equiv 2 \pmod 3, x \equiv 3 \pmod 5, x \equiv 2 \pmod 7$.	23 (модуль 105)	ПК-2
6	Проведите 3-раундовый тест Миллера-Рабина для числа 561. Скажите, признано ли 561 простым.	Составное (делится 3×187)	УК-1
7	Сгенерируйте параметры RSA: $p=61, q=53, e=17$. Вычислите n, $\varphi(n)$ и закрытый экспонент d.	$n=3233, \varphi=3120, d=2753$	ПК-2

Электронный документ

8	Зашифруйте сообщение $m=42$ публичным ключом RSA из пункта 7 ($n=3233, e=17$).	2557	ПК-2
9	Дешифруйте полученный в пункте 8 шифротекст 2557 с помощью приватного ключа $d=2753$.	42	ПК-2
10	Вычислите SHA-256-хеш строки «Hello».	2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824	ОПК-4
11	Укажите главную уязвимость шифра Цезаря.	Частотный анализ	УК-1
12	Найдите порядок элемента 2 в мультипликативной группе $Z13*$.	12	УК-1
13	Сформулируйте и докажите малую теорему Ферма для $a=7, p=13$.	$7^{12} \equiv 1 \pmod{13}$ (доказательство по индукции/по теореме)	УК-1
14	Решите дискретный логарифм: найти x такой, что $3^x \equiv 2 \pmod{11}$.	$x=7$ (потому-что $3^7=2187 \equiv 2$)	ПК-2
15	Опишите, почему протокол Диффи-Хеллмана уязвим к атаке «человек-по-середине» (Man-in-the-Middle).	Отсутствие аутентификации сторон; злоумышленник может подменить публичные значения ga, gb	ОПК-4
16	Выполните обмен ключами Диффи-Хеллмана: $p=23, g=5, a=6, b=15$. Найдите общий секрет.	2 (т.к. $A=5^6 \equiv 8, B=5^{15} \equiv 19, K=196 \equiv 8^{15} \equiv 2 \pmod{23}$)	ПК-2
17	Определите, является ли число 104 729 простым, используя детерминированный набор оснований Миллера-Рабина для 32-битных чисел (2, 7, 61).	Простое (не найдено ни одного «witness»)	УК-1
18	Укажите асимптотическую сложность алгоритма Евклида (по числу бит входных чисел).	$O(\log\min(a,b))$	УК-1
19	Назовите криптографическую хеш-функцию, используемую в протоколе Bitcoin.	SHA-256 (в комбинации с RIPEMD-160)	ОПК-4
20	В двух-строковом ответе отличите симметричное от асимметричного шифрования.	Симметричное – один общий секретный ключ; асимметричное – пара открытого/закрытого ключей, шифрование/подпись используют разные ключи.	ОПК-4