

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное учреждение высшего
образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет Информатики и Информационных Технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Теоретико-числовые методы криптографии

Кафедра

Информационных Технологий и Безопасности Компьютерных Систем ФИиИТ

Образовательная программа бакалавриата

10.03.01 Информационная безопасность

Направленность (профиль) подготовки

Безопасность компьютерных систем

Форма обучения

Очная, очно-заочная

Статус дисциплины:

входит в часть ОПОП,

формируемую участниками образовательных отношений

Махачкала, 2022

Рабочая программа дисциплины «Теоретико-числовые методы криптографии» составлена в 2022 году в соответствии с требованиями ФГОС ВО -бакалавриат по направлению подготовки 10.03.01 Информационная безопасность от «17» ноября 2020г. № 1427.

Разработчик(и): Кафедра ИТиБКС ст.пр. Мургузалыева А.А.

Рабочая программа дисциплины одобрена:

на заседании кафедры ИТиБКС от «13»_04_2022 г., протокол № 9

зав. кафедрой  Ахмедова З.Х.
(подпись)

на заседании Методической комиссии факультета ИиИГ

от «15»_04_2022г., протокол № 9

председатель  Бакмаев А.Ш.
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением

«31»_03_2022г.

Начальник УМУ  Гасангаджиева А.Г.
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина "Теоретико-числовые методы криптографии" входит в формируемую участниками образовательных отношений часть образовательной программы по направлению 10.03.01 Информационная безопасность.

Дисциплина реализуется на факультете ИиИТ кафедрой ИТиБКС.

Содержание дисциплины охватывает круг вопросов, связанных с базовыми принципами построения и математического обоснования криптографических систем.

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных - ОПК-3, ОПК-9 профессиональных – ПК-7, ПК-8.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, практические занятия, самостоятельная работа.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме – контрольная работа, коллоквиум и пр. и промежуточный контроль в форме зачета.

Объем дисциплины- ___3___ зачетные единицы, В том числе в академических часах -108 по видам учебных занятий

Очная форма обучения

Семестр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен)
	в том числе							
	Все го	Контактная работа обучающихся с преподавателем					СРС, в том числе экзамен	
		Все го	из них					
	Лекции		Лабораторные занятия	Практические занятия	КСР	контроль		
2	108	74	30	44			34	зачет

1. Цели освоения дисциплины

Целями освоения дисциплины "Теоретико-числовые методы криптографии" является изложение базовых принципов построения и математического обоснования криптографических систем

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина "Теоретико-числовые методы в криптографии" входит в формируемую участниками образовательных отношений часть образовательной программы по направлению 10.03.01 Информационная безопасность.

Изучение её базируется на следующих дисциплинах: «Алгебра и геометрия», «Языки программирования», «Математическая логика и теория алгоритмов», «Теория информации», «Информатика», «Дискретная математика».

В результате изучения этих дисциплин студент должен знать:

- основные понятия математической логики и теории алгоритмов;
- основные понятия и методы дискретной математики, включая дискретные функции, конечные автоматы, комбинаторный анализ;
- основы теории групп и теории групп подстановок;
- основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки сложности;
- основы Интернет-технологий; уметь:
- формализовать поставленную задачу;
- осуществлять программную реализацию алгоритма;
- проводить оценку сложности алгоритмов.

Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее: «Криптографические методы защиты информации», «Криптографические протоколы», Учебная практика, Производственная практика и Преддипломная практика, а также ВКР.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения) .

Код и наименование компетенции из ОПОП	Код и наименование индикатора достижения компетенций (в соответствии с ОПОП)	Планируемые результаты обучения	Процедура освоения
ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности;	ИД1.ОПК-3.1.Знает математические алгоритмы функционирования, принципы построения, модели хранения и обработки данных распределенных информационных систем и систем поддержки принятия решений ИД2.ОПК-3.2.Имеет навыки применения математические модели процессов и объектов при решении задач анализа и синтеза распределенных информационных систем и систем поддержки принятия решений. ИД3.ОПК-3.3. Владеет навыками построения математических моделей для реализации успешного функционирования распределенных информационных систем и систем поддержки принятия решений	Знать: основы дискретной алгебры и теории чисел; о теоретико-числовых основах двухключевой криптографии; Уметь: формализовать поставленную задачу; использовать основные математические методы, применяемые в синтезе и анализе типовых криптографических алгоритмов. Владеть: навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.	Устный опрос, письменный опрос, реферат, практическая работа, лабораторная работа
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ИД 1 ОПК-9.1.Знает основные понятия и задачи криптографии, математические модели криптографических систем; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации ИД 2 ОПК-9.2. Умеет применять математические модели для оценки стойкости СКЗИ и использовать в автоматизированных системах; пользоваться нормативными документами в области технической защиты информации ИД 3 ОПК-9.3. Владеет методами и средствами криптографической и технической защиты информации	Знать: основные понятия алгебры, теории конечных групп, колец и полей, основными понятия элементарной теории чисел. Уметь: исследовать и решать системы сравнений по произвольному модулю; – представлять действительные числа цепными дробями; – строить большие простые числа, – применять алгоритмы проверки чисел на простоту; построения больших простых чисел; – применять алгоритмы разложения чисел и многочленов на множители, Владеть: навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.	Устный опрос, письменный опрос, реферат, практическая работа, лабораторная работа
ПК-7 Обеспечение функционирования средств связи сетей связи специального назначения	ПК-7.1 Знать: основы дискретной алгебры и теории чисел; о теоретико-числовых основах двухключевой криптографии; ПК-7.2 Уметь: формализовать поставленную задачу; использовать основные математические методы, применяемые в синтезе и анализе типовых криптографических алгоритмов. ПК-7.3 Владеть: навыками, необходимыми для разработки математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность ; навыками, необходимыми для обоснования и выбора рационального решения по уровню обеспечения защищенности компьютерной системы с учетом заданных требований	Знать: основы дискретной алгебры и теории чисел; о теоретико-числовых основах двухключевой криптографии; Уметь: формализовать поставленную задачу; использовать основные математические методы, применяемые в синтезе и анализе типовых криптографических алгоритмов. Владеть: навыками, необходимыми для разработки математических моделей защищаемых процессов и средств защиты информации и систем, обеспечивающих информационную безопасность ; навыками, необходимыми для обоснования и выбора рационального решения по уровню обеспечения защищенности компьютерной системы с учетом заданных требований	Устный опрос, письменный опрос, реферат, практическая работа, лабораторная работа
ПК-8 Администрирование средств защиты информации в компьютерных системах и сетях	ПК-8.1. Теоретико-числовые методы и алгоритмы, применяемые в средствах защиты информации ПК-8.2. Решать сравнений по простому и составному модулям ПК-8.3. методами решения задач разложения больших целых чисел на множители	Знать: теоретико-числовых основы двухключевой криптографии; алгоритмы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах. Уметь: выполнить постановку задач криптоанализа и указать подходы к их решению; Владеть: навыками применения алгоритмов, основанных на теоретико-числовых принципах, к вопросам построения криптосистем и их анализу;	Устный опрос, письменный опрос, реферат, практическая работа, лабораторная работа

4. Объем, структура и содержание дисциплины.

4.1. Объем дисциплины составляет 3 зачетных единиц, 108 академических часов.

4.2. Структура дисциплины.

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Самостоятельная работа	Формы текущего контроля успеваемости (по неделям семестра) Форма промежуточной аттестации (по семестрам)
				Лекции	Практические занятия	Лабораторные занятия	Контроль самост. раб.		
	Модуль 1. (название модуля)								
1	Введение в математические проблемы криптографии. Основы теории чисел.			4		4		4	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
2	Теория сравнений. Вычеты.			4		4		4	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
3	Сравнения первой степени. Системы сравнений первой степени			2		4		6	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	<i>Итого по модулю 1:</i>			10		12		14	
	Модуль 2								
4	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.			6		6		8	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа			4		6		6	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	<i>Итого по модулю 2:</i>			10		12		14	
	Модуль 3								
	Алгоритмы криптоанализа шифров с открытым ключом.			6		6		10	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	Конечные группы и поля многочленов.			4		4		6	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	<i>Итого по модулю 3:</i>			10		10		16	
	ИТОГО:			30		44		34	зачет

4.3. Содержание дисциплины, структурированное по темам (разделам).

4.3.1. Содержание лекционных занятий по дисциплине.

Модуль 1.

1. **Введение в математические проблемы криптографии. Основы теории чисел.** Делимость, простые числа, наибольший общий делитель. Алгоритм Евклида, расширенный алгоритм Евклида. Цепные дроби. Асимптотический закон распределения простых чисел. Мультипликативные функции. Функция Эйлера.

2. **Теория сравнений. Вычеты.** Полная система вычетов, приведенная система вычетов. Z_n , Z_p , Z^*_n , Z^*_p Обратный элемент в Z_n Алгебраические структуры на целых числах. Теорема Эйлера, теорема Ферма, тест Ферма на простоту. Криптосистема RSA. Понижение степени сравнения.

3. **Сравнения первой степени. Системы сравнений первой степени.** Сравнения первой степени и их решение. Системы сравнений первой степени и их решение. Китайская теорема об

остатках и ее применения в криптографии (схема разделения секрета на ее основе и ее применение в RSA).

Модуль 2.

Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.

Квадратичные сравнения. Символ Лежандра. Закон взаимности. Существование решений квадратичного сравнения по простому модулю. Решение квадратичных сравнений по простому модулю. Символ Якоби и его свойства. Тест Соловея-Штрассена на простоту. Существование и количество решений квадратичного сравнения по составному модулю. Решение квадратичных сравнений по составному модулю. Квадраты и псевдоквадраты. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор. Криптосистемы Блюма-Гольдвассер, Гольдвассер-Микали.

1.Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа. Циклическая группа Z^*_p (U_p). Порождающий элемент и дискретный логарифм. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамала. Теоремы Сэлфриджа и Поклингтона. $(p-1)$ – тесты на простоту. Доказуемо простые числа общего вида. Числа Ферма, теорема Пепина, тест Пепина. Числа Мерсенна и тест Лукаса- Лемера. Теорема Диемитко и процедура генерации простых чисел ГОСТ Р34.10-94.

2. Алгоритмы криптоанализа шифров с открытым ключом. Элементы теории сложности. Оценки сложности по времени, по объему требуемой памяти. Полиномиальная сложность, субэкспоненциальная сложность, экспоненциальная сложность алгоритмов. Сложность элементарных операций. Теоретико-числовые проблемы, лежащие в основе двухключевых криптосистем – факторизация, дискретное логарифмирование. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета, ро-метод Полларда, $p-1$ – метод Полларда, методы случайных квадратов. Примеры, оценки сложности указанных алгоритмов. Алгоритмы дискретного логарифмирования. Метод прямого поиска, ро-метод Полларда, метод исчисления индексов, «шаг младенца- шаг великана». Примеры, оценки сложности указанных алгоритмов.

3. Конечные группы и поля многочленов. Многочлены над Z_p , Z_n . Сложение, умножение, факторизация многочленов. Неприводимые многочлены. Поля Галуа.

4.3.2. Содержание лабораторно-практических занятий по дисциплине.

Темы лабораторных занятий:

Модуль 1.

Тема 1: Введение в математические проблемы криптографии. Основы теории чисел.

1. Операции над целыми числами. Нахождение наибольшего общего делителя при помощи алгоритма Евклида, наименьшего общего кратного. Построение таблицы первых простых чисел с помощью решета Эратосфена. Нахождение канонического разложения числа на простые сомножители.

Тема 2: Теория сравнений. Вычеты.

2. Разложение дробей в цепные дроби при помощи алгоритма Евклида. Асимптотический закон распределения простых чисел – вычисление примерного количества простых чисел на заданном интервале.

3. Вычисление функции Эйлера от числа. Теория сравнений. Построение приведенной системы вычетов от по заданному модулю. Проверка сравнений.

4. Вычисление обратного элемента в Z_n при помощи расширенного алгоритма Евклида. Тест Ферма на простоту. Понижение степени сравнения при помощи теоремы Эйлера. Криптосистема RSA.

Тема 3: Сравнения первой степени. Системы сравнений первой степени

5. Сравнения первой степени и их решение.

6. Системы сравнений первой степени и их решение по Китайской теореме об остатках.

7. Контрольная работа.

Модуль 2.

Тема 4: Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту

8. Символ Лежандра. Существование решений квадратичного сравнения по простому модулю. Решение квадратичных сравнений по простому модулю.

9. Символ Якоби. Существование и количество решений квадратичного сравнения по составному модулю. Решение квадратичных сравнений по составному модулю.

10. Квадраты и псевдоквадраты. Проблема различения квадратов и псевдоквадратов, ее связь с задачей факторизации. Числа Блюма. BBS-генератор. Криптосистемы Блюма- Гольдвассер, Гольдвассер-Микали. Циклическая группа Z^*_p (U_p). Отыскание порождающего элемента. Контрольная работа.

Тема 5: Порождающий элемент и дискретный логарифм. Криптосистемы на их основе.

Доказуемо простые числа

11. $(p-1)$ – тесты на простоту на основе теорем Сэлфриджа и Поклингтона.

12. Числа Ферма, тест Пепина. Числа Мерсенна и тест Лукаса-Лемера. Процедура генерации простых чисел ГОСТ Р34.10-94.

Тема 6: Алгоритмы криптоанализа шифров с открытым ключом.

13. Алгоритмы факторизации. Метод пробных делений, метод Ферма, метод квадратичного решета.

14. Ро-метод Полларда, $p-1$ – метод Полларда, методы случайных квадратов. Примеры, оценки сложности указанных алгоритмов.

15. Алгоритмы дискретного логарифмирования. Метод прямого поиска, «шаг младенца-шаг великана», ро-метод Полларда.

16. Метод исчисления индексов, метод Полига-Хэллмана. Примеры, оценки сложности указанных алгоритмов.

Тема 7: Конечные группы и поля многочленов.

17. Вычисления в конечных кольцах многочленов. Сумма, произведение многочленов, разложение многочлена на сомножители.

18. Неприводимые многочлены, проверка многочлена на простоту. Нахождение обратного.

5. Образовательные технологии

Лекционный курс. Лекция является основной формой обучения в высшем учебном заведении. В ходе лекционного курса проводится систематическое изложение современных научных материалов:

теоретико-числовые, алгебраические, аналитические и вероятностные подходы к построению и анализу криптосистем;

математические основы криптографии;

математические методы, используемые в криптоанализе

Рекомендуемые образовательные технологии: встречи с представителями ведущих отечественных фирм по производству криптографической продукции, выступления экспертов и специалистов перед студентами, ознакомительные беседы с представителями потенциальных работодателей.

6. Учебно-методическое обеспечение самостоятельной работы студентов.

Методические материалы для обеспечения СРС готовятся преподавателем и могут размещаться на персональном сайте преподавателя, либо на платформе электронного обучения. Кроме того, на основе рабочей программы дисциплины может составляться план-график, где преподаватель устанавливает рекомендуемые сроки предоставления на проверку результатов самостоятельной работы студента: контрольных работ, отчетов по лабораторным практикумам, индивидуальных домашних заданий, рефератов, курсовых работ и др., советует использование основных и дополнительных источников литературы.

<http://eor.dgu.ru/Default/NProfileUMK/?code=13.03.02&profileId=43>

№	Раздел дисциплины	Вид работы	Объем в часах Очная форма обучения	Объем в часах Очно-заочная форма обучения
1	Основы теории чисел.	проработка учебного материала подготовка к занятиям	2	
2	Теория сравнений. Вычеты	проработка учебного материала подготовка к занятиям	4	
3	Сравнения первой степени. Системы сравнений первой степени	проработка учебного материала подготовка к занятиям	4	
4	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту	проработка учебного материала подготовка к занятиям	6	
5	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа	проработка учебного материала подготовка к занятиям	6	
6	Алгоритмы криптоанализа шифров с открытым ключом	проработка учебного материала подготовка к занятиям	6	

7	Конечные группы и поля многочленов	проработка учебного материала подготовка к занятиям	6	
	Итого		34	

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

7.2. Типовые контрольные задания

Вопросы

1. Основные понятия теории чисел. Теорема делимости.
2. Наибольший общий делитель и алгоритм Евклида.
3. Цепные дроби и алгоритм Евклида.
4. Наименьшее общее кратное. Простые числа.
5. Теоремы Евклида о простых числах. Решето Эратосфена.
6. Основные свойства простых чисел. Теорема о единственности разложения на простые сомножители.
7. Теорема о делителях числа и ее следствия.
8. Асимптотический закон распределения простых чисел.
9. Функция Эйлера, ее свойства.
10. Сравнения. Свойства сравнений.
11. Полная система вычетов, приведенная система вычетов. Алгебраические свойства, обратный элемент.
12. Теорема Эйлера, теорема Ферма. Следствие.
13. Тест Ферма на простоту. Числа Кармайкла. Теорема Кармайкла.
14. Применение теоремы Ферма в криптосистеме RSA.
15. Сравнения с одним неизвестным 1-й степени.
16. Система сравнений 1-й степени. Китайская теорема об остатках.
17. Применение Китайской теоремы об остатках в RSA и схема разделения секрета на ее основе.
18. Квадратичные сравнения по простому модулю.
19. Символ Лежандра и его свойства.
20. Решение квадратичных сравнений по простому модулю.
21. Число решений квадратичного сравнения по составному модулю.
22. Символ Якоби, его свойства. Тест Соловея-Штрассена.
23. Квадратичные сравнения по модулю RSA. Связь задач извлечения корней и факторизации. Криптосистема Рабина. (только для КБ)
24. Квадраты и псевдоквадраты. Числа Блюма. (только для КБ)
25. VBS-генератор. Криптосистема Блюма-Гольдвассер, криптосистема Гольдвассер- Микали. (только для КБ)
26. Тест Миллера-Рабина.
27. Порядок группы. Порядок элемента в группе. Порождающий элемент.
28. Существование порождающего элемента в Z^*n
29. Критерий Люка.
30. Теорема Сэлфриджа и тест Миллера.
31. Теорема Поклингтона и тест на простоту на ее основе.
32. Числа Ферма, теорема Пепина, тест Пепина.
33. Числа Мерсена. Тест Лукаса-Лемера.
34. Теорема Диемитко. Процедура генерации простых чисел ГОСТ Р 34.10-94.
35. Дискретный логарифм. Проблема Диффи-Хелмана. Криптосистема ЭльГамала.
36. Кольца многочленов.
37. Поле многочленов $GF(p, \alpha)$.
38. Проблема факторизации. Метод проных делений.
39. Метод Ферма факторизации.
40. Метод квадратичного решета.
41. Ро-метод Полларда факторизации.
42. $p-1$ – метод факторизации.
43. Методы случайных квадратов.
44. Задача дискретного логарифмирования. Метод прямого поиска.
45. Ро-метод Полларда дискретного логарифмирования.

46. Алгоритм Полига-Хеллмана.

47. Метод «Шаг младенца-шаг великана».

48. Метод исчисления порядка.

Пример варианта домашней контрольной работы №1

1. Вычислить НОД(a,b) двумя способами: алгоритмом Евклида с делением с остатком и бинарным алгоритмом Евклида. Сравнить количество итераций для этих алгоритмов. а) a=18, b=35; б) a=329, b=826; в) a=26, b=738; г) a=288, b=15.

2. Определить, являются ли числа a, b, c взаимно простыми? Попарно простыми? а) a=13, b=17, c=15; б) a=105, b=91, c=26; в) a=22, b=121, c=209.

3. Вычислить функцию Эйлера от следующих чисел: а) 13; б) 17; в) 9; г) 16; д) 6; е) 24; ж) 227; з) 725; и) 94836.

4. Пользуясь асимптотическим законом распределения простых чисел, вычислить примерное количество простых чисел в промежутке от 2 000 до 10 000.

5. Сколько нечетных чисел размера 32 бита (старший бит =1) следует перебрать, чтобы среди них с вероятностью не менее 0,95 нашлось хотя бы одно простое?

6. Выписать абсолютно наименьший и наименьший неотрицательный вычеты числа a по модулю b (понижать степени, пользуясь теоремой Эйлера), где а) a=2, b=15; б) a=13, b=20; в) a=26, b=7; г) a= -10, b=5; д) a=1210, b=7; е) a=513, b=9; ж) a=144, b=12; з) a= (2)101, b=165.

7. Выписать полную и приведенную системы наименьших неотрицательных вычетов по следующим модулям: а) 7; б) 16; в) 17; г) 21; д) 20; е) 5.

8. Верны ли следующие сравнения? а) $16 \equiv 3 \pmod{13}$; б) $-1 \equiv 1 \pmod{5}$; в) $-3 \equiv 5 \pmod{8}$; г) $32 \equiv 0 \pmod{4}$.

9. Вычислить a -1 mod b, если таковой существует, где а) a=18, b=35; б) a=3, b=256; в) a=16, b=89; г) a=21, b=15.

10. Решить сравнения а) $7x \equiv 3 \pmod{13}$; б) $-15x \equiv 15 \pmod{35}$; в) $35x \equiv 5 \pmod{24}$; г) $18x \equiv 13 \pmod{81}$.

11. Решить системы сравнений а) $3x \equiv 1 \pmod{4}$ $2x \equiv 3 \pmod{5}$ б) $3x \equiv 5 \pmod{7}$ $2x \equiv 1 \pmod{3}$ в) $6x \equiv 7 \pmod{11}$ $3x \equiv 1 \pmod{5}$ г) $5x \equiv 3 \pmod{7}$ $7x \equiv 2 \pmod{9}$ д) $2x \equiv 4 \pmod{5}$ $3x \equiv 5 \pmod{7}$ $5x \equiv 3 \pmod{8}$ е) $x \equiv 2 \pmod{3}$ $6x \equiv 5 \pmod{11}$ $3x \equiv 2 \pmod{4}$ ж) $x \equiv (2-1) \pmod{7}$ $4x \equiv 11 \pmod{13}$ $16x \equiv 5 \pmod{19}$ з) $x \equiv 13 \pmod{17}$ $3x \equiv 8 \pmod{121}$ $3x \equiv 2 \pmod{4}$

Пример варианта домашней контрольной работы №2

1. Вычислить символ Якоби: а) $(61/103)$; б) $(73/109)$; в) $(123/9)$; г) $(201/49)$; е) $(241/148)$; ф) $(459/175)$.

2. Выяснить, сколько решений имеет сравнение, не решая его. а) $x^2 \equiv 20 \pmod{31}$; б) $x^2 \equiv 21 \pmod{49}$; в) $x^2 \equiv 2 \pmod{55}$; г) $x^2 \equiv 89 \pmod{160}$.

3. Решить квадратичные сравнения а) $x^2 \equiv 13 \pmod{23}$; б) $x^2 \equiv 24 \pmod{53}$; в) $x^2 \equiv 10 \pmod{41}$; г) $x^2 \equiv 71 \pmod{77}$; е) $x^2 \equiv 7 \pmod{9}$; ф) $x^2 \equiv 40 \pmod{81}$; г) $x^2 \equiv 100 \pmod{231}$; h) $x^2 \equiv 1 \pmod{110}$; и) $x^2 \equiv 81 \pmod{176}$; j) $x^2 \equiv 17 \pmod{57}$.

Пример варианта домашней контрольной работы №3.

1. Сколько порождающих элементов в Z^*_m ? Найти порождающий элемент, если они существуют. а) m=214; б) m=85; в) m=202; г) m=23; д) m=343.

2. Какие из чисел 2, 3, 4, m-2, m-3, m-4 являются порождающими элементами Z^*_m ? а) m=11; б) m=46; в) m=242; г) m=169; д) m=280.

3. Проверить на простоту число m=299 тестом Поклингтона. Число итераций = 3. Основания a выбирать произвольно.

4. Факторизовать m=209 методом Ферма.

5. Факторизовать m методом квадратичного решета с решетками по модулям 4, 5, 7. а) m=299; б) m=403.

6. Факторизовать 205 ро-методом.

7. Факторизовать 639 методом случайных квадратов с базой {2,3,5,7}.

8. Вычислить $\log_2 3 \pmod{101-1}$ методом «шаг младенца-шаг великана».

9. Вычислить $\log_6 5 \pmod{103-1}$ ро-методом.

10. Вычислить $\log_5 2 \pmod{97-1}$ методом Полига-Хэллмана.

11. Вычислить $\log_5 71 \pmod{73-1}$ методом исчисления порядка.

Пример варианта контрольной работы №1.

1. Сколько нечетных чисел размера 256 бит (старший бит =1) следует перебрать, чтобы среди них с вероятностью не менее 0,95 нашлось хотя бы одно простое?

2. Вычислить $\varphi(15125)$. 3. Решить систему $\begin{cases} x \equiv -3 \pmod{41} \\ 3x \equiv 8 \pmod{17} \\ 2x \equiv 5 \pmod{11} \end{cases}$

Пример варианта контрольной работы №2.

Найти все корни квадратного сравнения $x^2 \equiv 385 \pmod{752}$. Проверить, есть ли среди них квадраты, псевдоквадраты?

Пример варианта контрольной работы №3.

1. Разложить на 2 сомножителя методом квадратичного решета $n=1841$. Решёта по модулям 4, 5, 9. 2. Вычислить $\log_{350}(\text{mod } 137 - 1)$ методом «шаг младенца-шаг великана».

7.3. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Общий результат выводится как интегральная оценка, складывающаяся из текущего контроля - 50 % и промежуточного контроля - 50 %.

Текущий контроль по дисциплине включает:

- посещение занятий - 10 баллов,
- участие на практических занятиях - баллов,
- выполнение лабораторных заданий - 30 баллов,
- выполнение домашних (аудиторных) контрольных работ - 10 баллов.

Промежуточный контроль по дисциплине включает:

- устный опрос - 10 баллов,
- письменная контрольная работа - 30 баллов,
- тестирование - 10 баллов.

8. Учебно-методическое обеспечение дисциплины.

а) основная литература:

1. Теоретико-числовые методы в криптографии [Электронный ресурс] : учебное пособие / . — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 107 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/75601.html>
2. Гультяева Т.А. Основы теории информации и криптографии [Электронный ресурс] : конспект лекций / Т.А. Гультяева. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2010. — 88 с. — 978-5-7782-1425-5. — Режим доступа: <http://www.iprbookshop.ru/44987.html>
3. Земор Ж. Курс криптографии [Электронный ресурс] / Ж. Земор. — Электрон. текстовые данные. — Москва, Ижевск: Регулярная и хаотическая динамика, Ижевский институт компьютерных исследований, 2006. — 256 с. — 5-93972-510-4. — Режим доступа: <http://www.iprbookshop.ru/16547.html>
4. Кнауб, Л.В. Теоретико-численные методы в криптографии [Электронный ресурс]: учебное пособие/ Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов – Красноярск: СибФУ, 2011. - 160 с. Режим доступа: <http://biblioclub.ru/index.php?page=book&id=229582> (дата обращения: 25.03.2015)
5. Ниссенбаум О.В. Теоретико-числовые методы в криптографии: сб. заданий: учеб.- метод. пособие, Ч.2. - Тюмень: Изд-во ТюмГУ. - 2012. - 40 с.
6. Ниссенбаум О.В. Теоретико-числовые методы в криптографии: сб. заданий: учеб.- метод. пособие, Ч.3. - Тюмень: Изд-во ТюмГУ. - 2014. - 40 с.

б) дополнительная литература:

1. Фирдман, И.А. Теоретико-числовые алгоритмы и их применение в криптографии [Электронный ресурс]: сборник задач/ И.А. Фирдман. - Омск: Омский государственный университет, 2011. - 19 с. Режим доступа: <http://biblioclub.ru/index.php?page=book&id=238201> (дата обращения: 25.03.2015).
2. Петров А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 446 с. — 978-5-4488-0091-7. — Режим доступа: <http://www.iprbookshop.ru/63800.html>
3. Кирпичников А.П. Криптографические методы защиты компьютерной информации [Электронный ресурс] : учебное пособие / А.П. Кирпичников, З.М. Хайбуллина. — Электрон. текстовые данные. — Казань: Казанский национальный исследовательский технологический университет, 2016. — 100 с. — 978-5-7882-2052-9. — Режим доступа: <http://www.iprbookshop.ru/79313.html>

4. Пашинцев В.П. Нестандартные методы защиты информации [Электронный ресурс] : лабораторный практикум / В.П. Пашинцев, А.В. Ляхов. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2016. — 196 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/63217.html>
5. Басалова Г.В. Основы криптографии [Электронный ресурс] / Г.В. Басалова. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 282 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/52158.html>
6. Учебно-методическое пособие по выполнению лабораторных работ по дисциплине Методы и средства защиты компьютерной информации [Электронный ресурс] / . — Электрон. текстовые данные. — М. : Московский технический университет связи и информатики, 2016. — 55 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/61497.html>
7. Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс] : лабораторный практикум / И.А. Калмыков, Д.О. Науменко, Т.А. Гиш. — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 109 с. — 2227-8397. — Режим доступа: <http://www.iprbookshop.ru/63099.htm>

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины.

1. Электронно-библиотечной системе IPRbooks . Режим доступа: www.iprbookshop.ru
2. eLIBRARY.RU[Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – . Режим доступа: <http://elibrary.ru/defaultx.asp> (дата обращения: 01.09.2022). – Яз. рус., англ.
3. Moodle[Электронный ресурс]: система виртуального обучением: [база данных] / Даг. гос. ун-т. – Махачкала, г. – Доступ из сети ДГУ или, после регистрации из сети ун-та, из любой точки, имеющей доступ в интернет. – URL: <http://moodle.dgu.ru/>(дата обращения: 22.08.2022).
4. Электронный каталог НБ ДГУ[Электронный ресурс]: база данных содержит сведения о всех видах литературы, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2010 – Режим доступа: <http://elib.dgu.ru>, свободный (дата обращения: 21.09.2022).
5. Сайт кафедры <http://iit.dgu.ru/> (дата обращения 15.09.2022)
6. <http://www.chaynikam.info> Компьютер для «чайников» (дата обращения 15.09.2022)
7. Национальный Открытый Университет «ИНТУИТ» – <http://www.intuit.ru/>(дата обращения 15.09.2022)
8. Интернет-энциклопедия «Википедия». – <https://ru.wikipedia.org/>(дата обращения 15.09.2018)

10. Методические указания для обучающихся по освоению дисциплины.

Для подготовки к коллоквиумам необходимо пользоваться конспектом лекций и [1] из списка основной литературы. Для выполнения домашних контрольных работ следует использовать [2,3] из основной литературы. Дополнительная литература в случае необходимости используется как справочная. Для получения расширенных и углубленных знаний по тематике рекомендуется пользоваться ссылками из списка интернет-ресурсов, приведенных в данном УМК, а также электронными и бумажными номерами научных журналов, имеющихся в научной библиотеке и сети интернет. Особенное внимание рекомендуется обратить на издания «Математические вопросы криптографии», «Прикладная дискретная математика», материалами конференций RealWorldCrypto, Crypto, Eurocrypt, Ruscrypt, Sibecrypt, Asiacypt.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем.

Предусмотрено использование электронной почты для связи студентов с преподавателями.

Программное обеспечение для лекций: MS PowerPoint (MS PowerPoint Viewer), Adobe Acrobat Reader, средство просмотра изображений, табличный процессор.

Программное обеспечение практической работы компьютерном классе: Linux, MS PowerPoint (MS PowerPoint Viewer), Adobe Acrobat Reader, средство просмотра изображений, Интернет, E-mail.

Программные продукты

- Операционная система: Windows XP

- Microsoft office.
- Программные средства сжатия данных. . WinRAR. WinArj. WinZip.

ДГУ

1. <http://www.edu.dgu.ru> электронные образовательные ресурсы образовательного сервера
2. <http://www.oglibrary.ru/data/demo/3400/34000003.ru> (Электронная библиотека «Нефть и газ», ресурс – И.В. Кузьмин Основы теории информации и кодирования).
3. Интернет Университет Информационных Технологий – <http://www.intuit.ru/>
4. Книги по информационным технологиям – <http://www.books.everonit.ru/>
5. Федеральный портал «Российское образование» - <http://www.edu.ru/>
6. Интегральный каталог ресурсов Федерального портала «Российское образование» - <http://soip-catalog.informika.ru/>
7. Федеральный фонд учебных курсов - <http://www.ido.edu.ru/ffec/econ-index.html>
8. Интернет-энциклопедия «Википедия». – <http://ru.wikipedia.com/>

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине.

Реализация учебной дисциплины требует наличия типовой учебной аудитории с возможностью подключения технических средств. Учебная аудитория должна иметь следующее оборудование:

- Компьютер, медиа-проектор, экран.
- Программное обеспечение для демонстрации слайд-презентаций.

Лабораторные занятия по дисциплине проводятся в специально оборудованном информационном классе факультета.

К каждой лабораторной работе имеются методические указания и рекомендации. Студенту дается задание, о выполнении которого он должен отчитаться перед преподавателем в конце занятия