МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет Информатики и Информационных Технологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Теоретико-числовые методы криптографии

Кафедра Информатики и Информационных Технологий

Образовательная программа

10.03.01 Информационная безопасность

Профиль подготовки

Безопасность компьютерных систем

Уровень высшего образования

Бакалавриат

Форма обучения

Очная, очно-заоная

Статус дисциплины: вариативная

Махачкала, 2020

Рабочая программа дисциплины "Теоретико-числовые методы криптографии" составлена в 2020 году в соответствии с требованиями ФГОС ВО по направлению 10.03.01 -Информационная безопасность (уровень бакалавриата) от 1 декабря 2016 г. №1515

Разработчик(и): ИиИТ Муртузалиева А.А.

Рабочая программа дисциплины одобрена:
на заседании кафедры ИиИТ от «13» _03_2020г., протокол № 8

Зав. кафедрой _____ Ахмедов С.А.
(подпись)

на заседании Методической комиссии факультета ИиИТ

от от «_12_» _03_2020__г., протокол №_8_.

председатель _____ Ахмедова З.Х.

Рабочая программа дисциплины согласована с учебно-методическим управлением «26» 03 2020г. _____
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина "Теоретико-числовые методы криптографии" входит в вариативную часть образовательной программы направлению 10.03.01 Информационная безопасность.

Дисциплина реализуется на факультете ИиИТ кафедрой ИиИТ.

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

Дисциплина нацелена на формирование следующих компетенций выпускника: общепрофессиональных - ОПК-2, ОПК-7 профессиональных – ПК-1, ПК-2., профессионально-специализированные - ПСК-1.2, ПСК1.3

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							
	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
	Всего	из них						
		Лекции	Лабораторные занятия	Практические занятия	КСР	контроль		
6	108	34	16				58	зачет

Оно-заочная форма обучения

Семестр	Учебные занятия							Форма промежуточной аттестации (зачет, дифференцированный зачет, экзамен
	в том числе							
	Контактная работа обучающихся с преподавателем						СРС, в том числе экзамен	
	Всего	из них						
		Лекции	Лабораторные занятия	Практические занятия	КСР	контроль		
7	108	26	14				68	зачет

1. Цели освоения дисциплины

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

2.Место дисциплины в структуре ООП бакалавриата

Дисциплина "Теоретико-числовые методы в криптографии" входит в вариативную часть образовательной программы *бакалавриата* 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 компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)
ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач	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.
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и	Знать: возможности сети Интернет для поиска и обработки данных и организации информационного обмена; Уметь: эффективно использовать

	особенностей функционирования объекта защиты	возможности современных ПЭВМ, компьютерных сетей и программных средств для решения прикладных задач, возникающих в процессе обучения в вузе и в ходе будущей профессиональной деятельности Владеть: навыками работы со справочно-поисковыми системами в глобальной сети Интернет
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	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.
ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знать: 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;
ПСК-1.2	способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	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.
ПСК-1.3	способность выполнять работу по самостоятельному построению алгоритмов, проведению их анализа и реализации в современных программных комплексах	Знать: 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;

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		2		6	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
2	Теория сравнений. Вычеты.			4		2		6	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
3	Сравнения первой степени. Системы сравнений первой степени			4		2		6	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	Итого по модулю 1:			12		6		18	
	Модуль 2. ***(название модуля)***								
1	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.			10		4		22	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	Итого по модулю 2:			10		4		22	
	Модуль 3								
	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа			4		2		6	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	Алгоритмы криптоанализа шифров с открытым ключом.			4		2		6	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	Конечные группы и поля многочленов.			4		2		6	Устный опрос, лабораторные задания, письменный опрос, коллоквиум

	Итого по модулю 3:			12		6		18	
	ИТОГО:			34		16		58	зачет

Очно-заочная форма обучения

№ 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.			2		2		6	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
2	Теория сравнений. Вычеты.			4		2		6	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
3	Сравнения первой степени. Системы сравнений первой степени			4		2		8	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	Итого по модулю 1:			10		6		20	
	Модуль 2. ***(название модуля)***								
	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту.			10		4		24	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	Итого по модулю 2:			8		4		24	
	Модуль 3								
	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа			4		2		8	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	Алгоритмы криптоанализа шифров с открытым ключом.			4		2		8	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	Конечные группы и поля многочленов.			4		2		8	Устный опрос, лабораторные задания, письменный опрос, коллоквиум
	Итого по модулю 3:			8		4		24	
	ИТОГО:			26		14		68	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. Zn, Zp, Z*n, Z* p Обратный элемент в Zn 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.

Модуль 3.

1.Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числа. Циклическая группа Z* p (Up). Порождающий элемент и дискретный логарифм. Задача дискретного логарифмирования. Криптосистемы Диффи-Хэллмана и Эль-Гамаля. Теоремы Сэлфриджа и Поклингтона. (n-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 Zp, Zn. 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 Zn 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 (Up). Отыскание порождающего элемента. Контрольная работа.
Модуль 3.
Тема 5: Порождающий элемент и дискретный логарифм. Криптосистемы на их основе.
Доказуемо простые числа
11. (n-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, р—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
1	Основы теории чисел.	проработка учебного материала подготовка к занятиям	8
2	Теория сравнений. Вычеты	проработка учебного материала подготовка к занятиям	8
3	Сравнения первой степени. Системы сравнений первой степени	проработка учебного материала подготовка к занятиям	8
4	Квадратичные сравнения и криптосистемы на их основе. Вероятностные тесты на простоту	проработка учебного материала подготовка к занятиям	8
5	Порождающий элемент и дискретный логарифм. Криптосистемы на их основе. Доказуемо простые числ	проработка учебного материала подготовка к занятиям	8
6	Алгоритмы криптоанализа шифров с открытым ключом	проработка учебного материала подготовка к занятиям	10
7	Конечные группы и поля многочленов	проработка учебного материала подготовка к занятиям	8
	Итого		58

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

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Перечень компетенций с указанием этапов их формирования приведен в описании образовательной программы.

Код компетенции из ФГОС ВО	Наименование компетенции из ФГОС ВО	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Процедура освоения
ОПК-2	способность применять соответствующий математический аппарат для решения профессиональных задач	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, лабораторные задания
ОПК-7	способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и	Знать: возможности сети Интернет для поиска и обработки данных и организации информационного обмена; Уметь: эффективно использовать возможности современных ПЭВМ, компьютерных сетей и программных средств для решения прикладных задач, возникающих в процессе	Устный опрос, письменный опрос, лабораторные задания

	содержания информационных процессов и особенностей функционирования объекта защиты	обучения в вузе и в ходе будущей профессиональной деятельности Владеть: навыками работы со справочно-поисковыми системами в глобальной сети Интернет	
ПК-1	способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	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, лабораторные задания
ПК-2	способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	Знать: 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, лабораторные задания
ПСК-1.2	способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований	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, лабораторные задания
ПСК-1.3	способность выполнять работу по самостоятельному построению алгоритмов, проведению их анализа и реализации в современных программных комплексах	Знать: 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, лабораторные задания

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. Наименьше 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. BBS-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 Поклнгтона 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 ЭльГамаля.
36. Кольца многочленов.
37. Поле многочленов GF(p α).
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 неотрица-тельных вычетов по следующим модулям: а) 7; б) 16; в) 17; г) 21; д) 20; е) 5.
8. Верны ли следующие сравнения? а) 16≡3(mod 13); б) -1≡1(mod 5); в) -3≡5(mod 8); г) 32≡0(mod 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≡3(mod 13); б)-15x≡15(mod 35); в)35x≡5(mod 24); г)18x≡13(mod 81).
11. Решить системы сравнений а) 3x≡1(mod 4) 2x≡3(mod 5) б) 3x≡5(mod 7) 2x≡1(mod 3) в) 6x≡7(mod 11) 3x≡1(mod 5) г) 5x≡3(mod 7) 7x≡2(mod 9) д) 2x≡4(mod 5) 3x≡5(mod 7) 5x≡3(mod 8) е) x≡2(mod 3) 6x≡5(mod 11) 3x≡2(mod 4) ж) x≡(2-1)(mod 7) 4x≡11(mod 13) 16x≡5(mod 19) з) x≡13(mod 17) 3x≡8(mod 121) 3x≡2(mod 4)

Пример варианта домашней контрольной работы №2

1. Вычислить символ Якоби: a) (61/ 103) ; b) (73/109) ; c) (123/ 9 ; d) (201 /49) ; e) (241 /148) ; f) (459 /175) .
2. Выяснить, сколько решений имеет сравнение, не решая его. a) x2≡20 (mod 31); b) x2≡21 (mod 49); c) x2≡2 (mod 55); d) x2≡89(mod 160).
3. Решить квадратичные сравнения a) x 2≡13 (mod 23); b) x 2≡24 (mod 53); c) x 2≡10 (mod 41); d) x2≡71 (mod 77); e) x2≡7 (mod 9); f) x2≡40 (mod 81); g) x2≡100 (mod 231); h) x2≡1 (mod 110); i) x 2≡81 (mod 176); j) x 2≡17 (mod 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 решетами 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 log23(mod 101–1) методом «шаг младенца–шаг великана».
9. Вычислить log 6 5 (mod 103–1) ро-методом.
10. Вычислить log 5 2 (mod 97–1) методом Полига-Хэллмана.
11. Вычислить log 5 71 (mod 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 φ(15125). 3. Решить систему ⎪ ⎩ ⎪ ⎨ ⎧ ≡ ≡ ≡ – x 3 (mod 41) 3x 8(mod 17) 2x 5(mod 11) 1

Пример варианта контрольной работы №2.

Найти все корни квадратичного сравнения x 2≡ 385 (mod 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 log350 (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, складывающая 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. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

а) основная литература:

1. Теоретико-числовые методы в криптографии [Электронный ресурс] : учебное пособие / . — Электрон. текстовые данные. — Ставрополь: Северо-Кавказский федеральный университет, 2017. — 107 c. — 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 c. — 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 c. — 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 c. — 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 c. — 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 c. — 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 c. — 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 c. — 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 c. — 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: 01.09.2018). – 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/(датаобращения: 22.08.2018).
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: 21.09.2018).
5. Сайт кафедры http://iit.dgu.ru/ (дата обращения 15.09.2018)
6. http://www.chaynikam.info Компьютер для «чайников» (дата обращения 15.09.2018)
7. Национальный Открытый Университет «ИНТУИТ» – http://www.intuit.ru/(дата обращения 15.09.2018)
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, Asiacrypt.

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.

1. http://www.edu.dgu.ru электронные образовательные ресурсы образовательного сервера ДГУ
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