МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Математические основы защиты информации и информационной безопасности

Кафедра дискретной математики и информатики
факультета математики и компьютерных наук

Образовательная программа магистратуры
02.04.02 Фундаментальная информатика и информационные технологии

Направленность (профиль) программы:
Информационные технологии

Форма обучения:
очная

Статус дисциплины: входит в обязательную часть ОПОП

Махачкала, 2022

2

Рабочая программа дисциплины «Математические основы защиты информации и информационной безопасности» составлена в 2022 году в соответствии с требованиями ФГОС ВО - магистратура по направлению подготовки 02.04.02 Фундаментальная информатика и информационные технологии от «23» августа 2017 г. № 811.

Разработчик: проф. по специальности 01.01.09 - «Дискретная математика и математическая кибернетика», докт. физ.-мат. наук, Магомедов А.М.

Рабочая программа дисциплины одобрена:

на заседании кафедры дискретной математики и информатики от «28» февраля 2022 г., протокол № 6;

зав. кафедрой _____ Магомедов А. М.
(подпись)

и

на заседании Методической комиссии факультета математики и компьютерных наук от «24» марта 2022 г., протокол № 4;

председатель _____ Ризаев М. К
(подпись)

Рабочая программа дисциплины согласована с учебно-методическим управлением

«31» марта 2022 г.

Начальник УМУ _____ Гасангаджиева А. Г.
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «Математические основы защиты информации и информационной безопасности» входит в обязательную часть образовательной программы магистратуры по направлению 02.04.02 - Фундаментальная информатика и информационные технологии.

Дисциплина реализуется на факультете математики и компьютерных наук кафедрой дискретной математики и информатики.

Содержание дисциплины охватывает круг вопросов, относящихся к математическим основам представления и защиты информации, роли NP-полных задач в повышении криптостойкости алгоритмов кодирования, электронной подписи.

Дисциплина способствует формированию следующих компетенций выпускника:

общепрофессиональных - ОПК-4, профессиональных - ПК-1, ПК 4.

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: лекции, лабораторные занятия.

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости: в форме разработки 4 комп. программ с защитой (+ экзамен).

Объем дисциплины – 5 зачетных единиц, в том числе в академических часах по видам учебных занятий:

Семестр	Учебные занятия								Форма промежуточной аттестации (зачет, дифференцированный зачет), экзамен
	в том числе								
	всего	Контактная работа обучающихся с преподавателем					КСР	СРС	
		Всего	из них						
			Лекции	Лабораторные занятия	Прак. занятия				
1	180	44	16	28	0		36	100	экзамен

1. Цели изучения дисциплины

Цели изучения дисциплины:

- освоение базовых методов защиты информации,
- изучение алгоритмов кодирования,
- повышение криптостойкости,
- изучение математических принципов, лежащих в основе создания электронной подписи,
- усвоение роли NP-полных задач в вопросах защиты информации.

Целями изучения дисциплины являются также:

- практическое создание алгоритмов кодирования с воплощением в компьютерные программы на языке высокого уровня;

- ознакомление с шифрованием открытым ключом, составление и отладка программы с созданием закрытой и открытой части ключа, шифрованием и дешифрованием данным методом;

- практическое освоение вопросов генерации секретного ключа на основе дискретного логарифмирования, представление о современном состоянии проблемы (наличие «теоретически» полиномиального алгоритма решения задачи).

2. Место дисциплины в структуре ОПОП магистратуры

Дисциплина входит в обязательную часть образовательной программы магистратуры по направлению 02.04.02 и изучается в соответствии с графиком учебного процесса в 1 год обучения магистратуры.

Успешному изучению дисциплины способствуют знания, полученные по дисциплине «Языки программирования» и «Дискретная математика», а также при изучении фундаментальных и общематематических дисциплин.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению подготовки.

Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности
(ОПК-4);

Способность понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания, современные языки программирования и программное обеспечение; операционные системы и сетевые технологии (ПК-1);

Способность применять в профессиональной деятельности современные языки программирования и методы параллельной обработки данных, операционные системы, электронные библиотеки и пакеты программ, сетевые технологии (ПК-4);

Код и наименование компетенции из ФГОС ВО	Код и наименование индикатора достижения компетенций	Планируемые результаты обучения (показатели достижения	Процедура освоения

		заданного уровня освоения компетенций)	
ОПК-4. Способен оптимальным образом комбинировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	***ОПК-4.1.*** *Знает принципы сбора и анализа информации, создания информационных систем на стадиях жизненного цикла.* ***ОПК-4.2.*** *Умеет осуществлять управление проектами информационных систем.* ***ОПК-4.3.*** *Имеет практический опыт анализа и интерпретации информационных систем.*	Знать: связи с темами дисциплины «Основы программирования» и средства современных языков программирования для выполнения по надежной защите информации Уметь: применять самостоятельно современные языки программирования для воплощения алгоритмов теории кодирования Владеть: основами разработки программ на языке C# для целей повышения компьютерной безопасности	Изучение класса BigInteger языка C#, освоение операций над объектами данного класса, необходимыми для выполнения упражнений по дисциплине защиты информации Реализация основных алгоритмов шифрования средствами языков высокого уровня Разработки, отладка и тестирование программ для алгоритмов шифрования
ПК-1. Способность понимать и применять в научно-исследовательской и прикладной деятельности современный математический аппарат, основные законы естествознания, современные языки программирования и программное обеспечение; операционные системы и сетевые технологии.	***ПК-1.1.*** *Знает основы ведения научной дискуссии и формы устного научного высказывания.* ***ПК-1.2.*** *Умеет вести корректную дискуссию в области информационных технологий, задавать вопросы и отвечать на поставленные вопросы по теме научной работы.* ***ПК-1.3.*** *Имеет практический опыт владения существующими методами и алгоритмами решения задач цифровой обработки сигналов, использования сети Интернет, аннотирования, реферирования, библиографического разыскания и описания, опыт работы с научными источниками.*	Знать: приемы усиления криптостойкости алгоритмов Уметь: реализовать алгоритмы с эшелонированными средствами защиты Владеть: навыками составления соответствующих программ	Изучение методов симметричного шифрования Освоение конвейерной модели защиты Лабораторные занятия по комплексному применению алгоритмов защиты
ПК-4. Способность применять в профессиональной деятельности современные	***ПК-4.1.*** *Знает современные языки программирования и методы параллельной обработки данных.*	Знать: основные признанные специалистами разных стран средства повышения	Изучение алгоритмов шифрования открытым ключом и на осно-

языки программирования и методы параллельной обработки данных, операционные системы, электронные библиотеки и пакеты программ, сетевые технологии	***ПК-4.2.*** *Умеет реализовывать численные методы решения прикладных задач в профессиональной сфере деятельности, пакеты программного обеспечения, операционные системы, электронные библиотеки, сетевые технологии.* ***ПК-4.3.*** *Имеет практический опыт разработки интеграции информационных систем.*	криптостойкости Уметь: использовать средства повышения криптостойкости Владеть: навыками реализации средств повышения качества алгоритмов криптографии	ве дискретного логарифмирования Составление программ для метода шифрования открытым ключом и методом Диффи-Хеллмана Отладка и тестирование программ

4. Объем, структура и содержание дисциплины

4.1. Объем дисциплины составляет 5 зачетных единиц, 180 аудиторных часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы контроля успеваемости
				Всего	Лек	Лаб.	Сам.	
Модуль 1. Введение в теорию информационной безопасности								
1	Основные понятия информационной безопасности	1	1	20	2	4	14	
2	Связь вопросов безопасности и сжатия информации	1	2	16	2	4	10	сост/защ.пр.
	Итого по модулю 1			36	4	8	24	
Модуль 2. Шифрование открытым ключом								
3	Шифрование с помощью случайных чисел	1	3	20	2	4	14	
4	Системы шифрования с открытым ключом	1	4	16	2	4	10	сост/защ.пр.
	Итого по модулю 2			36	4	8	24	
Модуль 3. Электронная цифровая подпись								
5	Криптографические методы, основанные на задаче дискретного логарифмирования		5	20	2	4	14	

6	Электронная цифровая подпись		6	16	2	4	10	сост/защ.пр.
	Итого по модулю 3			36	4	8	24	
Модуль 4. Перспективы и проблемы математических средств защиты информации								
7	Открытые задачи		7	18	2	2	14	
8	Перспективы квантовых процессоров		8	18	2	2	14	сост/защ.пр.
	Итого по модулю 4			36	4	4	28	
	Модуль 5. Подготовка к экзамену			36			36	экз.
	ИТОГО			180	16	28	136	

Очно-заочной и заочной форм обучения в магистратуре по направлению ФИИТ нет.

4.2. Содержание дисциплины, структурированное по разделам и темам

4.2.1. Содержание лекционных занятий по дисциплине

Модуль 1. Введение в теорию информационной безопасности

Тема 1. Основные понятия информационной безопасности. Методы информационной безопасности. Сервисы информационной безопасности. Угрозы информационной безопасности. Классификация криптографических методов защиты информации.

Тема 2. Связь вопросов безопасности и сжатия информации. ASCII и RLE – кодирование (run-length encoding). Две особенности кода Хаффмана. Таблица кодов. Алгоритм построения двоичного дерева. Программные средства визуализации дерева. Декодирование. Оптимальность кода Хаффмана. Недостатки кода Хаффмана.

Модуль 2. Шифрование открытым ключом

Тема 1. Шифрование с помощью случайных чисел. Ключ шифра. Симметричные методы. Методы повышения криптостойкости симметричных шифров: 1. Вычисление гаммы шифра по ключу более сложным способом. 2. Применение вместо xor более сложной (но обратимой) операции. 3. Предварительное перемешивание битов исходного сообщения по фиксированному алгоритму. Симметричный шифр Data Encryption Standard.

Тема 2. Системы шифрования с открытым ключом. Особенности систем с открытым ключом. Модулярная арифметика. Функция Эйлера. Алгоритм RSA. Генерация простых чисел. Криптостойкость RSA.

Модуль 3. Электронная цифровая подпись

Тема 1. Криптографические методы, основанные на задаче дискретного логарифмирования. Публичное вычисление секретного ключа. Два препятствия для его раскрытия. Протокол Диффи-Хеллмана. Использование средств языков программирования (BigInteger языка C#). Применение систем компьютерной математики. Новые сведения о сложности задачи дискретного логарифмирования.

Тема 2. Электронная цифровая подпись и ее свойства. Алгоритм создания электронной цифровой подписи. Алгоритм построения ЭЦП Эль-Гамаля.

Модуль 4. Перспективы и проблемы математических средств защиты информации

Тема 1. NP-полные задачи, лежащие в основе доверия к криптостойкости шифров. Задачи, для которых не выяснена принадлежность классу NP-полных задач.

Тема 2. Перспективы квантовых процессоров.

4.2.2. Содержание лабораторных занятий по дисциплине
Примечание. Указаны темы проектов, обязательных для выполнения на лабораторных занятиях.

Модуль 1. Введение в теорию информационной безопасности

Тема 1. Основные понятия информационной безопасности. Угрозы информационной безопасности. Классификация криптографических методов защиты информации.

Тема 2. Связь вопросов безопасности и сжатия информации. ASCII и RLE – кодирование (run-length encoding). Сравнительный анализ сжатия информации при кодировании методами ASCII и RLE. Построение и визуализация двоичного дерева (в алгоритме Хаффмана). Создание программы на языке C# для кодирования и декодирования методом Хаффмана.

Модуль 2. Шифрование открытым ключом

Тема 1. Шифрование с помощью случайных чисел. Ключ шифра. Симметричные методы. Методы повышения криптостойкости симметричных шифров: 1. Вычисление гаммы шифра по ключу более сложным способом. Применение xor. Симметричный шифр Data Encryption Standard.
Тема 2. Системы шифрования с открытым ключом. Особенности систем с открытым ключом. Модулярная арифметика. Функция Эйлера. Алгоритм RSA. Генерация простых чисел. Криптостойкость RSA.

Модуль 3. Электронная цифровая подпись

Тема 1. Криптографические методы, основанные на задаче дискретного логарифмирования. Публичное вычисление секретного ключа. Два препятствия для его раскрытия. Протокол Диффи-Хеллмана. Использование средств языков программирования (BigInteger языка C#).

Тема 2. Электронная цифровая подпись и ее свойства. Алгоритм создания электронной цифровой подписи. Алгоритм построения ЭЦП Эль-Гамаля.

Модуль 4. Перспективы и проблемы математических средств защиты информации

Тема 1. Задачи класса NP, лежащие в основе доверия к криптостойкости шифров. Открытые задачи.

Тема 2. Перспективы квантовых процессоров.

5. **Образовательные технологии**

Материал каждой лекции сопровождается компьютерной презентацией и демонстрацией решения задач в интерактивном режиме с использованием мультимедийного оборудования.

Предусмотрено регулярное общение студентов с лектором, лектора – с представителями российских и зарубежных компаний по электронной почте и по скайпу.

Предусмотрено изучение и использование функций систем компьютерной математики, которые прямо относятся к разделам теории чисел, связанным с защитой информации.

Несколько видеороликов из интернета отобраны в качестве особо востребованных на лекциях по мат. основам защиты информации и информационной безопасности (например, задача о выработке секретного ключа с использованием дискретного логарифмирования и др.)

6. Учебно-методическое обеспечение самостоятельной работы студентов

6.1. Виды и порядок выполнения самостоятельной работы
1. Изучение конспектов лекций и презентационных материалов (предоставляются электронные материалы).
2. Выполнение на языке C# (варианты: Delphi, Java) проектов, запланированных для лабораторных занятий
4. Подготовка к текущему и промежуточному контролю
5. Поиск материала на интернет-форумах
6. Подготовка к экзамену

Вид самостоятельной работы	Примерная трудоёмкость, а.ч.
Текущая СРС	
работа с лекционным материалом, с учебной литературой	*10*
опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	*16*
самостоятельное изучение разделов дисциплины	*12*
подготовка к лабораторным занятиям	*16*
подготовка к построению/защите комп. программ	*10*
подготовка к экзамену	*10*
Творческая проблемно-ориентированная СРС	
поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	*16*
исследовательская работа, участие в конференциях, семинарах, олимпиадах	*10*
Итого СРС:	*100*

6.2. Порядок контроля: 1. опрос на лабораторных занятиях, 2. Отчеты по проектам, 3. Коллоквиумы, 4. Экзамен.

Раздел (модуль. тема)	Вид самостоятельной работы и практическое содержание	Контрольные сроки (в нед.) и вид контроля	Уч.-мет. обеспечение (указаны источники из списка основной литературы)
1.1	Классификация угроз компьютерной безопасности	1 (проверка решения задач)	[2], тема 1.1
1.2	Методы сжатия	2 (устный опрос)	[2], тема 1.2

	Метод Хаффмана	сост/защ.пр.1	[3], т. 1.2
2.1	Шифрование методом случайных чисел	3 (проверка программы)	[2], тема 2.1
2.2	Шифрование открытым ключом	4 сост/защ.пр.2	[2], тема 2.2
3.1	Протокол Диффи-Хеллмана	5 (письменный опрос)	[3], тема 3.1
3.2	Создание электронной цифровой подписи	6 сост/защ.пр.3	[3], тема 3.2
4.1	Открытые задачи	7 (проверка программы)	Задачи «Сост. число», «Дискр. логар.»
4.2	Перспективы квантовых процессоров	7 сост/защ.пр.4	Круглый стол по статьям сети Инт.
	Темы 1.1-4.2 (подготовка к экзамену)	Экзамен	[1]-[3], электронные материалы лекционных занятий

Текущий контроль:

1. Проверка программ на языке C# (Delphi, Java) по обязательным проектам.
2. Промежуточная аттестация с представлением материалов аттестации в электронной форме.

Текущий контроль включает проверку знаний по текущему материалу и проверку выполнения соответствующих компьютерных программ. Подразумевается обмен по электронной почте.

Промежуточный контроль проводится в виде письменной работы, материалы выполнения (письменный ответ и проекты на языке высокого уровня) принимаются в электронном виде.

Итоговый контроль проводится в виде письменной работы с обязательным устным собеседованием по результатам предварительной проверки.

Критерии выставления оценок:

«отлично» - уверенное владение теоретическим материалом, отчет по всем проектам на C#,

«хорошо» -- уверенное владение теоретическим материалом, отчет по 75% проектов,

«удовлетворительно» -- знакомство с основными темами, отчет по 50% проектов, посещение 80% занятий.

Практические задания для самостоятельной работы

Задание 1. Составьте программу для метода Хаффмана: ввести с клавиатуры последовательность букв и цифр и вывести в файл таблицу кодов.

Задание 2. Составьте программу для метода Хаффмана: ввести с клавиатуры последовательность букв и цифр и вывести на экран таблицу кодов, размещая в каждой строке символ и его код.

Задание 3. Составьте программу для метода Хаффмана: пусть в файле построчно размещена таблица кодов и код сообщения. Выведите на экран декодированное сообщение. Число различных символов равно трем.

Задание 4. Как вычислить значение функции Эйлера с использованием системы Математика?

Задание 5. Составьте функцию на C# для проверки, является ли заданное число простым. Найдите количество простых чисел, не превышающих заданное n.

Задание 6. Составьте функцию для проверки, являются ли числа a и b взаимно простыми. С ее помощью найдите функцию Эйлера для 33.

Пример образцового выполнения задания для самостоятельного решения.

Задание. Файл xlsx зашифрован методом xor с некоторым неизвестным ключом, нам известен только зашифрованный файл, исходный файл и ключ неизвестны.

Требуется вычислить ключ и дешифровать полученный файл.

Решение.

Если зашифрованный файл зашифровать любым xlsx – файлом, то мы получим подряд идущие ключи. Объяснение: начало у любого xls-файла одно и то же.

```
static void Main(string[] args)
{
   // Шифруем файл FileToEncode.xlsx ключом в файле key.txt
   Encrypt("FileToEncode.xlsx", "encoded.txt", "key.txt");

   // Пытаемся угадать ключ, шифруя другим экселевским документом
   Encrypt("encoded.txt", "guess.txt", "RandomDocument.xlsx");

   // Проверяем корректность шифрования, используя исходный ключ
   Encrypt("encoded.txt", "decoded.xlsx", "key.txt");
}
static void Encrypt(string inputPath, string outputPath, string keyPath)
{
   byte[] input = File.ReadAllBytes(inputPath);
   byte[] key = File.ReadAllBytes(keyPath);
   byte[] result = new byte[input.Length];
   for (int i = 0; i < input.Length; ++i)
   {
      result[i] = (byte)(input[i] ^ key[i % key.Length]);
   }
   File.WriteAllBytes(outputPath, result);
}
```

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

7.1. Типовые контрольные задания

7.1.1. Темы рефератов и курсовых работ:

Несанкционированный доступ к информации, зашифрованной методом случайных чисел
Длинная целочисленная арифметика в задачах криптографии
Основные задачи современной криптографии
Современное состояние задачи дискретного логарифмирования
Протокол Диффи-Хеллмана. Надежность и проблемы
Реализация алгоритма шифрования открытым ключом
Точки уязвимости алгоритма шифрования открытым ключом

Эшелонированная защита
Соответствие сложности шифрования реальным целям защиты
Симметричные методы шифрования
Аутентификация с нулевым разглашением

7.1.2. **Типовые задания для текущего контроля**

Упражнение. Как разложить 4832 на простые множители? Затем вычислите функцию Эйлера для этого числа двумя способами.

Упражнение. Составьте программу, которая проверяет, является ли 3 первообразным корнем из 17.

Упражнение. С помощью какой функции системы Математика можно вычислить (наименьший) первообразный корень из 17?

Упражнение. Найдите любым доступным Вам способом остатки от деления 3^{54} и 3^{24} на 17.

Упражнение. Составьте программу на языке C# для проверки, что при a=54, b=24, p=17, q=3 выполняется равенство

$$(q^a \bmod p)^b \bmod p = (q^b \bmod p)^a \bmod p.$$

Упражнение. Составьте программу шифрования заданного файла методом xor с использованием ключа, записанного в другой заданный файл.

Упражнение. В текстовом файле задано 21 натуральное число, среди которых имеется точно одно бесповторное число, каждое из остальных встречается четное число раз. Составьте программу вычисления бесповторного числа.

Упражнение. Составьте программу вычисления закрытого ключа.

Упражнение. Приведите пример генерации открытого и закрытого ключа, отличный от приведенного на занятиях.

7.1.3. Типовые вопросы для промежуточного контроля

Основные задачи кодирования.

Объясните термины: кодирование, декодирование, коды, сообщения, участвующие в формулировке задачи кодирования.

Формулировка игры «НИМ». Два основных вопроса.

Сформулируйте необходимые и достаточные условия, при которых игра НИМ выигрышна для начинающего.

Пусть известно, что игра НИМ выигрышна для начинающего. Сформулируйте выигрышную стратегию.

Какими основными свойствами должна обладать функция кодирования F?

Процесс шифрования методом случайных чисел (с использованием xor). Процесс дешифрования.

Какие шифры называются симметричными? Приведите пример.

Каким основным недостатком обладает метод шифрования xor? Объясните.

Кто (отправитель или получатель сообщений) и как формируются открытый и закрытый ключи?

Шифрование открытым ключом. Каковы действия получателя сообщений после генерации ключей?

Шифрование открытым ключом. Каковы действия отправителя сообщения?

Что Вы знаете о криптостойкости шифрования открытым ключом? Какую роль при этом играет задача «Составное число»?

Что такое «Цифровая подпись»?

Кодирование ASCII и RLE (с использованием коэффициентов). Какой метод сжимает лучше?

Условия применения метода Хаффмана для сжатия. Что дано, что требуется получить?

Как строится двоичное дерево при кодировании методом Хаффмана?

Пусть применяется метод Хаффмана и двоичное дерево построено. Как определяются коды символов?

В чем суть метода Хаффмана? Из-за чего при этом методе достигается хорошее сжатие?

Пусть информация закодирована методом Хаффмана. Правило декодирования.

Какое свойство метода Хаффмана обеспечивает однозначное декодирование, а какое – оптимальное сжатие информации?

Функция Эйлера. Примеры.

Первообразный корень. Два определения.

Алгоритм Диффи-Хеллмана для вычисления общего секретного ключа.

Изложите причины, по которым в алгоритме Диффи-Хеллмана злоумышленник не в силах вычислить секретный ключ. Какую роль при этом играет использование простого p и его первообразного корня q?

Изложите действия Алисы в презентации алгоритма Диффи-Хеллмана и объясните, почему они приводят к выработке общего секретного ключа.

Сформулируйте задачу, NP-полнота которой могла бы послужить математической основой криптостойкости алгоритма Диффи-Хеллмана. Какой «теоретический» результат получен в противоположном направлении?

7.1.4. Билеты к экзамену (итоговый контроль)

Билет 1

1. Основные задачи кодирования.
2. Что такое «Цифровая подпись»?

Упражнение. Составьте программу для метода Хаффмана: ввести с клавиатуры последовательность букв и цифр и вывести в файл таблицу кодов.

Билет 2

1. Объясните термины: кодирование, декодирование, коды, сообщения, участвующие в формулировке задачи кодирования.
2. Что Вы знаете о криптостойкости шифрования открытым ключом? Какую роль при этом играет задача «Составное число»?

Упражнение. Составьте функцию для проверки, является ли заданное число i простым. Найдите количество простых чисел, не превышающих заданное n.

Билет 3

1. Формулировка игры «НИМ». Два основных вопроса.
2. Кто (отправитель или получатель сообщений) и как формируются открытый и закрытый ключи?

Упражнение. Составьте функцию для проверки, являются ли числа a и b взаимно простыми. С ее помощью найдите функцию Эйлера для 33.

Билет 4

1. Какими основными свойствами должна обладать функция кодирования F?
2. Шифрование открытым ключом. Каковы действия получателя сообщений после генерации ключей?

Упражнение. Составьте программу для метода Хаффмана: ввести с клавиатуры последовательность букв и цифр и вывести на экран таблицу кодов, размещая в каждой строке символ и его код.

Билет 5

1. Пусть применяется метод Хаффмана и двоичное дерево построено. Как определяются коды символов?

2. Алгоритм Диффи-Хеллмана для вычисления общего секретного ключа.

Упражнение. Составьте программу на языке C# для проверки, что при a=54, b=24, p=17, q=3 выполняется равенство

$$(q^a \ mod \ p)^b \ mod \ p = (q^b \ mod \ p)^a \ mod \ p.$$

Билет 6

1. Каким основным недостатком обладает метод шифрования xor? Объясните.
2. Кодирование ASCII и RLE (с использованием коэффициентов). Какой метод сжимает лучше?

Упражнение. Найдите любым доступным Вам способом остатки от деления 3^{54} *и* 3^{24} на 17.

Билет 7

1. Процесс шифрования методом случайных чисел (с использованием xor). Процесс дешифрования.

2. Условия применения метода Хаффмана для сжатия. Что дано, что требуется получить?

Упражнение. Составьте программу шифрования заданного файла методом xor с использованием ключа, записанного в другой заданный файл.

Билет 8

1. Как строится двоичное дерево при кодировании методом Хаффмана?

2. Изложите причины, по которым в алгоритме Диффи-Хеллмана злоумышленник не в силах вычислить секретный ключ. Какую роль при этом играет использование простого p и его первообразного корня q?

Упражнение. Как разложить 4832 на простые множители? Затем вычислите функцию Эйлера для этого числа двумя способами.

Билет 9

1. В чем суть метода Хаффмана? Из-за чего при этом методе достигается хорошее сжатие?

2. Изложите действия Алисы в презентации алгоритма Диффи-Хеллмана и объясните, почему они приводят к выработке общего секретного ключа.

Упражнение. В текстовом файле задано 21 натуральное число, среди которых имеется точно одно бесповторное число, каждое из остальных встречается четное число раз. Составьте программу вычисления бесповторного числа.

Билет 10

1. Шифрование открытым ключом. Каковы действия отправителя сообщения?
2. Сформулируйте задачу, NP-полнота которой могла бы послужить математической основой криптостойкости алгоритма Диффи-Хеллмана. Какой «теоретический» результат получен в противоположном направлении?

Упражнение. Составьте программу вычисления закрытого ключа.

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

Общий результат складывается из текущего контроля - 50% и промежуточного контроля - 50%.

Текущий контроль по дисциплине включает:

-- посещение занятий – 40%

- выполнение текущих лабораторных заданий – 30 %
- выполнение домашних (аудиторных) контрольных работ – 30 %.

Промежуточный контроль по дисциплине включает:

- устный опрос – 50 %,
- выполнение проектов в Autodesk 3ds Max – 50 %.

8. Учебно-методическое обеспечение дисциплины

а) адрес сайта

http://cathedra.dgu.ru/EducationalProcess.aspx?Value=18&id=6

б) Основная литература:

1) Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— Саратов: Профобразование, 2017.— 702 с.— Режим доступа: http://www.iprbookshop.ru/63594.html.— ЭБС «IPRbooks»

2) Морозов А.В. Информационное право и информационная безопасность. Часть 1 [Электронный ресурс]: учебник для магистров и аспирантов/ Морозов А.В., Филатова Л.В., Полякова Т.А.— Электрон. текстовые данные.— Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 436 с.— Режим доступа: http://www.iprbookshop.ru/72395.html.— ЭБС «IPRbooks»

3) Д. Кнут. Искусство программирования для ЭВМ, т. 2, Мир, 1977.

4) Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография. От примитивов к синтезу алгоритмов. – БХВ-Петербург, 2014. – с. 446.

в) Дополнительная литература:

1) 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.— Режим доступа: http://www.iprbookshop.ru/61497.html.— ЭБС «IPRbooks»

2) Соколов В.П. Кодирование в системах защиты информации [Электронный ресурс]: учебное пособие/ Соколов В.П., Тарасова Н.П.— Электрон. текстовые данные.— М.: Московский технический университет связи и информатики, 2016.— 94 с.— Режим доступа: http://www.iprbookshop.ru/61485.html.— ЭБС «IPRbooks»

3) Шаньгин Ф.Ф. Защита компьютерной информации: эффективные методы и средства. – М.:ДМК, 2012. – 542 с.

4) Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. -- Санкт-Петербург: «Профессионал», 2015. -- 479 с.

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», способствующих освоению дисциплины

1) eLIBRARY.RU [Электронный ресурс]: электронная библиотека / Науч. электрон. б-ка. — Москва, 1999 – . Режим доступа: http://elibrary.ru/defaultx.asp). – Яз. рус., англ.

2) 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/

3) Электронный каталог НБ ДГУ [Электронный ресурс]: база данных содержит сведения о всех видах лит, поступающих в фонд НБ ДГУ/Дагестанский гос. ун-т. – Махачкала, 2010 – Режим доступа: http://elib.dgu.ru, свободный.

4) Математические основы защиты информации // URL =http://window.edu.ru/catalog/pdf2txt/128/78128/59040?p_page=14 .

5) Математические методы защиты информации // URL =http://www.sgu.ru/structure/ computersciences/courses/bachelor-matematicheskie-metody-zashchity-informacii

6) Математические основы защиты информации // URL = http://pandia.ru/text/79/234/90844.php

10. Методические указания для обучающихся по улучшению освоения дисциплины

1) Рекомендуется скопировать на кафедре видеокурсы по дисциплине и электронные материалы по лекциям.

2) Упражнения по теории чисел, выполняемые по темам дисциплины, рекомендуется выполнить двумя способами, сравнивая результаты: с помощью C#-программирования и с помощью системы компьютерной математики.

3) При составлении программ на C# использовать класс BigInteger для операций с длинной целочисленной математикой.

4) Поскольку дисциплина изучается в первом семестре, где предусмотрена также и научно-исследовательская практика магистрантов, то рекомендуется уплотненное размещение лекционных занятий в расписании с тем, чтобы не прерывать компактный курс из 6 лекций.

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

Для проведения занятий используются среда Visual Studio (используется язык C#), система компьютерной математики Mathematica и операционная система Microsoft Windows, для общения со студентами активно используется электронная почта.

Студентам копируются 2 видео-урока (О числах Фибоначчи и Генерации секретного ключа) и электронные материалы всех 6 лекций.

12. Описание материально-технической базы, необходимой для осуществления обра-

зовательного процесса по дисциплине

Лабораторные занятия проводятся в компьютерных классах с современным аппаратным и программным обеспечением – классы 3-66 и 3-67 оснащены современными ПК (ОП – 4Gb), ноутбуком и мультимедиа-проектором, установлено необходимое программное обеспечение. На каждой лекции используется стационарное мультимедийное презентационное оборудование.