МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)

«СОГЛАСОВАНО»
Руководитель ОП

_____ Пак Т.В.

«УТВЕРЖДАЮ»
Директор департамента Математического
и компьютерного моделирования

_____ Сущенко А.А.

« 26» января 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Методы оптимизации
Направление подготовки 01.03.02 Прикладная математика и информатика
(Математические и компьютерные технологии)
Форма подготовки очная

курс 4 семестр 8
лекции 16 час.
практические занятия 00 час.
лабораторные работы 32 час.
в том числе с использованием МАО
всего часов аудиторной нагрузки 48 час.
самостоятельная работа 60 час.
в том числе на подготовку к экзамену 00 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет 8 семестр
экзамен не предусмотрен

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 01.03.02 Прикладная математика и информатика, утвержденного приказом Министерства образования и науки Российской Федерации от 10 января 2018 г. № 9 (с изменениями и дополнениями)

Рабочая программа обсуждена на заседании департамента математического и компьютерного моделирования, протокол № 6 от «05» марта 2022 г.

Директор департамента математического и компьютерного моделирования Сущенко А. А.
Составитель (ли): доцент И.П.Яровенко

Владивосток
2022

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании департамента:
Протокол от «_____» _____ 20___ г. № _____
Директор департамента _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании департамента:
Протокол от «_____» _____ 20___ г. № _____
Директор департамента _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании департамента:
Протокол от «_____» _____ 20___ г. № _____
Директор департамента _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании департамента:
Протокол от «_____» _____ 20___ г. № _____
Директор департамента _____ _____
(подпись) (И.О. Фамилия)

АННОТАЦИЯ

Рабочая программа учебной дисциплины «Компьютерная безопасность» разработана для студентов 4 курса, обучающихся по направлению 01.03.02 «Прикладная математика и информатика».

При изучении дисциплины охватывается следующий круг вопросов: докомпьютерная криптография, блочно-итеративные криптосистемы, криптосистемы с открытым ключом, современные подходы к защите информации.

В процессе изучения данного курса студенты должны овладеть базовыми знаниями в области криптологии и усовершенствовать свои навыки в решении прикладных математических задач, в разработке алгоритмов и реализации их в виде программ, а также в анализе текстов с описанием алгоритмов и документации к программным системам и утилитам. В результате изучения данного курса студенты должны приобрести навыки и умения, расширить эрудицию в области современных информационных технологий, но также познакомиться с некоторыми социальными функциями информатики.

Данный УМКД содержит некоторые материалы, которые представлены на странице курса, размещенной в Интернет и предназначенной для использования студентами в процессе обучения. Приведен перечень основных тем, излагаемых на лекциях, а также тексты задач, в процессе решения которых студенты вырабатывают и совершенствуют навыки и умения, необходимые для будущей профессиональной деятельности в сфере информационных технологий.

Курс включает в себя следующие основные темы

- Классическая криптография.
- Основы теории информации Шеннона.
- Блочные симметричные итеративные шифры.
- Элементы теории сложности.
- Системы с открытым ключом.
- Первообразные корни и их свойства.
- Протокол взаимной аутентификации.
- Современные криптографические протоколы для обеспечения секретности и идентификации.

– Квантовая криптография.

В рамках этого курса демонстрируется применение математических методов к формированию алгоритмов и протоколов, связанных с защитой информации. В курсе используются навыки и умения, полученные на предыдущих стадиях подготовки в рамках таких предметов, как дискретная математика, алгебра, теория вероятностей, языки программирования.

Цель изучения курса является освоение математических основ криптологии и принципов защиты информации при ее хранении, обработке и передаче, а также совершенствование навыков решения задач с использованием компьютера.

Задачи:

1. Изучение математических основ криптологии.
2. Выработка умений для анализа и реализации в виде программного обеспечения алгоритмов и протоколов, используемых при защите информации.
3. Формирование представлений о роли информационных технологий в жизни общества.

4. Тип задач	**Код и наименование профессиональной компетенции** **(результат освоения)**	**Код и наименование индикатора достижения компетенции**
Производственно-технологический	**ПК-5** Способен к анализу рынка новых решений в области наукоемких технологий и пакетов программ для решения прикладных задач	ПК-5.1 применяет методы анализа концептуальных моделей решаемых научно-исследовательских проблем и задач
		ПК-5.2 осуществляет целенаправленный анализ рынка новых решений в области наукоемких технологий и пакетов программ для решения прикладных задач
		ПК-5.3 выбирает методы исследования, соотносит проблему, цели, задачи, предмет и методы исследования, формулирует проблему, обосновывает актуальность и новизну решения

Код и наименование индикатора достижения компетенции	**Наименование показателя оценивания** **(результата обучения по дисциплине)**
ПК-5.1 применяет методы анализа концептуальных моделей решаемых научно-исследовательских проблем и задач	Знать: методологии науки и техники, методов исследования объектов профессиональной деятельности и разработки моделей, способов обеспечения качества исследований и требований стандартов по оформлению научно-исследовательских отчетов, исследования объектов профессиональной деятельности.

	Уметь: использовать методологии науки и техники, методов исследования объектов профессиональной деятельности.
	Владеть: навыками использования знаний естественнонаучных дисциплин, вычислительной техники и программирования для решения общих задач естествознания, техники, навыками применения знаний к теоретически м и практическим исследованиям
ПК-5.2 осуществляет целенаправленный анализ рынка новых решений в области наукоемких технологий и пакетов программ для решения прикладных задач	Знать: основы профессии, принципы архитектуры вычислительной техники и системы программного обеспечения; программную инженерию, технологии программирования и способы реализации программных проектов.
	Уметь: корректно ставить профессиональные задачи; использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач; самостоятельно проводить анализ результатов научно-исследовательской работы, делать обоснованные вывод.
	Владеть: способностью использовать профессиональные методы при анализе проблем в области профессиональной деятельности; способностью участвовать в создании информационных и компьютерных систем, программных проектов на всех этапах жизненного цикла.
ПК-5.3 выбирает методы исследования, соотносит проблему, цели, задачи, предмет и методы исследования, формулирует проблему, обосновывает актуальность и новизну решения	Знать: определения и свойства основных объектов профессиональной деятельности
	уметь: решать задачи вычислительного и теоретического характера, находить оптимальные решения с наименьшим риском ошибки.
	владеть: разнообразным профессиональным разработки, описания и оценки моделей объектов профессиональной деятельности

Общая трудоемкость дисциплины составляет 3 зачётных единиц (108 академических часов). 1 зачетная единица соответствует 36 академическим часам.

Видами учебных занятий и работы обучающегося по дисциплине могут являться:

Обозначение	Виды учебных занятий и работы обучающегося
Лек	Лекции
Лаб	Лабораторные работы
СР	Самостоятельная работа обучающегося в период теоретического обучения
Контроль	Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации

1. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Докомпьютерная криптография (6/36)

- Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Потоковые и блочные шифры.
- Докомпьютерная криптография . Шифры *Виженера*. Автоматический и бегущий выбор ключа.
- Шифры Вернама, Плейфейера, Хилла. Шифр одноразового блокнота.
- Энтропия и информация по Шеннону. Условие абсолютнойкриптостойкости шифра.

Раздел II. Блочные симметричные итеративные шифры (6/36)

- Шифр Файстеля. Структура шифра. Алгоритм дешифрования. Диффузия и конфузия.
- DES: шифрование и дешифрование. Лавинный эффект. Надежность. Криптоанализ.
- Режимы работы DES. Сцепление блоков. Шифрованная обратная связь. Двойной и тройной DES. Другие симметрично-блочные шифры.

Раздел III. Элементы теории сложности вычислений (4/36)

- Классы языков. Временная сложность вычислений. Классы P и NP. Примеры NP-трудных проблем. Языки составных и простых чисел.

Раздел IV. Криптосистемы с открытым ключом (10/36)

- Криптосистемы, базирующиеся на задаче о рюкзаке.
- Группы, кольца, области целостности, поля. Классы вычетов по модулю.
- Простые числа. Основная теорема арифметики. Теорема Евклида о существовании бесконечного множества простых чисел. Теорема о промежутках между простыми числами.
- Малая теорема Ферма. Теорема Эйлера.
- RSA: основные элементы криптосистемы. Шифрование и дешифрование.
- Греко-китайская теорема об остатках и ее применения.

- Возведение в степень с использованием метода последовательного возведения в квадрат.
- Теорема о корнях x^2=1 mod p для нечетного простого p. Рандомизация проверки простоты (WITNESS). Числа Карлмайкла.

Раздел V. Аутентификация (6/36)

- Первообразные корни и их свойства. Дискретные логарифмы.
- Протокол взаимной аутентификации. Схема обмена ключами Диффи-Хеллмана.

Раздел VI. Современные проблемы (4/36)

- Квантовая криптография.
- Доказательства без разглашения, протоколы электронного голосования, неотслеживаемость транзакций, разделение секретов и т. д.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

На лабораторных и практических работах проводится обсуждение и сдача решений задач, которые выдаются в процессе лекций. Также на лабораторных работах проводится обсуждение рефератов.

3. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

Вопросы к зачету / экзамену

– Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Потоковые и блочные шифры.

– Рандомизация проверки простоты (WITNESS). Числа Карлмайкла}

– Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Потоковые и блочные шифры.

– Протокол взаимной аутентификации. Схема обмена ключами Диффи-Хеллмана.

– Модулярные шифры. Шифры Виженера. Автоматический и бегущий выбор ключа.

– Теорема о корнях $x^2=1 \mod p$ для нечетного простого p.

– Шифры Вернама, Плейфейера, Хилла. Шифр одноразового блокнота. Абсолютно криптостойкие шифры.

– Греко-китайская теорема об остатках и ее применения.

– Шифр Файстеля. Структура шифра. Алгоритм дешифрования.

– Малая теорема Ферма. Теорема Эйлера.

– DES: алгоритмы шифрования и дешифрования. Надежность.

– Криптоанализ. Диффузия и конфузия.

– Возведение в степень с использованием метода последовательного возведения в квадрат.

– Тройной DES.

– Группы, кольца, области целостности, поля.

– Двойной DES.

– Криптосистемы, базирующиеся на задаче о рюкзаке.

– Режимы работы DES. Сцепление блоков.

– Обмен ключами по алгоритму BB84 (квантовая криптография).

– Простые числа. Основная теорема арифметики. Теорема Евклида о существовании бесконечного множества простых чисел. Теорема о промежутках между простыми числами.

– RSA: основные элементы криптосистемы. Шифрование и дешифрование.

4. ТЕМАТИКА И ПЕРЕЧЕНЬ КУРСОВЫХ РАБОТ И РЕФЕРАТОВ

Рефераты

Реферат объемом 2 стр. без обложки должен быть представлен и защищен до экзамена/зачета по согласованной теме (темы, предварительный список литературы и содержание для согласования нужно присылать по почте). Основное направление -- криптоанализ и отдельные составляющие изученных систем, а также современные криптографические протоколы, криптографические системы и т. п., которые не были затронуты на лекциях. Требуется подобрать и изучить современные источники и попытаться на двух стр. самостоятельно изложить материал со ссылками на библиографические описания использованных источников. Любое заимствование должно быть явно обозначено. Примеры рефератов, подготовленных в предыдущие годы, доступны на сайте (Алгоритм шифрования IDEA, Коллизии хэш-функций, Схема разделения секрета Шамира, протоколы для обеспечения секретности и идентификации и т. д.).

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(печатные и электронные издания)

1. Криптография и безопасность сетей [Электронный ресурс]: учебное пособие/ Б. А. Фороузан – Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. https://lib.dvfu.ru/lib/item?id=IPRbooks:IPRbooks-102017&theme=FEFU
2. Алгебраическая криптология [Электронный ресурс]: учебное пособие/ В. А. Романьков – Изд-во Омского университета, 2020. https://lib.dvfu.ru/lib/item?id=chamo:885384&theme=FEFU
3. Математические и компьютерные основы криптологии. - Минск: ООО "Новое знание", 2003.
4. Саломаа А. Криптография с открытым ключом. М.: Мир, 1996.
5. Столлингс В. Криптография и защита сетей: принципы и практика. М.: Изд. дом Вильямс, 2003.
6. Акритас А. Основы компьютерной алгебры. М.: Мир, 1994.
7. Смарт Н. Криптография. - Москва: Техносфера, 2005.
8. Брассар Ж. Современная криптология. - М.: Полимед, 1999.
9. Хопкрофт Дж., Ульман Дж., Мотвани Р. Введение в теорию автоматов, языков и вычислений. - М.: Изд. дом Вильямс, 2002.
10. Рябко Б. Я., Фионов А. Н. Защита информации. — 2-е изд. — М.: Горячая линия — Телеком, 2013.
11. Jonathan Katz, Yehuda Lindell Introduction to Modern Cryptography: Principles and Protocols, Chapman and Hall CRC, 2007.
12. Philip N. Klein A Cryptography Primer: Secrets and Promises. CambridgeUniversityPress, 2014.

13. Richard E. Blahut Cryptography and Secure Communication. CambridgeUniversityPress, 2014.

Дополнительная литература
(печатные и электронные издания)

1. Осипян В. О., Осипян К. В. Криптография в упражнениях и задачах Издательство: Гелиос АРВ, 2004.

2. Скембрей Дж, Мак-Клар С., Курц Дж. Секреты хакеров. Безопасность сетей - готовые решения. М.: Изд. дом Вильямс, 2001.

3. Ноден П., Китте К. Алгебраическаяалгоритмика (с упражнениями и решениями). - М.: Мир, 1994

4. Введение в криптографию /Под общ.ред. В. В. Ященко. - М.: МЦНМО: "ЧеРо", 1999.

5. Фергюсон Н., Шнайдер Б. Практическая криптография. -- М.: Вильямс, 2005.

6. Материалы, посвященные книге Столлингс В. "Криптография и защита сетей: принципы и практика". http://williamstallings.com/Crypto3e.html (запрошен 01.09.2013).

КОНСПЕКТЫ ЛЕКЦИЙ

Раздел I. Докомпьютерная криптография (6 час.)

1. Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Потоковые и блочные шифры.
2. Докомпьютерная криптография . Шифры *Виженера*. Автоматический и бегущий выбор ключа.
3. Шифры Вернама, Плейфейера, Хилла. Шифр одноразового блокнота.
4. Энтропия и информация по Шеннону. Условие абсолютнойкриптостойки шифра.

Источники:

- Математические и компьютерные основы криптологии. - Минск: ООО "Новое знание", 2003.
- Саломаа А. Криптография с открытым ключом. М.: Мир, 1996.
- Столлингс В. Криптография и защита сетей: принципы и практика. М.: Изд. дом Вильямс, 2003.
- Акритас А. Основы компьютерной алгебры. М.: Мир, 1994.

Раздел II. Блочные симметричные итеративные шифры (6 час.)

5. Шифр Файстеля. Структура шифра. Алгоритм дешифрования. Диффузия и конфузия.
6. DES: шифрование и дешифрование. Лавинный эффект. Надежность. Криптоанализ.
7. Режимы работы DES. Сцепление блоков. Шифрованная обратная связь. Двойной и тройной DES. Другие симметрично-блочные шифры.

Источники:

- Столлингс В. Криптография и защита сетей: принципы и практика. М.: Изд. дом Вильямс, 2003.

Раздел III. Элементы теории сложности вычислений (4 час.)

8. Классы языков. Временная сложность вычислений. Классы P и NP. Примеры NP-трудных проблем. Языки составных и простых чисел.

Источники:

- Хопкрофт Дж., Ульман Дж., Мотвани Р. Введение в теорию автоматов, языков и вычислений. - М.: Изд. дом Вильямс, 2002.
- Jonathan Katz, Yehuda Lindell Introduction to Modern Cryptography: Principles and Protocols, Chapman and Hall CRC, 2007.
- Richard E. Blahut Cryptography and Secure Communication. CambridgeUniversityPress, 2014.

Раздел IV. Криптосистемы с открытым ключом (10 час.)

9. Криптосистемы, базирующиеся на задаче о рюкзаке.
10. Группы, кольца, области целостности, поля. Классы вычетов по модулю.
11. Простые числа. Основная теорема арифметики. Теорема Евклида о существовании бесконечного множества простых чисел. Теорема о промежутках между простыми числами.
12. Малая теорема Ферма. Теорема Эйлера.
13. RSA: основные элементы криптосистемы. Шифрование и дешифрование.
14. Греко-китайская теорема об остатках и ее применения.
15. Возведение в степень с использованием метода последовательного возведения в квадрат.
16. Теорема о корнях x^2=1 mod p для нечетного простого p. Рандомизация проверки простоты (WITNESS). Числа Карлмайкла.

Источники:

1. Саломаа А. Криптография с открытым ключом. М.: Мир, 1996.
2. Математические и компьютерные основы криптологии. - Минск: ООО "Новое знание", 2003.
3. Jonathan Katz, Yehuda Lindell Introduction to Modern Cryptography: Principles and Protocols, Chapman and Hall CRC, 2007.
4. Richard E. Blahut Cryptography and Secure Communication. CambridgeUniversityPress, 2014.

Раздел V. Аутентификация (6 час.)

17. Первообразные корни и их свойства. Дискретные логарифмы.
18. Протокол взаимной аутентификации. Схема обмена ключами Диффи-Хеллмана.

Источники:

- Математические и компьютерные основы криптологии. - Минск: ООО "Новое знание", 2003.
- Richard E. Blahut Cryptography and Secure Communication. CambridgeUniversityPress, 2014.
- Jonathan Katz, Yehuda Lindell Introduction to Modern Cryptography: Principles and Protocols, Chapman and Hall CRC, 2007.

Раздел VI. Современные проблемы (4 час.)

19. Квантовая криптография.
20. Доказательства без разглашения, протоколы электронного голосования, неотслеживаемость транзакций, разделение секретов, протоколы для обеспечения секретности и идентификации и т. д.

Источники:

1. Брассар Ж. Современная криптология. - М.: Полимед, 1999.Введение в криптографию /Под общ.ред. В.В. Ященко. - М.: МЦНМО: "ЧеРо", 1999.Брассар Ж. Современная криптология. - М.: Полимед, 1999.
2. Richard E. Blahut Cryptography and Secure Communication. CambridgeUniversityPress, 2014.
3. Jonathan Katz, Yehuda Lindell Introduction to Modern Cryptography: Principles and Protocols, Chapman and Hall CRC, 2007.

МАТЕРИАЛЫ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Рекомендации по самостоятельной работе студентов

Самостоятельная работа студентов состоит из решения задач и подготовки реферата по согласованной теме.

Основные требования к содержанию реферата

Студент должен использовать только те материалы (научные статьи, монографии, пособия), которые имеют прямое отношение к избранной им теме.

По своей *структуре* реферат состоит из:

1. Введения, где студент формулирует проблему, подлежащую анализу и исследованию;

2. Основного текста, в котором последовательно раскрывается избранная тема. Возможно описание фрагментов кода, который разрабатывается в процессе подготовки реферата.

3. Заключения, где студент формулирует выводы, сделанные на основе основного текста.

4. Списка использованной литературы. В данной список включаются все источники, на которые имеются ссылки в тексте. Использование материалов Википедии является нежелательным.

Порядок сдачи реферата и его оценка

Реферат готовится студентами в течение семестра по тематике, согласуемой по почте. Защита рефератов проводится в рамках лабораторных работ. При защите реферата студент должен дать разъяснения и ответить на вопросы по тексту.

Тематика рефератов

1. Альтернативные системы с открытым ключом
2. Системы, базирующиеся на использовании эллиптических кривых
3. Протоколы для голосования

4. Разделение секретов

Задачи для самостоятельного решения

1. Докомпьютерная криптография:Показать, что нод(a,|A|)=1 н. и д. для однозначности дешифрования шифра c= a* m+b (mod |A|).

2. Докомпьютерная криптография:Описать обратное преобразование для модулярного шифра с a/=1. Будет ли оно модулярным шифром?

3. Докомпьютерная криптография:Сколько всего различных модулярных шифров в |A|-буквенном алфавите A (вывести формулу)? Посчитать по формуле для английского языка, где |A|=26.

4. Докомпьютерная криптография:Сколько возможных ключей позволяет использовать шифр Плейфейера? (Представить приблизительно в виде степени двойки.)

5. Докомпьютерная криптография:Реализовать (Scheme, Mathematica, Sage, ...) схему шифрования-дешифрования Плейфейера, подготовить тесты по методу белого ящика, продемонстрировать его работу и методику криптоанализа на достаточно длинном шифрованном тексте.

6. Докомпьютерная криптография:Расшифровать заданное сообщение ymjkwjvzjshdrjymtisjjixqt slhnumjwyjcyxytbtwp с использованием частотной таблицы (модулярный шифр с n=1).

7. Докомпьютерная криптография:Реализовать программу (Scheme, Mathematica, Sage, ...) для подсчета частоты встречаемости отдельных символов, пар, троек и т.д. Подготовить тесты. Продемонстрировать работу на достаточно длинном тексте. Сравнить результаты с известными.

8. Докомпьютерная криптография: Описать и реализовать (Scheme, Mathematica, Sage, ...) методику криптоанализа шифра Виженера (продемонстрировать методику криптоанализа на достаточно длинном шифрованном тексте).

9. Докомпьютерная криптография : Каким необходимым и достаточным условиям должен удовлетворять определитель матрицы E для того, чтобы

преобразование Хилла c=E m+s (mod |A|), c, m, s - n-мерные векторы, E - n*n-матрица, обладало свойством взаимной однозначности?

10. Докомпьютерная криптография:Какие из изученных докомпьютерных шифров являются групповыми, а какие нет (с доказательством)?

11. Докомпьютерная криптография:Показать, что шифр перестановки является линейным преобразованием в B^n, B={0,1}.

12. Докомпьютерная криптография: Сколько существует нелинейных криптопреобразований B^3->B^3?

13. Докомпьютерная криптография: Доказать, что энтропия скалярного источника дискретных сообщений, заданного вероятностями p_1,...,p_n, принимает максимальное значение т. и т. т., когда все p_i, i=1,..,n, совпадают. (Известно, что если некоторая функция h_n от p_1,...,p_n непрерывна по совокупности переменных и обладает дополнительно тремя свойствами: 1) ее максимум достигается при равных p_i, i=1,..,n, 2) иерархической аддитивности, 3) добавление к алфавиту еще одного символа с нулевой вероятностью не меняет ее значения, т.е. h_{n+1}(p_1,...,p_n,0)=h_{n}(p_1,...,p_n), то h_n необходимо имеет вид шенноновской энтропии: h_{n}(p_1,...,p_n)=-\lambda \sum_{i=1}^{n} p_i \logp_i, где \lambda>0).

14. Докомпьютерная криптография: Доказать свойство иерархическойаддитивности для векторного источника дискретных сообщений.

15. Применение теории информации: Какая информация будет получена в результате проведения зачета, если студент получает зачет с вероятностью 0.9, если он готовился, и 0.3, если нет, и известно, что 90% студентов готовились к зачету.

16. Докомпьютерная криптография: Для абсолютно криптостойкой системы I(\phi,\xi)=I(\xi,\phi)=0: информация об исходном тексте в открытом (зашифрованном) равна нулю.

17. Блочные симметричные итеративные шифры: Реализовать DES с использованием Scheme, Mathematica, Sage, ... и протестировать программу с использованием материалов со страницы Ronald R. Testingimplementationsof DES.

18. Блочные симметричные итеративные шифры: Разработать программы и тесты для демонстрации различных режимов использования DES (Scheme, Mathematica, Sage, ...).

19. Блочные симметричные итеративные шифры : Доказать свойство дополнительности DES (1): если C=DES(M,K), то C'=DES(M',K') (Z' - обозначает слово, составленное из дополнений соответствующих битов бинарного слова Z). (Используйте следующее равенство для логических переменных (x+y)'=x'+y).

20. Блочные симметричные итеративные шифры: Продемонстрировать лавинный эффект в DES: написать программу (Scheme, Mathematica, Sage), которая вычисляет расстояние Хемминга для результатов раундовых преобразований при изменении одного бита в исходном сообщении и в ключе. Для этого сгенерировать сообщение и ключ, а затем, изменив в сообщении ровно один бит случайным образом, рассчитать расстояние Хемминга между результатами раундовых преобразований. Вычислить также среднее расстояние по набору исходных сообщений для всех 16 раундов. Аналогичные действия проделать для фиксированного сообщения и изменений одного бита ключа.

21. Криптосистемы с открытым ключом: Доказать, что n_i^s=2^i, i=1, 2, … , 1) является минимальной супервозрастающей последовательностью, 2) может использоваться для кодирования любого числа (при достаточно большом k), 3) никакая другая не обладает свойством 2.

22. RSA: Оценить вероятность того, что 0 <w<n будет не взаимно просто с n=pq. Показать, что и при нод(n,w)/=1 расшифрование RSA сводится к возведению в степень d.

23. Пусть p=P[нод(a,b)=1, где a,b - два выбранные наугад числа].

- Доказать, что P[нод(a,b)=d, где a,b - два выбранные наугад числа] =p/d^2.
- Доказать, что \sum{d>=1} P[нод(a,b)=d, где a,b - два выбранные наугад числа]=1.
- Доказать, что p примерно равна 0.6.

24. Криптосистемы с открытым ключом: Исполнить WITNESS при a=7, n=561 и проинтерпретировать результат.

25. Криптосистемы с открытым ключом: Найти (678*973)mod 1813 (с использованием греко-китайской теоремы)

26. Криптосистемы с открытым ключом: Сгенерировать все компоненты RSA, протестировать кодирование/декодирование.

27. Криптосистемы с открытым ключом: Шесть профессоров начинают читать лекции по своим курсам в ПН, ВТ, СР, ЧТ, ПТ, СБ и читают их далее через 2, 3, 4, 1, 6, 5 дней соответственно. Лекции не читаются по ВС (отменяются). На какой по порядку неделе в первый раз все лекции выпадут на ВС и будут отменены?

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ

Вопросы к экзамену

1. Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Потоковые и блочные шифры.
2. Рандомизация проверки простоты (WITNESS). Числа Карлмайкла}
3. Схема Шеннона. Симметричные криптосистемы. Перестановки и подстановки. Одноалфавитные и многоалфавитные криптосистемы. Потоковые и блочные шифры.
4. Протокол взаимной аутентификации. Схема обмена ключами Диффи-Хеллмана.
5. Модулярные шифры. Шифры Виженера. Автоматический и бегущий выбор ключа.

6. Теорема о корнях $x^2=1 \mod p$ для нечетного простого p.
7. Шифры Вернама, Плейфейера, Хилла. Шифр одноразового блокнота. Абсолютно криптостойкие шифры.
8. Греко-китайская теорема об остатках и ее применения.
9. Шифр Файстеля. Структура шифра. Алгоритм дешифрования.
10. Малая теорема Ферма. Теорема Эйлера.
11. DES: алгоритмы шифрования и дешифрования. Надежность.
12. Криптоанализ. Диффузия и конфузия.
13. Возведение в степень с использованием метода последовательного возведения в квадрат.
14. Тройной DES.
15. Группы, кольца, области целостности, поля.
16. Двойной DES.
17. Криптосистемы, базирующиеся на задаче о рюкзаке.
18. Режимы работы DES. Сцепление блоков.
19. Обмен ключами по алгоритму BB84 (квантовая криптография).
20. Простые числа. Основная теорема арифметики. Теорема Евклида о существовании бесконечного множества простых чисел. Теорема о промежутках между простыми числами.
21. RSA: основные элементы криптосистемы. Шифрование и дешифрование.