Министерство образования и науки Российской Федерации
НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И УПРАВЛЕНИЯ «НИНХ»
Кафедра информационной безопасности

МЕТОДИЧЕСКОЕ РУКОВОДСТВО ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ОЧНОЙ ФОРМЫ ОБУЧЕНИЯ

Учебная дисциплина
КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Для студентов, обучающихся по направлению подготовки
10.03.01 «Информационная безопасность»
«Информационно аналитические тистемы финансового мониторинга»
без профиля

Новосибирск 2016

ОГЛАВЛЕНИЕ

РАЗДЕЛ 1. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПОДГОТОВКЕ К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ

1.1. Организация самостоятельной работы студентов по подготовке к лабораторным занятиям

Студенту рекомендуется следующая схема подготовки к лабораторному занятию по учебной дисциплине «Криптографические методы защиты информации»:

1. Проработать конспект лекций.
2. При необходимости обратиться к источникам основной и дополнительной литературы, рекомендованной по каждому из двух разделов учебной дисциплины.
3. Подготовить ответы на вопросы, входящие в структуру содержания лабораторного занятия по каждой теме соответствующего раздела учебной дисциплины.
4. При затруднениях сформулировать вопросы к преподавателю.

Формой текущего контроля самостоятельного изучения студентом отдельных тем является защита лабораторных работ и коллоквиумы.

1.2. Содержание лабораторных занятий

Лабораторные занятия по дисциплине «Криптографические методы защиты информации» проводятся в соответствии с учебно-тематическим планом и планом лабораторных занятий, отраженным в Рабочей программе.

Раздел 1. Основы криптографии

Тема 1.1. Введение в криптографию

1. Шифр Цезаря.
2. Криптоанализ шифра Цезаря.

Вопросы и задания для самостоятельной работы:

1. Реализуйте шифр Цезаря для зашифрования и расшифрования слов на русском или английском языке.
2. Реализуйте метод полного перебора ключей для шифра Цезаря.
3. Реализуйте шифр Цезаря для зашифрования и расшифрования файлов.

Тема 1.2. Требования к шифрам и их свойства

1. Вычисление энтропии.
2. График двоичной энтропии.
3. Аффинный шифр.

Вопросы и задания для самостоятельной работы:

1. Напишите программу вычисления энтропии.
2. Напишите программу, изображающую график двоичной энтропии.
3. Реализуйте аффинный шифр.

Тема 1.3. Основы криптографии с открытым ключом

1. Возведение в степень по модулю.
2. Дискретное логарифмирование.
3. Метод «Шаг младенца – шаг великана».

Вопросы и задания для самостоятельной работы:

1. Реализуйте алгоритм быстрого возведения в степень по модулю.
2. Реализуйте дискретное логарифмирование методом полного перебора.
3. Реализуйте дискретное логарифмирование методом «Шаг младенца – шаг великана».

Тема 1.4. Элементы теории чисел

1. Основные теоретико-числовые алгоритмы.

Вопросы и задания для самостоятельной работы:

1. Реализуйте проверку числа на простоту.
2. Реализуйте алгоритм Евклида.
3. Реализуйте расширенный алгоритм Евклида.
4. Реализуйте вычисление инверсий.

Тема 1.5. Системы шифрования с открытыми ключами

1. Система Диффи-Хеллмана.
2. Шифры с открытым ключом.

Вопросы и задания для самостоятельной работы:

1. Реализуйте системы Диффи-Хеллмана.
2. Реализуйте шифры Шамира, Эль-Гамаля и RSA.

Тема 1.1. Введение в криптографию

1. Шифр Цезаря.
2. Криптоанализ шифра Цезаря.

Вопросы и задания для самостоятельной работы:

1. Реализуйте шифр Цезаря для зашифрования и расшифрования слов на русском или английском языке.
2. Реализуйте метод полного перебора ключей для шифра Цезаря.
3. Реализуйте шифр Цезаря для зашифрования и расшифрования файлов.

Вопросы для подготовки к коллоквиуму

1. В чем принципиальное отличие современной криптографии от исторической криптографии?

2. Перечислите основных действующих лиц в криптографии.
3. Приведите примеры проблем, возникающих при передаче информации.
4. Опишите алгоритм и математическую формулу работы шифра Цезаря.
5. Опишите классическую схему секретной связи Шеннона.
6. Сформулируйте принцип Керкхоффса и объясните, зачем он нужен?
7. Опишите метод полного перебора ключей применительно к шифру Цезаря и оцените его сложность.
8. Что такое избыточность?
9. Объясните, что такое атака по шифротексту, по известному открытому тексту и выбранному открытому тексту.
10. Что такое асимметричные криптосистемы или криптосистемы с открытым ключом?
11. Опишите проблему хранения паролей в компьютере и проблему ПВО.
12. Дайте определение односторонней функции.
13. Дайте определение дискретного логарифма.
14. Объясните, как выполнить дискретное логарифмирование методом полного перебора.
15. Опишите идею алгоритма быстрого возведения в степень по модулю.
16. Опишите алгоритм быстрого возведения в степень по модулю и приведите пример.
17. Какова сложность алгоритма быстрого возведения в степень по модулю? Почему?
18. Объясните, как решается проблема хранения паролей и проблема ПВО с использованием односторонних функций.
19. Объясните, почему в ряде случаев использование секретных ключей проблематично. Приведите пример.

Раздел 2. Криптографические протоколы и алгоритмы

Тема 2.1. Электронная цифровая подпись

1. Протоколы цифровой подписи.
2. Выбор параметров для ЭЦП.

Вопросы и задания для самостоятельной работы:

1. Реализуйте цифровую подпись RSA.
2. Реализуйте цифровую подпись Эль-Гамаля.

Тема 2.2. Криптографические протоколы

1. Электронные деньги.
2. Ментальный покер.
3. Протокол Нидхама-Шредера.

Вопросы и задания для самостоятельной работы:

1. Реализуйте протокол Чаума реализации электронных денег.
2. Реализуйте протокол ментального покера для раздачи трех карт.
3. Реализуйте протокол Нидхама-Шредера.

Тема 2.3. Современные шифры с секретным ключом

1. Блочные шифры.
2. Поточные шифры.

Вопросы и задания для самостоятельной работы:

1. Реализуйте шифр TEA.
2. Реализуйте шифр RC6.
3. Реализуйте шифр RC4.

Тема 2.4. Случайные и псевдослучайные числа в криптографии

1. Генераторы ПСЧ.
2. Статистические тесты.

Вопросы и задания для самостоятельной работы:

1. Реализуйте линейный конгруэнтный генератор.
2. Реализуйте мультипликативный линейный конгруэнтный генератор.
3. Реализуйте критерий хи-квадрат.
4. Реализуйте тест «стопка книг».

Тема 2.5. Криптографические хеш-функции

1. Хеш-функции на основе блочных шифров.

Вопросы и задания для самостоятельной работы:

1. Реализуйте хеш-функцию на основе шифра TEA.

Тема 2.6. Практические аспекты использования шифрсистем

1. Программные реализации шифров.

Вопросы и задания для самостоятельной работы:

1. Реализуйте по три каких-либо блочных и поточных шифра.

Вопросы для подготовки к коллоквиуму

1. Какие требования предъявляются к виртуальной раздаче карт.
2. Опишите проблему подбрасывания монеты по телефону.
3. Опишите протокол подбрасывания монеты по телефону.
4. Как выбрать параметры для протокола ментального покера?
5. Опишите протокол ментального покера. Приведите пример.
6. Обоснуйте корректность протокола ментального покера.
7. Что такое доказательство с нулевым знанием?

8. Что такое проблема «Большого брата»?
9. Какие требования предъявляются к протоколу электронных денег?
10. Опишите протокол Чаума. Приведите пример.
11. Каковы недостатки системы Диффи-Хеллмана?
12. Опишите протокол Нидхама-Шредера. Приведите пример.
13. Опишите шифр Вернама. Приведите пример.
14. Какое главное достоинство и главный недостаток шифра Вернама?
15. Дайте определение энтропии. Приведите пример. Постройте график двоичной энтропии.
16. Что такое блочный шифр? Какие параметры есть у него?
17. Назовите 3-4 блочных шифра. Чему равны их параметры?
18. Назовите режимы использования блочных шифров.
19. Что такое поточный шифр?

1.3. Список библиографических источников для подготовки к лабораторным занятиям по разделам учебной дисциплины

Основное (обязательное) обеспечение

Библиографический список:

б) учебные пособия:

1. Основы криптографии : учеб. пособие для высш. учеб. заведений по гр. специальностям в обл. информ. безопасности / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – 3-е изд., испр. и доп. – М. : Гелиос АРВ, 2005. (МОРФ)

г) научная литература:

1. Бабаш, А. В. Криптография / Бабаш А. В., Шанкин Г. П. ; под ред. В. П. Шерсюка, Э. А. Применко. - М. : Солон – Пресс, 2007.
2. Рябко, Б. Я. Основы современной криптографии для специалистов по информационным технологиям / Б. Я. Рябко, А. Н. Фионов. – М. : Науч. мир, 2004.

Информационные источники: http://www.codeblocks.org/, http://www.microsoft.com/, http://www.oracle.com/

Программные продукты: интегрированные средства разработки Microsoft Visual Studio, CodeBlocks.

Дополнительное обеспечение

Библиографический список:

б) учебные пособия:

1. Черемушкин, А. В. Криптографические протоколы. Основные свойства и уязвимости : учеб. Пособие для студ. учреждений высш. проф. образования / А. В. Черемушкин .- М. : Изд. центр «Академия», 2009 .- 272 с . (УМО)

2. Черемушкин, А. В. Лекции по арифметическим алгоритмам в криптографии / А. В. Черемушкин .- М. : МНЦМО, 2002 .- 104 с . (УМО)
3. Введение в криптографию. Новые мат. дисциплины: [учебник] / [В. В. Ященко, Н. П. Варновский, Ю. В. Нестеренко и др.]; под ред. В. В. Ященко. – СПб.: МЦНМО : Питер, 2001.
4. Рябко Б.Я. Криптографические методы защиты информации учеб. пособие для вузов по специальностям: 201000 (210404) "Многоканальные телекоммуникационные системы", 201100 (201405) "Радиосвязь, радиовещание и телевидение", 201800 (210403) "Защищенные системы связи" / Б. Я. Рябко, А. Н. Фионов. М.: Горячая линия-Телеком, 2005. – 229 с. (УМО)

г) научная литература:

1. Зубов, А. Ю. Математика кодов аутентификации / А. Ю. Зубов .- М. : Гелиос АРВ, 2007 .- 480 с .
2. Пестунов А.И. Дифференциальный криптоанализ блочного шифра CAST-256 // Безопасность информационных технологий. – 2009. - №4. – С. 57-62.
3. Pestunov A. Differential Cryptanalysis of Reduced-Round MARS // Proc. XI International Symposium on Problems of Redundancy in Information and Control Systems. – Saint Petersburg. – 2007. – P. 197-201.
4. Пестунов А.И. Блочные шифры и их криптоанализ // Вычислительные технологии. – 2007. – Т. 12, спец. вып. №4. – С. 42-49.
5. Пестунов А.И. Статистический анализ современных блочных шифров // Вычислительные технологии. – 2006. – Т.12, №2. – С. 122-129.
6. Рябко Б.Я., Пестунов А.И. «Стопка книг» как новый статистический тест для случайных чисел // Проблемы передачи информации. – 2004. – Т.40, №1. – С. 73-78.

Информационные источники: http://www.intuit.ru/

Программные продукты: интегрированные средства разработки Eclipse, NetBeans, DevC++.

РАЗДЕЛ 2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЗАПЛАНИРОВАННЫХ ВИДОВ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Согласно Рабочему учебному плану организация самостоятельной работы студентов заключается в подготовке к лабораторным занятиям, выполнению одной расчетно-графической работы и одной курсовой работы.

2.1. Методические указания по выполнению РГР 1

Форма задания

РГР состоит из трех частей: *доклада*, *практического задания и реферата* (3-4 стр.).

Защита РГР проводится в 3 этапа:

1. *доклад* по выбранной теме;
2. защита *практического задания* (производится аналогично лабораторным работам);
3. *реферат*.

Сроки защиты РГР

Доклад – 1 месяц семестра;
Практическое задание – 2 месяц семестра;
Реферат – 3 месяц семестра.

Штрафные санкции

Если студент не выполняет доклад в назначенный ему день, то он получает 2 *штрафных задачи*. Если студент опаздывает со сдачей практического задания или реферата, то он также получает *штрафные задачи*: опоздание на 1 неделю = 1 штрафная задача.

Варианты РГР

1. Квадрат Полибия и тюремный шифр ([1, стр. 10], [2, стр. 18, 22]);
2. Диск Альберти ([1, стр. 13], [2, стр. 33]);
3. Шифры Тритемия и Виженера ([1, стр. 15, 18], [2, стр. 28, 43]);
4. Таблица Порта ([1, стр. 17], [2, стр. 36]);
5. Шифр Ардженти ([1, стр. 21], [2, стр. 34]);
6. Шифр перестановки и шифр Ришелье ([1, стр. 23], [2, стр. 14]);
7. Шифр Гронсфельда ([1, стр. 26]);
8. Шифр Кепплера и Галилея ([1, стр. 26], [2, стр. 55]);
9. Шифр Вернама ([1, стр. 38], [3, стр. 120]);
10. Шифр Плейфера ([1, стр. 33]);

Требования к выполнению заданий

Доклад (5-7 мин.) представляет собой небольшую презентацию, выполненную в PowerPoint или любом другом аналогичном редакторе. Презентация должна включать

- историю данного шифра;
- описание шифра;
- пример шифрования с его помощью (свой, не из книги);
- возможные алгоритмы его «взлома».

Практическое задание заключается в реализации выбранного шифра на ЭВМ (язык программирования любой). Программа должна иметь понятный пользователю интерфейс; студент должен хорошо ориентироваться в программном коде для того, чтобы он мог выполнить дополнительные задания, предложенные преподавателем.

Реферат должен быть объемом 2-4 страницы (титульный лист не нужен) и обязательно должен включать следующие аспекты:

- кто и когда изобрел алгоритм;
- описание алгоритма;
- псевдокод или код программы;
- где он применялся (применяется);
- почему сейчас не применяется;
- каковы достоинства алгоритма;

какие слабости есть у алгоритма, как можно его «взломать».

Литература

1. Основы криптографии : учеб. пособие для высш. учеб. заведений по гр. специальностям в обл. информ. безопасности / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – 3-е изд., испр. и доп. – М. : Гелиос АРВ, 2005. (МОРФ)
2. Бабаш, А. В. Криптография / Бабаш А. В., Шанкин Г. П. ; под ред. В. П. Шерсюка, Э. А. Применко. - М. : Солон – Пресс, 2007.
3. Рябко, Б. Я. Основы современной криптографии для специалистов по информационным технологиям / Б. Я. Рябко, А. Н. Фионов. – М. : Науч. мир, 2004.

2.2. Методические указания по выполнению курсового проекта

ЦЕЛИ КУРСОВОЙ РАБОТЫ

- научить студентов самостоятельно искать, структурировать и анализировать информацию, связанную с криптографическими алгоритмами и технологиями;
- предоставить студентам возможность выполнить доклад по теме своей работы и получить навыки публичных выступлений.

ПОРЯДОК ВЫПОЛНЕНИЯ КУРСОВОЙ РАБОТЫ

Шаг 1. Выбор темы курсовой работы

Тему курсовой работы студент может выбрать самостоятельно и согласовать ее с преподавателем. Если студент затрудняется с самостоятельным выбором темы, то он может выбрать одну из тех тем, которые предложит преподаватель. Примерные темы работ перечислены в *разделе 3*.

Преподаватель консультирует студента по вопросам, которые касаются курсовой работы. Если у студента возникают объективные непреодолимые трудности при выполнении курсовой работы, то в исключительных случаях (на усмотрение преподавателя) тема может быть изменена.

Шаг 2. Изучение литературы и анализ полученной информации

На этом шаге студент изучает предметную область, соответствующую теме курсовой работы. Производится анализ изучаемых объектов. Для этого производится выбор качественных и количественных характеристик данных объектов, приводится сравнительная таблица. На основании полученных данных делаются выводы, которые отражают важные сходства и различия изученных объектов.

Шаг 3. Подготовка и выполнение доклада

Во время выполнения доклада студент демонстрирует хорошее владение выбранной темой, излагает и описывает основные понятия и алгоритмы. Докладчик приводит результаты проведенного анализа, на основании которых делает выводы и дает рекомендации.

По окончании доклада студент получает замечания от преподавателя и других студентов, отвечает на вопросы. Далее эти вопросы и замечания должны быть учтены при оформлении курсовой работы.

Шаг 4. Оформление курсовой работы

Курсовая работа должна содержать описание проделанной работы и проведенного анализа. Правила оформления курсовой работы и детальное описание каждой из частей дается в *разделе 4*.

Шаг 5. Защита курсовой работы

Студент предоставляет преподавателю курсовую работу в печатном и электронном виде. Также предоставляется презентация в электронном виде. Ознакомившись с работой, преподаватель задает вопросы, делает замечания и выставляет оценку. Критерии оценивания приведены в *разделе 5*.

ПРИМЕРНЫЕ ТЕМЫ КУРСОВЫХ РАБОТ

	Тема	**Некоторые аспекты, на которые нужно обратить внимание**
1	Блочные шифры	Размер блока, размер ключа, количество раундов, сложность криптоанализа, изобретатель шифра, год изобретения, участие шифра в конкурсах, где используется.
2	Поточные шифры	Размер ключа, сложность криптоанализа, изобретатель шифра, год изобретения, участие шифра в конкурсах, где используется.
3	Хеш-функции	Размер хеш-значения, сложность криптоанализа, изобретатель шифра, год изобретения, участие шифра в конкурсах, где используется.
4	Криптоанализ блочных шифров	Методы криптоанализа, авторы этих методов, время изобретения, применение данных методов к шифрам (хеш-функциям), сложности изученных атак.
5	Криптоанализ	

	поточных шифров	
6	Криптоанализ хеш-функций	
7	Коды аутентичности сообщений	Типы кодов, сложность атак на них, как конструируются, какие проблемы решают.
8	Конкурс криптоалгоритмов NESSIE	Участники конкурса, финалисты, победители, опубликованные работы, итоги конкурса, время проведения, кто проводил.
9	Конкурс блочных шифров AES	
10	Конкурс поточных шифров eStream	
11	Проект CRYPTREC	
12	Конкурс SHA-3	
13	Цифровая подпись	Зачем нужна цифровая подпись, какие виды существуют, как их анализировать и строить атаки на них, кто из ученых приложил усилия для их исследования.
14	Криптосистемы на эллиптических кривых	Сравнение с обычными криптосистемами, какие системы существуют, сложность их использования и криптоанализа, авторы криптосистем, исследователи криптосистем.
15	Криптография в электронной коммерции и электронные деньги	Методы, проблемы, сферы применения.
16	Криптосистемы с открытым ключом	Какие существуют, какие лучше, какие хуже, где используются, какие задачи решают.
17	Исторические шифры	Сравнительные анализ, методы их криптоанализа, где и когда использовались.
18	Случайные числа	Методы их генерации и тестирования, сложность этих методов, рекомендации к применению.
19	Кодирование информации	Постановка задачи, методы, проблемы.
20	Сжатие информации	Постановка задачи, методы сжатия, сложность, эффективность.
21	Криптографические библиотеки в современных языках программирования	Какие алгоритмы включаются, почему, как используются, простота использования.
22	Стеганография	Что это, методы стеганографии, цифровая стеганография, историческая стеганография.
23	Стегоанализ	Методы стегоанализа, авторы, годы изобретения.
24	Простые числа	Методы их генерации и тестирования, сложность этих методов, рекомендации к применению.
25	Обзор программ для подбора паролей	Какие, как пользоваться, время подбора, как защититься, какие пароли можно подобрать и т.д.
26	Проблема распределения	Методы распределения ключей, авторы методов, проблемы.

	ключей	
27	Доказательство с нулевым знанием (с нулевым разглашением)	Постановка задачи, примеры таких доказательств, сложность.
28	Методы факторизации	Постановка задачи, где применяется, сложность методов, сравнение.
29	Методы дискретного логарифмирования	
30	Российские ГОСТы на криптоалгоритмы	Какие криптоалгоритмы стандартизуются, их криптоанализ, сложность, авторы.

ПРАВИЛА НАПИСАНИЯ КУРСОВОЙ РАБОТЫ

Общие требования по оформлению работы

Курсовой проект должен соответствовать требованиям внутренних стандартов НГУЭиУ (НИНХ). Содержание курсового проекта должно соответствовать дисциплине, преподаваемой в соответствии с государственным образовательным стандартом.

Текст работы необходимо подготовить с использованием текстового процессора Microsoft Word. Рекомендуется использовать шрифт Times New Roman (размер шрифта для основного текста 12 pt, интервал “обычный”), выравнивание абзацев «по ширине», размер полей: верхнего, нижнего, левого – 2 см; правого – 3,5 см. Страницы должны быть пронумерованы, в тексте следует выделять подзаголовки (в соответствии с содержанием работы).

Общий объем работы без приложений 20-30 страниц.

Требования к отдельным разделам курсовой работы

Титульный лист

Титульный лист оформляют в соответствии с образцом, приведенном в *приложении 1*. Титульный лист подписывает автор и руководитель курсового проекта. Фамилии лиц, подписывающих работу, приводятся справа от соответствующих подписей.

Содержание

Содержание включает порядковые номера и наименования основных разделов (при необходимости подразделов) работы, приложений с указанием их обозначения и заголовков. В правой стороне листа указывают номера страниц, с которых начинается та или иная часть работы.

Введение

Введение не нумеруют и размещают на отдельном листе. Во введении необходимо дать общее представление о том, какие проблемы решают изучаемые объекты. Назвать людей, которые приложили усилия к их разработке, указать важнейшие даты.

Основная часть

Основная часть содержит обстоятельный обзор с анализом по теме работы. Вырабатываются критерии, по которым оцениваются изучаемые объекты, приводятся сравнительные таблицы и графики. На основании исследований указываются достоинства и недостатки изучаемых объектов, даются рекомендации к их использованию в зависимости от возникшей ситуации.

Заключение

Как и введение, заключение не нумеруют. Его объем должен составлять 1-2 абзаца. В заключении описывается проделанная работа и перечисляются результаты проведенного анализа.

Список литературы

В список литературы включают все использованные при выполнении курсовой работы источники. Список дают в алфавитном порядке в соответствие с ГОСТ 7.1.84 (см. *Приложение 2*).

Приложения

Материал, дополняющий содержание курсового проекта размещают в приложениях. Это могут быть аналитические таблицы большого формата, графические и справочные материалы, описания алгоритмов и тексты программ, структурные и функциональные диаграммы, другая проектная документация.

КРИТЕРИИ ОЦЕНИВАНИЯ КУРСОВОЙ РАБОТЫ

Преподаватель оценивает по 4-х балльной системе (2, 3, 4, 5):

1. Презентация;
2. Ответы на вопросы после доклада;
3. Оформление курсовой работы;
4. Защита курсовой работы;
5. График выполнения курсовой работы.

Баллы суммируются, и итоговая оценка вычисляется так:

Количество баллов	**Итоговая оценка**
23, 24, 25	Отлично
19, 20, 21, 22	Хорошо
14, 15, 16, 17, 18	Удовлетворительно
10, 11, 12, 13	Неудовлетворительно

РАЗДЕЛ 3. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПОДГОТОВКЕ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Видом промежуточной аттестации студентов являются зачет и экзамен.

3.1. Список вопросов для подготовки к зачету

20. В чем принципиальное отличие современной криптографии от исторической криптографии?
21. Перечислите основных действующих лиц в криптографии.
22. Приведите примеры проблем, возникающих при передаче информации.
23. Опишите алгоритм и математическую формулу работы шифра Цезаря.
24. Опишите классическую схему секретной связи Шеннона.
25. Сформулируйте принцип Керкхоффса и объясните, зачем он нужен?
26. Опишите метод полного перебора ключей применительно к шифру Цезаря и оцените его сложность.
27. Что такое избыточность?
28. Объясните, что такое атака по шифротексту, по известному открытому тексту и выбранному открытому тексту.
29. Что такое асимметричные криптосистемы или криптосистемы с открытым ключом?
30. Опишите проблему хранения паролей в компьютере и проблему ПВО.
31. Дайте определение односторонней функции.
32. Дайте определение дискретного логарифма.
33. Объясните, как выполнить дискретное логарифмирование методом полного перебора.
34. Опишите идею алгоритма быстрого возведения в степень по модулю.
35. Опишите алгоритм быстрого возведения в степень по модулю и приведите пример.
36. Какова сложность алгоритма быстрого возведения в степень по модулю? Почему?
37. Объясните, как решается проблема хранения паролей и проблема ПВО с использованием односторонних функций.
38. Объясните, почему в ряде случаев использование секретных ключей проблематично. Приведите пример.
39. Какова цель системы Диффи-Хеллмана?
40. Как выбираются параметры p и g в системе Диффи-Хеллмана?
41. Опишите систему Диффи-Хеллмана. Приведите пример.
42. Обоснуйте, почему ключи, вычисляемые абонентами при помощи системы Диффи-Хеллмана, совпадут.
43. Почему Ева не может тоже вычислить ключ, получаемый при помощи

системы Диффи-Хеллмана?

44. Дайте определения простого числа и взаимно простых чисел. Приведите пример.
45. Сформулируйте основную теорему арифметики. Приведите примеры.
46. Дайте определение функции Эйлера. Приведите примеры.
47. Чему равна функция Эйлера от простого числа? Почему?
48. Чему равна функция Эйлера от произведения простых чисел? Почему?
49. Сформулируйте теорему Ферма и теорему Эйлера. Приведите примеры.
50. Что такое псевдопростое число по заданному основанию?
51. Дайте определение наибольшего общего делителя двух чисел.
52. Опишите алгоритм Евклида. Приведите пример. Опишите его рекурсивную и нерекурсивную реализацию.
53. Приведите постановку задачи, которую решает обобщенный (расширенный) алгоритм Евклида.
54. Опишите обобщенный алгоритм Евклида. Приведите пример.
55. Дайте определение инверсии. Приведите пример.
56. Где применяются инверсии в криптографии?
57. Как свести задачу вычисления инверсии к обобщенному алгоритму Евклида?
58. Как вычислить инверсию при помощи обобщенного алгоритма Евклида?
59. Чему приближенно равно количество простых чисел, не превосходящих заданное число? Приведите пример.
60. Объясните, как выбираются параметры для шифра Шамира.
61. Опишите шифр Шамира. Приведите пример.
62. Обоснуйте корректность и стойкость шифра Шамира.
63. Объясните, как выбираются параметры для шифра Эль-Гамаля.
64. Опишите шифр Эль-Гамаля. Приведите пример.
65. Обоснуйте корректность и стойкость шифра Эль-Гамаля.
66. Объясните, как выбираются параметры для шифра RSA.
67. Опишите шифр RSA. Приведите пример.
68. Обоснуйте корректность и стойкость шифра RSA.
69. Что такое односторонняя функция с лазейкой? Опишите эту лазейку.
70. В чем заключается недостаток шифра RSA?
71. В чем преимущества шифра RSA перед шифрами Шамира и Эль-Гамаля?
72. Приведите постановку задачи дискретного логарифмирования.
73. Какие методы дискретного логарифмирования существуют? Какова их сложность?
74. Приведите постановку задачи, которую решает метод «Шаг-младенца-шаг великана».

75. Опишите метод «Шаг младенца-шаг великана». Приведите пример.
76. Какова сложность метода «Шаг младенца-шаг великана»? Почему?
77. Какие требования предъявляются к цифровой подписи?
78. Опишите цифровую подпись RSA. Приведите пример.
79. Как выбираются параметры для цифровой подписи RSA?
80. Обоснуйте корректность и стойкость подписи RSA.
81. Опишите цифровую подпись Эль-Гамаля. Приведите пример.
82. Как выбираются параметры для цифровой подписи Эль-Гамаля?
83. Обоснуйте корректность и стойкость подписи Эль-Гамаля.

3.1. Список вопросов для подготовки к экзамену

1. См. все вопросы для подготовки к зачету.
2. Какие требования предъявляются к виртуальной раздаче карт.
3. Опишите проблему подбрасывания монеты по телефону.
4. Опишите протокол подбрасывания монеты по телефону.
5. Как выбрать параметры для протокола ментального покера?
6. Опишите протокол ментального покера. Приведите пример.
7. Обоснуйте корректность протокола ментального покера.
8. Что такое доказательство с нулевым знанием?
9. Что такое проблема «Большого брата»?
10. Какие требования предъявляются к протоколу электронных денег?
11. Опишите протокол Чаума. Приведите пример.
12. Каковы недостатки системы Диффи-Хеллмана?
13. Опишите протокол Нидхама-Шредера. Приведите пример.
14. Опишите шифр Вернама. Приведите пример.
15. Какое главное достоинство и главный недостаток шифра Вернама?
16. Дайте определение энтропии. Приведите пример. Постройте график двоичной энтропии.
17. Что такое блочный шифр? Какие параметры есть у него?
18. Назовите 3-4 блочных шифра. Чему равны их параметры?
19. Назовите режимы использования блочных шифров.
20. Что такое поточный шифр?
21. Почему возникает проблема синхронизации поточных шифров?
22. Назовите 3-4 поточных шифра.
23. Опишите шифр RC4.
24. Зачем нужны случайные числа в криптографии?
25. Что такое генератор псевдослучайных чисел?

26. Какие методы получения псевдослучайных последовательностей существуют?
27. Что такое статистический тест?
28. Назовите 3-4 статистических теста или критерия.
29. Опишите методы «очищения» псевдослучайных последовательностей Фон Неймана и Элайеса.
30. Дайте определение хеш-функции.
31. Дайте определение криптографической хеш-функции.
32. Что такое коллизия? Какие коллизии существуют?
33. Что такое «парадокс дней рождений»?
34. Что такое хеш-функция, задаваемая ключом?
35. Что такое бесключевая хеш-функция?
36. Как построить хеш-функцию на основе блочного шифра?
37. Назовите 3-4 криптографические хеш-функции.
38. Какие возможные атаки на хеш-функции существуют?
39. Назовите некоторые особенности использования вычислительной техники в криптографии.
40. Какие физические и организационные меры при использовании шифрсистем существуют?
41. Реализуйте изученные теоретико-числовые алгоритмы на ЭВМ.
42. Реализуйте какие-либо блочные шифры на ЭВМ.
43. Реализуйте изученные криптографические протоколы на ЭВМ.
44. Назовите российские и зарубежные стандарты на шифры с секретным ключом и хеш-функции.
45. Какие задачи в криптографии решаются при помощи хеш-функций?
    Назовите некоторые шифрсистемы с открытыми и секретными ключами.

3.2. Общие положения проведения зачета и экзамена

К зачету допускаются студенты, сдавшие все лабораторные работы.

На экзамене студенты получают три вопроса: теоретический, письменную задачу и практическое задание. Итоговая оценка ставится за выполнение всех заданий.

Приложение 1

Типовая форма титульного листа курсового проекта

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ЭКОНОМИКИ И УПРАВЛЕНИЯ «НИНХ»

Институт Прикладной информатики

Кафедра Информационной безопасности

КУРСОВОЙ ПРОЕКТ

_____

Учебная дисциплина: Криптографические методы защиты информации
Наименование направления: 090900.62 «Информационная безопасность
Ф.И.О студента: _____
Номер группы: _____
Номер зачетной книжки: _____
Дата регистрации курсового проекта кафедрой _____

Проверил: _____

Оценочное заключение:

Новосибирск 2011