10.02.05.01.МДК.02-2020-РП

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

УТВЕРЖДАЮ
Директор
_____ ..
«___»_____ 20__ г.

Фонд оценочных средств дисциплины

Криптографические средства защиты информации

Направление подготовки 10.02.05 Обеспечение информационной безопасности автоматизированных систем
Направленность (профиль) Техник по защите информации (9 кл)

Присваиваемая квалификация
"Техник по защите информации"

Формы обучения
очная

1 Паспорт фонда оценочных средств

№	Наименование разделов дисциплины	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
1	Введение. Предмет и задачи криптографии. История криптографии. Основные термины.	ОК 02.	Знать: источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач; Уметь: использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;	опрос обучающихся по контрольным вопросам, тестирование,
		ОК 03.	Знать: способы демонстрации принятых решений; Уметь: обосновывать, анализировать и корректировать результаты собственной работы;	
		ОК 04.	Знать: принципы работы в коллективе и команде, способы эффективного взаимодействия с коллегами, руководством, клиентами; Уметь: обосновать и анализировать работу членов команды (подчиненных);	
		ОК 05.	Знать: грамматику русского языка; Уметь: ясно формулировать и излагать мысли;	

2	Раздел 1. Математические основы защиты информации	ОК 07.	Знать: правила техники безопасности, ресурсосберегающие технологии в области телекоммуникаций; Уметь: использовать ресурсосберегающие технологии в области телекоммуникаций;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 08.	Знать: способы укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности; Уметь: выполнять правила техники безопасности для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;	
		ПК 2.4.	Знать: основные понятия криптографии и типовых криптографических методов и средств защиты информации; Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; Иметь практический опыт: применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;	

3	Раздел 2. Классическая криптография	ОК 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 09.	Знать: информационно-коммуникационные технологии профессиональной деятельности; Уметь: использовать информационные технологии в профессиональной деятельности;	
		ПК 2.4.	Знать: основные понятия криптографии и типовых криптографических методов и средств защиты информации; Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; Иметь практический опыт: применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;	

4	Раздел 3. Современная криптография	ОК 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 06.	Знать: современный этикет; Уметь: соблюдать нормы поведения и правила этикета;	
		ОК 10.	Знать: способы использования профессиональной документации; Уметь: использовать в профессиональной деятельности необходимую техническую документацию, в том числе на английском языке;	
		ПК 2.4.	Знать: основные понятия криптографии и типовых криптографических методов и средств защиты информации; Уметь: применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись; Иметь практический опыт: применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;	

2 Типовые контрольные задания или иные материалы

2.1 Оценочные средства при текущем контроле

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании.

Опрос по контрольным вопросам:

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Что такое шифрование?
2. Что такое кодирование?

Критерии оценивания:

- 85–100 баллов – при правильном и полном ответе на два вопроса;
- 65–84 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 25–64 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-24	25-64	65-84	85-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень контрольных вопросов:

Введение. Предмет и задачи криптографии. История криптографии. Основные термины.

1. Что такое шифрование?
2. Что такое кодирование?
3. Что изучает криптография?
4. Когда были известны первые алгоритмы шифрования?
5. Что такое криптостойкость?

Раздел 1. Математические основы защиты информации
Тема 1.1. Математические основы криптографии

1. Какую математическую функцию относительно легко вычислить, но трудно найти соответствующее значение аргумента?
2. Какие из разделов математики легли в основу современных методов криптографии?
3. Как называется наука, предметом которой являются математические способы преобразования информации с целью ее защиты от несанкционированных пользователей?
4. С каким алфавитом принято работать в теоретической криптографии ?
5. Какие виды математических последовательностей используются в криптографии?

Раздел 2. Классическая криптография
Тема 2.1. Методы криптографического защиты информации

1. Что представляет собой криптографическая система?
2. Что принято называть электронной подписью?
3. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?
4. Какими свойствами должен обладать генератор псевдослучайных чисел (ГПСЧ) для использования в криптографических целях?
5. Как называется криптографический алгоритм, в котором ключ, используемый для шифрования сообщений, может быть получен из ключа дешифрования и наоборот?

Тема 2.2. Криптоанализ

1. Какова цель криптоанализа?
2. С использованием каких инструментов позволяет раскрыть секретные сообщения криптоанализ ?
3. От чего зависит секретность сообщения по мнению О. Кирхгоффа?
4. Какие методы криптоанализа применяются для ассиметричных шифров?
5. Какие методы криптоанализа применяются для симметричных шифров?

Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел

1. Как поточный шифр выполняет преобразование входного сообщения?
2. Какими свойствами должен обладать генератор псевдослучайных чисел для использования в криптографических целях ?
3. Какой из генераторов псевдослучайных чисел является наиболее простым?
4. Какой алгоритм используется для шифрования паролей в ОС Windows, а также в протоколе SSL?
5. На чем основан принцип действия всех генераторов псевдослучайных чисел?

Раздел 3. Современная криптография
Тема 3.1. Кодирование информации. Компьютеризация шифрования.

1. Что представляет собой кодирование информации?
2. В чем заключается общая идея помехоустойчивого кодирования?
3. Какие коды используются в помехоустойчивом кодировании?
4. Какими свойствами обладает процедура шифрования данных?
5. Как называется ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст?

Тема 3.2. Симметричные системы шифрования

1. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования?
2. Какой алгоритм, использует симметричный ключ и алгоритм хэширования?
3. Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования?

4. Какой размер ключа в отечественном стандарте симметричного шифрования?

Тема 3.3. Асимметричные системы шифрования

1. В чем основные преимущества и недостатки асимметричных криптосистем?
2. Сколько используется ключей в асимметричных криптосистемах для шифрования и дешифрования?
3. Какими свойствами секретности должны обладать ключи в асимметричных системах шифрования?
4. Какие шифры (механизмы обмена ключами) относятся к асимметричным?
5. Какая связь существует между двумя ключами в асимметричной криптографии?

Тема 3.4. Аутентификация данных. Электронная подпись

1. Какие методы разрабатываются с целью обеспечения аутентификации?
2. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?
3. Какие существуют системы аутентификации и распределения ключей?
4. Что принято называть электронной (цифровой) подписью?
5. Что используют для создания цифровой подписи

Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации

1. Позволяет ли обмениваться ключами по незащищенным каналам связи Метод Диффи-Хеллмана?
2. Применяется ли для распределения ключей между пользователями информационной системы прямой обмен ключами между пользователями сети?
3. Как называют процесс согласования сессионного ключа в процессе информационного обмена ?
4. Какие существуют протоколы аутентификации?
5. Сколько шагов предусматривает аутентификация с помощью протокола Kerberos версии 5 ?

Тема 3.6. Криптозащита информации в сетях передачи данных

1. Что такое линейное шифрование?
2. Какой шифратор можно использовать для защиты передаваемой в Сеть информации?
3. Какой основной механизм обеспечивает конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе по сети Интернет?
4. Какие из приведенных криптографических алгоритмов используют в основе сетей Фейстеля?
5. Каким образом наиболее просто можно осуществить распределение ключей для сетей с большим количеством абонентов?

Тема 3.7. Защита информации в электронных платежных системах

1. Какие механизмы защиты должны быть реализованы для обеспечения функций защиты информации на отдельных узлах электронной платежной системы?
2. Какой протокол передачи данных обеспечивает лучшую защиту в системах электронных платежей?
3. Каковы преимущества и недостатки протокола SSL?
4. Какие ключи используются в протоколе SET?
5. Какой набор функций обеспечивает смарт-карта ?

Тема 3.8. Компьютерная стеганография

1. Что может являться файлом – контейнером для стеганографии?
2. Что такое метод LSB в стеганографии ?
3. Какие принципы лежат в основе стеганографии?
4. Что скрывает стеганография?
5. Что такое стеганографическая система или стегосистема?

Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате

Содержание отчета:

1.Тема работы.

2. Задачи задания.

4. Краткое описание хода выполнения.

5. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

6. Выводы

Критерии оценивания:

- 75 – 100 баллов – при раскрытии всех разделов в полном объеме

- 0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

Процедура защиты отчетов по заданиям:

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Какие принципы лежат в основе стеганографии?
2. Что скрывает стеганография?

Критерии оценивания:

- 85–100 баллов – при правильном и полном ответе на два вопроса;

- 65–84 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 25–64 баллов – при правильном и неполном ответе только на один из вопросов;

- 0–24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-24	25-64	65-84	85-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень заданий:

1.Задание к практическому занятию 1.1.1. Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений

1. Найти НОД двух натуральных чисел, используя алгоритм Евклида делением
2. Найти НОД двух натуральных чисел, используя алгоритм Евклида вычитанием
3. Решить диофантово уравнение с помощью алгоритма Евклида: 23x+4y-7x=-3y+15

Результаты зафиксировать в отчете.

2. Задание к практическому занятию 1.1.2. Проверка чисел на простоту

1. Рассмотреть процедуру проверки чисел на простоту с помощью тестов Ферма и Миллера-Рабина.
2. Рассмотреть схему нахождения наибольшего общего делителя с использованием расширенного алгоритма Эвклида.
3. Реализовать программно тест Ферма. Проверить на простоту целые числа в диапазоне [3,200].
4. Реализовать программно тест Миллера-Рабина. Проверить на простоту целые числа в диапазоне [3,200].
5. Реализовать программно расширенный алгоритм Эвклида. Найти наибольший общий делитель чисел, заданных преподавателем. Сделать вывод об их взаимной простоте.

Результаты зафиксировать в отчете.

3. Задание к практическому занятию 1.1.3. Решение задач с элементами теории чисел.

1. После деления двузначного числа на сумму его цифр в частном получается 7, а в остатке 6. После деления этого же числа на произведение его цифр в частном получается 3, а в остатке 11. Найдите это число.
2. Ученик перемножил два данных натуральных числа и допустил ошибку, увеличив произведение на 372. Поделив для проверки полученный результат на меньшее из данных чисел, ученик правильно получил в частном 90 и в остатке 29. Найдите данные числа.
3. На факультет подано от не медалистов на 600 заявлений больше, чем от медалистов. Девушек среди не медалистов больше, чем среди медалистов, в 5 раз, а юношей среди не медалистов больше, чем среди медалистов, в n раз, где n – натуральное число и . Найдите общее число заявлений, если среди медалистов юношей на 20 больше, чем девушек.
4. Ваня задумал простое трехзначное число, все цифры которого различны. На какую цифру оно может оканчиваться, если его последняя цифра равна сумме первых двух.

Результаты зафиксировать в отчете.

4. Задание к практическому занятию 2.1.1. Применение классических шифров замены

1. Создать программу, реализующую процесс шифрования/дешифрования текста по следующим алгоритмам: a. аддитивный моноалфавитный шифр с задаваемым смещением; b. мультипликативный моноалфавитный шифр с задаваемым смещением; c. шифр Плейфера. Разрабатываемая подпрограмма использует только алфавит абвгдеёжзийклмнопрстуфхцчшщъьыэюя
2. Провести частотный анализ символов зашифрованного текста для аддитивного и мультипликативного шифров. Вывести полученный числовые значения на экран.
3. С помощью полученной частоты встречаемости символов вручную провести и описать процесс дешифрование первых 15 символов зашифрованного сообщения.

Результаты зафиксировать в отчете.

5. Задание к практическому занятию 2.1.2. Применение классических шифров перестановки

1. Создать программу, реализующую процесс шифрования/дешифрования текста по изученным шифрам перестановки. Разрабатываемая подпрограмма использует только алфавит:

абвгдеёжзийклмнопрстуфхцчшщъьыэюя_,. АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЭЮЯ

При использовании шифра перестановки с ключом длина ключа и сам ключ должны задаваться пользователем. Длина исходного текста должна быть не менее 10000 символов.

Подсчет количества символов должен быть осуществлен самой программой и выведен в поле для ввода.

2. Создать подпрограмму, определяющую ключ шифрования для закрытого текста, зашифрованного комбинированным шифром. Правильность подобранного ключа определяется пользователем. Если ключ подобран неверно, то пользователь отвергает его и отправляет команду на подбор следующего значения ключа. Количество символов в зашифрованном тексте никак не ограниченно.

3. Дешифровать закрытые тексты заданий своего варианта. При шифровании использовался шифр с перестановками по ключу. Дешифрование можно выполнить как вручную, так и программно.

Задан шифртекст:

чбюЛтюолянн и з,уаосрон нтоюлбюь вю !
би оНдеепрсе тс аем.о уйдок
а, лНаивсеаул нкнпв,кояю ьр
лй оНыинпо од оггрипврд ояе о,о к й
мй еНоинти тр ыснан втзеаыен еапярьд
вя еНлеешм в те нонордготоааяет ьмнч

Результаты зафиксировать в отчете.

6. Задание к практическому занятию 2.1.3. Применение метода гаммирования

1. Выберите метод получения гаммы шифра (псевдослучайной последовательности чисел).
2. Реализуйте программный модуль в соответствии с полученным заданием.

При реализации необходимо учесть следующие моменты:

1) предусмотреть возможность задания пользователем гаммы шифра;

2) предусмотреть визуализацию всех пользовательских настроек;

3) для удобства тестирования и взаимодействия с другими модулями реализовать файловый ввод исходных данных и файловый вывод результата криптографического преобразования.

3. После реализации программного модуля выполните статистический анализ текста до криптографического преобразования и после него.

Варианты заданий:

1. Модуль для шифрования текста гаммированием по модулю.
2. Модуль для расшифровывания текста гаммированием по модулю.
3. Модуль для шифрования текста двоичным гаммированием.
4. Модуль для расшифровывания текста двоичным гаммированием.

Результаты зафиксировать в отчете.

7. Задание к практическому занятию 2.2.1. Криптоанализ шифра простой замены методом анализа частотности символов

1. Получить от преподавателя текстовый файл, содержащий большой художественный текст на русском языке в открытом виде.
2. С помощью программы «Частота символов» исследуйте частотность символов открытого теста.

3. Внести полученную статистику в отчет по работе (первые 15-20 символов). Пример отчета приведен на последней странице.
4. Получить от преподавателя текстовый файл, содержащий большой объем зашифрованного текста на русском языке.
5. Исследовать частотность зашифрованного текста и внести ее в отчет в виде, аналогичном пункту 2 (первые 15-20 символов).
6. Сравнивая реальную частотность символов русского языка, полученную в пункте 2, с частотностями зашифрованного текста, составить таблицу замен алгоритма шифрования и расшифровать зашифрованный текст, реализовав программу дешифровки. Дешифровке подвергните только первые 15-20 символов, наиболее часто встречающиеся в шифротексте. Сформированную таблицу замен внести в отчет по работе.
7. Выполнить эвристический анализ текста, полученного в результате дешифровки. По смыслу текста выявить те замены, которые оказались неверными, и сформировать верные замены. Доведите результат дешифровки до приемлемого (удобочитаемого) вида. Окончательную таблицу замен (с учетом эвристических подмен) внести в отчет по работе.

Результаты зафиксировать в отчете.

8. Задание к практическому занятию 2.2.2. Криптоанализ классических шифров методом полного перебора ключей

1. Выбрать шифротекст для своего варианта
2. Сформировать таблицу биграмм для эталонного текста на русском языке
3. Разработать программу для полного перебора ключей длины 3 в шифре Виженера и оценки вероятности для каждого расшифрованного исходного текста
4. Найти 10 расшифрованных строк с самой большой оценкой вероятности
5. Расшифровать шифротекст

Результаты зафиксировать в отчете.

9. Задание к практическому занятию 2.2.3. Криптоанализ шифра Вижинера

Используем Excel.

1. Выбрать значение ключа шифрования и криптограмму из табл. 1.10 в соответствии с номером варианта (от 1 до 26).
2. Расшифровать криптограмму выбранным ключом:
3. ввести текст криптограммы побуквенно в ячейки строки отформатированной области; важно, чтобы символы алфавита в таблице и символы вводимого слова были набраны в одном регистре;
4. строкой ниже получить числовой код символов шифруемого слова с помощью функции ВПР;
5. строкой ниже сформировать ключевую строку;
6. строкой ниже получить числовой код символов ключевой строки с помощью функции ВПР;
7. строкой ниже получить код символа открытого текста, вычтя по модулю 33 код текущего символа ключевой строки из кода текущего символа криптограммы, используя функцию ОСТАТ (рис. 1.44);
8. строкой ниже с помощью функции ВПР перевести полученный код криптограммы в символьный вид. Критерием правильности расшифрования является получение осмысленного слова.

Результаты зафиксировать в отчете.

10. Задание к практическому занятию 2.3.1. Применение методов генерации ПСЧ

Требуется Excel

1. Выбрать значения параметров BBS-генератора p, q и случайное число s согласно номеру варианта. Сформировать псевдослучайную последовательность.
2. В приложении MS Excel создать новую книгу, на первом листе ввести значения p, q, вычислить число Блюма п как их произведение, например =B1*B2. Ниже ввести значение случайного числа x.
3. Рассчитать элементы ряда x': • пронумеровать ячейки первого столбца от 0 до 7; • в первую ячейку второго столбца ввести формулу для вычисления x0 по формуле x0 = s'2 mod и, например =ОСТАТ(B4Л2;B3); • скопировать формулу на весь ряд.
4. Вычислить младшие биты чисел xг Значение младшего бита определяется остатком от деления числа на 2, поэтому для вычисления можно использовать функцию ОСТАТ, например =ОСТАТ(B5;2) для числа x0. Скопировать формулу на все ячейки диапазона.
5. Сформировать результирующую битовую псевдослучайную последовательность с помощью операции &, например =C5&C6&C7&C8&C9&C10& C11&C12, или функции СЦЕПИТЬ из группы Текстовые,

например =СЦЕПИТЬ(C5;C6;C7;C8;C9;C10;C11;C12). Значение результирующей последовательности: 11101111.

Результаты зафиксировать в отчете.

11. Задание к практическому занятию 3.1.1. Кодирование информации

1. Закодируйте свое имя, фамилию и отчество с помощью одной из таблиц (win-1251, KOI-8)

2. Раскодируйте ФИО соседа

3. Закодируйте следующие слова, используя таблицы ASCII-кодов: ИНФОРМАТИЗАЦИЯ, МИКРОПРОЦЕССОР, МОДЕЛИРОВАНИЕ

4. Раскодируйте следующие слова, используя таблицы ASCII-кодов:

88 AD E4 AE E0 AC A0 E2 A8 AA A0

50 72 6F 67 72 61 6D

43 6F 6D 70 75 74 65 72 20 49 42 4D 20 50 43

5. Текстовый редактор Блокнот

- Используя клавишу Alt и малую цифровую клавиатуру раскодировать фразу: 145 170 174 224 174 255 170 160 173 168 170 227 171 235;

Технология выполнения задания: При удерживаемой клавише Alt, набрать на малой цифровой клавиатуре указанные цифры. Отпустить клавишу Alt, после чего в тексте появится буква, закодированная набранным кодом.

- Используя ключ к кодированию, закодировать слово – зима;

Технология выполнения задания: Из предыдущего задания выяснить, каким кодом записана буква а. Учитывая, что буквы кодируются в алфавитном порядке, выяснить коды остальных букв.

6. Текстовый процессор MS Word.

Технология выполнения задания: рассмотрим на примере: представить в различных кодировках слово Кодировка

- Создать новый текстовый документ в Word;
- Выбрать – Команда – Вставка – Символ.
- В открывшемся окне «Символ» установить из: Юникод (шестн.),
- В наборе символов находим букву К и щелкнем на ней левой кнопкой мыши (ЩЛКМ).
- В строке код знака появится код выбранной буквы 041A (незначащие нули тоже записываем).
- У буквы о код – 043E и так далее: д – 0434, и – 0438, р – 0440, о – 043E, в – 0432, к – 043A, а – 0430.
- Установить Кириллица (дес.)
- К – 0202, о – 0238, д – 0228, и – 0232, р – 0240, о – 0238, в –0226, к – 0202, а –0224.

7. Открыть Word.

- Используя окно «Вставка символа» выполнить задания: Закодировать слово Forest
- Выбрать шрифт Courier New, кодировку ASCII(дес.) Ответ: 70 111 114 101 115 116
- Выбрать шрифт Courier New, кодировку Юникод(шест.) Ответ: 0046 006F 0072 0665 0073 0074
- Выбрать шрифт Times New Roman, кодировку Кирилица(дес.) Ответ: 70 111 114 101 115 116
- Выбрать шрифт Times New Roman, кодировку ASCII(дес.) Ответ: 70 111 114 101 115 116

Результаты зафиксировать в отчете.

12. Задание к практическому занятию 3.1.2. Программная реализация классических шифров

1. Разработать программу для шифрования и расшифровывания текста при помощи шифра перестановки или шифра замены. Программа должны обеспечивать:

- задание в командной строке режима работы (шифрование/расшифрование), имени входного файла, имени результирующего файла;
- ввод ключа шифрования/расшифрования с клавиатуры;
- шифрование информации, находящейся в текстовом файле, с записью результата в другой файл.

2. Зашифровать и расшифровать файл, с использованием разработанной программы.

Результаты зафиксировать в отчете.

13. Задание к практическому занятию 3.1.3.Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.

1. Для выполнения работы запускаем программу L_Lux.exe. После открытия главного окна программы определяем установленное в программе смещение для одноалфавитного метода с фиксированным смещением. При определении смещения после шифрования на гистограмме видно

строка считывается побуквенно и каждый символ имеющийся в этой строке увеличивается на 3. То есть а+3=г. Дешифрование происходит так же, как и шифрование только зашифрованная строка считывается побуквенно, представляется в массив и каждый элемент массива подменяется на другой элемент: а=г-3.

2. Для одноалфавитного метода шифрования с заданным смещением зашифровать, расшифровать текст и сравнить гистограммы. Расшифровка текста методом подбора смещения. Определим смещение методом подбора смещения для дешифрования исходного текста.

Искомый текст (смещение 8)

Дешифрование методом подбора (смещение 6)

Дешифрование методом подбора (смещение 4)

Дешифрование методом подбора (смещение 2)

3. Дешифровать зашифрованный текст методом постановки, вычислить закономерность перестановки символов. Данный метод заключается в том, что вся строка разбивается на блоки (от 1 до 9 символов) и символы в каждом блоке располагаются в определенной последовательности. В данном случае строка разбилась на блоки по 2 символа которые расположены в порядке 2 символ 1 символ.

4. Инверсное кодирование (по дополнению до 255). Как показано на рисунке нижу будет зашифрован данный текст (данная строка). Инверсный метод потому, что все символы строки обрабатываются и выводятся в обратном порядке как показано на диаграмме выше. Данный метод шифрования, является частным случаем одноалфавитной замены в алфавите мощности 256. Суть метода заключается в замене символа ASCII-кодировки с номером i на символ с номером 255-i. Аналогично проводится и операция дешифрования.

Результаты зафиксировать в отчете.

14. Задание к практическому занятию 3.2.1. Изучение программной реализации современных симметричных шифров

1.Ознакомьтесь с теоретическими основами блочного симметричного шифрования в конспектах лекций.

2.Получите вариант задания у преподавателя.

3.Напишите программу согласно варианту задания.

4.Отладьте разработанную программу и покажите результаты работы программы преподавателю.

Содержание отчета

- название и цель работы;
- вариант задания;
- листинг разработанной программы с комментариями;
- результаты работы программы.

Результаты зафиксировать в отчете.

15. Задание к практическому занятию 3.3.1. Применение различных асимметричных алгоритмов

В ОС Windows должны быть созданы две учетных записи: User1 и User2

1. Работая под первой учетной записью, запросите сертификат (если он не был получен ранее), после чего зашифруйте папку с любым тестовым файлом с помощью стандартных средств ОС - EFS. Проверьте, что будет происходить при добавлении файлов, переименовании папки, копировании ее на другой диск с файловой системой NFTS на том же компьютере, копировании папки на сетевой диск или диск с FAT.
2. Убедитесь, что другой пользователь не сможет прочитать зашифрованный файл.
3. Снова зайдите под первой учетной записью. В оснастке Certificates, удалите сертификат пользователя (несмотря на выдаваемые системой предупреждения). Завершите сессию пользователя в системе и войдите заново. Попробуйте открыть зашифрованный файл.
4. Зайдите в систему под встроенной учетной записью администратора и расшифруйте папку.

Результаты зафиксировать в отчете.

16. Задание к практическому занятию 3.3.2. Изучение программной реализации асимметричного алгоритма RSA

1. Реализовать программу для шифрования / дешифрования текстов, работающую по алгоритму RSA. Реализовать приложение для шифрования/ дешифрования, позволяющее вычислять открытый и закрытый ключи для алгоритма RSA:

1) числа p и q генерируются программой или задаются из файла;

2) числа p и q должны быть больше, чем 2128;

3) сгенерированные ключи сохраняются в файлы: открытый ключ – в один файл, закрытый – в другой.

4) исходный и зашифрованный тексты хранятся в файлах

2. Преподавателю демонстрируется работающая программа и предоставляется печатный отчёт. Отчёт содержит оформленный согласно требованиям код программы и несколько результатов работы программы. Необходимо объяснить принцип работы алгоритма при защите работы.
Результаты зафиксировать в отчете.

17. Задание к практическому занятию 3.4.1. Применение различных функций хеширования, анализ особенностей хешей

1. Реализовать приложение с графическим интерфейсом, позволяющее выполнять следующие действия.

1.1. Вычислять значение хэш-функции, заданной в варианте:

1) текст сообщения должен считываться из файла;

2) полученное значение хэш-функции должно представляться в шестнадцатеричном виде и сохраняться в файл;

3) при работе программы должна быть возможность просмотра и изменения считанного из файла сообщения и вычисленного значения хэш-функции.

1.2. Исследовать лавинный эффект на сообщении, состоящем из одного блока:

1) для бита, который будет изменяться, приложение должно позволять задавать его позицию (номер) в сообщении;

2) приложение должно уметь после каждого раунда (итерации цикла) вычисления хэш-функции подсчитывать число бит, изменившихся в хэше при изменении одного бита в тексте сообщения;

3) приложение может строить графики зависимости числа бит, изменившихся в хэше, от раунда вычисления хэш-функции, либо графики можно строить в стороннем ПО, но тогда приложение должно сохранять в файл необходимую для построения графиков информацию.

2. С помощью реализованного приложения выполнить следующие задания.

2.1. Протестировать правильность работы разработанного приложения.

2.2. Исследовать лавинный эффект при изменении одного бита в сообщении: для различных позиций изменяемого бита в сообщении построить графики зависимостей числа бит, изменившихся в хэше, от раунда вычисления хэш-функции (всего в отчѐте должно быть 2-3 графика).

2.3. Сделать выводы о проделанной работе.
Результаты зафиксировать в отчете.

18. Задание к практическому занятию 3.4.2. Применение криптографических атак на хеш-функции.

Проведение атаки перебором (bruteforce attack):

1. Используя программу для вскрытия паролей произвести атаку на зашифрованный файл. Область перебора – все печатаемые символы, длина пароля от 1 до 4 символов. Проверить правильность определенного пароля, распаковав файл и ознакомившись с его содержимым;

2. Выполнив пункт 1, сократить область перебора до фактически используемого (например, если пароль 6D1A – то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время.

Проведение атаки по словарю (dictionary attack):

1. Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например, love, god, table, admin и т.д.). Провести атаку по словарю;

2. Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.
Результаты зафиксировать в отчете.

19. Задание к практическому занятию 3.4.3. Изучение программно-аппаратных средств, реализующих основные функции ЭП

1. получите вариант задания у преподавателя;
2. сгенерируйте ЭЦП для сообщения;
3. проверьте подлинность ЭЦП для сообщения;
4. результаты и промежуточные вычисления оформите в виде отчета.

Результаты зафиксировать в отчете.

20. Задание к практическому занятию 3.5.1. Применение протокола ДиффиХеллмана для

обмена ключами шифрования.

1. Изучить схему обмена ключами Диффи-Хелмана.
2. Реализовать подпрограмму, определяющую для заданного числа первые 100 первообразных корней, отображая при этом суммарное время, затраченное на их поиск. Число может задаваться десятеричной, шестнадцатеричной и двоичной формах.
3. Вручную для первых 5 полученных числовых значений привести доказательство, что они действительно являются первообразными корнями заданного числа n.
4. Реализовать подпрограмму, моделирующую обмен ключами между абонентами по схеме Диффи-Хеллмана. Программа должна получать большие простые числа XA, XB и n случайным образом с помощью алгоритма генерации простого числа, а также предоставлять пользователю возможность задавать их.

Результаты зафиксировать в отчете.

21. Задание к практическому занятию 3.5.2. Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.

1. Проследите как происходит определение легальности клиента, логический вход в сеть, получение разрешения на продолжение процесса получения доступа к ресурсу через систему Kerberos.
2. Проследите как происходит получение разрешения на обращение к ресурсному серверу, например к файл серверу, серверу приложений, серверу удаленного доступа
3. Проследите как происходит получение разрешения на доступ к ресурсу. Изучите содержимое квитанции (билетов) на доступ к ресурсам.
4. Просмотрите системные журналы, логи на сервере Kerberos (на аутентификационной его части и на подсистеме, выдающей квитанции (билеты)), а также на ресурсных серверах.
5. Сделать выводы по работе и представить их в отчете.

Результаты зафиксировать в отчете.

22. Задание к практическому занятию 3.7.1. Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей

1. Определить время перебора всех паролей, состоящих из 6 цифр. Алфавит составляют цифры n=10. Длина пароля 6 символов k=6.
2. Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет. Алфавит составляют символы n=10.
3. Определить время перебора всех паролей с параметрами. Алфавит состоит из n символов. Длина пароля символов k. Скорость перебора s паролей в секунду. После каждого из m неправильно введенных паролей идет пауза в v секунд вариант n k s m v
4. Определить минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду. вариант n t s
5. Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет. Скорость перебора s паролей в секунду. вариант k t s

Результаты зафиксировать в отчете.

23. Задание к практическому занятию 3.8.1. Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ

1. Изучить основные возможности ПО Filigrana
2. Изучить механизм встраивания ЦВЗ с использованием векторного квантования
3. Рассмотреть алгоритмы встраивания ЦВЗ с использованием скалярного квантования
4. Изучить алгоритмы на основе слияния ЦВЗ и контейнера
5. Изучить методы маскирования ЦВЗ

Результаты зафиксировать в отчете.

24. Задание к практическому занятию 3.8.2. Реализация простейших стеганографических алгоритмов

1. Изучить алгоритмов на основе линейного встраивания данных
2. Изучить принципы встраивания информации с использованием квантования. Дизеризованные квантователи.

3. Рассмотреть методы встраивания информации на уровне коэффициентов
4. Изучить методы встраивания информации на уровне битовой плоскости
5. Изучить метод встраивания информации за счет энергетической разности между коэффициентами

Результаты зафиксировать в отчете.

Тестирование:

Критерии оценивания при тестировании:
- 100 баллов – при правильном и полном ответе на 10 вопроса;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–74	75–84	85–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример тестовых заданий:

Введение. Предмет и задачи криптографии. История криптографии. Основные термины.

1. Что такое шифрование?

1. способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
2. совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
3. удобная среда для вычисления конечного пользователя

2. Что такое кодирование?

1. преобразование обычного, понятного текста в код
2. преобразование
3. написание программы

3. Что является предметом науки криптография

1. способы шифрования и дешифрования
2. методы сокрытия факта передачи секретной информации
3. способы преобразования информации с целью ее защиты от несанкционированных пользователей

4. Первое известное применение шифра:

1. египетский текст
2. русский
3. нет правильного ответа

5. Выберите то, что относится к показателям криптостойкости:

1. количество всех возможных ключей
2. среднее время, необходимое для криптоанализа
3. количество символов в ключе

Раздел 1. Математические основы защиты информации

Тема 1.1. Математические основы криптографии

1. Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии

1. функцией Диффи-Хеллмана
2. односторонней функцией
3. функцией Эйлера
4. криптографической функцией

2. Какие из разделов математики легли в основу современных методов криптографии?

1. теория числе и абстрактная алгебра
2. теория кодирования и теория вероятности
3. теория сложности и теория дискретизации

3. Как называется наука, предметом которой являются математические способы преобразования информации с целью ее защиты от несанкционированных пользователей?

1. криптология
2. криптография
3. теория кодирования

4. В теоретической криптографии принято работать с алфавитом:

1. английским
2. любым национальным алфавитом
3. двоичных слов
4. 16-ричных слов

5. Какие виды математических последовательностей используются в криптографии:

1. детерминированные
2. случайные
3. неслучайные
4. бесконечные

Раздел 2. Классическая криптография

Тема 2.1. Методы криптографической защиты информации

1. Что представляет собой криптографическая система?

1. семейство T преобразований открытого текста, члены его семейства индексируются индексом k
2. программу
3. систему

2. Что принято называть электронной подписью?

1. присоединяемое к тексту его криптографическое преобразование
2. текст
3. зашифрованный текст

3. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?

1. криптографическое шифрование
2. компрессия
3. помехоустойчивое кодирование
4. эффективное кодирование

4. Какими свойствами должен обладать генератор псевдослучайных чисел (ГПСЧ) для использования в криптографических целях? (выбрать все верные)

1. период порождаемой последовательности должен быть как можно меньше
2. вероятности порождения различных значений ключевой последовательности должны как можно больше отличаться друг от друга
3. период порождаемой последовательности должен быть очень большой
4. вероятности порождения различных значений ключевой последовательности должны быть равны

5. Криптографический алгоритм, в котором ключ, используемый для шифрования сообщений, может быть получен из ключа дешифрования и наоборот, называют:

1. симметричным;
2. ассиметричным;
3. синхронным;
4. асинхронным

Тема 2.2. Криптоанализ

1. Цель криптоанализа:

1. Определение стойкости алгоритма
2. Увеличение количества функций замещения в криптографическом алгоритме
3. Уменьшение количества функций подстановок в криптографическом алгоритме
4. Определение использованных перестановок

2. Криптоанализ предусматривает раскрытие секретных сообщений:

1. со знанием хотя бы одного из ключей
2. без знания криптографического алгоритма
3. без знания ключа и без знания криптографического алгоритма
4. без знания ключа, но со знанием криптографического алгоритма

3. Фундаментальное допущение криптоанализа, впервые сформулированное О. Кирхгоффом, состоит в том, что:

1. секретность сообщения полностью зависит от ключа
2. секретность сообщения полностью зависит от алгоритма шифрования
3. секретность сообщения зависит от ключа и алгоритма шифрования

4. Какие методы криптоанализа применяются для ассиметричных шифров?

1. DES
2. AES
3. RSA
4. COS

5. Какие методы криптоанализа применяются для симметричных шифров?

1. DES
2. AES
3. RSA
4. COS

Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел

1. Поточный шифр выполняет преобразование входного сообщения:

1. блоками определенной длины
2. посимвольно

2. Для использования в криптографических целях генератор псевдослучайных чисел должен обладать следующими свойствами: (выбрать все верные)

1. период последовательности должен быть очень большой;
2. порождаемая последовательность должна быть "почти" случайной;
3. вероятности порождения различных значений должны быть в точности равны;
4. вероятности порождения различных значений должны быть различны

3. Какой из генераторов псевдослучайных чисел является наиболее простым?

1. Линейный конгруэнтный
2. Фибоначчи с запаздыванием
3. С квадратичным остатком (BBS)
4. На основе сдвиговых регистров с обратной связью

4. Какой алгоритм используется для шифрования паролей в ОС Windows, а также в протоколе SSL?

1. RC4
2. AES
3. TKIP

5. На чем основан принцип действия всех генераторов псевдослучайных чисел?

1. на физических явлениях или процессах, которые можно зафиксировать и сосчитать
2. на математических формулах

Раздел 3. Современная криптография

Тема 3.1. Кодирование информации. Компьютеризация шифрования.

1. Кодирование информации – это…

1. преобразование обычного, понятного текста в код
2. преобразование
3. написание программы

2. В чем заключается общая идея помехоустойчивого кодирования?

1. из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
2. уменьшается избыточность передаваемых сообщений
3. производится преобразование информации с целью сокрытия ее смысла
4. из всех допустимых кодовых слов считаются возможными не все, а лишь некоторые

3. Какие коды используются в помехоустойчивом кодировании?

1. Хэмминга
2. CRC
3. БЧХ
4. Рида – Соломона
5. Грэя

4. Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:

1. Оно обеспечивает проверку целостности и правильности данных
2. Оно требует внимательного отношения к процессу управления ключами
3. Оно не требует большого количества системных ресурсов
4. Оно требует передачи ключа на хранение третьей стороне (escrowed)

5. Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст:

1. Коллизия
2. Хэширование
3. MAC
4. Кластеризация ключей

Тема 3.2. Симметричные системы шифрования

1. Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:

1. 1
2. 2
3. 3

2. Алгоритм, использующий симметричный ключ и алгоритм хэширования:

1. HMAC+
2. 3DES
3. ISAKMP-OAKLEY
4. RSA

3. Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования?

1. сложение по модулю 2
2. нахождение остатка от деления на большое простое число
3. замена бит по таблице замен
4. перестановка бит
5. возведение в степень

4. Какой размер ключа в отечественном стандарте симметричного шифрования:

1. 56 бит;
2. 124 бит;
3. 256 бит.

5. Что является преимуществом симметричного шифрования:

1. скорость выполнения криптографических преобразований;
2. легкость внесения изменений в алгоритм шифрования;
3. секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
4. применение в системах аутентификации (электронная подпись).

Тема 3.3. Асимметричные системы шифрования

1. Верны ли утверждения? (выбрать все верные)

1. В асимметричных криптосистемах не решена проблема распределения ключей.
2. Асимметричные криптосистемы существенно медленнее симметричных.

2. Асимметричные криптосистемы для шифрования информации используют количество ключей…. ?

1. 1
2. 2
3. 3
4. 4

3. В асимметричных системах шифрования

1. открытый ключ доступен всем желающим, а секретный ключ известен только получателю сообщения
2. для зашифрования и расшифрования используется один ключ
3. секретный ключ доступен всем желающим, а открытый ключ известен только получателю сообщения
4. секретный и открытый ключи доступны всем желающим

4. Какие шифры (механизмы обмена ключами) относятся к асимметричным (выбрать все верные):

1. Диффи–Хелмана (D-H)
2. Ривест–Шамир–Адлеман (RSA)
3. Криптография эллиптической кривой (ECC)

5. Какая связь существует между двумя ключами в асимметричной криптографии?

1. логическая
2. физическая
3. математическая
4. никакая

Тема 3.4. Аутентификация данных. Электронная подпись

1. Какие методы разрабатываются с целью обеспечения аутентификации?

1. методы подтверждения подлинности сторон и самой информации в процессе информационного взаимодействия
2. методы присвоения уникального идентификатора взаимодействующим сторонам и самой информации в процессе информационного взаимодействия
3. оба ответа верны

2. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?

1. криптографическое шифрование
2. компрессия
3. помехоустойчивое кодирование
4. эффективное кодирование

3. Какая система является системой аутентификации и распределения ключей:

1. Kerberos
2. RSA
3. MD5

4. AES

4. Что принято называть электронной (цифровой) подписью?

1. присоединяемое к тексту его криптографическое преобразование
2. текст
3. зашифрованный текст

5. Выберите то, что используют для создания цифровой подписи:

1. Закрытый ключ получателя
2. Открытый ключ отправителя
3. Закрытый ключ отправителя
4. Открытый ключ получателя

Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации

1. Позволяет ли обмениваться ключами по незащищенным каналам связи Метод Диффи-Хеллмана?

1. да
2. нет

2. Применяется ли для распределения ключей между пользователями информационной системы прямой обмен ключами между пользователями сети?

1. да
2. нет

3. Процесс согласования сессионного ключа в процессе информационного обмена называют _____ ключей.

1. распределением
2. идентификацией
3. аутентификацией
4. хэшированием

4. Какой протокол аутентификации является менее надежным?

1. PAP
2. CHAP

5. Сколько шагов предусматривает аутентификация с помощью протокола Kerberos версии 5 ?

1. 2
2. 3
3. 4
4. 5

Тема 3.6. Криптозащита информации в сетях передачи данных

1. Линейное шифрование это:

1. иптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому
2. криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами
3. несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу

2. Какой шифратор можно использовать для защиты передаваемой в Сеть информации?

1. обычный шифратор
2. проходной шифратор
3. табличный шифратор

3. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе по сети Интернет:

1. Идентификация

2. Аутентификация
3. Авторизация
4. Экспертиза
5. Шифрование

4. Какие из приведенных криптографических алгоритмов используют в основе сетей Фейстеля?

1. DES
2. Rijndael
3. оба ответа верны

5. Каким образом наиболее просто можно осуществить распределение ключей для сетей с большим количеством абонентов?

1. в системах предварительного распределения секретных ключей
2. в системах открытого распределения секретных ключей
3. оба ответа верны

Тема 3.7. Защита информации в электронных платежных системах

1. Механизмы защиты, которые как минимум должны быть реализованы для обеспечения функций защиты информации на отдельных узлах электронной платежной системы: выбрать все верные

1. обеспечение управления доступом на оконечных системах;
2. контролирование целостности и обеспечение конфиденциальности сообщения;
3. обеспечение взаимной аутентификации абонентов;
4. ведение регистрации и контролирование целостности последовательности сообщений
5. хранение персональной информации клиентов

2. Какой протокол передачи данных обеспечивает лучшую защиту в системах электронных платежей?

1. SSL
2. SET

3. Выберите все верные утверждения относительно протокола SSL:

1. Отсутствие аутентификации покупателя
2. Наличие аутентификации покупателя и продавца
3. Невозможность использования при операциях с банковским счетом
4. Открытость реквизитов покупателя при передаче по сети
5. Является на сегодняшний день самым безопасным для передачи платежных сообщений

4. В протоколе SET предусмотрены следующие типы ключей, используемых участниками платежных транзакций: выбрать все верные

1. ключ для подписи сообщения (Digital Signature Key);
2. ключ для шифрования данных (Data Encipherment Key);
3. ключ для подписи сертификата (Certificate Signature Key);
4. ключ для подписи списка отозванных сертификатов (CRL Signature Key).
5. ключ для дешифрования данных (Data Decryption Key);

5. Смарт-карта обеспечивает следующий набор функций: выбрать все верные

1. разграничение полномочий доступа к внутренним ресурсам;
2. шифрование данных с применением различных алгоритмов;
3. формирование электронной цифровой подписи;
4. выполнение всех операций взаимодействия владельца карты, банка и торговца.
5. создание безопасного сетевого канала для передачи платежных данных
6. дешифрование данных с применением различных алгоритмов

Тема 3.8. Компьютерная стеганография

1. Что может являться файлом – контейнером для стеганографии? выбрать все верные

1. файл изображения
2. файл звука

3. видеофайл
4. файл Word
5. файл Excel
6. исполняемые файлы

2. В стеганографии метод LSB это:

1. метод наименее значимого бита;
2. эхо-метод;
3. метод фазового кодирования;
4. метод расширенного спектра;

3. Какие принципы лежат в основе стеганографии? выбрать все верные

1. некоторые файлы могут быть искажены без потери их функциональности
2. неспособности человека различать незначительные искажения в графических или мультимедийных файлах
3. контрольная сумма и размер файла, несущего зашифрованную информацию не изменяется

4. Выберите верное утверждение:

1. стеганография скрывает тело сообщения
2. стеганография скрывает тело сообщения и факт его присутствия

5. Стеганографическая система или стегосистема – это:

1. совокупность средств и методов, которые используются для формирования скрытого канала передачи информации;
2. совокупность средств и методов, которые используются для маскировки ценной информации

2.2 Оценочные средства при промежуточной аттестации

Формой промежуточной аттестации в третьем сесместре является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:
- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Тестирование:

Критерии оценивания при тестировании:
- 100 баллов – при правильном и полном ответе на 10 вопроса;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–74	75–84	85–100
Шкала оценивания	НЕУД	УД	ХОР	ОТЛ

Пример вариантов тестовых заданий:

Вариант 1.

1. Математическая функция, которую относительно легко вычислить, но трудно найти по

значению функции соответствующее значение аргумента, называется в криптографии

1. функцией Диффи-Хеллмана
2. односторонней функцией
3. функцией Эйлера
4. криптографической функцией

2. Какие из разделом математики легли в основу современных методов криптографии?

1. теория числе и абстрактная алгебра
2. теория кодирования и теория вероятности
3. теория сложности и теория дискретизации

3. Как называется наука, предметом которой являются математические способы преобразования информации с целью ее защиты от несанкционированных пользователей?

1. криптология
2. криптография
3. теория кодирования

4. В теоретической криптографии принято работать с алфавитом:

1. английским
2. любым национальным алфавитом
3. двоичных слов
4. 16-ричных слов

5. Какие виды математических последовательностей используются в криптографии:

1. детерминированные
2. случайные
3. неслучайные
4. бесконечные

6. Что представляет собой криптографическая система?

1. семейство T преобразований открытого текста, члены его семейства индексируются индексом k
2. программу
3. систему

7. Что принято называть электронной подписью?

1. присоединяемое к тексту его криптографическое преобразование
2. текст
3. зашифрованный текст

8. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?

1. криптографическое шифрование
2. компрессия
3. помехоустойчивое кодирование
4. эффективное кодирование

9. Какими свойствами должен обладать генератор псевдослучайных чисел (ГПСЧ) для использования в криптографических целях? (выбрать все верные)

1. период порождаемой последовательности должен быть как можно меньше
2. вероятности порождения различных значений ключевой последовательности должны как можно больше отличаться друг от друга
3. период порождаемой последовательности должен быть очень большой
4. вероятности порождения различных значений ключевой последовательности должны быть равны

10. Криптографический алгоритм, в котором ключ, используемый для шифрования сообщений, может быть получен из ключа дешифрования и наоборот, называют:

1. симметричным;
2. ассиметричным;

3. синхронным;
4. асинхронным

Вариант 2.

1. Что представляет собой криптографическая система?

1. семейство T преобразований открытого текста, члены его семейства индексируются индексом k
2. программу
3. систему

2. Что принято называть электронной подписью?

1. присоединяемое к тексту его криптографическое преобразование
2. текст
3. зашифрованный текст

3. Как называется преобразование информации с целью защиты от несанкционированного доступа, аутентификации и защиты от преднамеренных изменений?

1. криптографическое шифрование
2. компрессия
3. помехоустойчивое кодирование
4. эффективное кодирование

4. Какими свойствами должен обладать генератор псевдослучайных чисел (ГПСЧ) для использования в криптографических целях? (выбрать все верные)

1. период порождаемой последовательности должен быть как можно меньше
2. вероятности порождения различных значений ключевой последовательности должны как можно больше отличаться друг от друга
3. период порождаемой последовательности должен быть очень большой
4. вероятности порождения различных значений ключевой последовательности должны быть равны

5. Криптографический алгоритм, в котором ключ, используемый для шифрования сообщений, может быть получен из ключа дешифрования и наоборот, называют:

1. симметричным;
2. ассиметричным;
3. синхронным;
4. асинхронным

6. Математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, называется в криптографии

1. функцией Диффи-Хеллмана
2. односторонней функцией
3. функцией Эйлера
4. криптографической функцией

7. Какие из разделов математики легли в основу современных методов криптографии?

1. теория числе и абстрактная алгебра
2. теория кодирования и теория вероятности
3. теория сложности и теория дискретизации

8. Как называется наука, предметом которой являются математические способы преобразования информации с целью ее защиты от несанкционированных пользователей?

1. криптология
2. криптография
3. теория кодирования

9. В теоретической криптографии принято работать с алфавитом:

1. английским
2. любым национальным алфавитом
3. двоичных слов

4. 16-ричных слов

10. Какие виды математических последовательностей используются в криптографии:

1. детерминированные
2. случайные
3. неслучайные
4. бесконечные

Вариант 3.

1. Кодирование информации – это…

1. преобразование обычного, понятного текста в код
2. преобразование
3. написание программы

2. В чем заключается общая идея помехоустойчивого кодирования?

1. из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
2. уменьшается избыточность передаваемых сообщений
3. производится преобразование информации с целью сокрытия ее смысла
4. из всех допустимых кодовых слов считаются возможными не все, а лишь некоторые

3. В чем заключается общая идея помехоустойчивого кодирования?

1. из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
2. уменьшается избыточность передаваемых сообщений
3. производится преобразование информации с целью сокрытия ее смысла
4. из всех допустимых кодовых слов считаются возможными не все, а лишь некоторые

4. Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:

1. Оно обеспечивает проверку целостности и правильности данных
2. Оно требует внимательного отношения к процессу управления ключами
3. Оно не требует большого количества системных ресурсов
4. Оно требует передачи ключа на хранение третьей стороне (escrowed)

5. Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст:

1. Коллизия
2. Хэширование
3. MAC
4. Кластеризация ключей

6. Цель криптоанализа:

1. Определение стойкости алгоритма
2. Увеличение количества функций замещения в криптографическом алгоритме
3. Уменьшение количества функций подстановок в криптографическом алгоритме
4. Определение использованных перестановок

7. Криптоанализ предусматривает раскрытие секретных сообщений:

1. со знанием хотя бы одного из ключей
2. без знания криптографического алгоритма
3. без знания ключа и без знания криптографического алгоритма
4. без знания ключа, но со знанием криптографического алгоритма

8. Фундаментальное допущение криптоанализа, впервые сформулированное О. Кирхгоффом, состоит в том, что:

1. секретность сообщения полностью зависит от ключа
2. секретность сообщения полностью зависит от алгоритма шифрования
3. секретность сообщения зависит от ключа и алгоритма шифрования

9. Какие методы криптоанализа применяются для ассиметричных шифров?

1. DES
2. AES
3. RSA
4. COS

10. Какие методы криптоанализа применяются для симметричных шифров?

1. DES
2. AES
3. RSA
4. COS

Формой промежуточной аттестации в четвертом сесместре является экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:
- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 2 вопроса выбранных случайным образом и на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Ответ на вопросы:
Критерии оценивания при ответе на вопросы:
- 85–100 баллов – при правильном и полном ответе на два вопроса;
- 65–84 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 50–64 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–49 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-49	50-64	65-84	85-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень вопросов к экзамену:

1. Предмет криптографии. Определения. Задачи. Исторические примеры.
2. Виды атак на криптографические алгоритмы. Понятие стойкости.
3. Классификация алгоритмов шифрования. Примеры простейших шифров.
4. Шифры замены. Математическая модель. Примеры.
5. Шифры перестановки. Математическая модель. Примеры.
6. Шифры гаммирования. Математическая модель. Примеры.
7. Принципы построения блочных шифров. Схема Фейстеля.
8. Алгоритм симметричного шифрования DES.
9. Алгоритм симметричного шифрования ГОСТ 28147-99.
10. Алгоритм симметричного шифрования Rijndael.
11. Алгоритмы симметричного шифрования IDEA и Blowfish.
12. Режимы выполнения алгоритмов симметричного шифрования.
13. Поточные криптосистемы. Принципы построения. Классификация. Проблема синхронизации.
14. Линейные конгруэнтные генераторы. Линейные регистры сдвига.
15. Поточные шифры. Отличия от блочных. Стойкость. Методы анализа.
16. Примеры поточных шифров на основе LFSR.
17. Примеры поточных шифров, использующих аддитивные генераторы.
18. Примеры поточных шифров на основе FCSR.
19. Математические методы криптоанализа: метод опробывания, методы на основе теории статистических решений.
20. Линейный криптоанализ.
21. Разностный криптоанализ.
22. Основные принципы построения асимметричных криптосистем. Стойкость.
23. Шифросистема RSA. Стойкость.

24. Шифросистема Эль-Гамаля. Стойкость.
25. Шифросистема на основе принципа «рюкзака».
26. Шифросистема Рабина. Стойкость.
27. Алгоритм обмена ключами Диффи-Хеллмана.
28. Хэш-функции. Требования. Типы функций хэширования.
29. Атаки на функции хэширования.
30. Функция хеширования MD5.
31. Функция хеширования SHA-1.
32. Функция хеширования ГОСТ 3411-94.
33. Функция хеширования СТБ 1176.1-99.
34. Общие положения электронной цифровой подписи. Задачи. Требования.
35. Прямая и арбитражная цифровая подписи. Примеры.
36. Стандарт электронной цифровой подписи DSS.
37. Цифровая подпись на основе алгоритмов с открытыми ключами. Схема Фиата-Шамира.
38. Цифровая подпись Эль-Гамаля. Схема RSA.
39. Стандарт электронной цифровой подписи DSS.
40. Стандарт электронной цифровой подписи ГОСТ-Р 34.10-94.
41. Стандарт электронной цифровой подписи СТБ 1176.2-99.
42. Применение эллиптических кривых в криптографии. Алгоритм шифрования на основе эллиптических кривых.
43. Алгоритмы обмена ключами и электронной цифровой подписи на основе эллиптических кривых.
44. Стеганографические методы защиты информации. Основные понятия и определения. Области применения.
45. Общая модель стеганосистемы. Проблема устойчивости. Стегоанализ.
46. Методы сокрытия информации в неподвижных изображениях.
47. Методы сокрытия информации в текстовых данных.
48. Протоколы аутентификации. Двусторонняя аутентификация.
49. Протоколы аутентификации. Односторонняя аутентификация.

Тестирование:

Критерии оценивания при тестировании:

- 100 баллов – при правильном и полном ответе на 10 вопроса;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–74	75–84	85–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример вариантов тестовых заданий:

Вариант 1.

1. Линейное шифрование это:

1. иптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому
2. криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами
3. несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу

2. Какие из приведенных криптографических алгоритмов используют в основе сетей Фейстеля?

1. DES
2. Rijndael
3. оба ответа верны

3. Каким образом наиболее просто можно осуществить распределение ключей для сетей с большим количеством абонентов?

1. в системах предварительного распределения секретных ключей

2. в системах открытого распределения секретных ключей
3. оба ответа верны

4. Позволяет ли обмениваться ключами по незащищенным каналам связи Метод Диффи-Хеллмана?

1. да
2. нет

5. Какой протокол аутентификации является менее надежным?

1. PAP
2. CHAP

6. Сколько шагов предусматривает аутентификация с помощью протокола Kerberos версии 5 ?

1. 2
2. 3
3. 4
4. 5

7. Для использования в криптографических целях генератор псевдослучайных чисел должен обладать следующими свойствами: (выбрать все верные)

1. период последовательности должен быть очень большой;
2. порождаемая последовательность должна быть "почти" случайной;
3. вероятности порождения различных значений должны быть в точности равны;
4. вероятности порождения различных значений должны быть различны

8. Какой из генераторов псевдослучайных чисел является наиболее простым?

1. Линейный конгруэнтный
2. Фибоначчи с запаздыванием
3. С квадратичным остатком (BBS)
4. На основе сдвиговых регистров с обратной связью

9. Какой алгоритм используется для шифрования паролей в ОС Windows, а также в протоколе SSL?

1. RC4
2. AES
3. TKIP

10. На чем основан принцип действия всех генераторов псевдослучайных чисел?

1. на физических явлениях или процессах, которые можно зафиксировать и сосчитать
2. на математических формулах

Вариант 2.

1. Механизмы защиты, которые как минимум должны быть реализованы для обеспечения функций защиты информации на отдельных узлах электронной платежной системы: выбрать все верные

1. обеспечение управления доступом на оконечных системах;
2. контролирование целостности и обеспечение конфиденциальности сообщения;
3. обеспечение взаимной аутентификации абонентов;
4. ведение регистрации и контролирование целостности последовательности сообщений
5. хранение персональной информации клиентов

2. В протоколе SET предусмотрены следующие типы ключей, используемых участниками платежных транзакций: выбрать все верные

1. ключ для подписи сообщения (Digital Signature Key);
2. ключ для шифрования данных (Data Encipherment Key);
3. ключ для подписи сертификата (Certificate Signature Key);
4. ключ для подписи списка отозванных сертификатов (CRL Signature Key).
5. ключ для дешифрования данных (Data Decryption Key);

3. Смарт-карта обеспечивает следующий набор функций: выбрать все верные

1. разграничение полномочий доступа к внутренним ресурсам;
2. шифрование данных с применением различных алгоритмов;
3. формирование электронной цифровой подписи;
4. выполнение всех операций взаимодействия владельца карты, банка и торговца.
5. создание безопасного сетевого канала для передачи платежных данных
6. дешифрование данных с применением различных алгоритмов

4. Какая система является системой аутентификации и распределения ключей:

1. Kerberos
2. RSA
3. MD5
4. AES

5. Что принято называть электронной (цифровой) подписью?

1. присоединяемое к тексту его криптографическое преобразование
2. текст
3. зашифрованный текст

6. Выберите то, что используют для создания цифровой подписи:

1. Закрытый ключ получателя
2. Открытый ключ отправителя
3. Закрытый ключ отправителя
4. Открытый ключ получателя

7. В чем заключается общая идея помехоустойчивого кодирования?

1. из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
2. уменьшается избыточность передаваемых сообщений
3. производится преобразование информации с целью сокрытия ее смысла
4. из всех допустимых кодовых слов считаются возможными не все, а лишь некоторые

8. Какие коды используются в помехоустойчивом кодировании?

1. Хэмминга
2. CRC
3. БЧХ
4. Рида – Соломона
5. Грэя

9. Выберите правильное утверждение в отношении шифрования данных, выполняемого с целью их защиты:

1. Оно обеспечивает проверку целостности и правильности данных
2. Оно требует внимательного отношения к процессу управления ключами
3. Оно не требует большого количества системных ресурсов
4. Оно требует передачи ключа на хранение третьей стороне (escrowed)

10. Название ситуации, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст:

1. Коллизия
2. Хэширование
3. MAC
4. Кластеризация ключей

Вариант 3.

1. Какие принципы лежат в основе стеганографии? выбрать все верные

1. некоторые файлы могут быть искажены без потери их функциональности
2. неспособности человека различать незначительные искажения в графических или мультимедийных файлах
3. контрольная сумма и размер файла, несущего зашифрованную информацию не изменяется

2. Выберите верное утверждение:

1. стеганография скрывает тело сообщения
2. стеганография скрывает тело сообщения и факт его присутствия

3. Стеганографическая система или стегосистема – это:

1. совокупность средств и методов, которые используются для формирования скрытого канала передачи информации;
2. совокупность средств и методов, которые используются для маскировки ценной информации

4. В асимметричных системах шифрования

1. открытый ключ доступен всем желающим, а секретный ключ известен только получателю сообщения
2. для зашифрования и расшифрования используется один ключ
3. секретный ключ доступен всем желающим, а открытый ключ известен только получателю сообщения
4. секретный и открытый ключи доступны всем желающим

5. Какие шифры (механизмы обмена ключами) относятся к асимметричным (выбрать все верные):

1. Диффи–Хелмана (D-H)
2. Ривест–Шамир–Адлеман (RSA)
3. Криптография эллиптической кривой (ECC)

6. Какая связь существует между двумя ключами в асимметричной криптографии?

1. логическая
2. физическая
3. математическая
4. никакая

7. Алгоритм, использующий симметричный ключ и алгоритм хэширования:

1. HMAC+
2. 3DES
3. ISAKMP-OAKLEY
4. RSA

8. Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования?

1. сложение по модулю 2
2. нахождение остатка от деления на большое простое число
3. замена бит по таблице замен
4. перестановка бит
5. возведение в степень

9. Какой размер ключа в отечественном стандарте симметричного шифрования:

1. 56 бит;
2. 124 бит;
3. 256 бит.

10. Что является преимуществом симметричного шифрования:

1. скорость выполнения криптографических преобразований;
2. легкость внесения изменений в алгоритм шифрования;
3. секретный ключ известен только получателю информации и первоначальный обмен не требует передачи секретного ключа;
4. применение в системах аутентификации (электронная подпись).

2.3 Методические материалы, определяющие процедуры оценивания знаний, умений, практического опыта деятельности, характеризующие этапы формирования компетенций

При проведении текущего контроля по темам в конце занятия обучающиеся убирают все личные вещи с учебной мебели, достают листок чистой бумаги и ручку. На листке бумаги записываются Фамилия, Имя, Отчество, номер группы и дата проведения опроса. Далее преподаватель задает два вопроса, которые могут быть, как записаны на листке бумаги, так и нет. В течение пяти минут обучающиеся должны дать ответы на заданные вопросы, при этом использовать любую печатную и рукописную продукцию, а также любые технические средства не допускается. По истечении указанного времени листы с ответами сдаются преподавателю на проверку. Результаты оценивания ответов на вопросы доводятся до сведения обучающихся не позднее трех учебных дней после даты проведения опроса.

Если обучающийся воспользовался любой печатной или рукописной продукцией, а также любыми техническими средствами, то его ответы на вопросы не принимаются и ему выставляется 0 баллов. При проведении текущего контроля по лабораторным и(или) практическим занятиям обучающиеся представляют отчет по лабораторным и(или) практическим заданиям преподавателю.

Защита отчетов по лабораторным и(или) практическим заданиям может проводиться как в письменной, так и в устной форме. При проведении текущего контроля по защите отчета в конце следующего занятия по лабораторной и(или) практической работе. Преподаватель задает два вопроса, которые могут быть, как записаны, так и нет. В течение пяти минут обучающиеся должны дать ответы на заданные вопросы, при этом использовать любую печатную и рукописную продукцию, а также любые технические средства не допускается. По истечении указанного времени листы с ответами сдаются преподавателю на проверку. Результаты оценивания ответов на вопросы сразу доводятся до сведения обучающихся.

Обучающийся, который не прошел текущий контроль, обязан представить на промежуточную аттестацию все задолженности по текущему контролю и пройти промежуточную аттестацию на общих основаниях. Процедура проведения промежуточной аттестации аналогична проведению текущего контроля.