МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование кафедры полностью)

_____ М.О. Таныгин
(подпись)

«31» 08 2021 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости
и промежуточной аттестации обучающихся
по дисциплине

Методы и средства криптографической защиты информации
(наименование дисциплины)

10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»
(код и наименование ОПОП ВО)

Курск – 2021

Задания для проведения текущего контроля успеваемости

Юго-Западный государственный университет
Кафедра информационной безопасности

Вопросы для собеседования
по дисциплине «Методы и средства криптографической защиты информации»
(наименование дисциплины)

Тема 1 Введение в криптологию.

1. Назовите основные этапы истории развития криптологии как науки.
2. Каковы основные задачи криптологии как науки.
3. Назовите основные термины, используемые в криптографии.
4. Исторические сведения о системах и способах составления шифрованных писем.
5. Как были устроены первые криптосистемы.
6. Что такое криптоанализ.
7. Чем криптография отличается от криптоанализа.
8. Какое понятие шире криптография или криптология.

Тема 2 Классификация криптоалгоритмов.

1. Классификация систем шифрования.
2. Симметричное шифрование, достоинства и недостатки.
3. Асимметричное шифрование, достоинства и недостатки
4. Сравнение систем шифрования относительно друг друга.
5. Как происходит использование открытого ключа.

Тема 3 Симметричные криптоалгоритмы.

1. Основы симметричного шифрования.
2. Блочные и поточные системы шифрования.
3. Преимущества использования блочных и поточных систем шифрования
4. Недостатки использования блочных и поточных систем шифрования.
5. Достоинства и недостатки симметричного шифрования.

Тема 4 Потоковые шифраторы.

1. Регистр сдвига с линейной обратной связью.
2. Ассоциированный многочлен.
3. Поточные шифры.
4. Современные поточные шифры.
5. Комбинирование РСЛОС.
6. Наиболее распространенные поточные шифры.
7. Приведите примеры поточных шифров

Тема 5. Блочные криптоалгоритмы.

1. Что такое блочные криптоалгоритмы.
2. Как устроено блочное шифрование.
3. Какие режимы блочного шифрования вы знаете.
4. Как устроены режимы шифрования ECB и CBC, в чем их отличие.
5. Какой режим шифрования блочных шифров более стойкий к атакам удаления и вставки.
6. Сделайте обзор наиболее распространенных блочных шифров.

Тема 6. Сеть Фейштеля.

1. Алгоритмы многократного кодирования.
2. Раунды шифрования.
3. Что такое сеть Фейштеля.
4. Как устроен шифр DES.
5. Сколько раундов шифрования в шифре DES.
6. Как устроен алгоритм разворачивания ключа в шифре DES.

Тема 7. Ассиметричные криптоалгоритмы.

1. Что такое ассиметричные криптоалгоритмы.
2. Математические основы шифрования с открытым ключом.
3. Как используется открытый ключ.
4. Что такое секретный ключ.
5. Системы распределения ключей.
6. Достоинства и недостатки систем с открытым ключом.

Тема 8. Системы электронной цифровой подписи.

1. Что такое хэш функции.
2. Что такое однонаправленные функции.
3. Свойства криптографических хэш функций.
4. Схемы цифровой подписи.

5. Схема подписи с приложением.
6. Схема с цифровой подписью с восстановлением сообщения.

Тема 9. Алгоритмы обмена ключами. Разделение секрета.

1. Система управления симметричными ключами с предварительной частичной установкой.
2. Система управления симметричными ключами без предварительной частичной установки.
3. Схема Диффи-Хеллмана.
4. Схема Шамира.
5. Протокол Диффи-Хеллмана распределения ключей с тремя и более участниками.
6. Система управления ассиметричными ключами.
7. Цифровые сертификаты.
8. Центры сертификации.
9. Депонирование ключей. Encrypted File System (EFS).
10. Схема Шамира разделения секрета.

Тема 10. Применение программных симметричных систем шифрования.

1. Применение программных криптосистем шифрования.
2. Программная реализация симметричные системы шифрования.
3. Обзор основных программных продуктов на базе симметричных систем шифрования.
4. Приведите примеры программных симметричных систем шифрования отечественного производства.

Тема 11. Применение программных асимметричных систем шифрования.

1. Программная реализация асимметричные системы шифрования.
2. Обзор основных программных продуктов на базе асимметричных систем шифрования.
3. Программный продукт PGP.
4. Приведите примеры программных асимметричных систем шифрования отечественного производства

Тема 12. Стеганография. Основные понятия.

1. Что такое стеганография.
2. Дайте основные понятия стеганографии.

3. Что такое тайнопись.
4. Классическая стеганография.
5. Практическое использование стеганографии.
6. Обзор основных методов использования классической стеганографии.

Тема 13. Компьютерная стеганография.

1. Компьютерная стеганография.
2. Использование избыточности цифровой информации изображений.
3. Использование избыточности цифрового звука.
4. Использование избыточности цифрового видео.
5. Использование компьютерных форматов данных.
6. Применение компьютерной стеганографии.

Тема 14. Криптоанализ и криптостойкость. Основные методы криптоанализа.

1. Что такое криптоанализ.
2. Что такое криптостойкость.
3. Основные методы криптоанализа.
4. Оценка предельных мощностей взлома.
5. Понятие стойкости шифров.
6. Линейный криптоанализ.
7. Дифференциальный криптоанализ.

Тема 15. Анализ безопасности криптографических протоколов.

1. На чем основана безопасность криптографических протоколов.
2. Что такое доказуемая стойкость.
3. На чем основана проблема факторизации целых чисел.
4. В чем заключается проблема дискретного логарифма.
5. Теоретико-информационные оценки стойкости криптосистем.

Тема 16. Способы применения криптосистем для решения специальных задач.

1. Обзор способов применения криптосистем для решения специальных задач.
2. Как используются криптосистемы для аутентификации.
3. Удаленная идентификация пользователей.

4. Контроль целостности сообщений.

5. Невозможность отказа от авторства.

Критерии оценки:

– 0 баллов выставляется обучающемуся, если студент не может ответить на поставленные вопросы.

– 2 баллов выставляется обучающемуся, если доля правильных ответов от 50% до 90%.

– 4 балла выставляется обучающемуся, если доля правильных ответов более 90%.

Составитель М.А. Ефремов

«31» 08 2021 г.

Задания для проведения текущего контроля успеваемости

Юго-Западный государственный университет
Кафедра информационной безопасности

Контрольные вопросы для защиты
лабораторных работ
по дисциплине «Методы и средства криптографической защиты информации»
(наименование дисциплины)

Контрольные вопросы для защиты лабораторной работы №1.

1. Что понимается под моноалфавитными подстановками?
2. Приведите примеры моноалфавитных подстановок.
3. Что такое коэффициент сдвига?
4. Что такое мощность алфавита?
5. Что такое частотные характеристики символов?
6. Какова криптостойкость шифра моноалфавитной подстановки?

Контрольные вопросы для защиты лабораторной работы №2.

1. Какие подстановочные шифры вам известны, назовите их?
2. Что такое шифр Виженера?
3. Возможно ли применение статистических методов криптоанализа к полиалфавитным шифрам?
4. Что такое индекс соответствия криптограммы?

Контрольные вопросы для защиты лабораторной работы №3.

1. Какие подстановочные шифры вам известны, назовите их?
2. Какими методами возможно определение периода шифра?
3. В чем особенности применения метода Метод Ф. Казиски?
4. Как узнать длину первичных ключей?
5. Какую длину имеют первичные ключи, если длинна составного ключа равна 48, 60?
6. В чем отличие шифра Виженера от многопетлевых подстановок, какой метод более криптостойкий?

Контрольные вопросы для защиты лабораторной работы №4.

1. Какие бывают алгоритмы шифрования?
2. Что такое потоковый шифр?
3. Что такое скремблер?
4. Что такое дескремблер?
5. Для каких целей используют скремблеры и дескремблеры?
6. Какие типы скремблеров и дескремблеров вам известны?
7. Какие преимущества и недостатки самосинхронизирующихся скремблеров и дескремблеров вам известны?
8. Какие преимущества и недостатки аддитивных скремблеров и дескремблеров вам известны?

Контрольные вопросы для защиты лабораторной работы №5.

1. Что такое сдвиговый регистр?
2. Дайте определение шифрованию и расшифрованию сообщений.
3. Суть алгоритма Берлекэмпа-Месси.
4. Алгоритм отыскания начального заполнения

Контрольные вопросы для защиты лабораторной работы №6.

1. В чем отличие блочных от поточных шифров?
2. От чего зависит криптостойкость выбранного метода?
3. К каким шифрам относятся шифры перестановки?
4. Сколько всевозможных ключей может быть бля блока длинной 8, 10 символов?
5. В чем отличие простых перестановок от путей Гамильтона, где больше ключей шифрования?

Контрольные вопросы для защиты лабораторной работы №7.

1. К какому виду шифров относится шифр табличной перестановки?
2. С помощью какой формулы можно вычислить вероятности следования друг за другом всех возможных пар строк?
3. Дайте определение термину «диграмма».
4. Что необходимо для оценки вероятности следования строк друг за другом?
5. Какую задачу необходимо решить для расшифровки криптограммы в общем случае?
6. Какую роль выполняет таблица вероятностей?
7. Что необходимо предпринять, если использование таблицы вероятностей не дает результата?

Контрольные вопросы для защиты лабораторной работы №8.

1. Общая характеристика и обоснование схемы ЭЦП, построенной на основе заданного проверочного уравнения
2. Описание процедуры генерации подписи и формулирование требований к ней;
3. Оценка стойкости и безопасных размеров параметров криптосхемы;
4. Вывод формул для вычисления параметров *к* и *g;*
5. Анализ схемы на наличие слабостей и поиск вариантов усиления с минимальным модифицированием;

Контрольные вопросы для защиты лабораторной работы №9.

1. Что такое «разделение секрета»?
2. Что такое «тени» и как их вычислить?
3. Назовите схемы разделения секрета.
4. Достоинства схемы разделения секрета.
5. Недостатки схемы разделения секрета.

Контрольные вопросы для защиты лабораторной работы №10.

1. Какие программные криптосистемы шифрования вы знаете, назовите их.
2. Назовите основные функциональные возможности Kremlin?
3. Перечислите исполняемые файлы Kremlin?
4. Как осуществляется шифрование файлов?
5. Как происходит отправка зашифрованных сообщений?
6. С помощью каких процедур осуществляется безвозвратное удаление файлов?
7. Какими методами возможна очистка истории работы на компьютере при помощи Kremlin?
8. Какие функции КМИЗ выполняет Kremlin?

Контрольные вопросы для защиты лабораторной работы №11.

1. Для чего служит программный продукт Fox Secret?
2. Какие алгоритмы лежат в основе работы Fox Secret?
3. Каким образом шифруется сообщение?
4. Какие типы файлов можно использовать для скрытия данных?
5. Какие операции над секретами вам доступны в начале работы?
6. Какие типы секретов доступны в программе?
7. Какие типы контейнеров для помещения туда секретов реализуются в программе?
8. Как создать хранилище RSA ключей?
9. Как создать закрытый ключ?

10. Для чего используется всплывающее меню?
11. Как происходит восстановление исходных данных?
12. Для чего предназначена программа Fox Secret?

Контрольные вопросы для защиты лабораторной работы №12.

1. Для чего служит программный продукт PGP?
2. Какие алгоритмы лежат в основе работы PGP?
3. Каким образом шифруется сообщение?
4. Кто может расшифровать сообщение?
5. Каковы преимущества используемого способа шифрования?
6. Можно ли расшифровать сообщение с помощью ключа шифрования?
7. Что такое парольная фраза?
8. Опишите процесс отправки зашифрованного сообщения.
9. Перечислите три основных способа шифрования информации.
10. Как происходит расшифровка сообщений?
11. Для чего предназначена программа PGPdisk?
12. Каковы преимущества использования программы PGPdisk?

Контрольные вопросы для защиты лабораторной работы №13.

1. Что такое стеганография?
2. Что такое компьютерная стеганография?
3. Какие виды компьютерной стеганографии вы знаете?
4. Что такое файл-контейнер?
5. Какие файлы можно скрывать с помощью компьютерной стеганографии?
6. Какие программные продукты для реализации методов стеганографии вы знаете?
7. С какими файлами работает программа S-Tools? Назовите преимущества и недостатки программы.
8. С какими файлами работает программа Masker 7.0? Назовите преимущества и недостатки программы.

Контрольные вопросы для защиты лабораторной работы №14.

1. Опишите суть метода вероятных слов.
2. К какому типу криптосистем относится шифр Виженера?
3. Сколько существуют способов шифрования с помощью шифра Виженера?
4. Каким образом строится таблица Виженера?

5. В чем состоит процедура шифрования с помощью шифра Виженера, используя формулу?

6. Что необходимо сделать, если длина ключа меньше длины исходного сообщения?

7. Каковы особенности шифра с «бегущим ключом»?

1. Критерии оценки:

– 0 баллов выставляется обучающемуся, если студент не выполнил работу;

– 3 балла выставляется обучающемуся, если студент выполнил работу и доля правильных ответов от 50% до 90%.

– 6 баллов выставляется обучающемуся, если студент выполнил работу и доля правильных ответов более 90%.

Составитель М.А. Ефремов

«31» 08 2021 г.

Задания для проведения текущего контроля успеваемости

Юго-Западный государственный университет

Кафедра информационной безопасности

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

по дисциплине «Методы и средства криптографической защиты информации»

(наименование дисциплины)

Задания в закрытой форме

1	Преобразование открытого текста сообщения в закрытый называется:
	алгоритм шифрования
	обеспечение аутентификации
	цифровая запись
	процедура шифрования
2	Входные параметры процесса шифрования
	Ключ
	зашифрованный текст
	Алгоритм
	открытый текст
3	Какие из сервисов реализуются при использовании криптографических преобразований
	Алгоритм
	контроль целостности
	Аутентификация
	Шифрование
4	Что позволяет предотвратить использование криптографических преобразований:
	отказ от информации
	использование алгоритмов асимметричного шифрования
	обеспечение аутентификации
	утечку информации
5	Знание ключа позволяет:
	выполнить обратное преобразование
	предотвратить утечку информации
	обеспечить аутентификацию
	использовать криптографические сервисы безопасности

6	Какой алгоритм не используется при симметричном шифровании:
	побитовое шифрование
	блочное шифрование
	алгоритм Эль-Гамаля
	поточное шифрование
7	Какой из режимов алгоритма DES используется для построения шифров гаммирования?
	обратная связь по выходу
	обратная связь по шифротексту
	сцепление блоков шифра
	электронная кодовая книга
8	Какова длина блока алгоритма шифрования DES:
	64 бита
	5 байт
	56 бит
	16 бит
	18 бит
9	Чем определяется уровень надежности применяемых криптографических преобразований:
	значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях
	отношением количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию.
	использованием большого числа ключей для шифрования;
	сложностью комбинации символов, выбранных случайным образом;
10	Ниже перечислены механизмы защиты информационных систем от несанкционированного доступа. Что здесь лишнее:
	обеспечения целостности
	идентификация и аутентификация пользователей и субъектов доступа
	управление доступом
	регистрация и учет
	обеспечение постоянного числа пользователей сети
11	Как иначе называется симметричное шифрование:
	шифрование методом Бейтса
	шифрование с переменным ключом.
	шифрование с закрытым ключом
	шифрование с открытым ключом
12	Какое из этих утверждений является верным:
	у S-блоков ГОСТ 8-битовые входы и 4-битовые выходы.
	у S-блоков ГОСТ 4-битовые входы и выходы
	у S-блоков ГОСТ 4-битовые входы и 8-битовые выходы

	нет S-блоков
13	Что означает «многократное шифрование» применительно к блочным шифрам:
	повторное применение алгоритма шифрования к шифротек- сту с другими ключами
	увеличение числа этапов шифрования открытого текста
	повторное применение алгоритма шифрования к шифротек- сту с теми же ключами
	шифрование одного и того же блока открытого текста несколько раз с несколькими ключами
14	Шифрование – это:
	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст
	система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации
	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения или несанкционированного использования
	способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
15	Криптоанализ – это:
	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст
	система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации
	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения или несанкционированного использования
	способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
16	Криптосистема – это:
	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов с целью

	извлечения конфиденциальных параметров, включая открытый текст
	система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации
	раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения или несанкционированного использования
	способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
17	Что такое алфавит?
	Буквы и символы
	конечное множество используемых для кодирования информации знаков
	Множество знаков одного из языков
	Набор букв русского алфавита
18	Пусть пользователь А хочет передать пользователю Б сообщение m=10, зашифрованное с помощью алгоритма RSA Пользователь Б имеет следующие параметры: P=7, Q=11, d=47 Вычислите значение C зашифрованного сообщения
	C=53
	C=54
	C=55
19	Что в переводе с греческого языка означает слово «криптография»?
	Шифр
	Дешифрование
	Тайнопись
	Тайный шифр
20	Выберите вариант ответа, содержащий только простые числа
	2, 5, 10, 19, 37, 212
	2, 3, 7, 9, 11, 13, 15
	2, 5, 19, 37, 59, 101
	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
21	Для чего предназначен центр сертификации ключей? Выберите *неверный* вариант ответа:
	для регистрации абонентов
	для выделения специальных каналов связи абонентам
	для поддержания в актуальном состоянии справочника действующих сертификатов
	для выпуска списка досрочно отозванных сертификатов
	для изготовления сертификатов открытых ключей
22	Кем было выполнено доказательство существования абсолютно стойких криптографических алгоритмов:

	К. Шенноном
	Б. Паскалем
	Г. Вернамом
	Б. Шнайером
23	Что является целью криптографического преобразования информации:
	защита информации от всех случайных или преднамеренных изменений
	защита информации от случайных помех при передаче и хранении
	сжатие информации
	защита информации от несанкционированного доступа, аутентификация и защита от преднамеренных изменений
24	Как называется шифр, в котором каждый символ открытого текста заменяется некоторым, фиксированным при данном ключе, символом другого алфавита?
	шифром Цезаря
	шифром замены
	шифром одноалфавитной подстановки
	шифром многоалфавитной подстановки
25	Что общего имеют все методы шифрования с закрытым ключом?
	в них для шифрования и расшифрования информации используется один и тот же ключ
	в них производится сложение символов исходного текста и ключа по модулю, равному числу букв в алфавите
	в них для шифрования информации используется один ключ, а для расшифрования – другой ключ
	в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов
26	Алгоритм DES является:
	блочным алгоритмом асимметричного шифрования
	алгоритмом формирования электронной цифровой подписи
	блочным алгоритмом симметричного шифрования
	алгоритмом вычисления функции хеширования
27	Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования?
	возведение в степень
	замена бит по таблице замен
	перестановка бит
	сложение по модулю 2
	нахождение остатка от деления на большое простое число
28	Как называется однозначное преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины?
	Хеширование

	Гаммирование
	Коллизия
	Сложение по модулю 2
	Перестановка
29	В системе связи, применяющей шифр Эль-Гамаля известны следующие параметры P = 11, A = 3, X1 = 4 Вычислите открытый ключ Y1 В качестве ответа укажите его числовое значение
	12
	4
	8
	3
	2
30	Абоненты некоторой сети применяют цифровую подпись по стандарту ГОСТ Р3410-94 с общими параметрами p = 23, q = 11, a = 9 Найдите открытый ключ абонента Петрова для X = 10 В качестве ответа укажите числовое значение Y
	18
	20
	16
	14
31	Что такое «код»?
	совокупность знаков, а также система правил, позволяющая представлять информацию в виде набора таких знаков
	любой ряд допустимых знаков в соответствии с используемой системой правил
	система записи знаков, позволяющая обнаруживать и корректировать ошибки при хранении и передаче сообщений
	совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты
32	Пусть исходный алфавит содержит следующие символы: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО слово ПЕРЕСТАНОВКА
	ОЁЬУЬБЯОЖРХО
	КЕНТЛБЗОЕРЪХЭ
	ОЁЬУЬБЯОЪРХО
	ОЁКИНБЯОЪХРОТ
33	Какова длина хеш-кода, создаваемого алгоритмом ГОСТ 3411-94?
	256 байт
	256 бит
	64 байта
	64 бита
	128 бит
34	Какие существуют алгоритмы генерации псевдослучайных чисел?

	ГОСТ 28147-89
	RC4
	алгоритм с использованием сдвиговых регистров с обратной связью
	DES
35	С помощью обобщенного алгоритма Евклида найдите числа x и y, удовлетворяющие уравнению 21x +12y = НОД(21,12) В качестве ответа запишите через запятую сначала значение x, а затем без пробела – значение y Например, если при вычислениях получилось, что x=-5, а y=2, то ответ надо записать так: -5,2
	-1,2
	1,2
	1,3
	-1,-2
	2, -1
36	Расшифруйте сообщение ЕВВФМШБЬШ, зашифрованное шифром Цезаря, если известно, что исходное сообщение составлено из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯОтвет запишите заглавными русскими буквами без пробелов
	СООБЩЕНИЕ
	СООБЩЕСТВО
	ОСВЕЩЕНИЕ
	СОВЕЩАНИЕ
	ПОСВЯЩЕНИЕ
37	Каков размер входного блока обрабатываемой информации при использовании стандарта шифрования AES?
	48 байт
	48 бит
	56 бит
	64 бита
	128 бит
38	Какие факторы влияют на стойкость блочного алгоритма шифрования?
	длина ключа
	количество раундов
	год разработки
	длина сообщения
	используемые операции
39	Алгоритм Диффи-Хеллмана основан на трудности
	решения задачи факторизации
	возведения целых чисел в степень по модулю
	вычисления дискретных логарифмов
	разложения больших чисел на множители

40	Каким требованиям должна удовлетворять электронная цифровая подпись?
	подпись не связывается с конкретным сообщением и может быть перенесена на другой документ
	подпись неразрывно связывается с данным сообщением и не может быть перенесена на другой документ
	подпись воспроизводится только одним лицом, а подлинность ее может быть удостоверена многими
	подпись воспроизводится многими лицами, а ее подлинность может быть удостоверена только одним лицом
41	Выберите верные утверждения
	алгоритм RC4 можно использовать для генерации псевдослучайной ключевой последовательности при поточном шифровании информации
	линейные конгруэнтные генераторы псевдослучайных чисел не рекомендуется использовать для генерации ключевых последовательностей при поточном шифровании
	поточные шифры применяются для формирования электронной цифровой подписи
	алгоритм RC4 можно использовать для формирования хеш-кода
42	Вычислите 39 по модулю 10
	13
	3
	1
	10
	39
	9
43	Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: АБРИКОС – ЛМЬФЦЪЭ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)
	11
	12
	10
	9
	8
	7
44	Какие ключи и как должны применяться при использовании асимметричных криптографических алгоритмов для шифрования передаваемых данных?
	отправитель шифрует сообщение своим открытым ключом, а получатель расшифровывает сообщение закрытым ключом отправителя
	отправитель шифрует сообщение открытым ключом получателя, а получатель расшифровывает сообщение своим закрытым ключом

	отправитель шифрует сообщение своим закрытым ключом, а получатель расшифровывает сообщение открытым ключом отправителя
	отправитель шифрует сообщение закрытым ключом получателя, а получатель расшифровывает сообщение своим открытым ключом
45	Для чего используются в криптографии сдвиговые регистры с обратной связью?
	для формирования открытых ключей
	для формирования хеш-кода
	для сжатия информации
	для генерации псевдослучайных чисел
46	На сколько блоков будет разбито сообщение размером 512 байт для шифрования алгоритмом DES? Ответ запишите в виде одного числа
	64
	256
	128
47	Чему равна сумма по модулю 28 двоичных чисел 01011001 и 11111010? Варианты ответов представлены в двоичной системе счисления
	11101100
	01000001
	01010011
	10111010
48	Пусть исходный алфавит состоит из следующих знаков (символ «_» (подчеркивание) будем использовать для пробела): АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_ Расшифруйте сообщение ПРЖВДЪЕ, зашифрованное с помощью таблицы Вижинера и ключа ОРЕХ
	БАБОЧКА
	ЛАСТОЧКА
	БАБУШКА
	БОЧКА
49	Два источника генерируют по два символа Первый источник генерирует символы с равными вероятностями, второй – с различными. Для какого источника количество информации по Шеннону, приходящееся на один символ, будет больше?
	количество информации для рассматриваемых источников одинаково
	недостаточно данных для точного ответа
	для первого
	для второго
50	Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: ЯБЛОКО – ЗЙФЧУЧ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)

	11
	7
	9
	3
51	Укажите требования к алгоритмам шифрования с открытым ключом
	вычислительно легко создавать пару (открытый ключ, закрытый ключ)
	вычислительно легко зашифровать сообщение открытым ключом
	вычислительно легко, зная только открытый ключ и зашифрованное сообщение, восстановить исходное сообщение
	вычислительно легко, зная открытый ключ, определить соответствующий закрытый ключ
52	Вычислите 38 по модулю 10
	2
	3
	9
	1
53	Расшифруйте сообщение ИБЛКНАКУ, зашифрованное методом перестановки с фиксированным периодом d=8 с ключом 64275813
	ГЛУБИНКА
	КЛУБНИКА
	БЛАНК
	БУЛКА
54	Как называется «исторический» шифр, в котором каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите, о применении которого имеются документальные свидетельства?
	шифр Цезаря
	шифр Бэбиджа
	шифр Шеннона
	шифр Вижинера
55	Выберите вариант ответа, содержащий только простые числа
	2, 9, 23, 43, 59, 89, 101
	3, 13, 23, 43, 83, 113
	2, 5, 19, 37, 59, 133
	2, 5, 19, 39, 59, 101
56	Пусть пользователь А хочет передать пользователю Б сообщение m=10, зашифрованное с помощью алгоритма RSA Пользователь Б имеет следующие параметры: P=7, Q=17, d=53 Вычислите значение с зашифрованного сообщения:
	c=43
	c=39
	c=41
	c=40

57	Как называется структура в составе большой сети связи, занимающаяся генерированием ключей, их хранением и архивированием, заменой или изъятием из обращения старых и ненужных ключей?
	центр открытого шифрования
	устройство распределения ключей
	центр распределения ключей
	центр закрытого шифрования
58	Как называется функция, которая для строки произвольной длины вычисляет некоторое целое значение или некоторую другую строку фиксированной длины?
	хеш-функция
	функция Эйлера
	односторонняя функция
	функция гаммирования
59	Как называется сообщение, полученное после преобразования с использованием любого шифра?
	Имитовставкой
	Ключом
	закрытым текстом
	открытым текстом
60	Как называется натуральное число, которое делится, помимо самого себя и единицы, еще хотя бы на одно число?
	простое число
	каноническое число
	составное число
	криптографическое число
61	Может ли шифр с конечным ключом быть совершенным?
	Да
	в зависимости от параметров шифра
	Нет
	да, если это алгоритм шифрования с открытым ключом
62	Как называется метод шифрования, в котором входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов?
	шифр замены
	шифр многоалфавитной подстановки
	шифр асимметричного преобразования
	шифр перестановки
63	Какие требования предъявляются в настоящее время к блочным шифрам?
	алгоритм шифрования должен допускать как программную, так и аппаратную реализацию

	в пространстве возможных ключей шифра должно быть не менее 210 «надежных» ключей
	алгоритм шифрования должен содержать не более четырех простейших операций
	знание алгоритма шифрования не должно влиять на надежность защиты
64	Какие операции применяются в шифре, определяемом ГОСТ 28147-89?
	нахождение остатка от деления на большое простое число
	сложение по модулю 2
	циклический сдвиг
	возведение в степень
	замена бит по таблице замен
65	Чем определяется разрядность сдвигового регистра с обратной связью?
	количеством бит, которое может одновременно храниться в регистре сдвига
	температурой окружающей среды
	скоростью работы регистра
	количеством входов в устройстве генерации функции обратной связи
66	Односторонние функции, то есть функции, которые относительно легко вычислить, но практически невозможно найти по значению функции соответствующее значение аргумента, можно использовать для
	формирования хеш-кодов
	контроля и исправления ошибок при передаче информации
	шифрования сообщений
	формирования цифровой подписи
67	Алгоритм основан RSA на трудности
	деления больших целых чисел
	разложения больших чисел на множители
	вычисления дискретных логарифмов
	возведения целых чисел в степень по модулю
68	Зашифруйте методом перестановки с фиксированным периодом d=6 с ключом 436215 сообщение ПЕРЕСТАНОВКА
	КОЛЮЧКА
	ЕРТЕПСВОАНАК
	БАНЕКГШЛОХЪ
	РНГШЛОПАИЛИ
69	Чему равен результат выполнения операции циклического сдвига влево на 5 разрядов для шестнадцатеричного числа 0B5? Варианты ответов представлены в двоичной системе счисления
	10110110

	11101001
	10011011
	01010101
70	Выберите верные утверждения:
	чем больше период последовательности, порождаемой генератором псевдослучайных чисел, тем лучше
	линейные конгруэнтные генераторы псевдослучайных чисел рекомендуется использовать для генерации ключевых последовательностей при поточном шифровании
	поточные шифры применяются для проверки целостности сообщения
	поточные шифры не применяются для формирования электронной цифровой подписи
71	Для решения каких задач может использоваться алгоритм Диффи-Хеллмана?
	формирования общих секретных ключей
	шифрования сообщений
	формирования электронной цифровой подписи
	формирования хеш-значений
72	Расшифруйте сообщение ИЫЛРУДХРТ, зашифрованное шифром Цезаря, если известно, что исходное сообщение составлено из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ. Ответ запишите заглавными русскими буквами без пробелов
	БУДИЛЬНИК
	АТМОСФЕРА
	ЛУКОМОРЬЕ
	ВЕДОМОСТЬ
73	Определите ключ в системе шифрования, использующей перестановку с фиксированным периодом d=5 по паре открытых и зашифрованных сообщений: ИНФОРМАЦИЯ – НРФИОАЯЦМИ Ответ запишите в виде последовательности цифр без пробелов
	35214
	25314
	43125
	54213
74	Под целостностью понимают (выберите продолжение)
	гарантирование невозможности несанкционированного изменения порядка следования информации
	гарантирование невозможности несанкционированного изменения переносов в текстовой информации
	гарантирование невозможности несанкционированного изменения объема информации
	гарантирование невозможности несанкционированного изменения информации

75	Выберите вариант ответа, содержащий только взаимно простые числа
	7, 27, 77, 147
	4, 7, 15, 60
	5, 19, 32, 49
	5, 9, 27, 54
76	Как расшифровывается аббревиатура AES?
	Analytic Encryption Standard
	Advanced Encryption Standard
	American Extended Standard
	Advanced Extended Standard
77	Какая наука разрабатывает методы «вскрытия» шифров?
	линейная алгебра
	Криптоанализ
	Криптография
	теория чисел
78	Что такое «избыточность» помехоустойчивого кода?
	число информационных разрядов в кодовом слове
	число разрядов двух кодовых слов, в которых они различны
	характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом
	наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код
79	Как называется режим использования блочного шифра, в котором каждый блок исходных данных шифруется независимо от остальных блоков с применением одного и того же ключа шифрования?
	режим формирования электронной цифровой подписи
	режим создания хеш-кода
	режим простой поблочной замены
	режим сцепления блоков шифра
80	Как называется распределенный алгоритм, определяющий последовательность действий каждой из сторон?
	Протокол
	электронная цифровая подпись
	процесс шифрования
	хэш-функция
81	Определите наибольший общий делитель чисел 187 и 264
	13
	11
	9
	7
82	Определите наибольший общий делитель чисел 146 и 182
	6

	4
	2
	12
83	Определите наибольший общий делитель чисел 293 и 47
	47
	1
	13
	7
84	Определите наибольший общий делитель чисел 139 и 278
	1
	2
	139
	278
85	Под конфиденциальностью понимают (выберите продолжение):
	решение проблемы защиты информации от ее изменения со стороны лиц, не имеющих права доступа к ней
	решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, имеющих права доступа к ней
	решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней
	решение проблемы запуска программ со стороны лиц, не имеющих права доступа к ним
86	В чем заключается общая идея эффективного кодирования методом Хаффмана?
	из всех возможных кодовых слов считаются допустимыми не все, а лишь некоторые
	символам с меньшей вероятностью присваиваются более короткие коды, тогда как чаще встречающимся символам – более длинные
	символам с большей вероятностью присваиваются более короткие коды, тогда как реже встречающимся символам – более длинные
	производится замена цепочек или серий повторяющихся байтов на один кодирующий байт-заполнитель и счетчик числа их повторений
87	Какой способ реализации криптографических методов обладает максимальной скоростью обработки данных?
	Программный
	Электромеханический
	Аппаратный
	Ручной
88	Для решения каких задач можно использовать алгоритмы шифрования с открытым ключом?
	для распределения секретных ключей, используемых потом при шифровании документов симметричными методами
	для формирования цифровой подписи под электронными документами

	для помехоустойчивого кодирования передаваемых сообщений
	для шифрования передаваемых и хранимых данных в целях их защиты от несанкционированного доступа
89	Определите число натуральных чисел, не превосходящих 33 и взаимно простых с 33
	15
	14
	20
	1
90	Известно, что для некоторого источника сообщений количество информации по Хартли, приходящееся на 1 символ, равно 5 битам Чему равно количество символов в алфавите источника сообщений?
	32
	64
	128
	256
91	Что такое «минимальное кодовое расстояние»?
	число контрольных разрядов в кодовом слове
	число разрядов двух кодовых слов, в которых они различны
	наименьшее из всех расстояний по Хэммингу для любых пар различных кодовых слов, образующих код
	характеристика помехоустойчивого кода, показывающая, насколько увеличена длина кодового слова по сравнению с обычным непомехоустойчивым кодом
92	Что называют открытым ключом в асимметричных методах шифрования?
	ключ, который не обязательно хранить в секрете
	ключ, который должен храниться в секрете
	ключ, который используется для выработки имитовставки
	любой ключ, используемый для шифрования или расшифрования
93	Определите число натуральных чисел, не превосходящих 59 и, взаимно простых с 59
	27
	16
	58
	3
94	Определите наибольший общий делитель чисел 64 и 89
	1
	2
	32
	4
	12
95	Определите наибольший общий делитель чисел 325 и 208
	2

	11
	13
	55
96	С точки зрения криптографии, энтропия сообщения определяет …
	длину сообщения
	максимальное количество бит информации, которое может быть передано одним символом рассматриваемого языка, при условии, что все последовательности символов равновероятны
	количество символов, которые необходимо раскрыть, чтобы узнать содержание сообщения
	количество информации, приходящееся на один символ сообщения
97	Какой язык обладает минимальной избыточностью сообщений?
	Язык, в котором все символы равновероятны и могут встречаться в сообщениях независимо друг от друга в любом порядке
	Язык, в котором только два символа
	Язык, в котором как можно больше символов
	Язык, в котором некоторые символы гораздо вероятнее других
98	Длина ключа в алгоритме AES составляет
	64 байта
	56 байт
	Длина ключа может быть переменной в зависимости от используемого количества раундов
	256 бит
99	Какая операция наиболее быстро выполняется при программной реализации алгоритмов шифрования?
	возведения в степень
	нахождения остатка от деления на большое простое число
	вычисления дискретных логарифмов
	сложения по модулю 2
100	Расшифруйте сообщение ЖКИЛШЪОБМ, зашифрованное шифром Цезаря, если известно, что исходное сообщение составлено из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ. Ответ запишите заглавными русскими буквами без пробелов
	КРИПТОГРАФИЯ
	КОМПЬЮТЕР
	КЛАВИАТУРА
	ОСВЕЩЕНИЕ

Задания в открытой форме

1. Дайте определения основынм понятиям криптологии.
2. О чём гласит теорема о делении с остатком.
3. Назовите алгоритм действий при разделении секрета.
4. Что такое сравнения первой степени.
5. Для чего нужна китайская теорема об остатках.
6. Дайте определение шифру полиалфавитной подстановке.
7. Что такое стеганография?
8. Для чего нужна программа PGP?
9. Назовите свойства функции Эйлера.
10. Алгоритм решения сравнений первой степени.

Задания на установление правильной последовательности

1. Установить правильную последовательность:

Найти НОД для чисел 28 и 64.

Находим произведение одинаковых простых множителей и записываем ответ;

Разложим на простые множители данные числа;

Подчеркиваем одинаковые простые множители в обоих числах.

2. Установите правильную последовательность.

1. Выбор ключа К длиной М символов.
2. Символы исходного текста последовательно замещаются символами, выбираемыми из $T_ш$ по следующему правилу:
   1) определяется символ k_m ключа К, соответствующий замещаемому символу s_{or};
   2) находится строка i в $T_ш$, для которой выполняется условие $k_m=b_{i1}$;
   3) определяется столбец j, для которого выполняется условие: $s_{or}=b_{1j}$;
   4) символ s_{or} замещается символом b_{ij}.
3. Под каждым символом s_{0r} исходного текста длиной I символов размещается символ ключа k_m, (рис. 3.5). Ключ повторяется необходимое число раз.
4. Построение матрицы шифрования $T_ш,=(b_{ij})$ размерностью [(M+1), R] для выбранного ключа К.
5. Полученная зашифрованная последовательность разбивается на блоки определенной длины, например, по четыре символа. Последний блок дополняется, при необходимости, служебными символами до полного объема.

3. Установите правильную последовательность.

Процедура создания ключей:

А) вычисляется функция Эйлера;

Б) выбираются два простых числа;

В) выбирается открытый ключ, как произволное число взаимно простое к функции Эйлера;

Г)вычисляется произведение простых чисел;

Д) вычисляется секретный ключ d, как обратное число к открытому ключу по модулю функции Эйлера;

Е) публикуется открытый ключ

4. Установите правильную последовательность.

Процедура опознавания с использованием простого пароля может быть представлена в виде следующей последовательности действий:

1) пользователь вводит пароль;

2) пользователь посылает запрос на доступ к компьютерной системе и вводит свой идентификатор;

3) система запрашивает пароль;

4) система сравнивает полученный пароль с паролем пользователя, хранящимся в базе эталонных данных системы защиты, и разрешает доступ, если пароли совпадают; в противном случае пользователь к ресурсам компьютерной системы не допускается.

5. Установите правильную последовательность.

Процесс стеганографии:

1) Выбор информационного файла;

2) Кодирование файла;

3) Отправление сокрытого сообщения по электронной почте и его декодирование;

4) Выбор стеганографической программы;

5) Выбор файла-контейнера.

Задание на установление соответствия

1. Установите соответствие:

Пусть хеш-функция y=h(x1x2…xn) определяется как результат выполнения побитовой операции «сумма по модулю 2» для всех байтов сообщения, представленного в двоичном виде Длина хеш-кода равна 8 битам Для каждого из шести сообщений, записанных в левом столбце, найдите соответствующий результат вычисления хеш-функции из правого столбца Все сообщения и значения хеш-функции представлены в шестнадцатеричном формате

Сообщения:

а) 34 0A9 0B6

б) 32 7F 0B3

в) 1A 0B4 96

г) 0D2 0C1 0B2

д) 0E4 36 29

е) 21 0AE 54

Значения хеш-функции

1) 38

2) 2B

3) 0DB

4) 0A1

5) 0FB

6) 0FE

2. Установите соответствие:

1. Криптосистема;
2. Криптоанализ;
3. Криптография

А) раздел прикладной математики, изучающий модели, методы, алгоритмы,

программные и аппаратные средства анализа криптосистемы или её входных и выходных сигналов с целью извлечения конфиденциальных параметров, включая открытый текст;

Б) система, реализованная программно, аппаратно или программно - аппаратно и осуществляющая криптографическое преобразование информации;

В) раздел прикладной математики, изучающий модели, методы, алгоритмы, программные и аппаратные средства преобразования информации (шифрования) в целях сокрытия её содержания, предотвращения или несанкционированного использования.

3. Установите соответствие. Длина ключа:

а) AES

б) DES

в) ГОСТ 28147-89

1) 256 бит

2) переменная

3) 56 бит

4. Установить соответствие:

(1) шифр одноалфавитной подстановки

(2) шифр многоалфавитной подстановки

(3) шифр перестановки

(4) шифр Цезаря

а) метод шифрования, в котором входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов;

б) каждая буква исходного текста заменялась буквой, стоящей на некоторое фиксированное число мест дальше в алфавите;

в) каждый символ открытого текста заменяется некоторым, фиксированным при данном ключе, символом другого алфавита?

г) это совокупность шифров простой замены, которые используются для шифрования очередного символа открытого текста согласно некоторому правилу.

5. Установите соответствие расположения зон безопасности:

а) Чему равен результат выполнения операции циклического сдвига влево на 5 разрядов для шестнадцатеричного числа 0B5?

б) Чему равен результат выполнения операции циклического сдвига влево на 5 разрядов для двоичного числа 10101100?

в) Чему равен результат выполнения операции циклического сдвига влево на 7 разрядов для одного байта, хранящего шестнадцатеричное значение 37?

(1) 10010101

(2) 10011011

(3) 10110110

Компетентностно-ориентированные задачи

1. Решить сравнение 2160x≡807(mod1317)

2. Решить систему сравнений:

$$\begin{cases} x \equiv 13\ mod\ (18) \\ x \equiv 19\ mod\ (29) \\ x \equiv 12\ mod\ (17) \end{cases}$$

3. Найти НОД 57824 и 2151 и его разложение.
4. Решить сравнение, используя подходящие дроби: 9x≡12(mod21)
5. Составить таблицу индексов по модулю 78.
6. Решить сравнение: $x^{35} \equiv 17(mod67)$.
7. Пусть исходный алфавит содержит следующие символы: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ Зашифруйте с помощью шифра Вижинера и ключа ЯБЛОКО слово ПОДСТАНОВКА
8. Определите ключи шифра Цезаря, если известны следующая пара открытый текст – шифротекст: ВИНОГРАД – ШЯДЕЩЖЦЪ (исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ)
9. Пусть исходный алфавит состоит из следующих знаков (символ «_» (подчеркивание) будем использовать для пробела): АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_ Расшифруйте сообщение ЪРОЕШШОФФВП, зашифрованное с помощью таблицы Вижинера и ключа ОРЕХ
10. Чему равна сумма по модулю 28 шестнадцатеричных чисел 9E и 0A3? Варианты ответов представлены в двоичной системе счисления Примечание: десятичные или шестнадцатеричные числа необходимо сначала перевести в двоичный вид

Критерии оценки:

— задание в закрытой форме — 2 балла,
— задание в открытой форме — 2 балла,
— задание на установление правильной последовательности — 2 балла,
— задание на установление соответствия — 2 балла,
— решение компетентностно-ориентированной задачи — 3 балла.

Составитель М.А. Ефремов

«31» 08 2021 г.