Название учреждения, в котором выполнялась данная диссертационная работа

На правах рукописи

Фамилия Имя Отчество

Название диссертационной работы

Специальность XX.XX.XX ”—
«Название специальности»

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
уч. степень, уч. звание
Фамилия Имя Отчество

Город ”— 20XX

ЗМІСТ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

СЛОВАРЬ ТЕРМИНОВ

Открытый (исходный) текст — данные (не обязательно текстовые), передаваемые без использования криптографии.

Шифротекст, шифрованный (закрытый) текст — данные, полученные после применения криптосистемы.

Шифр, криптосистема — совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.

Символ — это любой знак, в том числе буква, цифра или знак препинания.

Алфавит — конечное множество используемых для кодирования информации символов. Стандартный алфавит может быть изменён или дополнен символами.

Ключ — параметр шифра, определяющий выбор конкретного преобразования данного текста. В современных шифрах криптографическая стойкость шифра целиком определяется секретностью ключа (принцип Керкгоффса).

Шифрование — процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.

Расшифровывание — процесс нормального применения криптографического преобразования шифрованного текста в открытый.

Асимметричный шифр, двухключевой шифр, шифр с открытым ключом — шифр, в котором используются два ключа, шифрующий и расшифровывающий. При этом, зная лишь ключ зашифровывания, нельзя расшифровать сообщение, и наоборот.

Открытый ключ — тот из двух ключей асимметричной системы, который свободно распространяется. Шифрующий для секретной переписки и расшифровывающий — для электронной подписи.

Секретный ключ, закрытый ключ — тот из двух ключей асимметричной системы, который хранится в секрете. Криптоанализ — наука, изучающая математические методы нарушения конфиденциальности и целостности информации.

Система шифрования (шифрсистема) — это любая система, которую можно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме адресата.

Криптостойкостью — это характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. способность противостоять

криптоанализу).

Криптоаналитик — учёный, создающий и применяющий методы криптоанализа. Криптография и криптоанализ составляют криптологию, как единую науку о создании и взломе шифров (такое деление привнесено с запада, до этого в СССР и России не применялось специального деления).

Криптографическая атака — попытка криптоаналитика вызвать отклонения в атакуемой защищённой системе обмена информацией. Успешную криптографическую атаку называют взлом или вскрытие.

Дешифрование (дешифровка) — процесс извлечения открытого текста без знания криптографического ключа на основе известного шифрованного. Термин дешифрование обычно применяют по отношению к процессу криптоанализа шифротекста (криптоанализ сам по себе, вообще говоря, может заключаться и в анализе криптосистемы, а не только зашифрованного ею открытого сообщения).

Криптографическая стойкость — способность криптографического алгоритма противостоять криптоанализу.

Имитозащита — защита от навязывания ложной информации. Другими словами, текст остаётся открытым, но появляется возможность проверить, что его не изменяли ни случайно, ни намеренно. Имитозащита достигается обычно за счет включения в пакет передаваемых данных имитовставки.

Имитовставка — блок информации, применяемый для имитозащиты, зависящий от ключа и данных.

Электронная цифровая подпись(электронная подпись) — асимметричная имитовставка (ключ защиты отличается от ключа проверки). Другими словами, такая имитовставка, которую проверяющий не может подделать.

Центр сертификации — сторона, чья честность неоспорима, а открытый ключ широко известен. Электронная подпись центра сертификации подтверждает подлинность открытого ключа.

Хеш-функция — функция, которая преобразует сообщение произвольной длины в число («свёртку») фиксированной длины. Для криптографической хеш-функции (в отличие от хеш-функции общего назначения) сложно вычислить обратную и даже найти два сообщения с общей хеш-функцией.

ВСТУП

Использовать можно в двух системах:

Первый вариант — это выполняются первые 8 работ и получают нужную оценку.

Второй вариант — каждое задание добавляет балы, общая сумма балов определяет итоговую оценку. (Данная система более правильна и гибка, но требует набирать балы за работу)

ЛАБОРАТОРНА РОБОТА 1

ОСНОВЫ ШИФРОВАНИЯ. СИММЕТРИЧНЫЕ ШИФРЫ

Мета роботи: Изучить основные типы шифров. Исследование симметричных методов шифрование. Получение практических навыков изученных методов шифровки сообщений.

Теоретические ведомости

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:

– защиту конфиденциальности;

– защиту целостности.

Проблемы защиты конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

1. Виды криптосистем

Для многих обывателей термин «криптография» означает что-то загадочное и таинственное. Однако в настоящее время различные виды шифрования можно встретить буквально везде — это и простые кодовые замки на дипломатах, и многоуровневые системы защиты секретных файлов. Люди сталкиваются с ней, когда вставляют в банкомат карточку, совершают денежные переводы, покупают через интернет товары, общаются по Skype, отправляют письма на электронную почту. Любые дела, связанные с информацией, так или иначе имеют отношение к криптографии. Но, несмотря на всё многообразие сфер применения, в настоящее время существует всего несколько способов шифрования. Все эти методы криптографии относятся к двум видам криптографических систем: симметричным (с секретным ключом) и ассиметричным (с открытым ключом).

1.1. Симметричный метод. Симметричные системы позволяют шифровать и расшифровывать информацию с помощью одного и того же ключа. Расшифровать криптографическую систему секретного ключа невозможно, если дешифровщик не обладает секретным ключом.

1.2. Асимметричный метод. В криптографических системах с открытым ключом пользователи обладают собственным открытым и частным закрытым ключами. К открытому ключу имеют доступ все пользователи, и информация шифруется именно с его помощью. А вот для расшифровки необходим частный ключ, находящийся у конечного пользователя. В отличие от криптограмм с секретным ключом в такой системе участниками являются не две, а три стороны. Третья может представлять собой сотового провайдера или, например, банк. Однако эта сторона не заинтересована в хищении информации, поскольку она заинтересована в правильном функционировании системы и получении положительных результатов.

1.3. Блочные шифры. Это функция шифрования, которая применяется к блокам текста фиксированной длины. Текущее поколение блочных шифров работает с блоками текста длиной 256 бит (32 байт). Такой шифр принимает на вход 256-битовый открытый текст и выдаёт 256-битовый шифрованный текст.

Блочный шифр является обратимым: существует функция дешифрования, которая принимает на вход 256-битовый шифрованный текст и выдаёт исходный 256-битовый открытый текст. Открытый и шифрованный текст всегда имеет один и тот же размер, который называется размером блока *(block size)*.

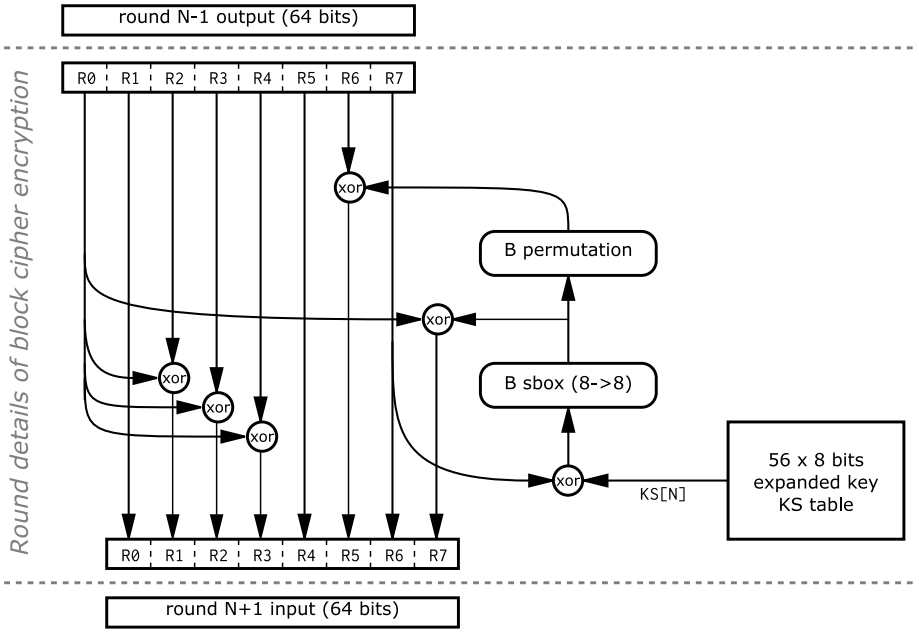

Рисунок 1.1 — Подробный разбор алгоритма блочного скремблирования DVB

1.4. Потоковые шифры. Потоковые шифры представляют собой разновидность гаммирования и преобразуют открытый текст в шифрованный

последовательно по 1 биту. Генератор ключевой последовательности выдаёт последовательность бит $k_1,k_2,\ldots,k_i,\ldots$ Эта ключевая последовательность складывается по модулю 2 с последовательностью бит исходного текста $p_1,p_2,\ldots,p_i,\ldots$ для получения шифрованного текста:

$$c_i = p_i \oplus k_i; \tag{1.1}$$

На приемной стороне шифрованный текст складывается по модулю 2 с идентичной ключевой последовательностью для получения исходного текста:

$$c_i \oplus k_i = p_i \oplus k_i \oplus k_i = p_i; \tag{1.2}$$

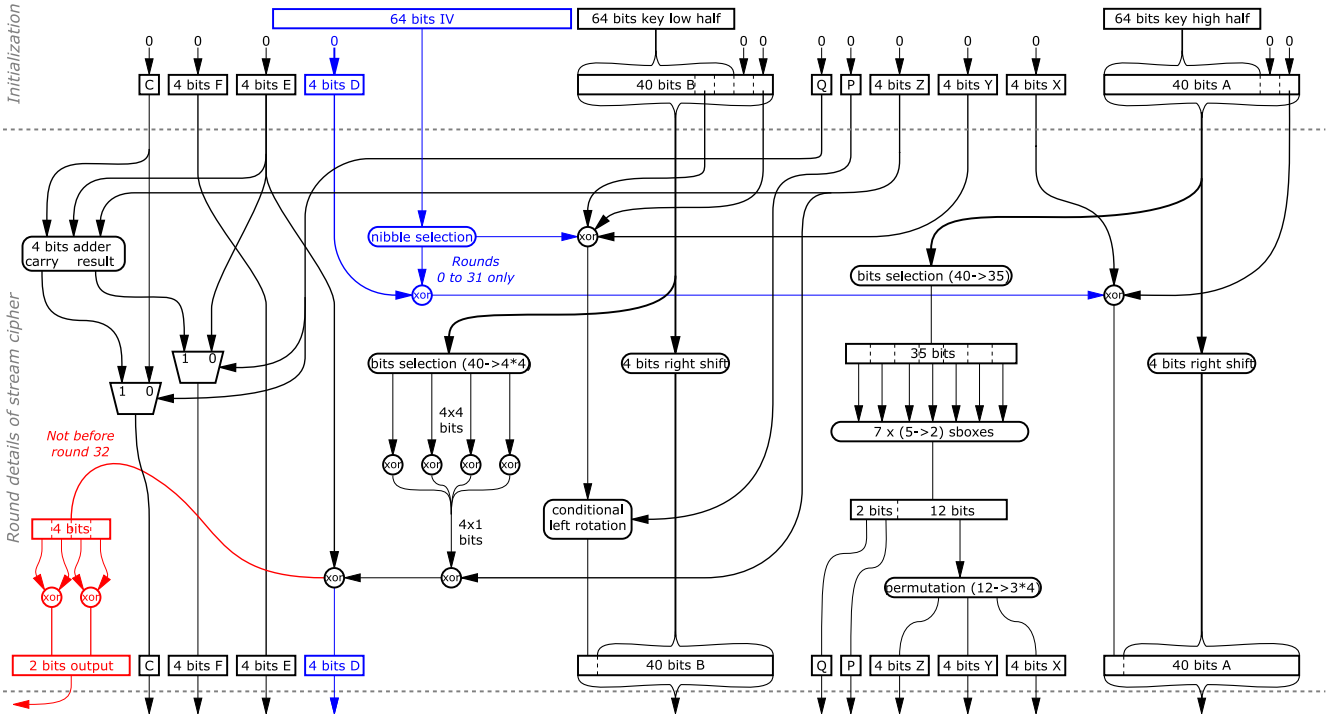

Рисунок 1.2 — Подробный разбор алгоритма потокового скремблирования DVB

Стойкость системы целиком зависит от внутренней структуры генератора ключевой последовательности. Если генератор выдаёт последовательность с небольшим периодом, то стойкость системы будет невелика. Напротив, если генератор будет выдавать бесконечную последовательность истинно случайных бит, то мы получим «ленту однократного использования» с идеальной стойкостью.

Реальная стойкость потоковых шифров лежит где-то посредине между стойкостью простой моноалфавитной подстановки и «ленты однократного использования». Генератор ключевой последовательности выдаёт поток битов,

который выглядит случайным, но в действительности является детерминированным и может быть в точности воспроизведен на приемной стороне. Чем больше генерируемый поток похож на случайный, тем больше усилий потребуется от криптоаналитика для взлома шифра.

1.5. Криптографические протоколы. В современной криптографии большое внимание уделяется не только созданию и исследованию шифров, но и разработке криптографических протоколов.

Протокол — это последовательность шагов, которые предпринимают две или большее количество сторон для совместного решения задачи. Все шаги следуют в порядке строгой очередности, и ни один из них не может быть сделан прежде, чем закончится предыдущий. Кроме того, любой протокол подразумевает участие, по крайней мере, двух сторон.

Криптографический протокол — это такая процедура взаимодействия двух или более абонентов с использованием криптографических средств, в результате которой *абоненты* достигают своей цели, а их *противники* – не достигают. В основе протокола лежит набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах. Каждый криптографический протокол предназначен для решения определённой задачи.

Рассмотрим простейший протокол для обмена конфиденциальными сообщениями между двумя сторонами, которые будем называть `абонент №1` и `абонент №2`. Пусть `абонент №1` желает передать зашифрованное сообщение `абоненту №2`. В этом случае их последовательность действий должна быть следующей.

1. Абоненты выбирают систему шифрования *(например, шифр Цезаря)*.
2. Абоненты договариваются о ключе шифрования.
3. `Абонент №1` шифрует исходное сообщение с помощью ключа выбранным методом и получает зашифрованное сообщение.
4. Зашифрованное сообщение пересылается `абоненту №2`.
5. `Абонент №2` расшифровывает зашифрованное сообщение с помощью ключа и получает открытое сообщение.

Этот протокол достаточно прост, однако он может действительно использоваться на практике. Криптографические протоколы могут быть простыми и сложными в зависимости от назначения.

2. Сферы применения криптографии.

В настоящее время криптография прочно вошла в нашу жизнь. Перечислим лишь некоторые сферы применения криптографии в современном информатизированном обществе:

- шифрование данных при передаче по открытым каналам связи (например, при совершении покупки в Интернете сведения о сделке);
- обслуживание банковских пластиковых карт;
- хранение и обработка паролей пользователей в сети;
- сдача бухгалтерских и иных отчётов через удалённые каналы связи;
- банковское обслуживание предприятий через локальную или глобальную сеть;
- безопасное от несанкционированного доступа хранение данных на жёстком диске компьютера.

Средства обеспечения информационной безопасности можно разбить на четыре группы:

- организационные средства (действия общего характера, предпринимаемые руководством организации, и конкретные меры безопасности, имеющие дело с людьми);
- законодательные средства (стандарты, законы, нормативные акты и т.д.);
- программно-аппаратные средства (системы идентификации и аутентификации; системы шифрования дисковых данных;
- системы аутентификации электронных данных и т.д.);
- криптографические средства (электронная цифровая подпись, шифрования, аутентификация и др.).

3. Оценка надёжности шифров

Методы оценки качества криптоалгоритмов, используемые на практике:

1. всевозможные попытки их вскрытия;
2. анализ сложности алгоритма дешифрования;
3. оценка статистической безопасности шифра.

В первом случае многое зависит от квалификации, опыта, интуиции криптоаналитика и от правильной оценки возможностей противника. Обычно считается, что противник знает шифр, имеет возможность его изучения, знает некоторые характеристики открытых защищаемых данных, например тематику сообщений, их

стиль, стандарты, форматы и т. п. Рассмотрим следующие примеры возможностей противника:

1. противник может перехватывать все зашифрованные сообщения, но не имеет соответствующих им открытых текстов;

2. противник может перехватывать все зашифрованные сообщения и добывать соответствующие им открытые тексты;

3. противник имеет доступ к шифру (но не ключам!) и поэтому может зашифровывать и расшифровывать любую информацию.

Во втором случае оценку стойкости шифра заменяют оценкой минимальной сложности алгоритма его вскрытия. Однако получение строго доказуемых оценок нижней границы сложности алгоритмов рассматриваемого типа не представляется возможным. Иными словами, всегда возможна ситуация, когда алгоритм вскрытия шифра, сложность которого анализируется, оказывается вовсе не самым эффективным.

Сложность вычислительных алгоритмов можно оценивать числом выполняемых элементарных операций, при этом, естественно, необходимо учитывать их стоимость и затраты на их выполнение. В общем случае это число должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютерных систем. Качественный шифр невозможно раскрыть способом более эффективным, чем полный перебор по всему ключевому пространству, при этом криптограф должен рассчитывать только на то, что у противника не хватит времени и ресурсов, чтобы это сделать.

Алгоритм полного перебора по всему ключевому пространству это пример так называемого экспоненциального алгоритма. Если сложность алгоритма выражается неким многочленом (полиномом) от n, где n - число элементарных операций, такой алгоритм носит название полиномиального.

В третьем случае считается, что надежная криптосистема с точки зрения противника является «чёрным ящиком», входная и выходная информационные последовательности которого взаимно независимы, при этом выходная зашифрованная последовательность является псевдослучайной. Поэтому смысл испытаний заключается в проведении статистических тестов, устанавливающих зависимость изменений в зашифрованном тексте от изменений символов или битов в исходном тексте или ключе, а также анализирующих, насколько выходная зашифрованная последовательность по своим статистическим свойствам приближается к истинно случайной последовательности. Случайность текста шифровки

можно приближённо оценивать степенью её сжатия при использовании алгоритма Лемпела-Зива, применяемого в архиваторах IBM PC. Если степень сжатия больше 10%, то можно считать криптосистему несостоятельной.

Задания

Выполнение первой работы не предусматривает использование специализированного ПО. Все задания должны быть выполнены способом расчёта.

Выполнение действий должно сопровождаться соответствующими заметками в отчёте.

Уровень 1.

1. Зашифровать 5-ю различными методами свои ФИО.
2. Приложить ключи к отчёту.
3. Составить инструкцию для расшифровки.
4. Выбрать данные соответствующие варианту из табл.
5. Используя данные по варианту расшифровать криптотекст.
6. Записать результаты в отчёт.

Уровень 2.

1. Используя ключ из табл. определить шифр.
2. Написать алгоритм шифровки-дешифровки заданным способом. Алгоритм должен быть представлен в виде подробной блок-схемы.

Пример выполнения работы

Варианты

Вопросы для контроля

1. Криптография и её роль в обществе.
2. Объяснить цель и задачи криптографии.
3. Пояснить какие бывают криптографические методы.
4. Виды криптографии и их классификация.
5. Отличие симметричных и асимметричный шифров.
6. Пояснить что такое исходный текст, шифр, ключ.

7. Принцип подбора ключа в симметричных криптосистемах.
8. Принцип работы симметричных шифров. Приведите примеры.
9. Принцип работы асимметричных шифров. Приведите примеры.
10. Преимущества и недостатки симметричный систем.
11. Шифры одиночной перестановки и перестановки по ключевому слову. Шифр Гронфельда.
12. Шифры двойной перестановки. Шифрование с помощью магического квадрата.
13. Шифр многоалфавитной замены и алгоритм его реализации.
14. Пояснить алгоритм шифрации двойным квадратом. Шифр Enigma.

ЛАБОРАТОРНА РОБОТА 2

РАБОТА С PKI

Мета роботи: Изучить методы генерации простых чисел, проверку на простоту числа и реализовать алгоритм ДХМ.

Теоретические ведомости

Подробнее о асимметричных криптосистемах.

1. **Методы генерации простых чисел**
2. **Известные на алгоритмы**
3. **Алгоритма ДХМ**

История, цель и важность

3.1. Принцип работы алгоритма.

3.2. Пример реализации. блок схема(как там мороки много)

Задания

Стандартный алгоритм для выполнения работы — Алгоритм ДХМ. Не запрещено использовать более новые алгоритмы, соответствующие тем же принципам что и данный ДХМ.

Вариант задания указан в табл..

Уровень 1.

1. Описать последовательность выполнения алгоритма для шифрования задания по варианту указаному выше.
2. Исследовать использование алгоритма в различных сферах ИБ. Указать реальное применение данного алгоритма.

Уровень 2.

1. Составить программу для реализации алгоритма ДХМ.
2. Произвести поэтапный обмен между двумя клиентами.
3. Предоставить все промежуточные данные, как на табл.
4. Продемонстрировать шифрованный блок и записать его в отчёт.

Уровень 3.

1. Разработать приложение клиент-клиент обмена информацией между несколькими людьми. Используя асинхронный алгоритм шифрования.
2. Продемонстрировать выполнение приложения.
3. Предоставить исходный код в дополнение отчёта.

Приложение может быть составлено в любом варианте, например: онлайн передача, запись в шифрованный файл, почтовый шифр и другие.

Пример выполнения работы

Варианты

Вопросы для контроля

1. Асимметричные системы.
2. Привести примеры асимметричных алгоритмов.
3. Криптосистемы. Использование асимметричный алгоритмов.
4. Преимущества и недостатки асимметричный систем.
5. Методы подбора ключа в асимметричных криптосистемах.
6. Сферы использование асимметричных алгоритмов.
7. Описать однонаправленные функции. Привести примеры.

ЛАБОРАТОРНА РОБОТА 3

CISCO. ТОПОЛОГИЯ СЕТЕЙ

Мета роботи: Напомнить основные концепции сети, их связи, уязвимости и основные узлы.

Теоретические ведомости

1. Информационная среда

Сеть со стороны ИБ.

Основые «дыры» в сети

2. Пути несанкционированного доступа

2.1. Средства защиты информации. (всяко-разно)Ссылка на вики по этой теме

– Маршрутизатор как способ защиты. (обязательно включить) - Фильтрование сети

- экранирование сети

Защита информации в сети Интернет:

Задания

Уровень 1.

1. Изучить предложенную топологию в Cisco. Представлена на рис.
2. Изменить модель по варианту.
    а) Построить реализацию заданной сети в Cisco или другом ПО.
    б) Указать недостатки заданной системы.

Уровень 2.

1. Настроить маршрутизатор по варианту.
    а) Шаг 1.
    б) Шаг 2.
    в) Шаг 3.
    г) Шаг 4.
    д) Шаг 5.
    е) Шаг 6.

ж) Шаг 7.

и) Шаг 8.

2. Разделение подсети, протокол RIP

Пример выполнения работы

Варианты

Вопросы для контроля

1. Какие есть средства защиты частной сети?
2. Что такое шлюз сетевого уровня?
3. Преимущества и недостатки использования сетевых экранов.
4. Что такое списки доступа? Каковы их цели и применение?
5. Приведите пример списка доступа.
6. Что такое маска подсети?
7. Каков принцип маски и как происходит фильтрация пакетов

ЛАБОРАТОРНА РОБОТА 4

ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

Мета роботи: Принцип работы, особенности, создание и использование ЭЦП.

Теоретические ведомости

Что такое ЭЦП. (электронная подпись)

1. **Структура сертификата**
2. **Преимущества ЭЦП**
3. **Недостатки ЭЦП**
4. **Применение ЭЦП**

(Интернет, https)алгоритмы и т.д.

4.1. Текущие требования к стойкости ЭЦП.

5. **Проверка подлинности ЭЦП**

Задания

Уровень 1.

1. Выбрать и отобразить реестр сертификатов на Вашем устройстве.
2. Опишите состав сертификата.
3. Выберите шифрованный блок данных.
4. Опишите полный путь данного сертификата к main-центру раздачи разрешений.

Уровень 2.

1. Создайте самоподписной сертификат.
2. Внесите его в свой реестр.
3. Приложите данные в отчёт.

Уровень 3.

1. Напишите алгоритм для создания подписанного сертификата.
2. Создайте сертификат подписанный ЭЦП из прошлого задания.
3. Приложите пример работы программы и подписанный сертификат.

Пример выполнения работы

Пример будет включать создание ЭПЦ как самостоятельно, так и используя ПО.

Варианты

Вопросы для контроля

1. Что такое электронно-цифровая подпись?
2. Каков принцип работы ЭЦП?
3. Почему ЭЦП используется в большинстве систем проверки документации?
4. Опишите этапы шифрования-дешифровки.
5. Как подпись обеспечивает целостность данных?
6. Случаи небезопасного использования ЭПЦ?
7. Где на компьютере могут храниться цифровые подписи?
8. Как проверить надёжность ЭПЦ?

ЛАБОРАТОРНА РОБОТА 5

СИСТЕМЫ АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЯ

Мета роботи: Освоить основные принципы систем автоматической авторизации пользователя.

Теоретические ведомости

«Нужно заменить систему KERBEROS на другую с подобным принципом работы»

Задания

Пример выполнения работы

Варианты

Вопросы для контроля

ЛАБОРАТОРНА РОБОТА 6

ПАКЕТЫ АНТИВИРУСНОЙ ЗАЩИТЫ

Мета роботи: Изучение способов защиты системы с помощью различного ПО. Научиться выбирать ПО для защиты системы.

Теоретические ведомости

Что такое вирус.

1. **История**
2. **Классификация**
3. **Виды антивирусной защиты**

Задания

Уровень 1.

1. По варианту выбрать систему.
2. Исследовать систему на стойкость, защиту.
3. Описать основные угрозы и способы взлома выбранной системы.
4. Анализ и выбор ПО для комплексной защиты.

Предоставить результат в виде отчета с подробным описанием слабых сторон системы, указать способы защиты и написать инструкцию для выбранного ПО.

Пример выполнения работы

Варианты

Вопросы для контроля

ЛАБОРАТОРНА РОБОТА 7

ПАССИВНЫЙ АНАЛИЗ ДАННЫХ

Мета роботи: Изучить способы анализа данных для дальнейшего применения. Применение пакета данных в целях защитных и атакующих систем.

Теоретические ведомости

Зачем нужен анализ данных в ИБ.

1. **Виды анализа данных**
2. **Выбор средств для пассивного анализа**

Выборка и поиск атак на ресурс используя методы пасивного анализа.

Задания

1. Выбрать задание по варианту из табл.
2. Провести пассивный анализ интернет трафика.
3. Провести выборку на массиве данных.
4. Запустить фишинговую угрозу.
5. Собрать дополнительные данные и найти вирус с помощью данного метода.
6. Отобразить результаты в отчёте.

Пример выполнения работы

Варианты

Вопросы для контроля

1. Что такое анализ данных в ИБ?
2. Какие бывают методы анализа?
3. Какое ПО для анализа данных вы знаете?
4. Как работает метод пассивного анализа?

5. Как работает метод активного анализа?
6. Какова надёжность методов анализа данных?
7. Какие особенности, достоинства и недостатки анализа вы знаете?

ЛАБОРАТОРНА РОБОТА 8

АРХИВАЦИЯ ДАННЫХ

Мета роботи: Выполнить исследование алгоритмов архивации данных. Использовать алгоритм Хаффмана и Лемпеля-Зива для архивации. Восстановить данные после

Теоретические ведомости

1. Архивация данных

2. Алгоритмы архивации данных

2.1. Алгоритм Хаффмана.

2.2. Алгоритм Лемпеля-Зива.

3. Актуальность архивации

4. Восстановление данных

Задания

1. Взять данные соответственно варианту из табл.
2. Удалить лишнюю информацию методом Хаффмана.
3. Провести операцию методом Лемпеля-Зива.
4. Сравнить результаты проведённых операций.
5. Описать актуальность архивации.
6. Сделать выводы по применению методов сжатия в различных криптосистемах.

Пример выполнения работы

Варианты

Вопросы для контроля

1. Что такое архивация данных?
2. Цель архивации?
3. Какие Вы знаете методы архивации?
4. Опишите принцип дерева Хаффмана.
5. Опишите алгоритм LZ77 или его аналог.
6. Сферы применения заданных алгоритмов.
7. Как выбрать алгоритм, если данные заранее известны?

РЕКОМЕНДАЦІЇ

ДОДАТОК А

ДОПОЛНЕНИЕПЕРВОЕ

Очередной подраздел приложения

И ещё один подраздел приложения