Титулка

Зміст

[Список сокращений и условных обозначений 4](#_Toc510731220)

[Словарь терминов Вступ 4](#_Toc510731221)

[Вступ 4](#_Toc510731222)

[1 Основы шифрования. Симметричные шифры 4](#_Toc510731223)

[Теоретические ведомости 4](#_Toc510731224)

[Задания 4](#_Toc510731225)

[Ход работы 4](#_Toc510731226)

[Вопросы для самоконтроля 4](#_Toc510731227)

[2 Работа с PKI 5](#_Toc510731228)

[Теоретические ведомости 5](#_Toc510731229)

[Задания 5](#_Toc510731230)

[Ход работы 5](#_Toc510731231)

[Вопросы для самоконтроля 5](#_Toc510731232)

[3 Cisco. Топология сетей 6](#_Toc510731233)

[Теоретические ведомости 6](#_Toc510731234)

[Задания 6](#_Toc510731235)

[Ход работы 6](#_Toc510731236)

[Вопросы для самоконтроля 6](#_Toc510731237)

[4 Электронно-цифровая подпись 7](#_Toc510731238)

[Теоретические ведомости 7](#_Toc510731239)

[Задания 7](#_Toc510731240)

[Ход работы 7](#_Toc510731241)

[Вопросы для самоконтроля 7](#_Toc510731242)

[5 Системы авторизации пользователя 8](#_Toc510731243)

[Теоретические ведомости 8](#_Toc510731244)

[Задания 8](#_Toc510731245)

[Ход работы 8](#_Toc510731246)

[Вопросы для самоконтроля 8](#_Toc510731247)

[6 Пакеты антивирусной защиты 9](#_Toc510731248)

[Теоретические ведомости 9](#_Toc510731249)

[Задания 9](#_Toc510731250)

[Ход работы 9](#_Toc510731251)

[Вопросы для самоконтроля 9](#_Toc510731252)

[7 Пассивный анализ данных 10](#_Toc510731253)

[Теоретические ведомости 10](#_Toc510731254)

[Задания 10](#_Toc510731255)

[Ход работы 10](#_Toc510731256)

[Вопросы для самоконтроля 10](#_Toc510731257)

[8 Архивация данных 11](#_Toc510731258)

[Теоретические ведомости 11](#_Toc510731259)

[Задания 11](#_Toc510731260)

[Ход работы 11](#_Toc510731261)

[Вопросы для самоконтроля 11](#_Toc510731262)

[Додаток А 12](#_Toc510731263)

[Додаток Б 13](#_Toc510731264)

1. Список сокращений и условных обозначений
2. 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.

1. Введение

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)

# Основы шифрования. Симметричные шифры

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

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. Шифры одиночной перестановки и перестановки по ключевому слову. Шифр Гронфельда.
11. Шифры двойной перестановки. Шифрование с помощью магического квадрата.

# Работа с PKI

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Cisco. Топология сетей

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Электронно-цифровая подпись

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Системы авторизации пользователя

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Пакеты антивирусной защиты

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Пассивный анализ данных

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Архивация данных

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

1. Додаток А
2. Додаток Б