Титулка

ЗМІСТ

Список сокращений и условных обозначений **4**

Словарь терминов **5**

Введение **8**

1 Основы шифрования. Симметричные шифры **9**

Теоретические ведомости 9

Задания 9

Ход работы 9

Вопросы для самоконтроля 9

2 Работа с PKI **10**

Теоретические ведомости 10

Задания 10

Ход работы 10

Вопросы для самоконтроля 10

3 Cisco. Топология сетей **11**

Теоретические ведомости 11

Задания 11

Ход работы 11

Вопросы для самоконтроля 11

4 Электронно-цифровая подпись **12**

Теоретические ведомости 12

Задания 12

Ход работы 12

Вопросы для самоконтроля 12

5 Системы авторизации пользователя **13**

Теоретические ведомости 13

Задания 13
Ход работы 13
Вопросы для самоконтроля 13
6 Пакеты антивирусной защиты 14
Теоретические ведомости 14
Задания 14
Ход работы 14
Вопросы для самоконтроля 14
7 Пассивный анализ данных 15
Теоретические ведомости 15
Задания 15
Ход работы 15
Вопросы для самоконтроля 15
8 Архивация данных 16
Теоретические ведомости 16
Задания 16
Ход работы 16
Вопросы для самоконтроля 16
Додаток А 17
Додаток Б 18

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.

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)

1 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.

2 РАБОТА С PKI

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

3 CISCO. ТОПОЛОГИЯ СЕТЕЙ

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

4 ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

5 СИСТЕМЫ АВТОРИЗАЦИИ ПОЛЬЗОВАТЕЛЯ

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

6 ПАКЕТЫ АНТИВИРУСНОЙ ЗАЩИТЫ

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

7 ПАССИВНЫЙ АНАЛИЗ ДАННЫХ

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

8 АРХИВАЦИЯ ДАННЫХ

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

ДОДАТОК А

ДОДАТОК Б