Титулка

ЗМІСТ

Список сокращений и условных обозначений **4**

Словарь терминов **5**

Введение **8**

1 МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ **9**

Теоретические ведомости 9

1 Симметричные криптосистемы 10

Задания 12

Вопросы для самоконтроля 14

2 Взлом. Частотная атака **16**

Теоретические ведомости 16

Задания 16

Ход работы 16

Вопросы для самоконтроля 16

3 СИММЕТРИЧНЫЕ ШИФРЫ. Часть 1 ..... **17**

Теоретические ведомости 17

Задания 17

Ход работы 17

Вопросы для самоконтроля 17

4 Симметричные шифры. Часть 2 ..... **18**

Теоретические ведомости 18

Задания 18

Ход работы 18

Вопросы для самоконтроля 18

5 Взлом. Часть 2 ..... **19**

Теоретические ведомости 19

Задания 19
Ход работы 19
Вопросы для самоконтроля 19
6 Асимметричные шифры. Часть 1 20
Теоретические ведомости 20
Задания 20
Ход работы 20
Вопросы для самоконтроля 20
7 Асимметричные шифры. Часть 2 21
Теоретические ведомости 21
Задания 21
Ход работы 21
Вопросы для самоконтроля 21
8 Электронно-цифровая подпись 22
Теоретические ведомости 22
Задания 22
Ход работы 22
Вопросы для самоконтроля 22
Додаток А 23
Додаток Б 24

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 МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Тема: Методы защиты информации. Классификация криптосистем.

Цель: Изучить основные методы криптографической защиты информации, использовать полученные знания для сокрытия путём шифрования.

Теоретические ведомости

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость того, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Постепенно защита информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации; даже проводится ФЗ о защите информации, который рассматривает проблемы и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

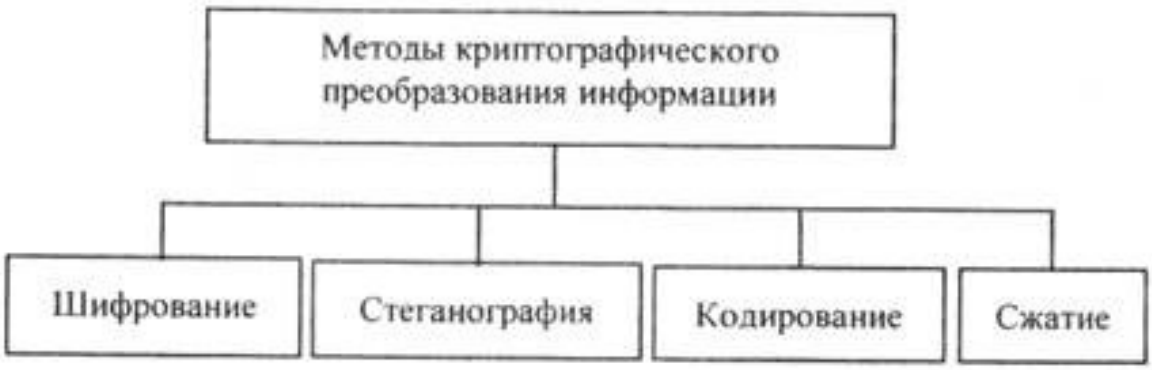

Рисунок 1.1 – Пример вставки рисунков

1 Симметричные криптосистемы

1.1 Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение «Неясное становится ещё более непонятным» записывается в таблицу из 5 строк и 7 столбцов по столбцам.

Таблица 1.1

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Ё	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ-НЯЕЕО-ЯОЕТЯ-СВЕЛП-НСТИЩ-ЕОЫНА-ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает метод *одиночной перестановки* по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово - **ЛУНАТИК**, получим следующую таблицу:

Таблица 1.2 – Метод перестановки по ключу

Л	У	Н	А	Т	И	К
4	**7**	**5**	**1**	**6**	**2**	**3**
Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

До перестановки

→ →

А	И	К	Л	Н	Т	У
1	**2**	**3**	**4**	**5**	**6**	**7**
С	Н	Я	Н	Н	Б	О
Я	Е	Т	Е	О	О	Е
Е	П	Н	Я	В	Л	С
Щ	О	Ы	С	И	Е	Т
Е	Н	М	Н	Т	Е	А

После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН-БОЯЕТ-ЕООЕЕ-ПНЯВЛ-СЩОЫС-ИЕТЕН-МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины её строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются алгоритмы двойных перестановок. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в таблице

Таблиця 1.3 – Метод перестановки по ключу

	2	**4**	**1**	**3**
4	П	Р	И	Е
1	З	Ж	А	Ю
2	-	Ш	Е	С
3	Т	О	Г	О

	1	**2**	**3**	**4**
4	И	П	Е	Р
1	А	З	Ю	Ж
2	Е	-	С	Ш
3	Г	Т	О	О

	1	2	3	4
1	А	З	Ю	Ж
2	Е	-	С	Ш
3	Г	Т	О	О
4	И	П	Е	Р

Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы. В результате перестановки получена шифровка:

АЗЮЖЕ_СШГТООИПЕР

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3x3 их 36, для 4x4 их 576, а для 5x5 их 14400.

В средние века для шифрования применялись и магические квадраты. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведённой в квадрате нумерации и затем переписать содержимое таблицы по строкам.

В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

Число магических квадратов очень резко возрастает с увеличением размера его сторон:

– для таблицы $3\times3\Rightarrow1$ существует только один квадрат;

– для таблицы $4\times4\Rightarrow880$;

– для таблицы $5\times5\Rightarrow250000$.

Задания

В соответствии с вашим вариантом из табл. 1.4 зашифровать текст используя методы криптографической защиты представленные ниже. Регистр должен быть учтён.

1) Шифры перестановки:

a) метод перестановки по ключу;
b) алгоритм двойной перестановки;
c) магические квадраты.

2) Шифры замены:

a) шифр Цезаря;
b) Аффиный шифр;
c) шифр Виженера;

d) шифра Плейфера.

3) Выполнить шифрование методом гаммирования.

Записать результаты шифрования в отчёт, сравнить методы, выбрать оптимальный для заданной фразы и аргументировать свой выбор.

Таблиця 1.4 **– Список фраз для шифрования**

1	6 x 6	небольшое сообщение для тестирования
2	3 x 13	В атмосфере происходит около 1800 гроз.
3	7 x 4	федеральное законодательство
4	4 x 6	Международные стандарты;
5	3 x 13	самая дорогая пицца в мире стоит $1000.
6	4 x 9	применение информационных технологий
7	3 x 12	административный уровень секретности
8	3 x 11	83% младших братьев выше старших
9	3 x 11	обеспечение доступа к информации
10	10 x 4	Индонезия расположена на 17508 островах.
11	4 x 7	у рыбы сарган зеленые кости.
12	8 x 4	язык хамелеона длиннее его тела
13	6 x 4	защищенность информации.
14	5 x 6	в озеро Байкал впадает 336 рек
15	3 x 10	гоночный болид едет по трассе.
16	8 x 3	опасность ’’открывается”
17	4 x 8	процесс обеспечения целостности
18	4 x 9	рекомендация использования терминов
19	5 x 6	обеспечивающее ее формирование
20	5 x 5	общегосударственный орган
21	8 x 4	технических средств ее передачи
22	3 x 11	ворон и ворона — два разных вида.
23	5 x 6	наибольший ущерб субъектам ИБ
24	9 x 3	информационная безопасность
25	8 x 4	ущерб при сервисном обслуживании
26	5 x 7	свойство аутентичности пользователя
27	8 x 4	данные были действия выполнены?!
28	6 x 6	законодательный уровень безопасности
29	8 x 4	из множества потенциально угроз
30	4 x 9	Защита процессов, процедур, программ

Вопросы для самоконтроля

4) Криптография и её роль в обществе.

5) Объяснить цель и задачи криптографии.

6) Пояснить какие бывают криптографические методы.

7) Виды криптографии и их классификация.

8) Отличие симметричных и асимметричный шифров.

9) Пояснить что такое исходный текст, шифр, ключ.

10) Принцип подбора ключа в симметричных криптосистемах.

11) Принцип работы симметричных шифров. Приведите примеры.

12) Принцип работы асимметричных шифров. Приведите примеры.

13) Шифры одиночной перестановки и перестановки по ключевому слову. Шифр Гронфельда.

14) Шифры двойной перестановки. Шифрование с помощью магического квадрата.

2 ВЗЛОМ. ЧАСТОТНАЯ АТАКА

Тема: Тема.

Цель: Опишите цель.

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

3 СИММЕТРИЧНЫЕ ШИФРЫ. ЧАСТЬ 1

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

4 СИММЕТРИЧНЫЕ ШИФРЫ. ЧАСТЬ 2

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

5 ВЗЛОМ. ЧАСТЬ 2

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

6 АСИММЕТРИЧНЫЕ ШИФРЫ. ЧАСТЬ 1

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

7 АСИММЕТРИЧНЫЕ ШИФРЫ. ЧАСТЬ 2

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

8 ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ

Тема: Тема.

Цель: Опишите цель

Теоретические ведомости

Задания

Ход работы

Вопросы для самоконтроля

ДОДАТОК А

ДОДАТОК Б