Титулка

Зміст

[Список сокращений и условных обозначений 4](#_Toc510895975)

[Словарь терминов 5](#_Toc510895976)

[Введение 8](#_Toc510895977)

[1 МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ 9](#_Toc510895978)

[Теоретические ведомости 9](#_Toc510895979)

[1 Симметричные криптосистемы 10](#_Toc510895980)

[Задания 14](#_Toc510895981)

[Вопросы для самоконтроля 16](#_Toc510895982)

[2 Взлом. Частотная атака Ошибка! Закладка не определена.](#_Toc510895983)

[Теоретические ведомости 18](#_Toc510895984)

[Задания 18](#_Toc510895985)

[Ход работы 18](#_Toc510895986)

[Вопросы для самоконтроля 18](#_Toc510895987)

[3 СИММЕТРИЧНЫЕ ШИФРЫ. Часть 1 19](#_Toc510895988)

[Теоретические ведомости 19](#_Toc510895989)

[Задания 19](#_Toc510895990)

[Ход работы 19](#_Toc510895991)

[Вопросы для самоконтроля 19](#_Toc510895992)

[4 Симметричные шифры. Часть 2 20](#_Toc510895993)

[Теоретические ведомости 20](#_Toc510895994)

[Задания 20](#_Toc510895995)

[Ход работы 20](#_Toc510895996)

[Вопросы для самоконтроля 20](#_Toc510895997)

[5 Взлом. Часть 2 21](#_Toc510895998)

[Теоретические ведомости 21](#_Toc510895999)

[Задания 21](#_Toc510896000)

[Ход работы 21](#_Toc510896001)

[Вопросы для самоконтроля 21](#_Toc510896002)

[6 Асимметричные шифры. Часть 1 22](#_Toc510896003)

[Теоретические ведомости 22](#_Toc510896004)

[Задания 22](#_Toc510896005)

[Ход работы 22](#_Toc510896006)

[Вопросы для самоконтроля 22](#_Toc510896007)

[7 Асимметричные шифры. Часть 2 23](#_Toc510896008)

[Теоретические ведомости 23](#_Toc510896009)

[Задания 23](#_Toc510896010)

[Ход работы 23](#_Toc510896011)

[Вопросы для самоконтроля 23](#_Toc510896012)

[8 Электронно-цифровая подпись 24](#_Toc510896013)

[Теоретические ведомости 24](#_Toc510896014)

[Задания 24](#_Toc510896015)

[Ход работы 24](#_Toc510896016)

[Вопросы для самоконтроля 24](#_Toc510896017)

[Додаток А 25](#_Toc510896018)

[Додаток Б 26](#_Toc510896019)

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)

# МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

**Тема:** Методы защиты информации. Классификация криптосистем.

**Цель:** Изучить простые 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.

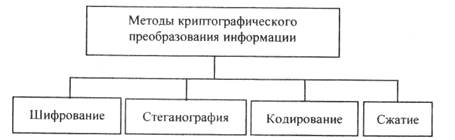


Рисунок . – Пример вставки рисунков

### Симметричные криптосистемы

#### 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.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Таблиця . | | | | | |
| 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:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Таблиця . – Метод перестановки по ключу | | | | | | | | | | | | | |
| Л | У | Н | А | Т | И | К |  | А | И | К | Л | Н | Т | | У |
| **4** | **7** | **5** | **1** | **6** | **2** | **3** |  | **1** | **2** | **3** | **4** | **5** | **6** | | **7** |
| Н | О | Н | С | Б | Н | Я | → | С | Н | Я | Н | Н | Б | | О |
| Е | Е | О | Я | О | Е | Т |  | Я | Е | Т | Е | О | О | | Е |
| Я | С | В | Е | Л | П | Н | → | Е | П | Н | Я | В | Л | | С |
| С | Т | И | Щ | Е | О | Ы |  | Щ | О | Ы | С | И | Е | | Т |
| Н | А | Т | Е | Е | Н | М |  | Е | Н | М | Н | Т | Е | | А |
| **До перестановки** | | | | | | |  | **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 . – Метод перестановки по ключу | | | | | | | | | | | | | | | | |
|  | **2** | **4** | **1** | **3** |  | | **1** | **2** | **3** | **4** |  | | 1 | 2 | 3 | 4 |
| **4** | П | Р | И | Е |  | 4 | И | П | Е | Р |  | **1** | А | З | Ю | Ж |
| **1** | З | Ж | А | Ю | 1 | А | 3 | Ю | Ж | **2** | Е | - | С | Ш |
| **2** | - | Ш | Е | С | 2 | Е | - | С | Ш | **3** | Г | Т | О | О |
| **3** | Т | О | Г | О | 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 3х3 их 36, для 4х4 их 576, а для 5х5 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.

Таблиця . – Исходный текст с идентификаторами

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П | Р | И | Е | З | Ж | А | Ю | \_ | Ш | Е | С | Т | О | Г | О |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

Таблиця . – Магический квадрат

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | 3 | 2 | 13 |  | О | И | Р | Т |
| 5 | 10 | 11 | 8 | → | З | Ш | Е | Ю |
| 9 | 6 | 7 | 12 | ← | - | Ж | А | С |
| 4 | 15 | 14 | 1 |  | Е | Г | О | П |

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

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

* для таблицы  существует только один квадрат;
* для таблицы ;
* для таблицы .

### Шифры простой замены

#### Система шифрования Цезаря.

Основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на *K* букв. Известная фраза Юлия Цезаря **VENI VINI VICI** – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в **SBKF SFAF SFZF** (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретён так называемый полибианский квадрат размером 5 x 5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже её в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

### Шифры сложной замены

#### Шифр Гронсфельда

Это модификация шифра Цезаря с использованием числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно так же, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

1. Пусть в качестве ключа используется группа из трех цифр – 314.
2. Тогда Сообщение СОВЕРШЕННО СЕКРЕТНО.
3. Ключ 3143143143143143143.
4. Шифровка ФПЖИСЬИОССАХИЛФИУСС.

В шифрах *многоалфавитной замены* для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).В компьютере операция шифрования соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

### Гаммирование

Процесс зашифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков аналогичной длины  ,  где - побитовое сложение,.

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные.

Исходное сообщение из букв русского алфавита преобразуется в числовое сообщение заменой каждой его буквы числом по следующей таблице:

Таблиця . – Числовая замена букв

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ж | З | И | К | Л | М | Н | О | П |
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 |
| Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ы | Э | Ю | Я |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |



Исходное сообщение ОТДУШКА. Для шифрования числового сообщения используется шифрующий отрезок последовательности А1, А2, ... подходящей длины, начинающийся с, , , , , .

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Исходное сообщение | О | Т | Д | У | Ш | К | А |
| Числовое исходное сообщение | 13 | 17 | 4 | 18 | 23 | 9 | 0 |
| Шифрующий отрезок | 1 | 5 | 6 | 17 | 8 | 19 | 3 |
| Числовое шифрованное сообщение | 14 | 23 | 10 | 5 | 1 | 28 | 3 |
| Шифрованное сообщение | П | Ш | Л | Е | Б | Ю | Г |

Помним, что в выбранном алфавите 30 символов.

## Задания

В соответствии с вашим вариантом из табл. Таблиця 1.7 зашифровать текст используя методы криптографической защиты представленные ниже. Регистр должен быть учтён.

1. Шифры перестановки:
   1. метод перестановки по ключу;
   2. алгоритм двойной перестановки;
   3. магические квадраты.
2. Шифры замены:
   1. шифр Цезаря;
   2. Аффиный шифр;
   3. шифр Виженера;
   4. шифра Плейфера.
3. Выполнить шифрование методом гаммирования.

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

|  |  |  |
| --- | --- | --- |
| Таблиця 1.7 – Список фраз для шифрования | | |
| 1 | 6 х 6 | небольшое сообщение для тестирования |
| 2 | 3 х 13 | В атмосфере происходит около 1800 гроз. |
| 3 | 7 х 4 | федеральное законодательство |
| 4 | 4 х 6 | Международные стандарты; |
| 5 | 3 х 13 | самая дорогая пицца в мире стоит $1000. |
| 6 | 4 х 9 | применение информационных технологий |
| 7 | 3 х 12 | административный уровень секретности |
| 8 | 3 х 11 | 83% младших братьев выше старших |
| 9 | 3 х 11 | обеспечение доступа к информации |
| 10 | 10 х 4 | Индонезия расположена на 17508 островах. |
| 11 | 4 х 7 | у рыбы сарган зеленые кости. |
| 12 | 8 х 4 | язык хамелеона длиннее его тела |
| 13 | 6 х 4 | защищенность информации. |
| 14 | 5 х 6 | в озеро Байкал впадает 336 рек |
| 15 | 3 х 10 | гоночный болид едет по трассе. |
| 16 | 8 х 3 | опасность ’’открывается” |
| 17 | 4 х 8 | процесс обеспечения целостности |
| 18 | 4 х 9 | рекомендация использования терминов |
| 19 | 5 х 6 | обеспечивающее ее формирование |
| 20 | 5 х 5 | общегосударственный орган |
| 21 | 8 х 4 | технических средств ее передачи |
| 22 | 3 х 11 | ворон и ворона — два разных вида. |
| 23 | 5 х 6 | наибольший ущерб субъектам ИБ |
| 24 | 9 х 3 | информационная безопасность |
| 25 | 8 х 4 | ущерб при сервисном обслуживании |
| 26 | 5 х 7 | свойство аутентичности пользователя |
| 27 | 8 х 4 | данные были действия выполнены?! |
| 28 | 6 х 6 | законодательный уровень безопасности |
| 29 | 8 х 4 | из множества потенциально угроз |
| 30 | 4 х 9 | Защита процессов, процедур, программ |

## Вопросы для самоконтроля

1. Криптография и её роль в обществе.
2. Объяснить цель и задачи криптографии.
3. Пояснить какие бывают криптографические методы.
4. Что такое шифрование?
5. Как происходит процесс шифровки/дешифровки сообщения?
6. Как наложение гаммы влияет на исходный текст?

# Исследование безопасности Шифров

**Тема:** Исследование безопасности шифров. Применение частотного анализа для взлома шифротекста.

**Цель:** Изучить методы взлома криптосистем, провести частотный анализ и расшифровать текст.

## Теоретические ведомости

**Моноалфавитный подстановочный шифр** – шифр, в котором каждой букве исходного алфавита поставлена в соответствие одна буква шифра.

Например, возьмем слово **КУКУРУЗА**. Пусть букве **К** текста соответствует буква А шифра, букве **У** текста соответствует буква Б шифра, букве **Р** текста соответствует буква В шифра, букве **З** текста соответствует буква Г шифра, букве **А** текста соответствует буква Д шифра. После подстановки букв шифра вместо букв исходного теста слово **КУКУРУЗА** в зашифрованном виде будет выглядеть как АБАБВБГД. Недостатком подобного шифрования является то, что, если какая-то буква встречается в исходном тексте чаще всего, то и соответствующая ей буква шифра в зашифрованном тексте также встречается чаще всего. На рисунке Рисунок 2.1 приведены частоты встречаемости букв в английском тексте.

Рисунок . – Пример вставки рисунков

Для примера можно взять текст из сайта Use the "Insert Citation" button to add citations to this document.

составленный

## Задания

## Ход работы

## Вопросы для самоконтроля

# СИММЕТРИЧНЫЕ ШИФРЫ. Часть 1

**Тема:** Тема.

**Цель:** Опишите цель

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

1. Отличие симметричных и асимметричный шифров.
2. Пояснить что такое исходный текст, шифр, ключ.
3. Принцип подбора ключа в симметричных криптосистемах.
4. Принцип работы симметричных шифров. Приведите примеры.

# Симметричные шифры. Часть 2

**Тема:** Тема.

**Цель:** Опишите цель

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Взлом. Часть 2

**Тема:** Тема.

**Цель:** Опишите цель

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Асимметричные шифры. Часть 1

**Тема:** Тема.

**Цель:** Опишите цель

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Асимметричные шифры. Часть 2

**Тема:** Тема.

**Цель:** Опишите цель

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

# Электронно-цифровая подпись

**Тема:** Тема.

**Цель:** Опишите цель

## Теоретические ведомости

## Задания

## Ход работы

## Вопросы для самоконтроля

1. Перелік використаних джерел

Use the "Insert Citation" button to add citations to this document.

1. Додаток Б