Титулка

Зміст

[Список сокращений и условных обозначений 4](#_Toc511509969)

[Словарь терминов 5](#_Toc511509970)

[Введение 8](#_Toc511509971)

[1 Методи захисту інформації 9](#_Toc511509972)

[Теоретичні відомості 9](#_Toc511509973)

[1.1 Симетричні криптосистеми 10](#_Toc511509974)

[1.2 Шифри простої заміни 12](#_Toc511509975)

[1.3 Шифри складної заміни 13](#_Toc511509976)

[1.4 Гамування 14](#_Toc511509977)

[Завдання 15](#_Toc511509978)

[Питання для самоконтролю 16](#_Toc511509979)

[2 Исследование безопасности Шифров 18](#_Toc511509980)

[Теоретические ведомости 18](#_Toc511509981)

[Задания 19](#_Toc511509982)

[Ход работы 19](#_Toc511509983)

[Вопросы для самоконтроля 19](#_Toc511509984)

[3 СИММЕТРИЧНЫЕ ШИФРЫ. Часть 1 20](#_Toc511509985)

[Теоретические ведомости 20](#_Toc511509986)

[Задания 20](#_Toc511509987)

[Ход работы 20](#_Toc511509988)

[Вопросы для самоконтроля 20](#_Toc511509989)

[4 Симметричные шифры. Часть 2 21](#_Toc511509990)

[Теоретические ведомости 21](#_Toc511509991)

[Задания 21](#_Toc511509992)

[Ход работы 21](#_Toc511509993)

[Вопросы для самоконтроля 21](#_Toc511509994)

[5 Взлом. Часть 2 22](#_Toc511509995)

[Теоретические ведомости 22](#_Toc511509996)

[Задания 22](#_Toc511509997)

[Ход работы 22](#_Toc511509998)

[Вопросы для самоконтроля 22](#_Toc511509999)

[6 Асимметричные шифры. Часть 1 23](#_Toc511510000)

[Теоретические ведомости 23](#_Toc511510001)

[Задания 23](#_Toc511510002)

[Ход работы 23](#_Toc511510003)

[Вопросы для самоконтроля 23](#_Toc511510004)

[7 Асимметричные шифры. Часть 2 24](#_Toc511510005)

[Теоретические ведомости 24](#_Toc511510006)

[Задания 24](#_Toc511510007)

[Ход работы 24](#_Toc511510008)

[Вопросы для самоконтроля 24](#_Toc511510009)

[8 Электронно-цифровая подпись 25](#_Toc511510010)

[Теоретические ведомости 25](#_Toc511510011)

[Задания 25](#_Toc511510012)

[Ход работы 25](#_Toc511510013)

[Вопросы для самоконтроля 25](#_Toc511510014)

[Перелік використаних джерел 26](#_Toc511510015)

[Додаток Б 27](#_Toc511510016)

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)

# Методи захисту інформації

**Тема:** Методи захисту інформації. Класифікація криптосистем.

**Цель:** Вивчити прості методі криптографічного захисту інформації, використовувати отримані знання для приховування шляхом шифрування.

## Теоретичні відомості

Поява нових інформаційних технологій і розвиток потужних комп'ютерних систем зберігання і обробки інформації підвищили рівні захисту інформації та викликали необхідність того, щоб ефективність захисту інформації росла разом зі складністю архітектури зберігання даних. Поступово захист інформації стає обов'язковим: розробляються всілякі документи щодо захисту інформації; формуються рекомендації; навіть проводиться ФЗ про захист інформації, який розглядає проблеми і завдання захисту інформації, а також вирішує деякі унікальні питання захисту інформації.

Таким чином, загроза захисту інформації зробила засоби забезпечення інформаційної безпеки однією з обов'язкових характеристик інформаційної системи.

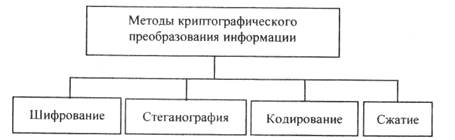


Рисунок . – Методи криптографічного перетворення

### Симетричні криптосистеми

#### Шифри перестановки

В шифрах середньовіччя часто використовувалися таблиці, за допомогою яких виконувалися прості процедури шифрування, засновані на перестановці букв в повідомленні. Ключем в даному випадку є розміри таблиці. Наприклад, повідомлення «Неясное становится ещё более непонятным» записується в таблицю з 5 рядків і 7 стовпців за стовпцями.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Таблиця 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 отримання шифрованого повідомлення текст зчитується по рядкам і групується по 5 букв:

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

Дещо більшою стійкістю до розкриття володіє метод *одиночної перестановки* по ключу. Він відрізняється від попереднього тим, що стовпчики таблиці переставляються за ключовим словом, фразою або набору чисел довжиною в рядок таблиці. Використовуючи в якості ключа слово - **ЛУНАТИК**, отримаємо наступну таблицю:

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** | | | | | | |  | **Після перестановки** | | | | | | |

У верхньому рядку лівої таблиці записаний ключ, а номери під буквами ключа визначені відповідно до природного порядку відповідних букв ключа в алфавіті. Якщо в ключі зустрілися б однакові літери, вони б нумерувались зліва направо. Виходить шифровка:

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

Для забезпечення додаткової прихованості можна повторно шифрувати повідомлення, яке вже було зашифровано. Для цього розмір другої таблиці підбирають так, щоб довжини її рядків і стовпців відрізнялися від довжин рядків і стовпців першої таблиці. Найкраще, якщо вони будуть взаємно простими.

Крім алгоритмів одиночних перестановок застосовуються алгоритми подвійних перестановок. Спочатку в таблицю записується текст повідомлення, а потім по черзі переставляються стовпці, а потім рядки. При розшифровці порядок перестановок був зворотний. Приклад даного методу шифрування показаний в таблиці.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

Ключем до шифру є номери стовпців 2413 и номери рядків 4123 початкової таблиці. В результаті перестановки отримане шифрування:

АЗЮЖЕ\_СШГТООИПЕР

Число варіантів подвійної перестановки досить швидко зростає зі збільшенням розміру таблиці: для таблиці 3х3 їх 36, для 4х4 їх 576, а для 5х5 їх 14400.

У середньовіччя для шифрування застосовувалися і магічні квадрати. Магічними квадратами називаються квадратні таблиці з вписаними в їх клітини послідовними натуральними числами, починаючи з одиниці, які дають в сумі по кожному стовпцю, кожному рядку і кожній діагоналі одне і те ж число. Для шифрування необхідно вписати вихідний текст за наведеною в квадраті нумерацією і потім переписати вміст таблиці по рядках.

Таблиця 1.4 – Початковий текст з ідентифікаторами

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 1.5 – Магічний 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 результаті виходить шифротекст, сформований завдяки перестановці букв початкового повідомлення.

Число магічних квадратів дуже різко зростає зі збільшенням розміру його сторін:

* для таблиці  існує тільки один квадрат;
* для таблиці ;
* для таблиці .

### Шифри простої заміни

#### Система шифрування Цезаря.

Заснований на заміні кожної букви повідомлення на іншу букву того ж алфавіту, шляхом зміщення від початкової букви на K букв. Відома фраза Юлія Цезаря **VENI VINI VICI** - прийшов, побачив, переміг, зашифрована за допомогою даного методу, перетворюється в **SBKF SFAF SFZF** (при зміщенні на 4 символи).

Грецьким письменником Полібієм за 100 років до н.е. був винайдений так званий полібіанський квадрат розміром 5 x 5, заповнений алфавітом у випадковому порядку. Грецький алфавіт має 24 літери, а 25-м символом є пробіл. Для шифрування на квадраті знаходили букву тексту і записували в шифротекст букву, розташовану нижче її в тому ж стовпці. Якщо буква виявлялася в нижньому рядку таблиці, то брали верхню букву з того ж стовпця.

### Шифри складної заміни

#### Шифр Гронсфельда

Це модифікація шифру Цезаря з використанням числового ключа. Для цього під буквами повідомлення записують цифри числового ключа. Якщо ключ коротше повідомлення, то його запис циклічно повторюють. Шифротекст отримують приблизно так само, як в шифрі Цезаря, але відраховують не третю букву за алфавітом (як в шифрі Цезаря), а ту, яка зміщена за алфавітом на відповідну цифру ключа.

1. Нехай в якості ключа використовується група із трьох цифр – 314.
2. Тоді повідомлення СОВЕРШЕННО СЕКРЕТНО.
3. Ключ 3143143143143143143.
4. Шифрування ФПЖИСЬИОССАХИЛФИУСС.

В шифри *багатоалфавітної заміни* для шифрування кожного символу початкового повідомлення застосовується свій шифр простої заміни (свій алфавіт).

У комп'ютері операція шифрування відповідає додаванню кодів ASCII символів повідомлення і ключа по модулю 256.

### Гамування

Процес шифрування полягає в генерації гами шифру і накладення цієї гами на вихідний відкритий текст. Перед шифруванням відкриті дані розбиваються на блоки  однакової довжини (по 64 біта). Гамма шифру виробляється у вигляді послідовності блоків  аналогічної довжини , де  - побітове додавання, .

Процес розшифрування зводиться до повторної генерації шифру тексту і накладення цієї гами на зашифровані дані .

Початкове повідомлення з букв російського алфавіту перетворюється в числове повідомлення заміною кожної його букви числом по наступній таблиці:

Таблиця . – Числова заміна 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 |



Початкове повідомлення ОТДУШКА. Для шифрування числового повідомлення використовується шифруючий відрізок послідовності А1, А2, ... підходящої довжини, що починається з , , , , , .

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Початкове повідомлення | О | Т | Д | У | Ш | К | А |
| Числове початкове повідомлення | 13 | 17 | 4 | 18 | 23 | 9 | 0 |
| Шифруючий відрізок | 1 | 5 | 6 | 17 | 8 | 19 | 3 |
| Числове шифроване повідомлення | 14 | 23 | 10 | 5 | 1 | 28 | 3 |
| Шифроване повідомлення | П | Ш | Л | Е | Б | Ю | Г |

Пам’ятаємо, що у вибраному алфавіті 30 символів.

## Завдання

У відповідності з вашим варіантом із табл. Таблиця 1.7 зашифрувати текст, використовуючи методи криптографічного захисту, представлені нижче. Регістр повинен бути врахований.

1. Шифри перестановки:
   1. метод перестановки по ключу;
   2. алгоритм подвійної перестановки;
   3. магічні квадрати.
2. Шифри заміни:
   1. шифр Цезаря;
   2. Аффінний шифр;
   3. шифр Віженера;
   4. шифр Плейфера.
3. Виконати шифрування методом гамування.

Записати результати шифрування у звіт, порівняти методи, обрати оптимальний для заданої фрази і аргументувати свій вибір.

Таблиця . – Список фраз для шифрування

|  |  |  |
| --- | --- | --- |
| 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 |

## Питання для самоконтролю

1. Криптографія та її роль у суспільстві.
2. Пояснити мету та завдання криптографії.
3. Пояснити, які бувають криптографічні методи.
4. Що таке шифрування?
5. Як відбувається процес шифрування/дешифрування повідомлення?
6. Як накладення гамми впливає на початковий 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