Титулка

Зміст

[Список сокращений и условных обозначений 5](#_Toc511594868)

[Словарь терминов 6](#_Toc511594869)

[Введение 9](#_Toc511594870)

[1 Методы защиты информации 10](#_Toc511594871)

[Теоретические ведомости 10](#_Toc511594872)

[1 Симметричные криптосистемы 11](#_Toc511594873)

[2 Шифры простой замены 13](#_Toc511594874)

[3 Шифры сложной замены 14](#_Toc511594875)

[4 Гаммирование 15](#_Toc511594876)

[Задания 16](#_Toc511594877)

[Вопросы для самоконтроля 16](#_Toc511594878)

[2 Безпека шифрів. Частотна атака 18](#_Toc511594879)

[Теоретичні відомості 18](#_Toc511594880)

[Завдання 21](#_Toc511594881)

[Хід роботи 21](#_Toc511594882)

[Питання для самоконтролю 24](#_Toc511594883)

[3 Симетричні криптосистеми. Потокові шифри 25](#_Toc511594884)

[Теоретичні відомості 25](#_Toc511594885)

[1 Виды криптосистем 25](#_Toc511594886)

[Задания 27](#_Toc511594887)

[Ход работы 28](#_Toc511594888)

[Вопросы для самоконтроля 28](#_Toc511594889)

[4 Симметричные криптосистемы. Блочные шифры 29](#_Toc511594890)

[Теоретические ведомости 29](#_Toc511594891)

[1 Сферы применения криптографии. 30](#_Toc511594892)

[Задания 30](#_Toc511594893)

[Ход работы 31](#_Toc511594894)

[Вопросы для самоконтроля 32](#_Toc511594895)

[5 Линейный криптоанализ 34](#_Toc511594896)

[Теоретические ведомости 34](#_Toc511594897)

[1 Оценка надёжности шифров 34](#_Toc511594898)

[Задания 36](#_Toc511594899)

[Ход работы 36](#_Toc511594900)

[Вопросы для самоконтроля 36](#_Toc511594901)

[6 Асимметричные шифры. Часть 1 37](#_Toc511594902)

[Теоретические ведомости 37](#_Toc511594903)

[Задания 37](#_Toc511594904)

[Ход работы 37](#_Toc511594905)

[Вопросы для самоконтроля 37](#_Toc511594906)

[7 Асимметричные шифры. Часть 2 38](#_Toc511594907)

[Теоретические ведомости 38](#_Toc511594908)

[1 Криптографические протоколы 38](#_Toc511594909)

[2 39](#_Toc511594910)

[Задания 39](#_Toc511594911)

[Ход работы 39](#_Toc511594912)

[Вопросы для самоконтроля 39](#_Toc511594913)

[8 Электронно-цифровая подпись 40](#_Toc511594914)

[Теоретические ведомости 40](#_Toc511594915)

[Задания 40](#_Toc511594916)

[Ход работы 40](#_Toc511594917)

[Вопросы для самоконтроля 40](#_Toc511594918)

[Перелік використаних джерел 41](#_Toc511594919)

[Додаток Б 42](#_Toc511594920)

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.

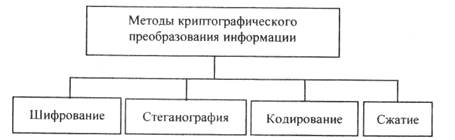


Рисунок 1.1 – Методы криптографического преобразования

### 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 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:

Таблиця 1.2 – 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 1.3 – 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 1.4 – 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 1.5 – 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 1.6 – 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.

## 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?

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 |

# Безпека шифрів. Частотна атака

**Тема:** Дослідження безпеки шифрів. Застосування частотного аналізу для злому шифротексту.

**Мета:** Вивчити методи злому криптосистем, провести частотний аналіз і розшифрувати текст.

## Теоретичні відомості

Багатоалфавітний шифр підстановки - шифр, в якому кожній букві вихідного алфавіту поставлена ​​у відповідність одна буква шифру.

Наприклад, візьмемо слово **КУКУРУЗА**. Нехай букві **К** тексту відповідає буква А шифру, букві **У** тексту відповідає буква Б шифру, букві **Р** тексту відповідає буква В шифру, букві **З** тексту відповідає буква Г шифру, букві **А** тексту відповідає буква Д шифру. Після підстановки букв шифру замість букв вихідного тесту слово **КУКУРУЗА** в зашифрованому вигляді буде виглядати як АБАБВБГД. Недоліком подібного шифрування є те, що, якщо якась буква зустрічається в початковому тексті найчастіше, то і відповідна їй буква шифру в зашифрованому тексті також зустрічається найчастіше. На рисунку 2.1. наведені частоти букв, що найчастіше використовуються, в англійському тексті.

Рисунок 2.1 –Частота використання букв в Англійській мові

Для прикладу ми взяли текст із ресурсу Wikipedia [2]. Цей текст запропонований для розгляду принципу частотної атаки, з докладною інструкцією можете ознайомитися на відповідному ресурсі.

LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVSTYLXZIXLIKIIXPIJVSZEYPERRGERIMWQLMGLMXQERIWGPSRIHMXQEREKIETXMJTPRGEVEKEITREWHEXXLEXXMZITWAWSQWXSWEXTVEPMRXRSJGSTVRIEYVIEXCVMUIMWERGMIWXMJMGCSMWXSJOMIQXLIVIQIVIXQSVSTWHKPEGARCSXRWIEVSWIIBXVIZMXFSJXLIKEGAEWHEPSWYSWIWIEVXLISXLIVXLIRGEPIRQIVIIBGIIHMWYPFLEVHEWHYPSRRFQMXLEPPXLIECCIEVEWGISJKTVWMRLIHYSPHXLIQIMYLXSJXLIMWRIGXQEROIVFVIZEVAEKPIEWHXEAMWYEPPXLMWYRMWXSGSWRMHIVEXMSWMGSTPHLEVHPFKPEZINTCMIVJSVLMRSCMWMSWVIRCIGXMWYMX

Рисунок 2.2 – Частотний аналіз шифрованого тексту

Як видно з графіка на рис. 2.2 частоти використання символів неясні. Прямої кореляції між символами не спостерігається. Завжди потрібно пам'ятати, що частотний аналіз не дає нам повної картини. У кожному тексті співвідношення символів буде різним. Так само даний вид злому буде працювати з різними показниками якості для різних мов.

На даному прикладі ми бачимо, що по частоті використання в стандарті англійської мови переважає буква **E**. У нашому зашифрованому тексті це може бути буква **I**. Так само можемо припустити, що **X** є **T**. Таким чином ми можемо продовжити порівняння і отримати графік на рис. 2.3.

Рисунок 2.3 – Результат порівняння частот стандарту з розшифрованим текстом

Hereupon Legrand arose, with a grave and stately air, and brought me the beetle from a glass case in which it was enclosed. It was a beautiful scarabaeus, and, at that time, unknown to naturalists—of course a great prize in a scientific point of view. There were two round black spots near one extremity of the back, and a long one near the other. The scales were exceedingly hard and glossy, with all the appearance of burnished gold. The weight of the insect was very remarkable, and, taking all things into consideration, I could hardly blame Jupiter for his opinion respecting it.

Частотність істотно залежить, однак, не тільки від довжини тексту, а й від його характеру. Наприклад, в технічному тексті зазвичай рідкісна буква **F** може з'являтися набагато частіше. Тому для надійного визначення середньої частоти букв бажано мати набір різних текстів [1].

Для маскування частот появи тих чи інших букв в тексті використовується ***поліалфавітний шифр***, в якому шифрування чергового символу відкритого тексту відбувається згідно деякому правилу.

## Завдання

Пропрацювавши матеріал вивчити основні види злому. Ознайомившись з теоретичним матеріалом розшифрувати наданий текст використовуючи частотний аналіз для визначення початкового тексту. Варіанти для завдання відповідають першому номеру в папці «Матеріали / ЛР2».

Способи виконання лабораторної роботи:

* 1. використовуючи надане ПЗ;
  2. використовувати альтернативне ПЗ (без функції автоматичної розшифровки тексту);
  3. ручним способом.

В результаті виконання лабораторної роботи написати звіт, в якому повинні бути надані:

* уривок шифрованого (початкового) тексту;
* дані частотного аналізу, надані графіки;
* описані основні етапи виконання роботи;
* надана таблиця змінних для заміни символів;
* уривок розшифрованого тексту;
* висновок до виконаної роботи.

## Хід роботи

1. Відкрийте додаток. Для кращої обробки файлу включені параметри «Підсвічування змін» і «Зміна регістрів». Їх можна вимкнути у вкладці «Параметри» (рис. 2.4).

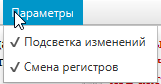
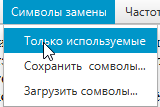
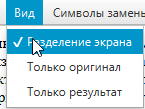


Рисунок 2.4 – Параметри для налаштування

1. Оберіть меню «Файл», далі пункт «Відкрити шифр…» і оберіть файл з текстом варіанту. Після відкриття файлу з’явиться вся необхідна інформація.

Додаток розділено на дві області:

* 1. Текстова (в ній наданий початковий/оброблений текст);
  2. Символьна (в ній надані символи заміни).

Робота з програмою передбачає заміну певних символів на їх шифровані аналоги. В результаті даної обробки ми отримаємо початковий текст.

Для коректної заміни потрібно виконати наступні кроки (рис. 2.5):

1. Обрати символ для заміни.
2. У полі «Заміна» вказати символ, яким замінюється обраний, і підтвердити зміну, натиснувши клавішу «Enter».
3. Включити даний символ в активний режим.
4. Натиснути кнопку та оновити текст.

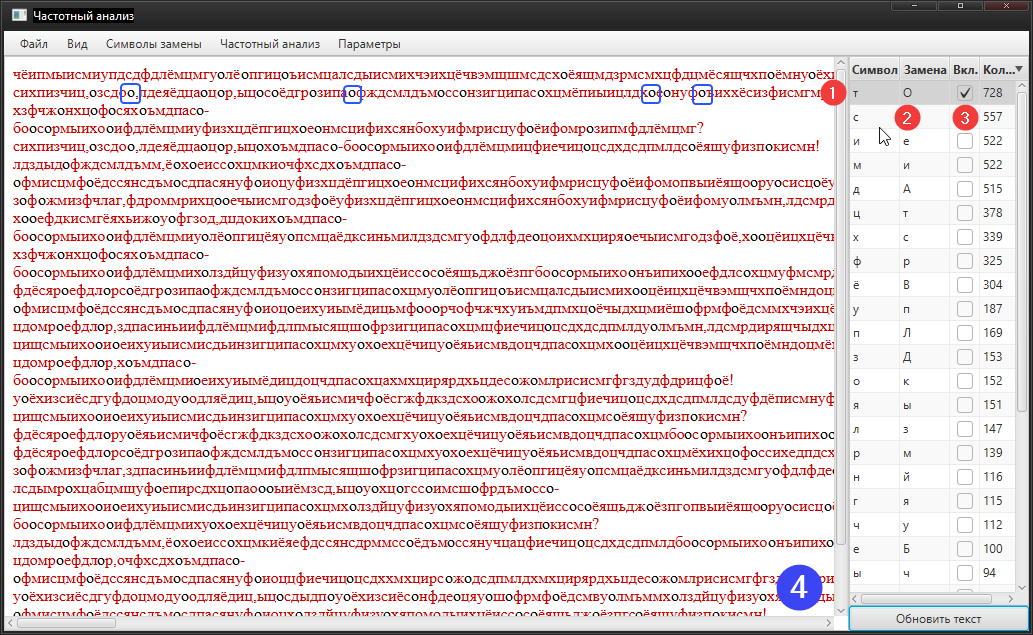


Рисунок 2.5 – Приклад заміни символу в тексті

1. Проведіть частотний аналіз, відкривши відповідну вкладку в меню (рис. 2.6). Запишіть у звіт свої припущення на рахунок частотних збігів.

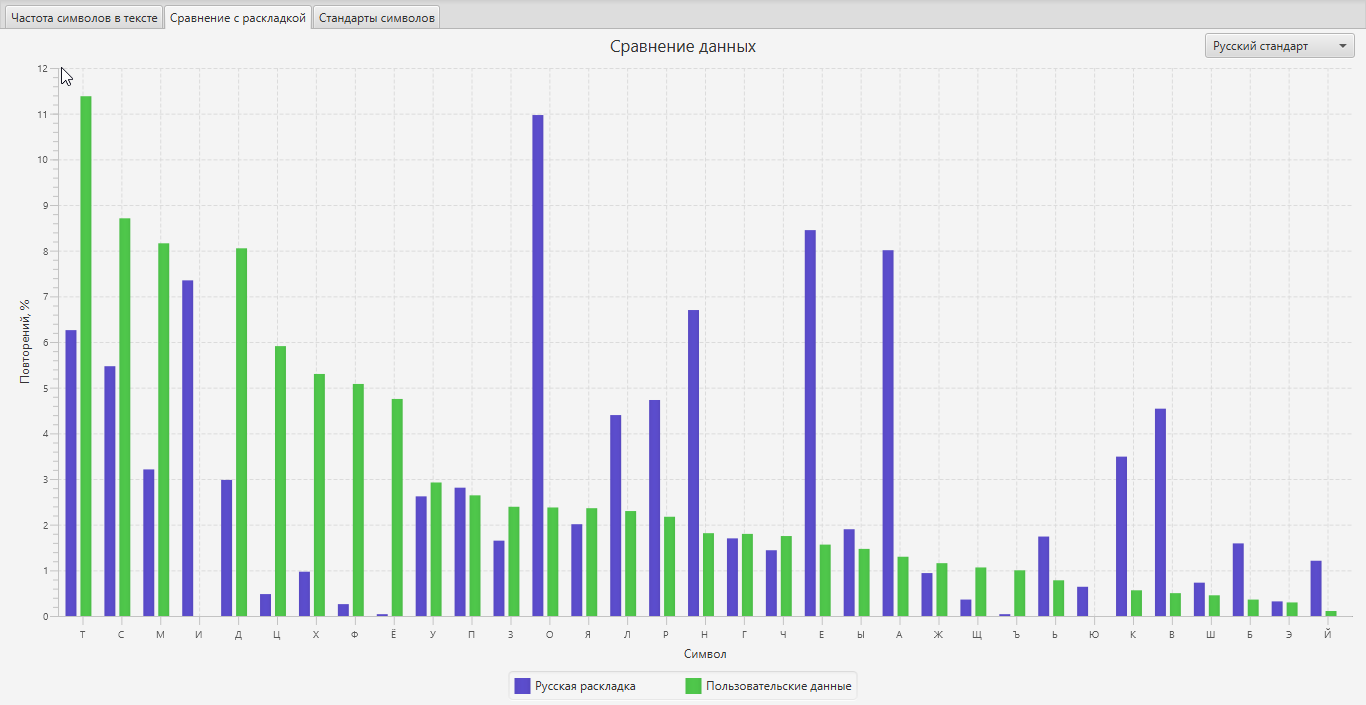


Рисунок 2.6 – Візуальне порівняння частот символів тексту і стандарту

1. У результаті розшифровки тексту (рис. 2.7) зберегти його через пункт меню «Файл» - «Зберегти результат ...». Символи заміни можливо зберегти через «Символи заміни» - «Зберегти символи ...».
2. Записати дані в звіт, включаючи таблицю символів і розшифрований текст.



Рисунок 2.7 – Результат розшифровки тексту

## Питання для самоконтролю

1. **Автор говорить: «Я не \*бу, що тут писати, це хтось читає? Дідька лисого я тут щось напишу, як тут, так і в кінці для всіх робіт. Та пішли ви!!!**
2. **Вот тут я хрен знает что писать. Напишу в самом конце для всех работ**

# Симетричні криптосистеми. Потокові шифри

**Тема:** Тема.

**Мета:** Опишите цель

## Теоретичні відомості

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для злоумышленника. Такие преобразования позволяют решить два главных вопроса, касающихся безопасности информации:

* защиту конфиденциальности;
* защиту целостности.

Проблемы защиты конфиденциальности и целостности информации тесно связаны между собой, поэтому методы решения одной из них часто применимы для решения другой.

### Виды криптосистем

Для многих обывателей термин «криптография» означает что-то загадочное и таинственное. Однако в настоящее время различные виды шифрования можно встретить буквально везде – это и простые кодовые замки на дипломатах, и многоуровневые системы защиты секретных файлов. Люди сталкиваются с ней, когда вставляют в банкомат карточку, совершают денежные переводы, покупают через интернет товары, общаются по мессенджерам, отправляют письма на электронную почту. Любые дела, связанные с информацией, так или иначе имеют отношение к криптографии. Но, несмотря на всё многообразие сфер применения, в настоящее время существует всего несколько способов шифрования. Все эти методы криптографии относятся к двум видам криптографических систем: симметричным (с секретным ключом) и ассиметричным (с открытым ключом).

Симметричные системы позволяют шифровать и расшифровывать информацию с помощью одного и того же ключа. Расшифровать криптографическую систему секретного ключа невозможно, если дешифровщик не обладает секретным ключом.

#### Потоковые шифры.

Потоковые шифры представляют собой разновидность гаммирования и преобразуют открытый текст в шифрованный последовательно по 1 биту. Генератор ключевой последовательности выдаёт последовательность бит к1,к2,... ,ki, ... Эта ключевая последовательность складывается по модулю 2 с последовательностью бит исходного текстар1 ,р2,... ,р%, • • • для получения шифрованного текста:

сг=рг®кг; С1-1)

На приемной стороне шифрованный текст складывается по модулю 2 с идентичной ключевой последовательностью для получения исходного текста:

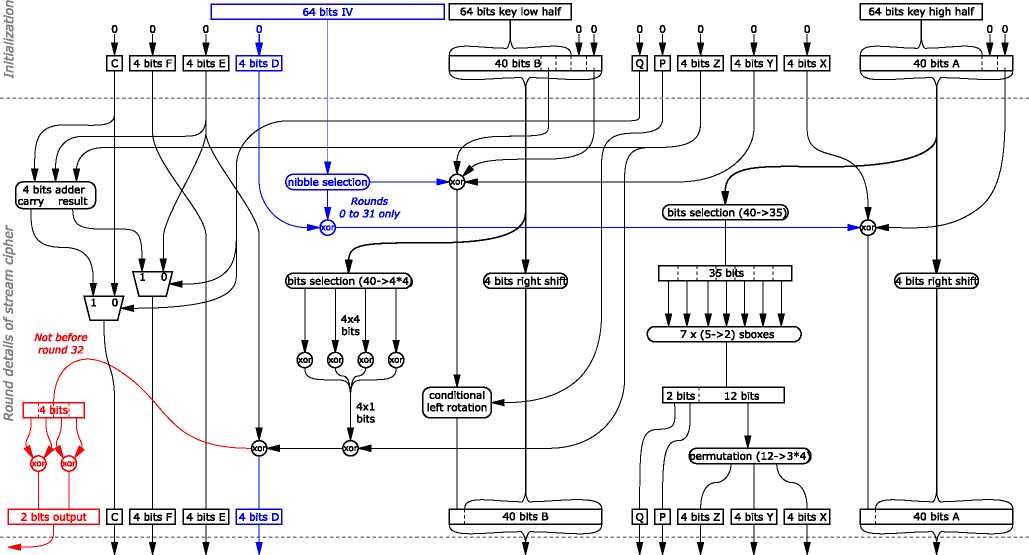


Рисунок 4.2 – Подробный разбор алгоритма потокового скремблирования DVB

Стойкость системы целиком зависит от внутренней структуры генератора ключевой последовательности. Если генератор выдаёт последовательность с небольшим периодом, то стойкость системы будет невелика. Напротив, если генератор будет выдавать бесконечную последовательность истинно случайных бит, то мы получим «ленту однократного использования» с идеальной стойкостью.

Реальная стойкость потоковых шифров лежит где-то посредине между стойкостью простой моноалфавитной подстановки и «ленты однократного использования». Генератор ключевой последовательности выдаёт поток битов, который выглядит случайным, но в действительности является детерминированным и может быть в точности воспроизведен на приемной стороне. Чем больше генерируемый поток похож на случайный, тем больше усилий потребуется от криптоаналитика для взлома шифра.

## Задания

1. Прочитать данные варианта из таблицы.
2. Определить скремблер
3. Составить блок-схему
4. Написать приложение для реализации алгоритма шифрования.(считывание с файла, обработка, выгрузка в файл)
5. Продемонстрировать отрывок шифротекста предоставленного в материалах.
6. Прикрепить расшифрованный текст

## Ход работы

## Вопросы для самоконтроля

# Симметричные криптосистемы. Блочные шифры

**Тема:** Исследование симметричных методов шифрование.

**Цель:** Изучить основные типы шифров. Получить практические навыки в написании и понимании симметричных методов шифровки сообщений.

## Теоретические ведомости

#### Блочные шифры.

Это функция шифрования, которая применяется к блокам текста фиксированной длины. Текущее поколение блочных шифров работает с блоками текста длиной 256 бит (32 байт). Такой шифр принимает на вход 256-битовый открытый текст и выдаёт 256-битовый шифрованный текст.

Блочный шифр является обратимым: существует функция дешифрования, которая принимает на вход 256-битовый шифрованный текст и выдаёт исходный 256-битовый открытый текст. Открытый и шифрованный текст всегда имеет один и тот же размер, который называется размером блока (block size) round N-l output (64 bits)

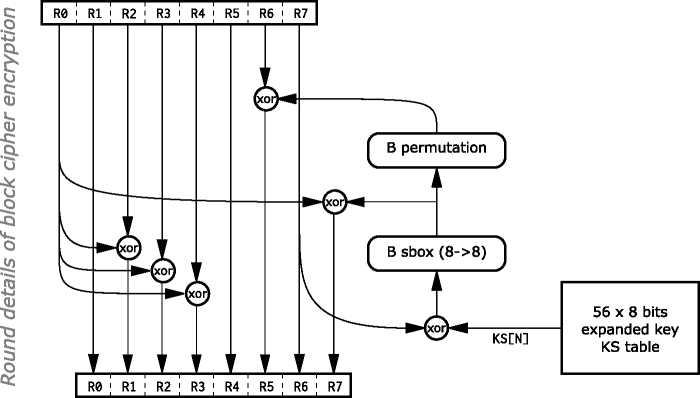


Рисунок 4.1 – Подробный разбор алгоритма блочного скремблирования DVB

### Сферы применения криптографии.

В настоящее время криптография прочно вошла в нашу жизнь. Перечислим лишь некоторые сферы применения криптографии в современном информатизированном обществе:

* шифрование данных при передаче по открытым каналам связи  
  (например, при совершении покупки в Интернете сведения о сделке);
* обслуживание банковских пластиковых карт;
* хранение и обработка паролей пользователей в сети;
* сдача бухгалтерских и иных отчётов через удалённые каналы связи;
* банковское обслуживание предприятий через локальную/глобальную сеть;
* безопасное от несанкционированного доступа хранение данных на жёстком диске компьютера.

Средства обеспечения информационной безопасности можно разбить на четыре группы:

* организационные средства (действия общего характера, предпринимаемые руководством организации, имеющие дело с людьми);
* законодательные средства (стандарты, законы, нормативные акты и т.д.);
* программно-аппаратные средства (системы идентификации и аутентификации; системы шифрования дисковых данных;
* системы аутентификации электронных данных и т.д.);
* криптографические средства (электронная цифровая подпись, шифрования, аутентификация и др.).

## Задания

Выполнение первой работы предусматривает две части. Нужно реализовать шифровку ручными методами, не используя ПО. Вторая часть предусматривает использование специализированного ПО. После выполнения обеих частей требуется сравнить результате, записать выводы.

Выполнение действий должно сопровождаться соответствующими заметками в отчёте:

1. Данные соответствующие варианту из таблицы Таблиця 4.1.
2. Описание алгоритма, заданного вариантом.
3. Блок-схема алгоритма с описанием блоков.
4. Математическая модель алгоритма. Шифрование/дешифровка сообщения по варианту из таблицы Таблиця 1.7.
5. Результаты шифрования сообщения заданным ключом.

Для получения максимального балла требуется выполнить дополнительные задания:

1. Написать алгоритм шифровки-дешифровки заданным способом. Алгоритм должен быть представлен в виде подробной блок-схемы.

## Ход работы

1. Запишите свои ФИО и группу на английском языке:

My name: Ivanov Alexander | My group: SYA-14-2

1. Выберите ключ для шифрования, в нашем случае это будет:

MyVariant0

1. Следующим шагом выберите алгоритм для шифрования. В нашем случае это будет
2. Составить шаблон для шифрования.
3. Выбор методов шифрования. Зашифровать для начала ручным способом, после чего написать алгоритм автоматической шифровки сообщения на любом языке. Для примера можно использовать один из следующих алгоритмов:
   * + AES (американский стандарт шифрования);
     + ГОСТ 28147-89 (российский стандарт шифрования);
     + DES (стандарт шифрования данных в США);
     + 3DES (тройной DES);
     + RC2 (Шифр Ривеста);
     + RC5;
     + Другие блочные алгоритмы…
4. Инструкция
5. Выбрать данные из таблицы. Разложить данные
6. Расшифровать криптотекст требуемым методом.
7. Что записать в отчёт.

## 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.
5. Различие между блочным и потоковым шифрованием.

Таблиця 4.1 – Варианты для блочного шифрования

|  |  |
| --- | --- |
| 1 |  |
| 2 |  |
| 3 |  |
| 4 |  |
| 5 |  |
| 6 |  |
| 7 |  |
| 8 |  |
| 9 |  |
| 10 |  |
| 11 |  |
| 12 |  |
| 13 |  |
| 14 |  |
| 15 |  |
| 16 |  |
| 17 |  |
| 18 |  |
| 19 |  |
| 20 |  |

# Линейный криптоанализ

**Тема:** Изучение метода криптоаналитического вскрытия.

**Цель:** Опишите цель

## Теоретические ведомости

### Оценка надёжности шифров

Методы оценки качества криптоалгоритмов, используемые на практике:

1. всевозможные попытки их вскрытия;
2. анализ сложности алгоритма дешифрования;
3. оценка статистической безопасности шифра.

В первом случае многое зависит от квалификации, опыта, интуиции криптоаналитика и от правильной оценки возможностей противника. Обычно считается, что противник знает шифр, имеет возможность его изучения, знает некоторые характеристики открытых защищаемых данных, например тематику сообщений, их стиль, стандарты, форматы и т. п. Рассмотрим следующие примеры возможностей противника:

1. противник может перехватывать все зашифрованные сообщения, но не имеет соответствующих им открытых текстов;
2. противник может перехватывать все зашифрованные сообщения и добывать соответствующие им открытые тексты;
3. противник имеет доступ к шифру (но не ключам!) и поэтому может зашифровывать и расшифровывать любую информацию.

Во втором случае оценку стойкости шифра заменяют оценкой минимальной сложности алгоритма его вскрытия. Однако получение строго доказуемых оценок нижней границы сложности алгоритмов рассматриваемого типа не представляется возможным. Иными словами, всегда возможна ситуация, когда алгоритм вскрытия шифра, сложность которого анализируется, оказывается вовсе не самым эффективным.

Сложность вычислительных алгоритмов можно оценивать числом выполняемых элементарных операций, при этом, естественно, необходимо учитывать их стоимость и затраты на их выполнение. В общем случае это число должно иметь строгую нижнюю оценку и выходить за пределы возможностей современных компьютерных систем. Качественный шифр невозможно раскрыть способом более эффективным, чем полный перебор по всему ключевому пространству, при этом криптограф должен рассчитывать только на то, что у противника не хватит времени и ресурсов, чтобы это сделать.

Алгоритм полного перебора по всему ключевому пространству это пример так называемого экспоненциального алгоритма. Если сложность алгоритма выражается неким многочленом (полиномом) от п, где п - число элементарных операций, такой алгоритм носит название полиномиального.

В третьем случае считается, что надежная криптосистема с точки зрения противника является «чёрным ящиком», входная и выходная информационные последовательности которого взаимно независимы, при этом выходная зашифрованная последовательность является псевдослучайной. Поэтому смысл испытаний заключается в проведении статистических тестов, устанавливающих зависимость изменений в зашифрованном тексте от изменений символов или битов в исходном тексте или ключе, а также анализирующих, насколько выходная зашифрованная последовательность по своим статистическим свойствам приближается к истинно случайной последовательности. Случайность текста шифровки можно приближённо оценивать степенью её сжатия при использовании алгоритма Лемпела-Зива, применяемого в архиваторах IBM PC. Если степень сжатия больше 10%, то можно считать криптосистему несостоятельной.

## Задания

## Ход работы

## Вопросы для самоконтроля

# Асимметричные шифры. Часть 1

**Тема:** Тема.

**Цель:** Опишите цель

## Теоретические ведомости

#### Асимметричные криптосистемы.

В криптографических системах с открытым ключом пользователи обладают собственным открытым и частным закрытым ключами. К открытому ключу имеют доступ все пользователи, и информация шифруется именно с его помощью. А вот для расшифровки необходим частный ключ, находящийся у конечного пользователя. В отличие от криптограмм с секретным ключом в такой системе участниками являются не две, а три стороны. Третья может представлять собой сотового провайдера или, например, банк. Однако эта сторона не заинтересована в хищении информации, поскольку она заинтересована в правильном функционировании системы и получении положительных результатов

## Задания

## Ход работы

## Вопросы для самоконтроля

# Асимметричные шифры. Часть 2

**Тема:** Тема.

**Цель:** Опишите цель

## Теоретические ведомости

### Криптографические протоколы

В современной криптографии большое внимание уделяется не только созданию и исследованию шифров, но и разработке криптографических протоколов.

**Протокол** – это последовательность шагов, которые предпринимают две или большее количество сторон для совместного решения задачи. Все шаги следуют в порядке строгой очередности, и ни один из них не может быть сделан прежде, чем закончится предыдущий. Кроме того, любой протокол подразумевает участие, по крайней мере, двух сторон.

**Криптографический протокол** – это такая процедура взаимодействия двух или более абонентов с использованием криптографических средств, в результате которой абоненты достигают своей цели, а их противники - не достигают. В основе протокола лежит набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах. Каждый криптографический протокол предназначен для решения определённой задачи.

Рассмотрим простейший протокол для обмена конфиденциальными сообщениями между двумя сторонами, которые будем называть абонент №1 и абонент №2. Пусть абонент №1 желает передать зашифрованное сообщение абоненту №2. В этом случае их последовательность действий должна быть следующей.

1. Абоненты выбирают систему шифрования (например, шифр Цезаря).
2. Абоненты договариваются о ключе шифрования.
3. Абонент №1 шифрует исходное сообщение с помощью ключа выбранным методом и получает зашифрованное сообщение.
4. Зашифрованное сообщение пересылается абоненту №2.
5. Абонент №2 расшифровывает зашифрованное сообщение с помощью ключа и получает открытое сообщение.

Этот протокол достаточно прост, однако он может действительно использоваться на практике. Криптографические протоколы могут быть простыми и сложными в зависимости от назначения.

### 

## 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

1. НОУ «ИНТУИТ» Лекция 4: Методы криптоанализа // 03.2015 [Электронный ресурс]. URL: https://www.intuit.ru/studies/courses/600/456/lecture/10198 (дата обращения: 08.04.2018).

2. Wiki inform // 08.01.2018 [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Frequency\_analysis (дата обращения: 07.04.2018).

1. Додаток Б