МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФАКУЛЬТЕТ КОМПЬЮТЕРНЫХ И ФИЗИКО-МАТЕМАТИЧЕСКИХ НАУК

КАФЕДРА ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Отчёт по лабораторной работе №2 по дисциплине «Методы и средства защиты информации»

**Криптоанализ одноалфавитных шифров**

|  |  |
| --- | --- |
| Выполнил: студент группы ФИб-4302-51-00 \_\_\_\_\_\_\_\_\_\_\_ | / Д.А. Савин / |
| студент группы ФИб-4302-51-00 \_\_\_\_\_\_\_\_\_\_\_ | / П.А. Мохов / |
| студент группы ФИб-4302-51-00 \_\_\_\_\_\_\_\_\_\_\_ | / В.А. Жаворонков/ |
| Проверил: доцент каф. ПМиИ \_\_\_\_\_\_\_\_\_\_\_ | / Д.Ю. Ляпунов / |

Киров 2021

**Cодержание**

[Введение 3](#_Toc88041131)

[1 Анализ предметной области 4](#_Toc88041132)

[1.1 Основные понятия и определения 4](#_Toc88041133)

[2 Обзор метода одноалфавитного шифра подстановки 6](#_Toc88041134)

[1.1 Пример криптоанализа шифра замены 7](#_Toc88041135)

[1.2 Разработка дополнительного программного обеспечения 9](#_Toc88041136)

[3 Вывод 13](#_Toc88041137)

[4 Тест 14](#_Toc88041138)

[Библиографический список 16](#_Toc88041139)

Приложение Отчет по лабораторной работе 2(2).docx, 118КБ, редакция от 6.11.2021, Отправлен в Teams 8.11.2021 Ляпунову Д.Ю.

# Введение

Цель работы: научиться расшифровывать текст методом одно алфавитного шифра подстановки.

Задачи:

1. Поиск литературных источников, представляющих информацию по данной теме.
2. Обзор метода одно алфавитного шифра подстановки.
3. Формулировка соответствующих выводов.
4. Разработка тестов для закрепления материала по данной теме.

# Анализ предметной области

## Основные понятия и определения

*Шифрование* представляет собой сокрытие информации от неавторизованных лиц с предоставлением в это же время авторизованным пользователям доступа к ней. Пользователи называются авторизованными, если у них есть соответствующий ключ для дешифрования информации. Это очень простой принцип. Вся сложность заключается в том, как реализуется весь этот процесс.

Еще одной важной концепцией, о которой необходимо знать, является то, что целью любой системы шифрования является максимальное усложнение получения доступа к информации неавторизованными лицами, даже если у них есть зашифрованный текст и известен алгоритм, использованный для шифрования. Пока неавторизованный пользователь не обладает ключом, секретность и целостность информации не нарушается.

С помощью шифрования обеспечиваются три состояния безопасности информации.

1. Конфиденциальность. Шифрование используется для *сокрытия информации* от неавторизованных пользователей при передаче или при хранении.
2. Целостность. Шифрование используется для предотвращения изменения информации при передаче или хранении.
3. Идентифицируемость. Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им.

Термины, связанные с шифрованием:

*Обычный текст*. Информация в исходном виде. Также называется открытым текстом.

*Шифрованный текст*. Информация, подвергнутая действию алгоритма шифрования.

*Алгоритм*. Метод, используемый для преобразования *открытого текста* в шифрованный текст.

*Ключ*. Входные данные, посредством которых с помощью алгоритма происходит преобразование *открытого текста* в шифрованный или обратно.

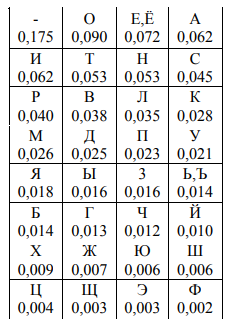
*Шифрование*. Процесс преобразования *открытого текста* в шифр.

*Дешифрование*. Процесс преобразования шифра в *открытый текст*.[[1](#_Библиографический_список)]

# 2 Обзор метода одноалфавитного шифра подстановки

Криптоанализ шифра простой замены основан на использовании статистических закономерностей языка. Так, например, известно, что в русском языке частоты букв распределены следующим образом:

Таблица 1. Частоты букв русского языка (в 32-буквенном алфавите со знаком пробела)



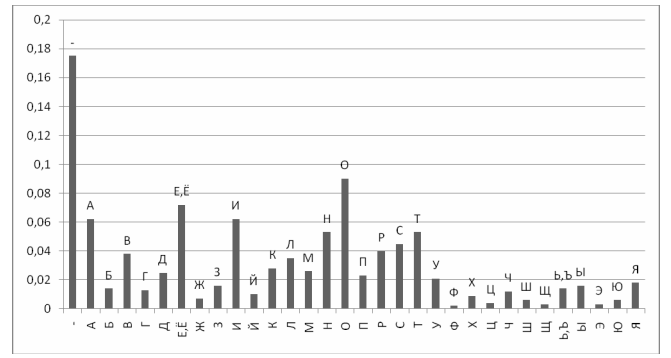


Рисунок 1. Диаграмма частот букв русского языка

Для получения более точных сведений об открытых текстах можно строить и анализировать таблицы k-грамм при k>2, однако для учебных целей вполне 26 достаточно ограничиться биграммами. Неравновероятность k -грамм (и даже слов) тесно связана с характерной особенностью открытого текста – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Так, для русского языка такими привычными фрагментами являются наиболее частые биграммы и триграммы: СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО, КО, СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА Полезной является информация о сочетаемости букв, то есть о предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм. Имеется в виду таблица, в которой слева и справа от каждой буквы расположены наиболее предпочтительные "соседи" (в порядке убывания частоты соответствующих биграмм). В таких таблицах обычно указывается также доля гласных и согласных букв (в процентах), предшествующих (или следующих за) данной букве.

## Пример криптоанализа шифра замены

Известно, что зашифровано стихотворение Р. Киплинга в переводе С.Я. Маршака. Шифрование заключалось в замене каждой буквы на двузначное число. Отдельные слова разделены несколькими пробелами, знаки препинания сохранены. Таблица частот букв русского языка приведена выше.

|  |
| --- |
| 30 29 15 10 17 29 22 25 31 15 33 35 41 43 45 35 57 45 25 17 59 15 10 25 41 25 69, 59 78 29 82 25 78 25 17 15 10 88 90 78 25 62 25 22 10 57 73 79 35 67 78 90 88 29 45 35 29, 54 57 90 31 90 73 22 88 15 88 29 15 17 69 41 25 15, 70 17 90 57 43 59 15 78 15 62 22 25 17 57 25 69 88 15 82 17 25 88 29 45 35… |

Подсчитаем частоты шифрообразований:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | 29 | 15 | 10 | 17 | 22 | 25 | 31 | 33 | 35 | 41 | 43 | 45 | 57 |
| Количество | 7 | 10 | 4 | 7 | 4 | 12 | 2 | 1 | 5 | 3 | 2 | 4 | 5 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | 59 | 69 | 78 | 82 | 88 | 90 | 62 | 73 | 79 | 67 | 54 | 70 |
| Количество | 3 | 3 | 4 | 2 | 6 | 5 | 1 | 2 | 1 | 1 | 1 | 1 |

Из таблицы частот букв русского языка видно, что чаще всего встречается буква О, на втором месте Е. В нашем шифр-тексте чаще всего встречается обозначение 25 (12 раз), на втором месте идет обозначение 15 (10 раз), остальные обозначения им существенно уступают. Поэтому можем выдвинуть гипотезу: 25=О, 15=Е. Однако, текст у нас не очень большой, поэтому закономерности русского языка проявляются в нем не обязательно в строгом соответствии с таблицей частот букв русского языка. Поэтому возможен и вариант: 25=Е, 15=О. Но тогда последнее слово в третьей строке имеет окончание ЕО, что возможно, но все же более вероятный вариант ОЕ. Итак, будем работать с текстом, считая, что 25=О, 15=Е. Теперь нам поможет знак препинания: «29, …». Крайне маловероятно, чтобы запятая стояла после согласной. Итак, 29 – гласная, причем вероятнее всего 29=И или 29=А, т.к. гласные Я, Ю, Э, У встречаются в осмысленных текстах на русском языке намного реже, чем И и А, что не противоречит таблице частот шифр-текста. В последней строке: 88 15, но 15=Е, следовательно, 88 – согласная, причем наиболее вероятные значения – это Н и Т. Итак, 25=О, 15=Е, 29=А (А И) , 88= (Н Т) . Теперь третье слово в третьей строке имеет 4 варианта:

• 29=И, 88=Н: 22 Н Е Н И Е

• 29=И, 88=Т: 22 Т Е Т И Е

• 29=А, 88=Н: 22 Н Е Н А Е

• 29=А, 88=Т: 22 Т Е Т А Е

Из рассмотренных вариантов лишь один является осмысленным, и он позволяет найти значение 22. Имеем: 22=М и третье слово в третье строке М Н Е Н И Е. Теперь рассмотрим второе слово в первой строке. Е 10 17 И, причем 10 и 17 – согласные, и это не М и не Н. Наиболее вероятное слово Е С Л И, т.е. 10=С, 17=Л. Конечно, если мы, продолжая работать с текстом, вдруг получим «нечитаемое» слово, то придется вернуться к этому этапу и рассмотреть другие варианты. Однако, это маловероятно, поскольку вряд ли в стихотворении были слова наподобие Е Р Т И, Е В Л И и т.п. 31 Далее, первое слово второй строки: 59 78 И, причем 59 и 78 – согласные, и это не С, не Л, не М и не Н. Так что это слово П Р И, т.е. 59=П, 78=Р. Тогда шестое слово первой строки 45 О Л П Е, что дает значение 45=Т и тогда при 57=В получаем фрагмент «…В Т О Л П Е…». Также второе слово последней строки П Е Р Е 62 дает нам значение 62=Д. Далее рассмотрим начало второй строки: «П Р И 82 О Р О Л Е С Н 90 Р О Д О М …». Из него следует, что 82=К и 90=А. Зная, что 82=К, посмотрим на самое последнее слово К Л О Н И Т 35, откуда станет ясно, что 35=Ь. Перед последней атакой выпишем текст, заменяя известные обозначения буквами.

И Е С Л И М О 31 Е 33 Ь 41 43 Т Ь В Т О Л П Е С О 41 О 69, П Р И К О Р О Л Е С Н А Р О Д О М С В 73 79 Ь 67 Р А Н И Т Ь И, 54 В А 31 А 73 М Н Е Н И Е Л 69 41 О Е, 70 Л А В 43 П Е Р Е Д М О Л В О 69 Н Е К Л О Н И Т Ь…

Из последней строки: 69=Ю, тогда слова Л Ю 41 О Е и С О 41 О Ю определяют 41: 41=Б. Теперь из четвертого слова первой строки Б 43 Т Ь получаем, что 43=Ы. А первое слово из последней строки 70 Л А В Ы – это Г Л А В Ы. Слово в первой строке М О 31 Е 33 Ь угадывается из контекста: М О Ж Е Ш Ь, т.е. 31=Ж, 33=Ш. Теперь второе слово в третьей строке запишется как 54 В А Ж А 73, откуда, с учетом контекста: 54=У, 73=Я. После этого окончание второй строки имеет вид «… С В Я 79 Ь 67 Р А Н И Т Ь». Легко определяются буквы 79=З, 67=Х.

Ответ: И Е С Л И М О Ж Е Ш Ь Б Ы Т Ь В Т О Л П Е С О Б О Ю, П Р И К О Р О Л Е С Н А Р О Д О М С В Я З Ь Х Р А Н И Т Ь И, У В А Ж А Я М Н Е Н И Е Л Ю Б О Е, Г Л А В Ы П Е Р Е Д М О Л В О Ю Н Е К Л О Н И Т Ь… [[2](#_Библиографический_список)]

## Разработка дополнительного программного обеспечения

Для удобства расшифровки зашифрованного сообщения можно реализовать следующее:

Зашифрованное соощение:

я\_рчюмжтучсю\_ютжч\_ужыьъюэчжчяюхфучрчя\_рчюмжтучыж\_юкуырчв\_жэиохмбрачяюттжээпачжэножэч\_юммрэьюыьч\_жмкрв\_юежычяу\_угежйуээпучмююзщуэрцчрчнуъчмжъпъчяюъюсчяюзутрньчж\_ърлчсосуэюнюечяюмыучяюзутпчя\_жернуыьмнеючв\_жэиррчэумбюыьбюч\_жхчя\_реыубжырчусючбч\_жмкрв\_юебучкрв\_юечяюмыучмъу\_нрч\_юммрэьюыцчусючмпэчзюэжеуэно\_ч\_юммрэьюыьчжчяюхфучрчеэобчжэножэч\_юммрэьюыьчя\_ютюыфрырчусючтуыючечнюче\_уъцчя\_жернуыьмнеючв\_жэиррчя\_реыубжыючбч\_жзюнучъэюфумнеючб\_рянюс\_жвюечбюню\_пучеъумнучюз\_жхюепежырчнжбчэжхпежуъпачйу\_эпачбжзрэунчжэножэоч\_юммрэьюылчя\_рэжтыуфрнчтюбн\_рэжчмюсыжмэючбюню\_юачмнюабюмньчкрв\_жчтюыфэжчюя\_утуыцньмцчертюъчхжкрв\_юежээюачрэвю\_ъжиррчтыцчеюуээюсюче\_уъуэрчтюмнжнюйэюачзотунчцеыцньмцчмнюабюмньчумырчмююзщуэручмчя\_рбжхюъчж\_ъуамбюъочяют\_жхтуыуэрлчэучзотунч\_жмкрв\_юежэючя\_юнреэрбюъчгюнцчзпчтючъюъуэнжчрмяюыэуэрцчяюыойжнуыуъчжчтыцчтряыюъжнрйумбюачяюйнпчкрв\_чтюыфуэчюзумяуйрежньчмюг\_жээюмньчэжчтумцнбрчыун

Процедура подсчета частот букв в зашифрованном сообщении:

|  |
| --- |
| public static void decrypt\_mess\_count(string s)  {  string text = s;  string AlreadyDone = "";  string[,] Result = new string[text.Length, 2];  int i = 0, l = 0;  foreach (char ch in text)  {  i = 0;  foreach (char c in text)  {  if (ch == c) i++;  }  if (AlreadyDone.Contains(ch) != true)  {  // Console.WriteLine(ch + " повторяется " + i.ToString() + " раз ");  Result[l, 0] = ch.ToString();//символ  Result[l, 1] = (Math.Round((double)i / s.Length, 3)).ToString(); //кол-во повторов  AlreadyDone += ch; l++;  }  }  for (int k = 0; k < AlreadyDone.Length; k++)  {  Console.WriteLine("{0} - {1}", Result[k, 0], Result[k, 1]);  }  } |

Получили примерную частоту появления символов в зашифрованном сообщении:

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

С помощью этого можно начать расшифровывать сообщение.

В итоге получилось такое сообщение:

«при осаде города реальмон а позже и при осаде ларошели французский подданный антуан россиньоль расшифровал перехваченные сообщения и тем самым помог победить армию гугенотов после победы правительство франции несколько раз привлекали его к расшифровке шифров после смерти россиньоля его сын бонавентур россиньоль а позже и внук антуан россиньоль продолжили его дело в то время правительство франции привлекало к работе множество криптографов которые вместе образовывали так называемый черный кабинет антуану россиньолю принадлежит доктрина согласно которой стойкость шифра должна определяться видом зашифрованной информации для военного времени достаточной будет являться стойкость если сообщение с приказом армейскому подразделению не будет расшифровано противником хотя бы до момента исполнения получателем а для дипломатической почты шифр должен обеспечивать сохранность на десятки лет»

# 3 Вывод

В ходе лабораторной работы был изучен метод одноалфавитного шифра подстановки, суть его работы, а также плюсы и минусы.

# 4 Тест

Савин Д.А, Мохов П.А, Жаворонков В.А, Криптоанализ одноалфавитных шифров, 6.11.2021.

* + - 1. Что такое шифрование?

а) способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого

б) совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств

в) удобная среда для вычисления конечного пользователя

* + - 1. Как называется шифр, в котором каждый символ открытого текста заменяется некоторым, фиксированным при данном ключе, символом другого алфавита?

а) шифром одноалфавитной подстановки

б) шифром многоалфавитной подстановки

в) шифром замены

* + - 1. Что общего имеют все методы шифрования с закрытым ключом?

а) в них для шифрования информации используется один ключ, а для расшифрования – другой ключ

б) в них входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов

в) в них для шифрования и расшифрования информации используется один и тот же ключ

* + - 1. Алфавит – это…

а) конечное множество используемых для кодирования знаков

б) буквы текста

в) нет правильного ответа

* + - 1. Как называется метод шифрования, в котором входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов?  
         а) шифром одноалфавитной подстановки  
         б) шифром многоалфавитной подстановки  
         в) шифром перестановки  
         г) шифром цезаря
      2. Каким образом в пропорциональных или монофонических шифрах уравнивается частота появления зашифрованных знаков?   
         а) это связано с тем, что в качестве замены символам обычно выбираются числа   
         б) для замены символов исходного текста используется не один, а несколько алфавитов   
         в) для замены встречающихся часто, используется относительно большое число возможных эквивалентных для замены; для менее испольхуемых исхожных знаков используется один или два эквивалента   
         г) совместно с заменой применяется перестановка символов
      3. Как называется сообщение, полученное после преобразования с использованием любого шифра?   
         а) закрытым текстом   
         б) имитовставкой   
         в) ключом   
         г) открытым текстом
      4. Под целостностью понимают…   
         а) гарантирование невозмможности несанкционированного изменения объема информации   
         б) гарантирование невозможности несанкционированного изменения информации   
         в) гарантирование невозможности несанкционированного изменения порядка следования информации   
         г) гарантирование невозможности несанкционированного изменения переносов текстовой информации
      5. Символы исходного текста складываются с символами некой случайной последовательности – это…   
         а) алгоритм гаммирования   
         б) алгоритм перестановки   
         в) алгоритм аналитических преобразований
      6. Как связаны ключи друг с другом в системе с открытым ключом   
         а) математически   
         б) логически   
         в) алгоритмически
      7. Как осуществляется дешифрование текста при аналитических преобразованиях   
         а) деление матрицы на вектор  
         б) умножение матрицы на вектор   
         в) перемножение матриц
      8. Блок управления – это…   
         а) устройство криптографической заданности данных   
         б) проходной шифратор

в) основной модуль шифратора, который «заведует» работой всех остальных

|  |  |
| --- | --- |
| 1 | а |
| 2 | а |
| 3 | в |
| 4 | а |
| 5 | в |
| 6 | в |
| 7 | а |
| 8 | б |
| 9 | а |
| 10 | а |
| 11 | б |
| 12 | в |

# Библиографический список

1. Мэйволд, Э. Безопасность сетей / Мэйволд Э. - Москва : Национальный Открытый Университет "ИНТУИТ", 2016. (Шаг за шагом) - ISBN 5-9570-0046-9. (дата обращения: 3.11.2021)
2. О. Н. ЖДАНОВ, И. А. КУДЕНКОВА КРИПТОАНАЛИЗ КЛАССИЧЕСКИХ ШИФРОВ. (дата обращения: 3.11.2021)