Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра программной инженерии

**Отчет к лабораторной работе**:

«Исследование криптографических шифров на основе подстановки (замены) символов»

Выполнила:

студентка 3 курса 6 группы

Дикун Игорь Вячеславович

Минск 2023

1. **Теоретические сведения**

Сущность подстановочного шифрования состоит в том, что, исходный текст (из множества М) и зашифрованный текст (из множества С) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм подстановки.

Если исходить из того, что используемые алфавиты являются конечными множествами, то в общем случае каждой букве ax алфавита AM (ax∈ AM) для создания сообщения Мi (Мi ∈ M) соответствует буква ay или множество букв{АхС} для создания шифртекста Сi (Сi ∈ С). Важно, чтобы во втором случае любые два множества (например, {АхС}b и {АхС}n, b≠n, 1 ≤ b, n, x, y ≤ N, N – мощность алфавита), используемые для замены разных букв открытого текста, не пересекались:

{АхС}b ∩ {АхС}n=0.

Если в сообщении Мi содержится несколько букв ax, то каждая из них заменяется на символ ay либо на любой из символов {АхС}. За счет этого с помощью одного ключа можно сгенерировать различные Сi для одного и того же Мi. Так как множества {АхС}b и {АхС}n попарно не пересекаются, то по каждому символу Сi можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения Мi он заменяет. В силу этого открытое сообщение восстанавливается из зашифрованного однозначно.

Приведенные утверждения справедливы для следующих типов подстановочных шифров:

* моноалфавитных (шифры однозначной замены или простые подстановочные),
* полиграммных,
* омофонических (однозвучные шифры или шифры многозначной замены),
* полиалфавитных.

**Моноалфавитные шифры подстановки**

В данных шифрах операция замена производится только над каждым одиночным символом сообщения Мi. Для наглядной демонстрации шифра простой замены достаточно выписать под заданным алфавитом тот же алфавит, но в другом порядке или, например, со смещением. Записанный таким образом алфавит называют алфавитом замены.

Максимальное количество ключей для любого шифра этого вида не превышает N!, где N – количество символов в алфавите.

Для математического описания криптографического преобразования предполагаем, что зашифрованная буква ay (ay ∈ Сi), соответствующая символу aх (aх∈ Мi), находится на позиции

y ≡ x + k (mod N), (2.1)

где x, y – индекс (порядковый номер, начиная с 0) символа в используемом алфавите, k – ключ.

Для расшифрования сообщения Сi необходимо произвести расчеты обратные, т. е.:

х ≡ у – k (mod N). (2.2)

Одним из существенных недостатков моноалфавитных шифров является их низкая криптостойкость. Зачастую метод криптоанализа базируется на частоте встречаемости букв исходного текста.

Система шифрования Цезаря с ключевым словом (лозунгом) также является одноалфавитной системой подстановки. Особенностью этой системы является использование ключевого слова (лозунга) для смещения и изменения порядка символов в алфавите подстановки (желательно, чтобы все буквы ключевого слова были различными). Ключевое слово пишется в начале алфавита подстановки.

Применяя одновременно операции сложения и умножения по модулю n над элементами множества (индексами букв алфавита), можно получить систему подстановок, которую называют аффинной системой подстановок Цезаря. Определим процедуру зашифрования в такой системе:

y ≡ ax + b (mod N),

где a и b – целые числа.

При этом взаимно однозначные соответствия между открытым текстом и шифртекстом будут иметь место только при выполнении следующих условий: 0 ≤ a, b< N, наибольший общий делитель (НОД) чисел a, b равен 1, т.е. эти числа являются взаимно простыми.

**Полиграммные шифры**

В таких шифрах одна подстановка соответствует сразу нескольким символам исходного текста.

Первым известным шифром этого типа является шифр Порты. Шифр представляется в виде таблицы. Наверху горизонтально и слева вертикально записывался стандартный алфавит. В ячейках таблицы записываются числа в определенном порядке.

Шифрование выполняется парами букв исходного сообщения. Первая буква пары указывает на строку, вторая – на столбец. В случае нечетного количества букв в сообщении Мi к нему добавляется вспомогательный символ, например, «А».

С точки зрения криптостойкости рассматриваемый тип шифров имеет преимущества перед моноалфавитными шифрами. Это связано с тем, что распределение частот групп букв значительно более равномерное, чем отдельных символов. Во-вторых, для эффективного частотного анализа требуется больший размер зашифрованного текста, так как число различных групп букв значительно больше, чем мощность алфавита.

**Омофонические шифры**

Омофонические шифры (омофоническая замена) или однозвучные шифры подстановки создавались с целью увеличить сложность частотного анализа шифртекстов путем маскировки реальных частот появления символов текста с помощью омофонии.

При шифровании символ исходного сообщения заменяется на любую подстановку из «своего» столбца. Если символ встречается повторно, то, как правило, используют разные подстановки. Например, исходное сообщение «АБРАМОВ» после зашифрования может выглядеть так: «357 990 374 678 037 828 175».

Книжный шифр. Заметным вкладом греческого ученого Энея Тактика в криптографию является предложенный им так называемый книжный шифр. После Первой мировой войны книжный шифр приобрел иной вид. Шифрозамена для каждой буквы определялась набором цифр, которые указывали на номер страницы, строки и позиции в строке (вспомните пример использования такого шифра известными героями фильма «17 мгновений весны»). Даже с формальной стороны отсутствие полной электронной базы изданных к настоящему времени книг делает процедуру взлома шифра практически не выполнимой.

**Полиалфавитные шифры**

Полиалфавитные (или многоалфавитные) шифры состоят из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования.

Диск Альберти. В «Трактате о шифрах» [10] Альберти приводит первое точное описание многоалфавитного шифра на основе шифровального диска.

Он состоял из двух дисков – внешнего неподвижного и внутреннего подвижного дисков, на которые были нанесены буквы алфавита. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене ее на букву с внутреннего диска, стоящую под ней. После этого внутренний диск сдвигался на одну позицию и шифрование второй буквы производилось уже по-новому шифралфавиту. Ключом данного шифра являлся порядок расположения букв на дисках и начальное положение внутреннего диска относительно внешнего.

Таблица Трисемуса. В 1518 году в развитии криптографии был сделан важный шаг благодаря появлению в Германии первой печатной книги по криптографии. Аббат Иоганнес Трисемус, настоятель монастыря в Вюрцбурге, написал книгу «Полиграфия», в которой он описал ряда шифров, один из которых развивает идею многоалфавитной подстановки. Зашифрование осуществляется так: заготавливается таблица подстановки (так называемая «таблица Трисемуса» – таблица со стороной равной N, где N – мощность алфавита), где первая строка – это алфавит, вторая – алфавит, сдвинутый на один символ, и т. д. При зашифровании первая буква открытого текста заменяется на букву, стоящую в первой строке, вторая – на букву, стоящую во второй строке, и т.д. После использования последней строки вновь возвращаются к первой.

Таким образом, ключом в таблицах Трисемуса является ключевое слово и размер таблицы. При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Шифр Виженера. В 1586 г. французский дипломат Блез Виженер представил перед комиссией Генриха III описание простого, но довольно стойкого шифра, в основе которого лежит таблица Трисемуса.

В этом шифре мы имеем дело с последовательностью сдвигов, циклически повторяющейся. Основная идея заключается в следующем. Создается таблица (таблица Виженера) размером N·N (N – число знаков в используемом алфавите). Эти знаки могут включать не только буквы, но и, например, пробел или иные знаки. В первой строке таблицы записывается весь используемый алфавит. Каждая последующая строка получается из предыдущего циклического сдвига последней на 1 символ влево. Таким образом, при мощности алфавита (английского языка) равной 26, необходимо выполнить последовательно 25 сдвигов для формирования всей таблицы.

Роторные машины. Идеи Альберти и Виженера использовались при создании электромеханических роторных машин первой половины ХХ века. Некоторые из них использовались в разных странах вплоть до 1980-х годов. В большинстве из них использовались роторы (механические колеса), взаимное расположение которых определяло текущий алфавит шифрозамен, используемый для выполнения подстановки. Наиболее известной из роторных машин является немецкая машина времен Второй мировой войны «Энигма». Более детальному изучению и практическому анализу «Энигмы» далее будет посвящена отдельная лабораторная работа.

К полиалфавитным относится также шифр на основе «одноразового блокнота».

1. **Практическая часть**

В данной лабораторной работе необходимо разработать пользовательское приложение, которое должно реализовывать следующие операции:

* выполнять зашифрование/расшифрование текстовых документов, созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки для немецкого алфавита:

1. На основе соотношений (2.1) и (2.2); k = 7
2. Таблица Трисемуса, ключевое слово – enigma

* формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;
* оценивать время выполнения операций зашифрования/расшифрования.
  1. Для выполнения первого задания были разработаны функции для шифрования и расшифрования сообщений шифром на основе соотношений при k = 7. Для того, чтобы расшифровать достоверно уже зашифрованный текст, в польский алфавит были добавлены символы препинания и пробела: [aäbcdefghijklmnoöpqrsßtuüvwxyz].

В данном шифре при шифровании используется соотношение (2.1), k = 7 по варианту.

Например:

Возьмем символ “p”.

Найдем индекс данного символа в польском алфавите [aäbcdefghijklmnoöpqrsßtuüvwxyz]. В данном алфавите 30 символов. Индекс равен 18.

Теперь считаем новый индекс по соотношению (2.1).

y = 18 + 7 (mod 30) = 25.

Данному индексу соответствует символ “ü”.

Дешифрование основано на соотношении (2.2).

Например:

Возьмем символ “ ü ”.

Найдем индекс данного символа в польском алфавите [aäbcdefghijklmnoöpqrsßtuüvwxyz]. В данном алфавите 30 символов. Индекс равен 25.

Теперь считаем новый индекс по соотношению (2.2).

y = 25 - 7 (mod 30) = 18.

Данному индексу соответствует символ “p”.

На рисунке 2.1 представлены результаты выполнения функций шифрования и расшифрования, также видно время выполнения данных операций.

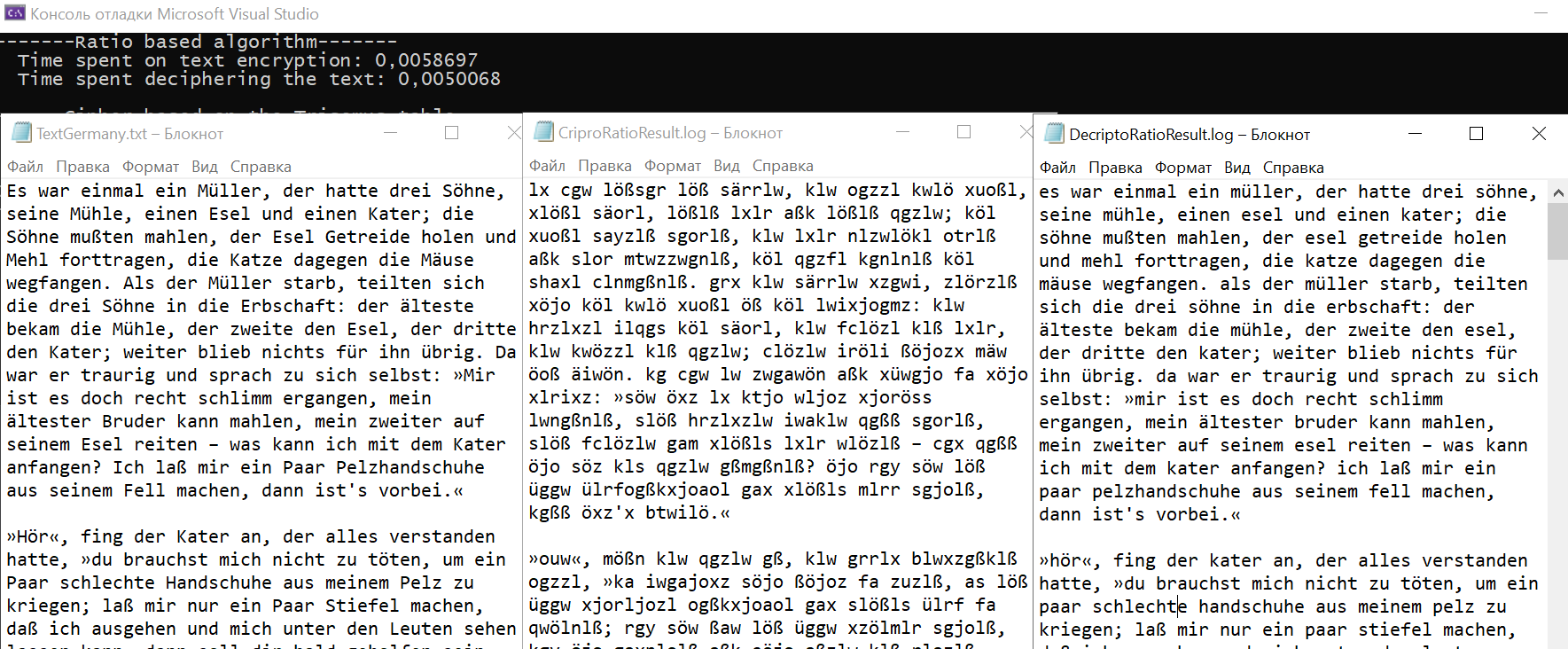


Рисунок 2.1 – Результат шифрования и расшифрования на основе соотношений

В результате, обращаю внимание, итоговый текс совпадает с исходным, что означает, что шифрование и расшифрование прошло успешно.

Дальше построим гистограмму частоты появления символов в начальном и зашифрованном тексте (рисунок 2.2):

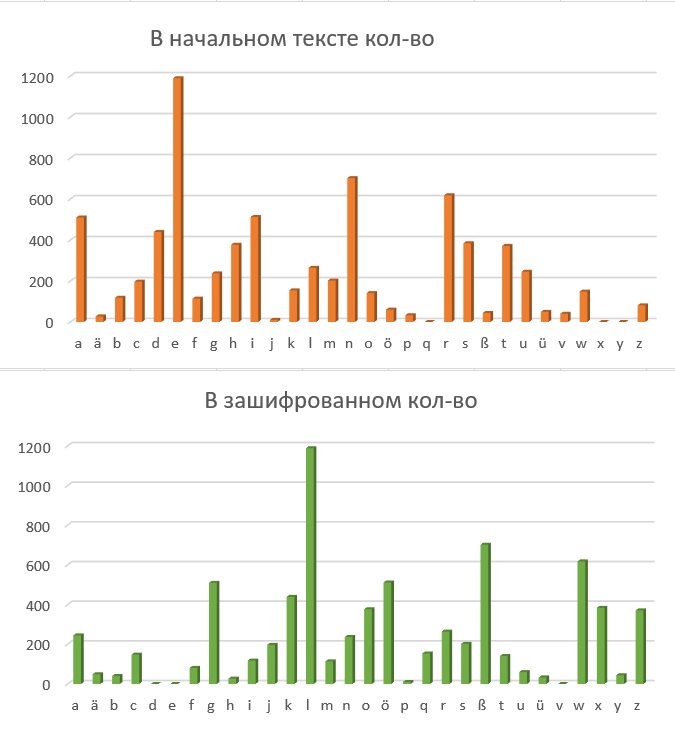


Рисунок 2.2 – Гистограмма частоты появления символов в исходном тексте

В итоге, невооружённым глазом можно заметить, что показатели-столбцы зашифрованных элементов просто сдвинут на 7, что и оправдывается формулой соотношения 2.1.

* 1. Рассмотрим пример шифрования исходного текста с помощью так называемой таблицы Трисемуса с применением ключевого слова. Для начала нужно избавиться от повторяющихся символов в ключевом слове. Далее его нужно вписать в таблицу, размером m×n, где m – строки таблицы, а n – столбцы, сформированную на основании исходного алфавита. Потом следует последовательно, начиная с последней буквы ключевого слова, дописать остальные символы исходного алфавита, исключая буквы, имеющиеся в ключевом слове. Таким образом формируется новый алфавит на основе исходного и ключевого слова.

Таблица 2.1 – Таблица Трисемуса

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **e** | **n** | **i** | **g** | **m** |
| **a** | ä | b | c | d |
| f | h | j | k | l |
| o | ö | p | q | r |
| s | ß | t | u | ü |
| v | w | x | y | z |

Далее при шифровании происходит замена символа входного текста на стоящий в сформированной таблице на одну позицию ниже его. Если входной символ является самым нижним в таблице, то он заменяется на символ, стоящий в этом же столбце в самом верху.

Дешифрование производится в обратном порядке: символы зашифрованного сообщения заменяются на символы, стоящие выше их на одну позицию столбца, в котором они находятся.

Результаты вычисления скорости выполнения шифрования и дешифрования с помощью таблицы Трисемуса представлены на рисунке 2.6.

Мы можем увидеть, что дешифрование зашифрованного текста занимает немного больше времени, чем шифрование, так как алгоритм при дешифровании является более сложным, следовательно, машине требуется немного больше времени для выполнения данной операции.

На рисунке 2.3 представлены результаты выполнения функций шифрования и расшифрования, также видно время выполнения данных операций.

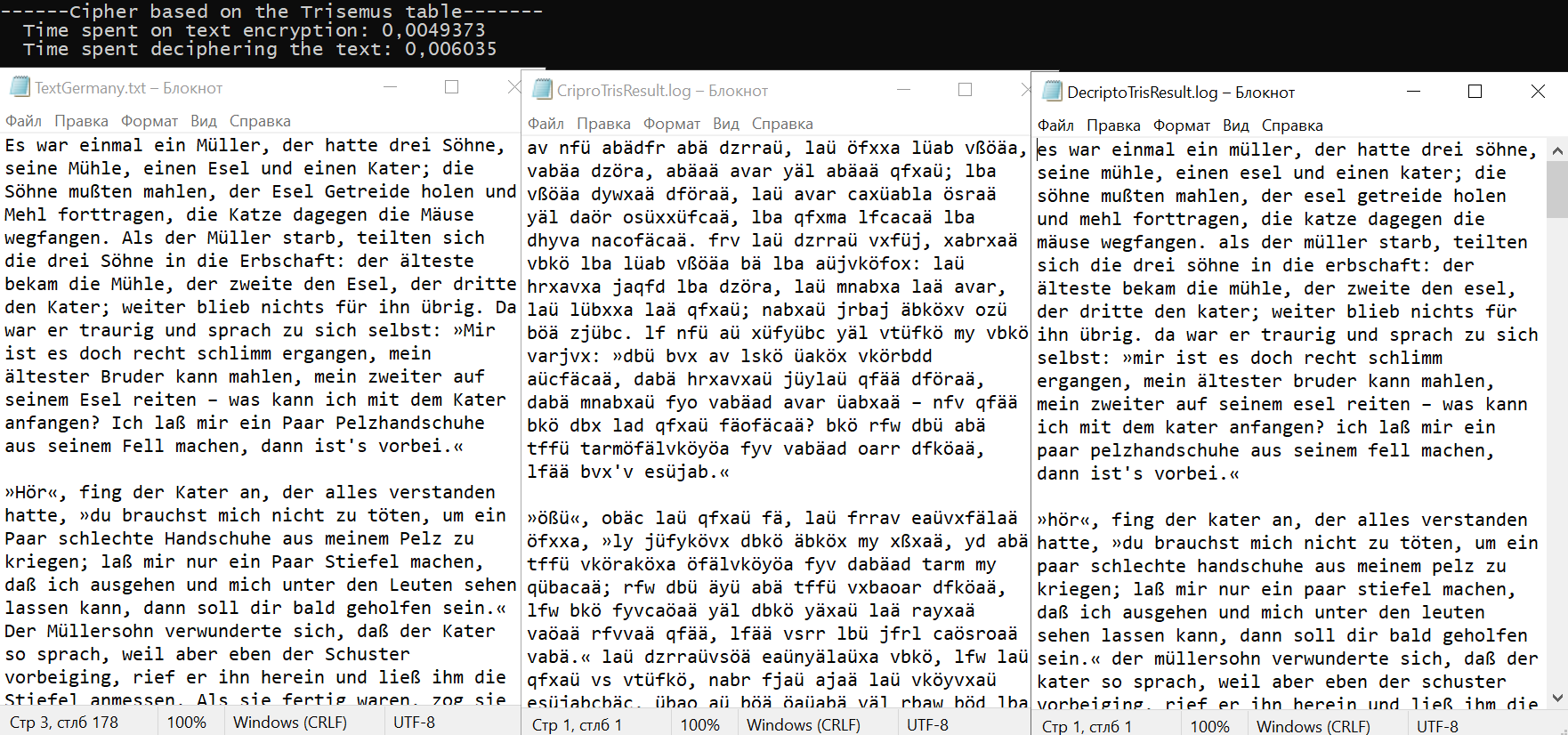


Рисунок 2.3 – Результат шифрования и расшифрования на основе таблицы Трисемуса

Мы видим, что все расшифрованные символы соответствуют каждому символу исходного сообщения. Значит, алгоритм дешифрования зашифрованного текста работает правильно.

Также приложение генерирует гистограммы частот появления символов в исходном и зашифрованном текстах, которые представлены на рисунке 2. И рисунке 2.4 соответственно.

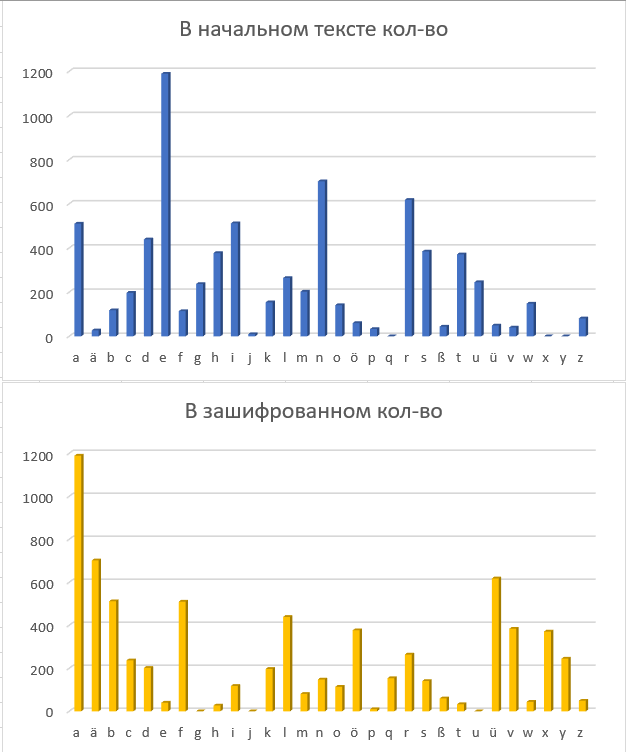


Рисунок 2.4 – Гистограмма частоты появления символов в исходном тексте

**Вывод**

В данной лабораторной работе были закреплены теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости шифров. Были ознакомлены с особенностями реализации и свойствами различных подстановочных шифров. Было разработано приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования. Были проведены исследования криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.