**Российский университет транспорта (МИИТ)**

**Институт транспортной техники и систем управления**

**Кафедра «Управление и защита информации»**

# Отчет

**по практическому заданию**

**по теме «Разработка семейства полиалфавитных шифров: шифр 1»**

**по дисциплине «Криптографические методы защиты информации»**

Выполнил:

Студент группы ТКИ-342

Дроздов А.Д.

Проверил:

Доцент кафедры УиЗи, к.т.н., с.н.с.

Михалевич И.Ф.

Москва 2023

**Оглавление**

## Задание

1. Разработать базовый полиалфавитный шифр.
2. Разобрать таблицы шифрования/расшифрования для шифра №1.
3. Подготовить, зашифровать и расшифровать сообщение.
4. Провести анализ слабостей шифра.
5. Оформить отчет.

## Исходные данные

1. Тип полиалфавитного шифра – квадрат Виженера (базовый, первая строка начинается с первого символа алфавита шифра).
2. Первая строка квадрата соответствует моноалфавитному шифру студента.
3. Первичный ключ шифра – ШИФРОВАНИЕ
4. Ключевая последовательность – повторение первичного ключа до размера передаваемого сообщения.
5. Передаваемое сообщение: «Уважаемый Игорь Феодосьевич, спешу сообщить Вам о том, что практическая работа 5 выполнена и готова к проверке. Дроздов Антон Дмитриевич 03.12.2002. Уважаемый Антон Дмитриевич, я безмерно рад нашему сотрудничеству, надеюсь на его дальнейшее успешное и взаимовыгодное развитие. С уважением, Игорь Феодосьевич».

# 1. Краткие теоритические сведения о шифре

## 1.1 Определения шифра и ключа

Шифр – система заранее оговоренных обратимых преобразований защищаемой информации (текста, изображений, аудио, видео, ...) с помощью ключа.

Ключ – переменный параметр для обратимых преобразований защищаемой информации (данных).

Ключ – минимальная информация, необходимая для обратимого преобразования защищаемой информации (шифрования и расшифрования, формирования и проверки контрольных сумм, ...).

## 1.2. Составные элементы шифра

- алфавит;
- алгоритмы обратимых преобразований исходного сообщения в криптограммы и обратного преобразования криптограмм в открытое сообщение (зашифрования и расшифрования);
- множество ключей.

## 1.3. Алфавит

Алфавит – набор уникальных символов для записи шифрованных сообщений (буквы, цифры, знаки препинания, специальные символы, ...).

Мощность алфавита –полное число символов алфавита.

Мощность алфавита (в общем случае):

- русского языка – 33
- английского – 26

Алфавит может дополнительно включать цифры, знаки препинания, специальные символы.

### 1.4. Определение шифра в общем случае

Шифр (общий случай) –множество обратимых функций отображения Ek множества открытых сообщений M на множество криптограмм C, зависящих от выбранного ключа шифрования k из множества KE и соответствующие им обратные функции расшифрования Dk , зависящие от выбранного ключа расшифрования из множества KD , отображающие множество криптограмм C на множество открытых сообщений M.

Запись алгоритма шифрования (общего)

$Ek , k \in KED : M \rightarrow C ,$

$Dk , k \in KED : C \rightarrow M ,$

$\forall k \in KE \; \exists k \in KD ,$

$\forall m \in M : Ek(m) = c ,$

$\forall c \in C : Dk(c) = m$

### 1.5. Полиалфавиный шифр

Полиалфавитный шифр замены – шифр, при котором символы исходного сообщения заменяются символами исходного алфавита с переменным сдвигом по ключу.

Полиалфавитный шифр на основе ключевой последовательности:

Первичный ключ – любое слово или фраза.

Ключевая последовательность – последовательность символов, сформированная повторением первичного ключа до размера шифруемого сообщения.

$M_i$ – символ на $i$-й позиции сообщения, $i \in Z$.

$C_i$ – символ на $i$-й позиции криптограммы.

$C_i$ – суперпозиция $i$-го символа сообщения и $i$-го символа ключевой последовательности.

$C_i = M_i \,\&\, S_i$

$M_i = C_i \,\&\, S_i$

### 1.6. Полиалфавитный шифр на основе ключевой последованности

Шифр Виженера – метод простого полиалфавитного шифра замены на основе ключевого слова, преобразованного в одноразмерный с сообщением ключ, задающий переменный параметр $k_i$ сдвига символов исходного сообщения.

$k_i$ – переменный параметр сдвига по ключевому слову.

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

Рисунок 1 – Квадрат Виженера

## 2. Практическая часть

### 2.1. Зашифровка сообщения

Ниже, на рисунке 2, представлена таблица порядка действий зашифровки исходного текста инициатора, а на рисунке 3, представлена таблица результата шифрования и длины сообщений.

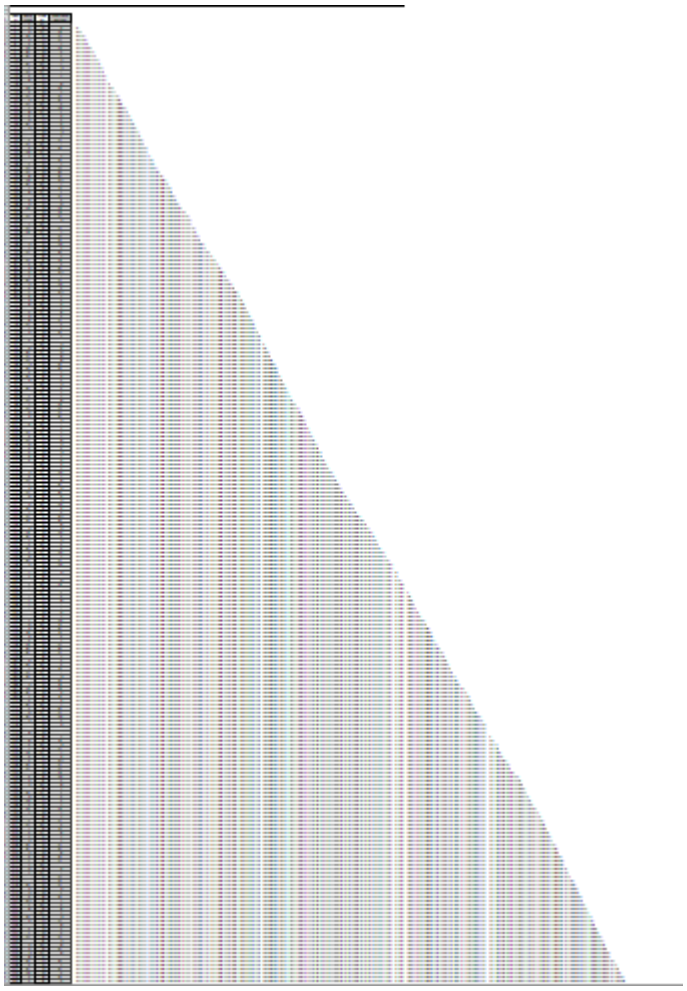


Рисунок 2 – Зашифровка сообщения

| Передаваемое сообщение | Длина сообщения: |
|---|---|
| УВАЖАЕМЫЙ ИГОРЬ ФЕОДОСЬЕВИЧ, СПЕШУ СООБЩИТЬ ВАМ О ТОМ, ЧТО ПРАКТИЧЕСКАЯ РАБОТА 5 ВЫПОЛНЕНА И ГОТОВА К ПРОВЕРКЕ. ДРОЗДОВ АНТОН ДМИТРИЕВИЧ 03.12.2002. УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ, Я БЕЗМЕРНО РАД НАШЕМУ СОТРУДНИЧЕСТВУ, НАДЕЮСЬ НА ЕГО ДАЛЬНЕЙШЕЕ УСПЕШНОЕ И ВЗАИМОВЫГОДНОЕ РАЗВИТИЕ. С УВАЖЕНИЕМ, ИГОРЬ ФЕОДОСЬЕВИЧ | 307 |
| **Зашифрованное сообщение** | **Длина сообщения:** |
| ,КФЦОЗМЯСДЮЛ20.БФТЦЙ6ЩЦ ХРЮЧЛЯЦЪ7Н ЭНУОЫЙЮЮЪГ ПЯВММЦДЦЮОНЩГЫЭФ6ИЮ2ЦЩЕЮТЕКЭ4РГРТНЗЧКЯЯЬНПТХЕЧРУ УЬФОПИ/Д33ОЬДЕЭТКХЭШОЬЙДЫКДШХ6ЮЫБДЩРЧ8РЦГЦЩ А.ВМ.СЕБ22КЭШЪИГЬРУОЫЦЗЕ5ЪZ9НЖМХЪХ0НЦШ5А ЯЖЭЮ1ОХЮПОМЩЕЬЗЮРЭМ9ЯЦ6Ь43ТПНЧНЦК7ОНПАСН394УЭОЬБРЦДЬЯЯ ЬЗЙЭНЧЫЯ58УЪННЬНДЭЯЦЧОЖМЫКЮЫЦШЭЬЗ`ЭИМЪР6ШУ ЮЯШГЬИЪХЫКЕЩДЮЛ20.БФТЦЙ6ЩЦ ХРК | 304 |

Рисунок 3 – Результат шифрования

## 2.2. Расшифровка сообщения

Ниже, на рисунке 4, представлена таблица порядка действий расшифровки текста, для получения исходного, а на рисунке 5, представлена таблица результата расшифровки и длины сообщений.

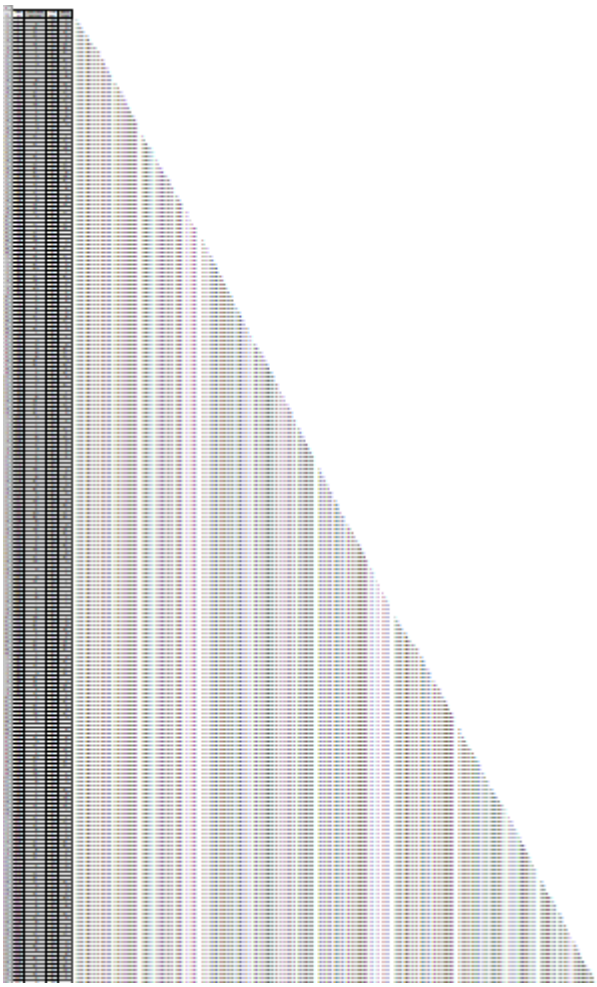


Рисунок 4 – Расшифровка сообщения

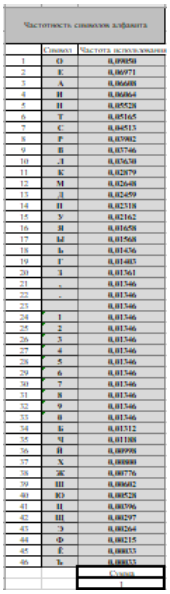
| Зашифрованное сообщение | Длина сообщения: |
|---|---|
| ,К‡ЦОЗМ8СДОЛ20.Б‡ТЦЙЯЩГХРКЧЛЗЦ'Н ЭНУОЬЙЙОО'ЬГПРВММЦД.ЦОЮЩТЬЗ‡ЙИОЦЩЕЮТЕКЭАРПРТНЗ.ЧКВ.ЯЬНИТХЕЧРУ'УЬ‡ОПИДЗЗЮЬДЕЭТКХЗШЮЬЙДЫКДШХ‰ЮЫБДШРЧЯРЩТЦЦ<br>А,ВМ.СЕБ22КЗШЬИЪРУОЫЦЗБ5'ЪЭНЖМЭ'ЪХОНЦШ5А ЭЖЭП0ХЮПОМШЕЬЭ1Р63МОЗЦЄЬ4ЭТПИ4НЦ.К'ОНПАСНЭ94'УЭОБВРЦДЬЯЯ ЬЗЙЯНКЧЫ5ЯУЪННЬНДОЗЦЧЮКМЫКЮЫЦШЭЬЭ ЭИМЪРЄШУ ЮЗШЬИЪХЫКЕЦЖДОЛ20.Б‡ТЦЙЯЩГХРК | 306 |
| **Расшифрованное сообщение** | **Длина сообщения:** |
| УВАЖАЕМЫЙ ИГОРЬ ‡ЕОДОСЬЕВИЧ, СПЕШУ СООБЩИТЬ ВАМ О ТОМ, ЧТО ПРАКТИЧЕСКАЯ РАБОТА 5 ВЫПОЛНЕНА И ГОТОВА К ПРОВЕРКЕ. ДРОЗДОВ АНТОН ДМИТРИЕВИЧ 03.12.2002. УВАЖАЕМЫЙ АНТОН ДМИТРИЕВИЧ, Я БЕЗМЕРНО РАД НАШЕМУ СОТРУДНИЧЕСТВУ, НАДЕЮСЬ НА ЕГО ДАЛЬНЕЙШЕЕ УСПЕШНОЕ И ВЗАИМОВЫГОДНОЕ РАЗВИТИЕ. С УВАЖЕНИЕМ, ИГОРЬ ‡ЕОДОСЬЕВИ | 306 |

Рисунок 5 – Результат расшифровки

## 3. Анализ частотности текста

### 3.1. Таблица и график частотности исходного алфавита

Ниже, на рисунке 6, представлена таблица частотности исходного алфавита в порядке уменьшения, а на рисунке 7, представлен график построенный на основе данной таблицы.



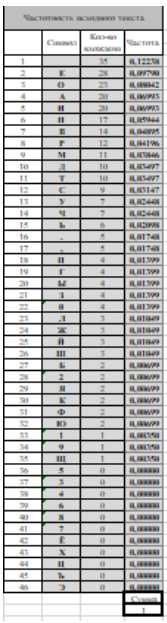
| Частотность символов алфавита | | |
|---|---|---|
| | Символ | Частота использования |
| 1 | О | 0,090850 |
| 2 | Е | 0,069771 |
| 3 | А | 0,066698 |
| 4 | И | 0,060864 |
| 5 | Н | 0,055528 |
| 6 | Т | 0,053165 |
| 7 | С | 0,046513 |
| 8 | Р | 0,039002 |
| 9 | В | 0,037446 |
| 10 | Л | 0,035630 |
| 11 | К | 0,028279 |
| 12 | М | 0,026648 |
| 13 | Д | 0,024559 |
| 14 | П | 0,023318 |
| 15 | У | 0,021621 |
| 16 | Я | 0,018658 |
| 17 | Ы | 0,015568 |
| 18 | Ь | 0,014436 |
| 19 | Г | 0,014085 |
| 20 | З | 0,013761 |
| 21 | , | 0,013546 |
| 22 | . | 0,013546 |
| 23 | | 0,013546 |
| 24 | 1 | 0,013546 |
| 25 | 2 | 0,013546 |
| 26 | 3 | 0,013546 |
| 27 | 4 | 0,013546 |
| 28 | 5 | 0,013546 |
| 29 | 6 | 0,013546 |
| 30 | 7 | 0,013546 |
| 31 | 8 | 0,013546 |
| 32 | 9 | 0,013546 |
| 33 | 0 | 0,013546 |
| 34 | Ъ | 0,013512 |
| 35 | Ч | 0,011108 |
| 36 | Й | 0,009998 |
| 37 | Х | 0,009000 |
| 38 | Ж | 0,007776 |
| 39 | Ш | 0,006602 |
| 40 | Ю | 0,005528 |
| 41 | Ц | 0,003596 |
| 42 | Щ | 0,002597 |
| 43 | Э | 0,002264 |
| 44 | Ф | 0,002215 |
| 45 | Ё | 0,000833 |
| 46 | Ъ | 0,000833 |
| | | Сумма |
| | | 1 |

Рисунок 6 – Таблица частоты исходного алфавита


Рисунок 7 – График частотности исходного алфавита

### 3.2. Таблица и график частотности исходного текста

Ниже, на рисунке 8, представлена таблица частотности использования алфавита в исходном тексте в порядке уменьшения, а на рисунке 9, представлен график построенный на основе данной таблицы.



Частотность исходного текста

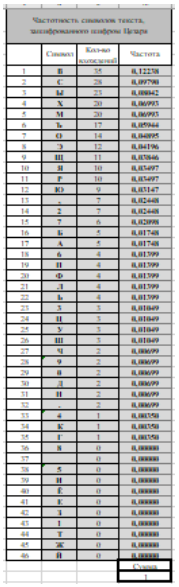
| | Символ | Кол-во вхождений | Частота |
|---|---|---|---|
| 1 | | 35 | 0,12238 |
| 2 | Е | 28 | 0,09790 |
| 3 | О | 25 | 0,08042 |
| 4 | А | 20 | 0,06993 |
| 5 | И | 20 | 0,06993 |
| 6 | Н | 17 | 0,05944 |
| 7 | В | 14 | 0,04895 |
| 8 | Р | 12 | 0,04196 |
| 9 | М | 11 | 0,03846 |
| 10 | Д | 10 | 0,03497 |
| 11 | Т | 10 | 0,03497 |
| 12 | С | 9 | 0,03147 |
| 13 | У | 7 | 0,02448 |
| 14 | Ч | 7 | 0,02448 |
| 15 | Ь | 6 | 0,02098 |
| 16 | . | 5 | 0,01748 |
| 17 | , | 5 | 0,01748 |
| 18 | П | 4 | 0,01399 |
| 19 | Г | 4 | 0,01399 |
| 20 | Ы | 4 | 0,01399 |
| 21 | З | 4 | 0,01399 |
| 22 | О | 4 | 0,01399 |
| 23 | Л | 3 | 0,01049 |
| 24 | Ж | 3 | 0,01049 |
| 25 | Й | 3 | 0,01049 |
| 26 | Ш | 3 | 0,01049 |
| 27 | Б | 2 | 0,00699 |
| 28 | 2 | 2 | 0,00699 |
| 29 | Я | 2 | 0,00699 |
| 30 | К | 2 | 0,00699 |
| 31 | Ф | 2 | 0,00699 |
| 32 | Ю | 2 | 0,00699 |
| 33 | 1 | 1 | 0,00350 |
| 34 | 9 | 1 | 0,00350 |
| 35 | Щ | 1 | 0,00350 |
| 36 | 5 | 0 | 0,00000 |
| 37 | 3 | 0 | 0,00000 |
| 38 | 4 | 0 | 0,00000 |
| 39 | 6 | 0 | 0,00000 |
| 40 | 8 | 0 | 0,00000 |
| 41 | 7 | 0 | 0,00000 |
| 42 | Ё | 0 | 0,00000 |
| 43 | Х | 0 | 0,00000 |
| 44 | Ц | 0 | 0,00000 |
| 45 | Ъ | 0 | 0,00000 |
| 46 | Э | 0 | 0,00000 |
| | | | Сумма |
| | | | 1 |

Рисунок 8 – Таблица частоты исходного текста


Рисунок 9 – График частотности исходного текста

### 3.3. Таблица и график частотности зашифрованного текста (шифр Цезаря)

Ниже, на рисунке 10, представлена таблица частотности использования алфавита в зашифрованном тексте в порядке уменьшения, а на рисунке 11, представлен график построенный на основе данной таблицы.



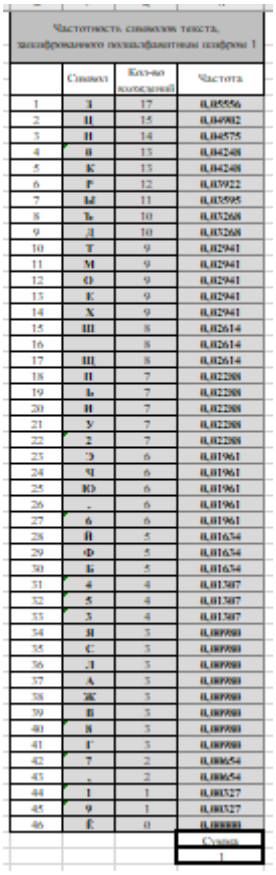
| Частотность символов текста, зашифрованного шифром Цезаря | | | |
|---|---|---|---|
| | Символ | Кол-во совпадений | Частота |
| 1 | В | 35 | 0,12238 |
| 2 | С | 28 | 0,09790 |
| 3 | Ы | 23 | 0,08042 |
| 4 | Х | 20 | 0,06993 |
| 5 | М | 20 | 0,06993 |
| 6 | Ъ | 17 | 0,05944 |
| 7 | О | 14 | 0,04895 |
| 8 | Э | 12 | 0,04196 |
| 9 | Щ | 11 | 0,03846 |
| 10 | Я | 10 | 0,03497 |
| 11 | Р | 10 | 0,03497 |
| 12 | Ю | 9 | 0,03147 |
| 13 | , | 7 | 0,02448 |
| 14 | 2 | 7 | 0,02448 |
| 15 | 7 | 6 | 0,02098 |
| 16 | Б | 5 | 0,01748 |
| 17 | А | 5 | 0,01748 |
| 18 | 6 | 4 | 0,01399 |
| 19 | П | 4 | 0,01399 |
| 20 | Ф | 4 | 0,01399 |
| 21 | Л | 4 | 0,01399 |
| 22 | Ь | 4 | 0,01399 |
| 23 | З | 3 | 0,01049 |
| 24 | Ц | 3 | 0,01049 |
| 25 | У | 3 | 0,01049 |
| 26 | Ш | 3 | 0,01049 |
| 27 | Ч | 2 | 0,00699 |
| 28 | 9 | 2 | 0,00699 |
| 29 | 0 | 2 | 0,00699 |
| 30 | Д | 2 | 0,00699 |
| 31 | Н | 2 | 0,00699 |
| 32 | . | 2 | 0,00699 |
| 33 | 4 | 1 | 0,00350 |
| 34 | К | 1 | 0,00350 |
| 35 | Г | 1 | 0,00350 |
| 36 | 8 | 0 | 0,00000 |
| 37 | 5 | 0 | 0,00000 |
| 38 | И | 0 | 0,00000 |
| 39 | Ё | 0 | 0,00000 |
| 40 | Е | 0 | 0,00000 |
| 41 | 3 | 0 | 0,00000 |
| 42 | 1 | 0 | 0,00000 |
| 43 | Т | 0 | 0,00000 |
| 44 | Ж | 0 | 0,00000 |
| 45 | Й | 0 | 0,00000 |
| 46 | | | Сумма |
| | | | 1 |

Рисунок 10 – Таблица частоты зашифрованного текста


Рисунок 11 – График частотности зашифрованного текста

### 3.4. Таблица и график частотности зашифрованного текста (шифр 1)

Ниже, на рисунке 12, представлена таблица частотности использования алфавита в зашифрованном тексте в порядке уменьшения, а на рисунке 13, представлен график построенный на основе данной таблицы.



| | Символ | Кол-во вхождений | Частота |
|---|---|---|---|
| 1 | З | 17 | 0,05556 |
| 2 | Щ | 15 | 0,04902 |
| 3 | П | 14 | 0,04575 |
| 4 | Ь | 13 | 0,04248 |
| 5 | К | 13 | 0,04248 |
| 6 | Р | 12 | 0,03922 |
| 7 | Ы | 11 | 0,03595 |
| 8 | Ъ | 10 | 0,03268 |
| 9 | Д | 10 | 0,03268 |
| 10 | Т | 9 | 0,02941 |
| 11 | М | 9 | 0,02941 |
| 12 | О | 9 | 0,02941 |
| 13 | Е | 9 | 0,02941 |
| 14 | Х | 9 | 0,02941 |
| 15 | Ш | 8 | 0,02614 |
| 16 | | 8 | 0,02614 |
| 17 | Щ | 8 | 0,02614 |
| 18 | П | 7 | 0,02288 |
| 19 | Ь | 7 | 0,02288 |
| 20 | И | 7 | 0,02288 |
| 21 | У | 7 | 0,02288 |
| 22 | 2 | 7 | 0,02288 |
| 23 | Э | 6 | 0,01961 |
| 24 | Ч | 6 | 0,01961 |
| 25 | Ю | 6 | 0,01961 |
| 26 | . | 6 | 0,01961 |
| 27 | 6 | 6 | 0,01961 |
| 28 | Й | 5 | 0,01634 |
| 29 | Ф | 5 | 0,01634 |
| 30 | Б | 5 | 0,01634 |
| 31 | 4 | 4 | 0,01307 |
| 32 | 5 | 4 | 0,01307 |
| 33 | 3 | 4 | 0,01307 |
| 34 | Я | 3 | 0,00980 |
| 35 | С | 3 | 0,00980 |
| 36 | Л | 3 | 0,00980 |
| 37 | А | 3 | 0,00980 |
| 38 | Ж | 3 | 0,00980 |
| 39 | В | 3 | 0,00980 |
| 40 | 8 | 3 | 0,00980 |
| 41 | Г | 3 | 0,00980 |
| 42 | 7 | 2 | 0,00654 |
| 43 | , | 2 | 0,00654 |
| 44 | 1 | 1 | 0,00327 |
| 45 | 9 | 1 | 0,00327 |
| 46 | Ё | 0 | 0,00000 |
| | | | Сумма |
| | | | 1 |

Рисунок 12 – Таблица частоты зашифрованного текста


Рисунок 13 – График частотности зашифрованного текста

## 4. Заключение

В ходе выполнения данной практической работы было реализован полиалфавитный шифр на основе квадрата Виженера, таблицы шифрования/расшифрования, зашифровано и расшифровано сообщение. Проведен анализ слабостей шифра, приведены таблицы и гистограммы

частотности символов исходного алфавита и сообщения, зашифрованного разработанным шифром, описаны слабости шифра. Проведен сравнительный анализ моноалфавитного и полиалфавитного шифров, в результате чего выяснилось, что последний обладает большей криптостойкостью. Получены навыки в работе с полиалфавитными шифрами в Excel.