|  |  |
| --- | --- |
| **Российский университет транспорта (МИИТ)**  **Институт транспортной техники и систем управления**  **Кафедра «Управление и защита информации»** | |
| **Отчет**  **по практическому заданию**  **по теме «Разработка многоалфавитного шифра замены»**  **по дисциплине**  **«Криптографические методы защиты информации»** | |
|  | **Выполнил:**  студент группы ТКИ-341  Порхун Д.Д.  **Проверил:**  Доцент кафедры УиЗИ к.т.н., с.н.с.  Михалевич И.Ф. |
| Москва 2023 | |

Оглавление

[Задание 3](#_Toc129456105)

[ИСХОДНЫЕ ДАННЫЕ 4](#_Toc129456106)

[1. Краткие теоритические сведения по шифру цезаря 5](#_Toc129456107)

[2. Блокнот с алфавитом 7](#_Toc129456108)

[3. Шифрование исходного текста 8](#_Toc129456109)

[3.1. Исходный текст 8](#_Toc129456113)

[3.2. Шифрование 9](#_Toc129456114)

[3.3. Зашифрованный текст 12](#_Toc129456115)

[4. Расшифровка текста 12](#_Toc129456116)

[4.1. Исходный текст 12](#_Toc129456120)

[4.2. Расшифрование 13](#_Toc129456121)

[4.3. Расшифрованный текст 15](#_Toc129456122)

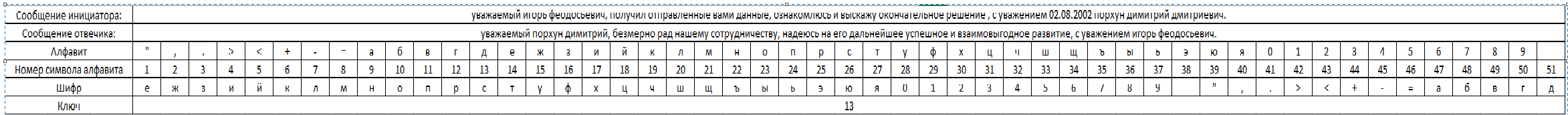
[5. Анализ слабостей шифра цезаря 16](#_Toc129456123)

[Заключение 17](#_Toc129456124)

Задание

* Разработать моноалфавитный шифр, таблицы шифрования / расшифрования (для варианта шифра);
* Подготовить сообщение (конкатенация сообщений инициатора и ответчика);
* Зашифровать и расшифровать сообщение;
* Провести анализ слабостей шифра (привести таблицы и гистограммы частотности символов исходного алфавита и сообщения, зашифрованного разработанным шифром, описать слабости шифра);
* Оформить отчет.

ИСХОДНЫЕ ДАННЫЕ



# Краткие теоритические сведения по шифру цезаря

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, ...).

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

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 –26Алфавит может дополнительно включать цифры, знаки препинания, специальные символы

Шифр (общий случай) – множество обратимых функций отображения множества открытых сообщений на множество криптограмм , зависящих от выбранного ключа шифрования из множества и соответствующие им обратные функции расшифрования , зависящие от выбранного ключа расшифрования из множества , отображающие множество криптограмм на множество открытых сообщений

Запись алгоритма шифрования (общего):

Моноалфавитныйшифр:

*K* – ключ, 0 < *K* ≤ n ;

n – мощность алфавита.

– символ на *i*-ой позиции исходного сообщения, *i* ∊ N

– символ на *i* – ой позиции криптограммы.

Шифр Цезаря – метод создания просто моноалфавитного шифра на основе ключа с остоянным параметром сдвига на *K* символов.

*i* – позиция символа в алфаите шифра;

*–* исходный и зашифрованные символы;

*K –* параметр сдвига (ключ);

*N –* мощность алфавита.

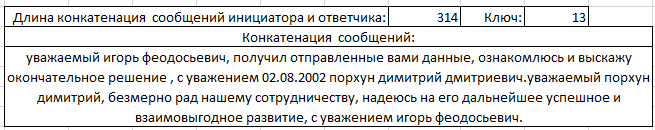
# Блокнот с алфавитом

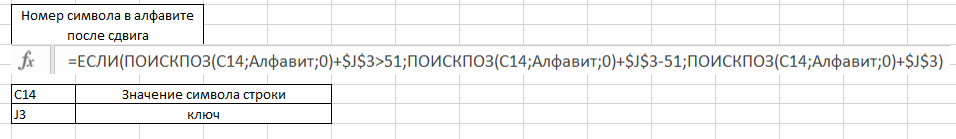


# Шифрование исходного текста

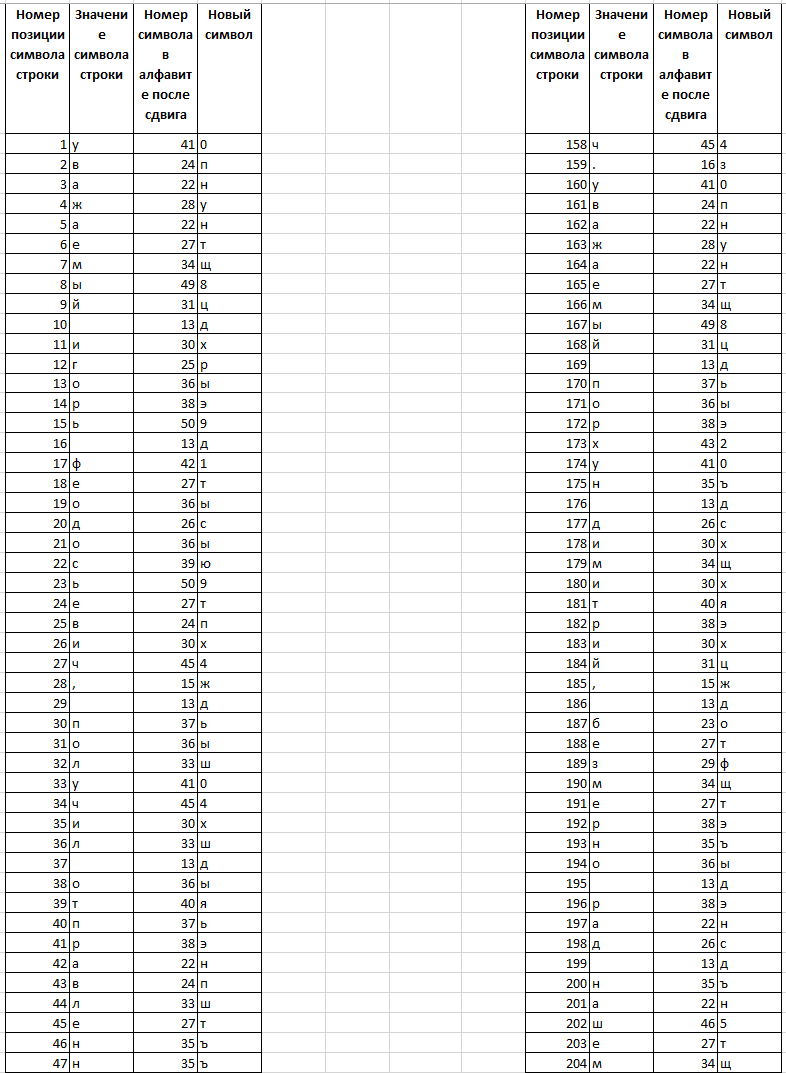


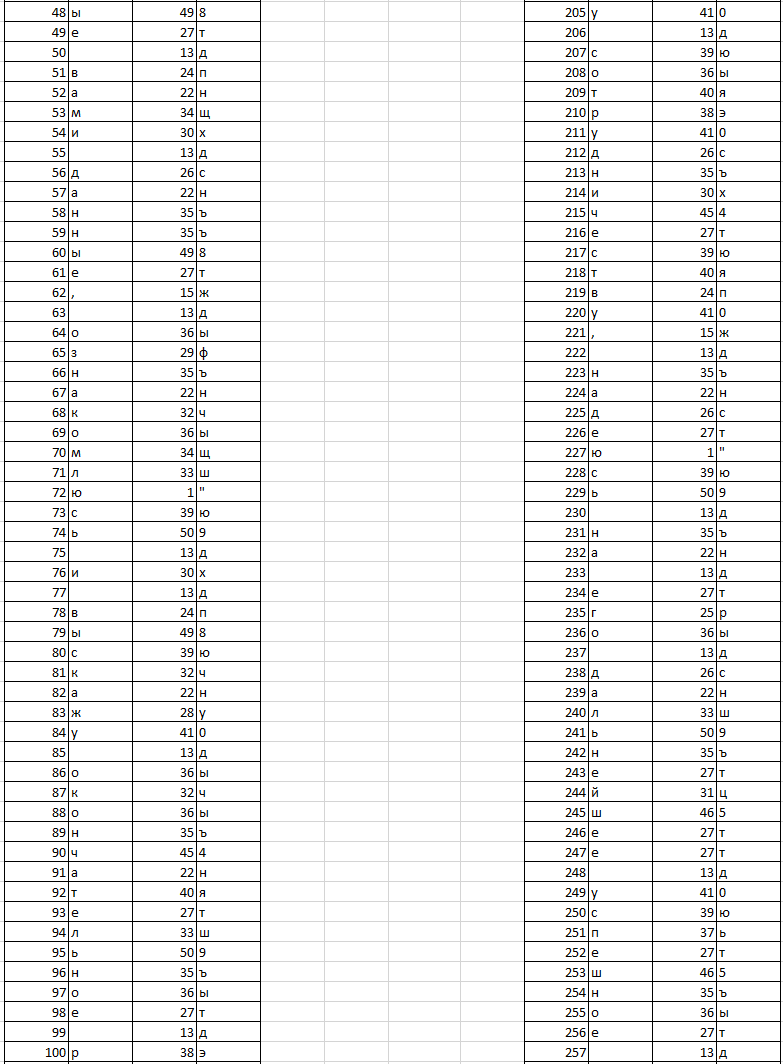
## Исходный текст

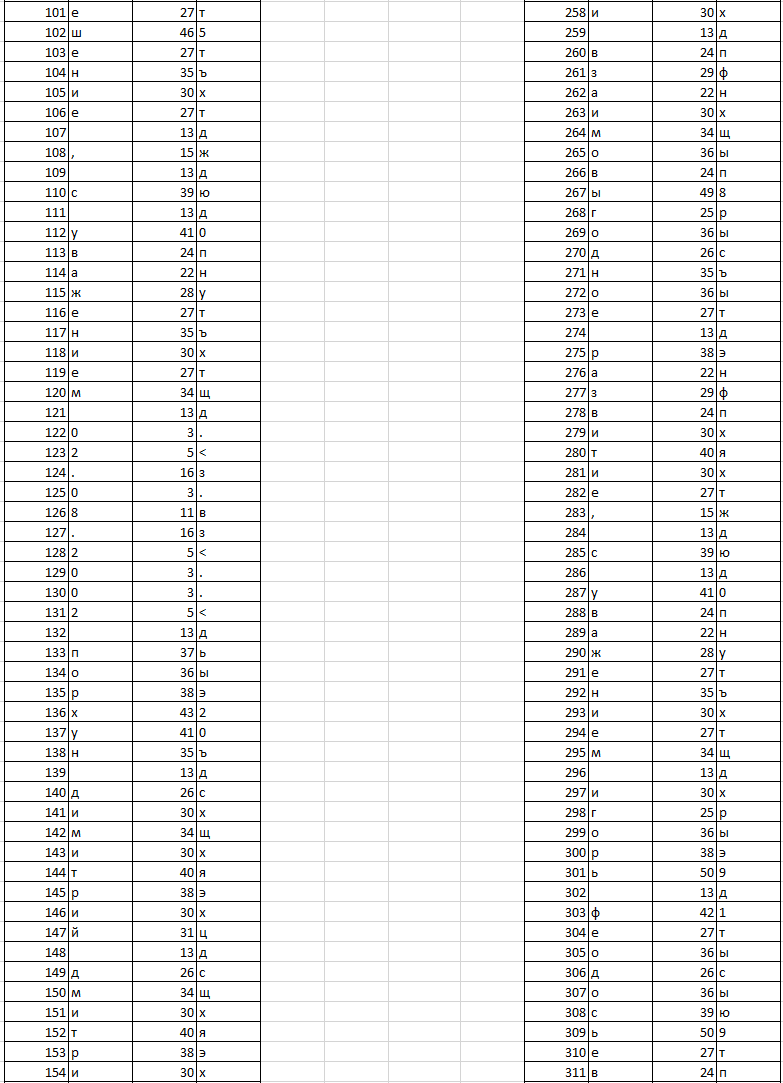


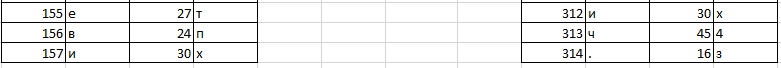


## Шифрование

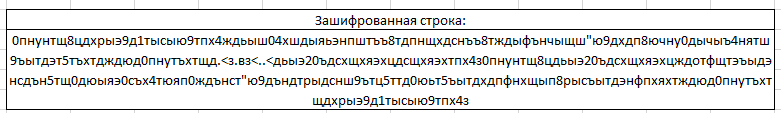








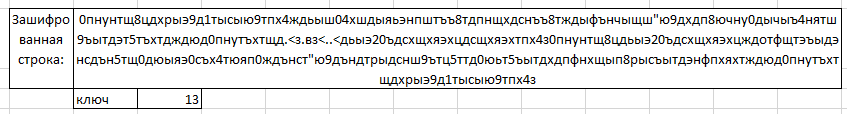
## Зашифрованный текст

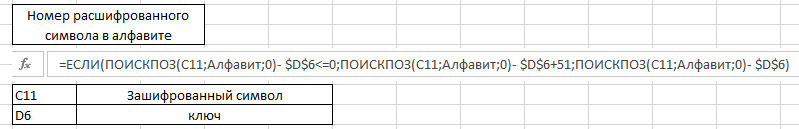


# Расшифровка текста

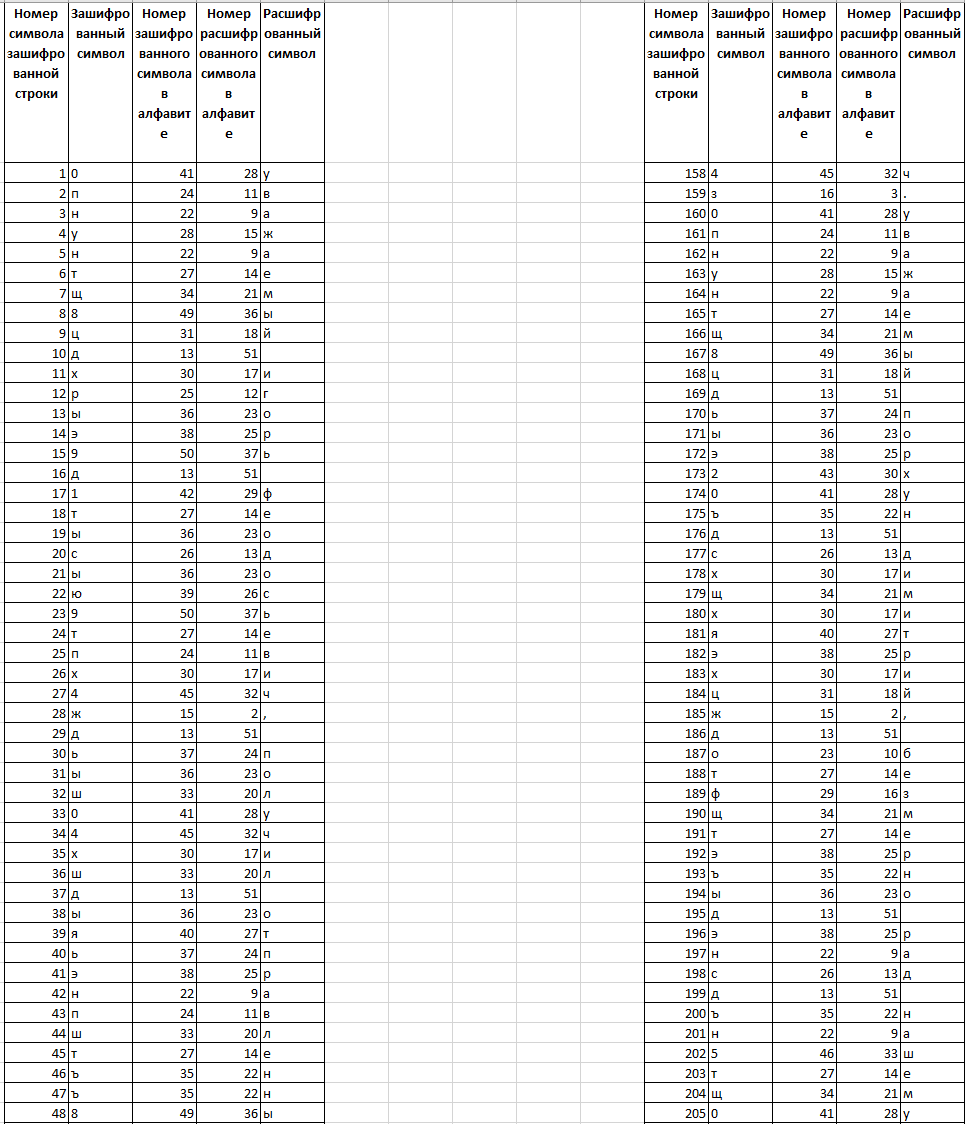


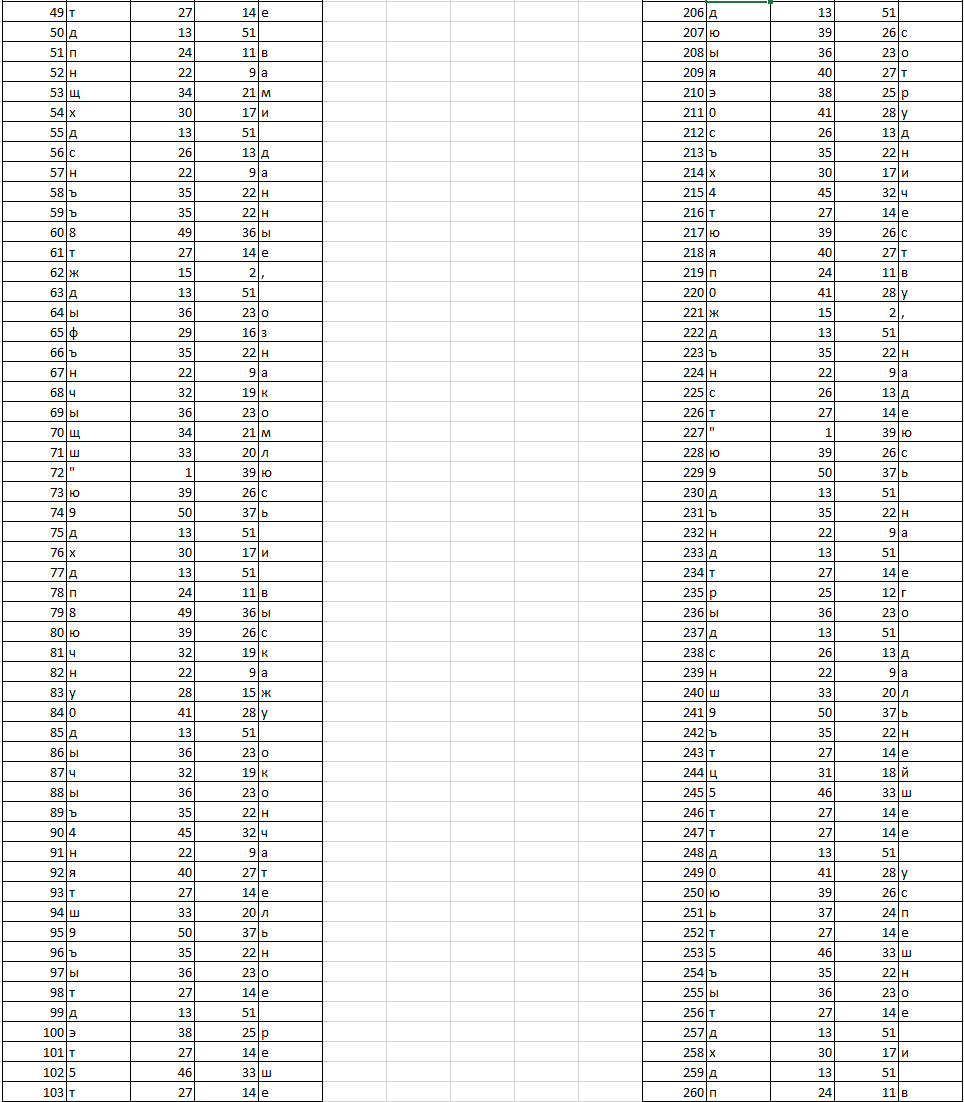
## Исходный текст

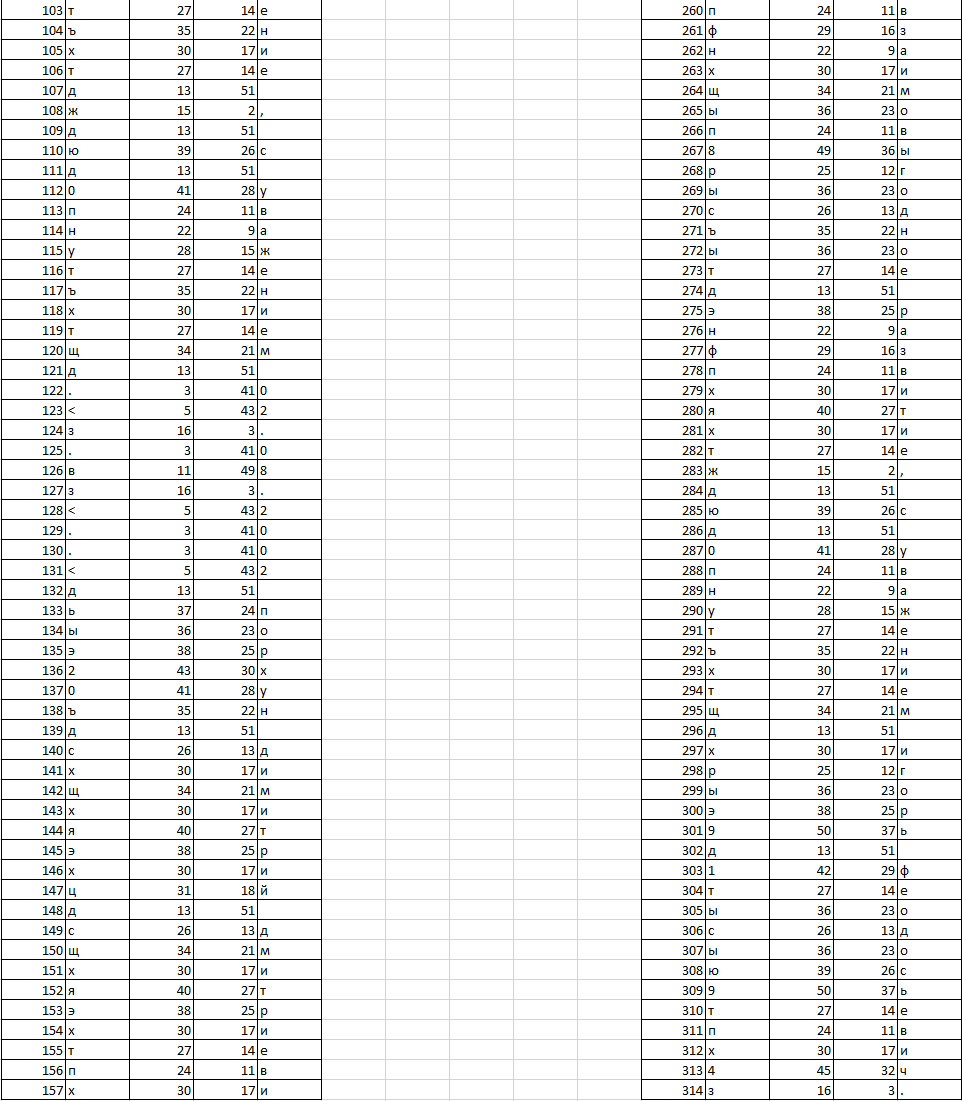




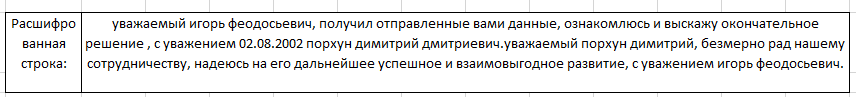
## Расшифрование



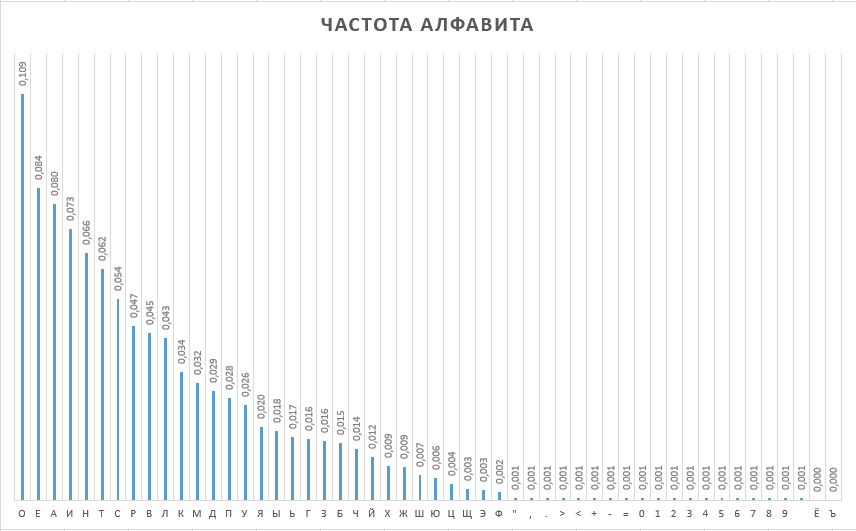




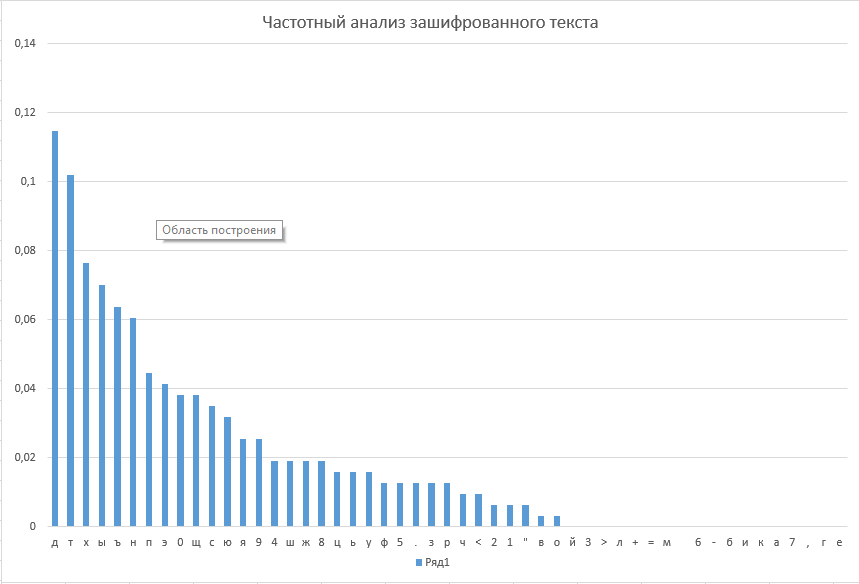
## Расшифрованный текст



# Анализ слабостей шифра цезаря







Заключение

В ходе решения практического задания реализован шифр Цезаря. Шифр Цезаря – достаточно простой в реализации шифр, однако он подвержен простому перебору, так как существует малое количество ключей, а также уязвим для частотного анализа текста.