Министерство образования и науки Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

Институт кибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА № 2**

**Основы частотного криптоанализа**

по дисциплине «Основы информационной безопасности»

Выполнил

студент гр. 4851003/10002 Билан Н.С.

Руководитель

ст. преподаватель Зубков Е.А

1. **ЦЕЛЬ РАБОТЫ**

Цель работы – приобретение навыков криптоанализа, а также ознакомление со способом дешифрования криптограмм на примере применения метода частотного криптоанализа.

**2. ЗАДАЧИ**

1. Разработать программу, реализующую функции инструмента крипто аналитика.

2. С использованием разработанной программы расшифровать криптограмму, выданную преподавателем.

**3. ХОД РАБОТЫ**

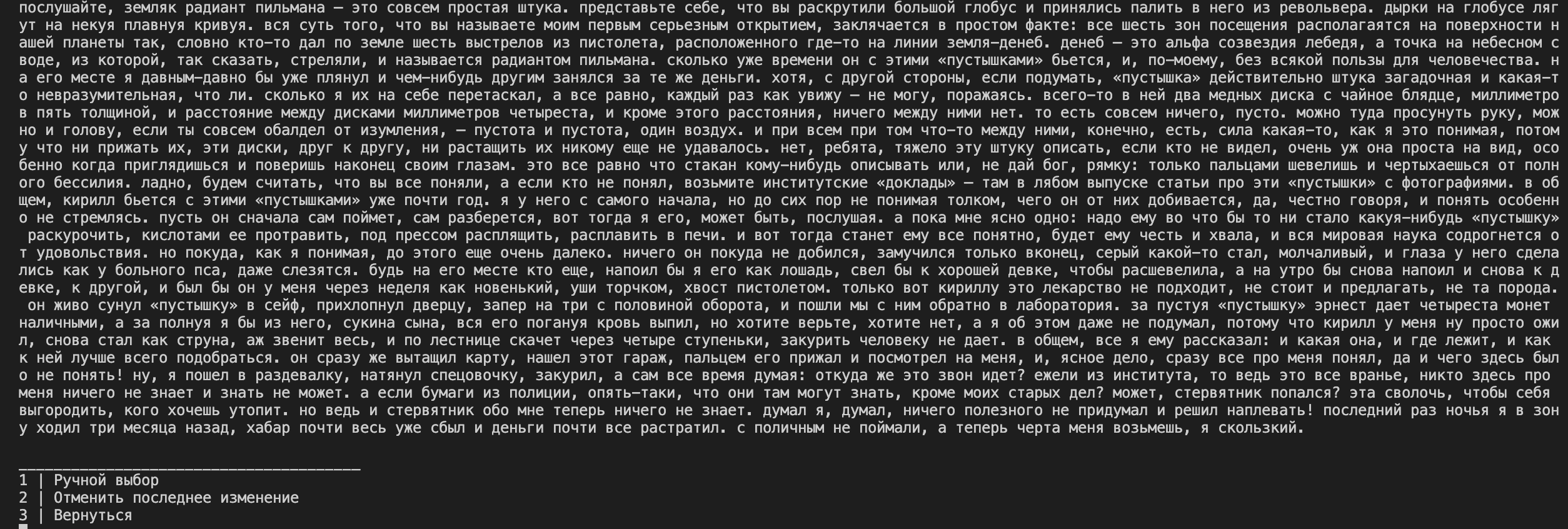
В ходе работы был реализован алгоритм частотного анализа букв в криптограмме. На основе количества появлений каждой буквы в исходной криптограмме этот алгоритм отсортировывает буквы в порядке убывания частоты, сопоставляя частоты букв в исходной криптограмме с частотами букв в русском языке. Процедура *outPossReplace(cryprAlp[], realTextSize)* выводит предполагаемые замены букв в консоль. Хранение количества появлений букв осуществляется в массиве ***wchInfo*** *freqOfSymb[]*. Создана структура ***wchInfo***, в полях которой хранится сам символ ***wchar\_t*** *chr* и количество встреч оного ***unsInt*** *count*. Хранение текущего состояния криптограммы осуществляется в массиве ***wchar\_t*** *history[][]*. При запуске программы вызывается процедура *usrInterface(&cur\_st, freqOfSymb, history, sizeOfText, letNumb, outFName)*, через которую осуществляется доступ пользователя к использованию реализованного в программе функционала.

Была реализована как процедура единичной замены одной буквы на другую (во всей криптограмме сразу), так и функция автозамены всех букв в соответствии с их частотным распределением. Следует отметить, что вследствие отклонения фактического частотного распределения в сравнении с теоретическим, и чем меньше по размерам текст, тем больше отклонение, автозамена оставляет текст в большом регистре, дабы оставить возможность изменения текста ручным методом (при ручном методе регистр изменяется в малый).

Для работы был взят текст книги, пропущенный через алгоритм Цезаря. Исходя из частотного распределения букв была сделана замена буквы “Х” на “о”. Далее, исходя из большого количества отдельно стоящих букв “П”, была сделана предположительная замена буквы “П” на “и”. В тексте, в нескольких местах, было найдено слово «ДЩо», перед которым стояло тире. Вследствие этого было выдвинуто предположение о том, что букву «Д» можно заменить на «э», а «Щ» на букву «т». Так же, в тексте было найдено слово «этиУи», что навело на мысль замены буквы «У» на «м». Следующее найденное слово было «Штоит», вследствие чего буква «Ш» была заменена на «с». Словосочетание «оЗ этом» намекнуло на замену «З» на «б». Слово «сЛбЛ» к замене «Л» на «е». В слове «соИсем» очевидно виднелась буква «в» на месте «И». После всех этих замен большинство слов в криптограмме становятся понятны или различимы. Замены букв далее производятся по смыслу.

**4. РЕЗУЛЬТАТЫ**

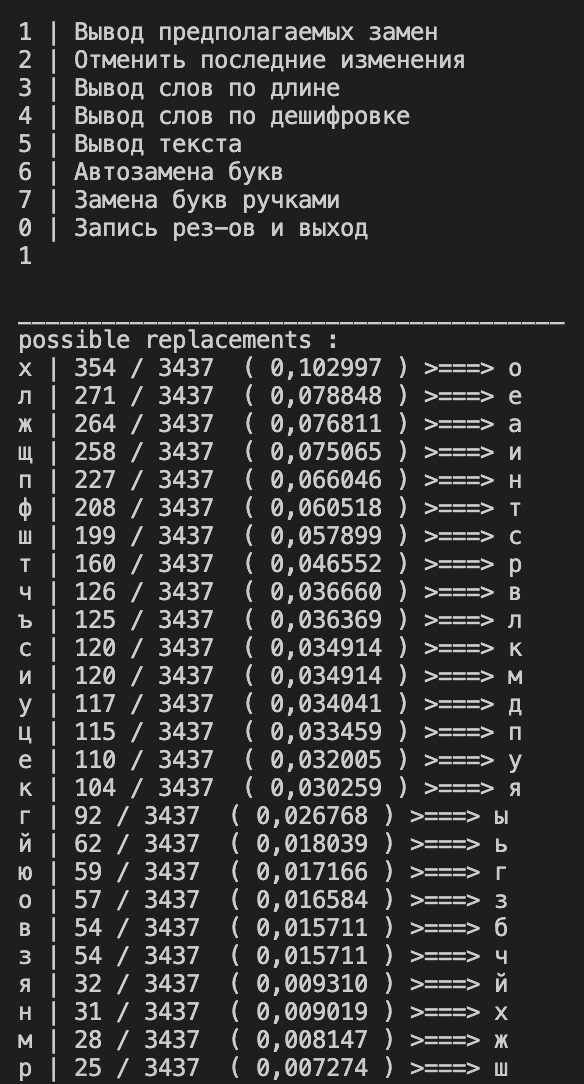
Результатом работы программы является полностью дешифрованный текст. Он представлен на рисунке 1.

**Рисунок 1. Результат работы программы.**

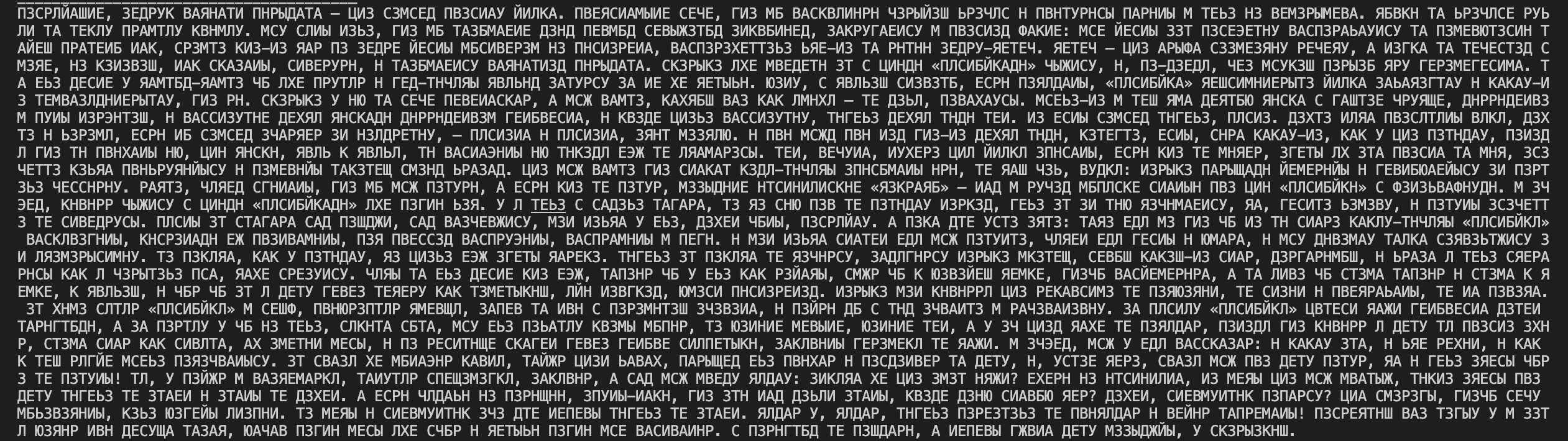
(Была замечена проблема с расшифровкой, заключающаяся в том, что программой учитывается лишь 32 буквы без Ё, но сайт, работающий с алгоритмом Цезаря, использует все 33 буквы алфавита, потому «Я» и «Ю» иногда могут находится на местах друг друга).

На следующих рисунках приведены примеры работы вспомогательных функций, реализованных в программе.

**Рисунок 2. Вывод слов по количеству расшифрованных букв.**



**Рисунок 3. Предполагаемые на основе частотного анализа замены.**

**Рисунок 4. Результат работы функции автозамены букв.**

**5. ВЫВОД**

На основе метода частотного криптоанализа была разработана программа-инструмент для расшифровки криптограмм, использующих моноалфавитную подстановку. В ней реализованы функции замены букв, вывода слов, сгруппированных по длине или количеству расшифрованных букв, хранения и отката истории замен. Также с её помощью удалось расшифровать выданную криптограмму. В общей сложности на лабораторную было потрачено ~ 10-12 часов.

**КОНТРОЛЬНЫЕ ВОПРОСЫ**

1. Что такое шифр моноалфавитной подстановки?

**Шифр моноалфавитной подстановки** - метод шифрования текста с использованием, так называемого, нормативного алфавита и алфавита шифрования путём взаимооднозначного соответствия символов нормативного алфавита и алфавита шифрования.

1. Укажите недостатки моноалфавинтой подстановки?  
   Главным недостатком моноалфавитного шифрования является слабая защищённость криптограммы, что выливается в уязвимость дешифровки.
2. Какова сложность дешифрации методом прямого перебора для сообщения, зашифрованного шифром моноалфавитной подстановки?  
   Сложность дешифрации методом прямого перебора для сообщения, зашифрованного шифром моноалфавитной подстановки равна мощности нормативного алфавита, так как в итоге нужно будет сделать ровно столько замен, сколько символов содержит нормативный алфавит.
3. Какие условия упрощают частотный анализ?  
   Частотный анализ тем легче, чем меньше мощность нормативного алфавита и чем больше входной текст, так как придётся делать меньше замен и сам частотный анализ облегчается вследствие возможности нахождения часто встречающихся в речи слов.
4. Получится ли правильно дешифрованная криптограмма, если произвести все замены в соответствии с частотами появления букв в русском языке? Ответ обосновать.  
   Нет, не получится, так как частотное распределение букв исходной криптограммы слабо соответствует частотному распределению букв русского языка. В частном случае какие-то буквы могут встречаться реже или чаще, как и специфические слова, вследствие чего автозамена может лишь намекнуть на потенциальные буквы, сузив потенциальные замены от 32 до 4-10.