**Подготовил: Филиппов Александр, ЕТ-225**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

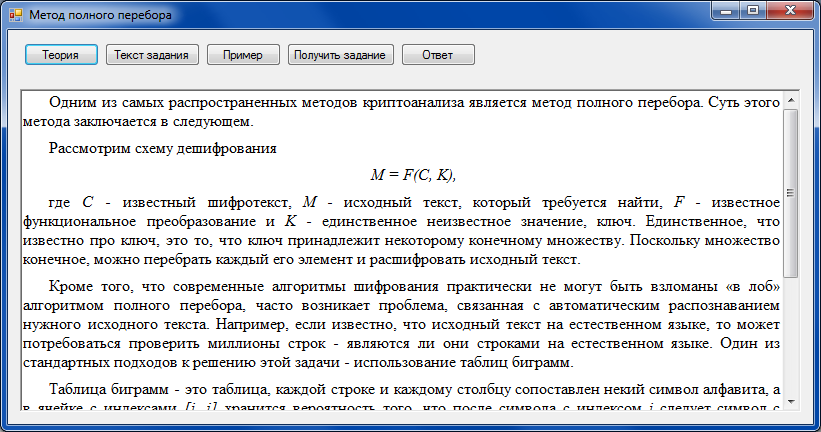
**Лабораторная работа «Криптоанализ методом полного перебора»**

## Общая информация

Необходимо разработать модуль лабораторной работы «Криптоанализ методом полного перебора».

Окно лабораторной работы должно иметь собственно основное окно, и 5 кнопок (см. рисунок 1):

1. теория;
2. текст задания;
3. пример выполнения задания;
4. получение задания;
5. проверка ответа.



Рисунок

Кнопки «Теория», «Текст задания» и «Пример» изменяют содержание основного окна на содержимое соответствующих им блоков. Кнопка «Получить задание» должна вызывать стандартное диалоговое окно выбора папки. Кнопка «Ответ» вызывает содержимое блока «Ответ» в отдельной форме. По умолчанию основное окно отображает блок «Теория».

## Теоретический материал и текст задания

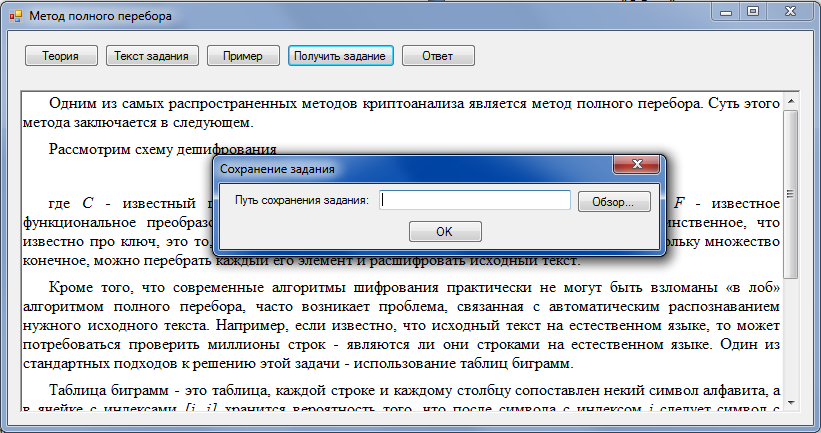
Теоретический материал и текст задания, которые необходимо отобразить, приведёны в приложении.

## Пример

Пример приведён в приложении.

## Получение задания

Блок должен содержать кнопку «Получить задание», при нажатии на которую вызывается окно для ввода пути сохранения задания (см. рисунок 3) с дополнительной кнопкой "Обзор", по нажатию на которую вызывается стандартный диалог выбора папки.



Рисунок

Выдаваемое задание должно соответствовать году обучения, семестру и варианту, выбранных в главном меню. Генерировать нужно таким образом, чтобы оно оставалось неизменным для года, семестра и варианта.

Шаги генерации:

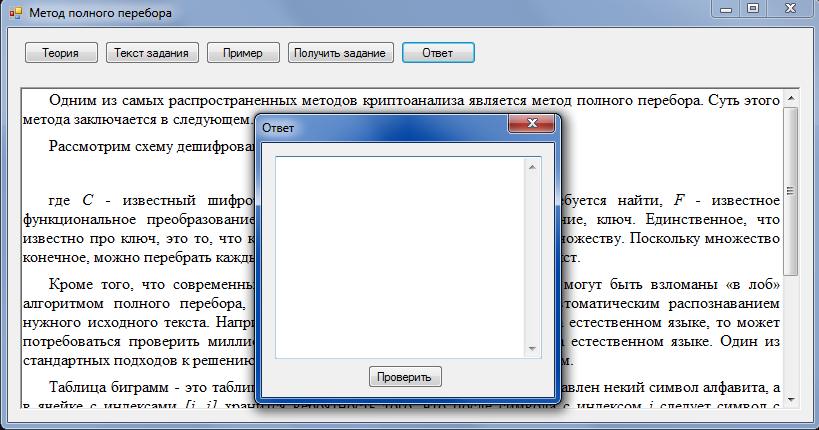
1. выбрать случайным образом отрывок текста на русском языке (длиной приблизительно 1500 символов) из ресурсов проекта, причём отрывок должен начинаться с начала слова и заканчиваться концом слова;
2. сгенерировать случайным образом ключ из 3 символов русского алфавита;
3. зашифровать отрывок ключом с помощью шифра Виженера по следующей формуле: c[i]=(x[i]+k[i])mod(33), где c[i] — номер i-го символа шифротекста, x[i] — номер i-го символа текста, k[i]— номер i-го символа ключа. Ключ записывается циклически. Символы букв нумеруются в порядке их следования в алфавите (без буквы Ё), номер пробела 33.

Символы отрывка, ключа и шифротекста должны быть в верхнем регистре.

Заданием, которое выдаётся пользователю, является шифротекст.

## Проверка ответа

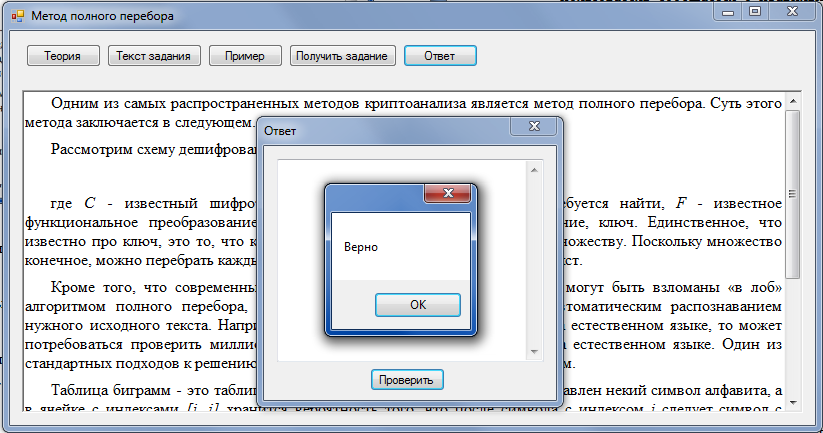
Блок проверки должен содержать поле для ввода текста, а также кнопку «Проверить» (см. рисунок 4), при нажатии на которую вызывается процедура проверки, после чего пользователь сообщается о правильности ответа. Если введённый пользователем текст совпадает со сгенерированным, то ответ верен.



Рисунок

В строке ответа необходимо убирать все символы, кроме заглавных букв русского алфавита. Также необходимо убирать все лишние пробелы в конце и в начале строки.

Если он соответствует выбранному при генерации задания отрывку, то задание выполнено верно/неверно, и это отображается в соответствующем окне (см. рисунок 5).



Рисунок

## Требования к тестированию

При тестировании разработанной программы необходимо обработать следующие исключительные ситуации:

1. Для блока «Получение задания»:

* выход за пределы общего текста при выборе отрывка для генерации задания;
* несуществующий путь для ввода полученного задания;
* незаданный путь для ввода полученного задания;

1. Для блока «Проверка ответа»:

* выход за пределы общего текста при генерации правильного ответа;
* лишние символы при сравнении строки ответа студента и правильного ответа.

При несуществующем или незаданном пути пользователю должны быть выведены соответствующие сообщения.

Выход за пределы общего текста должен быть предотвращен на этапе разработки программы.

При сравнении строки ответа студента и правильного ответа все лишние символы (указанные в пункте 5) в строке ответа должны быть исключены.

## Требования к программной документации

Для создания программной документации необходимо разработать руководство пользователя на основе «ГОСТ 19.505-79. ЕСПД. Руководство оператора. Требования к содержанию и оформлению». Это руководство должно включать в себя следующие разделы:

* назначение программы;
* условия выполнения программы;
* выполнение программы;
* сообщения пользователю.

ПРИЛОЖЕНИЕ

**Теория**

**Криптоанализ методом полного перебора**

Одним из самых распространенных методов криптоанализа является метод полного перебора. Суть этого метода заключается в следующем.

Рассмотрим схему дешифрования

*M = F(C, K),*

где *C* — известный шифротекст, *M* — исходный текст, который требуется найти, *F* — известное функциональное преобразование и *K* — единственное неизвестное значение, ключ. Единственное, что известно про ключ, это то, что ключ принадлежит некоторому конечному множеству. Поскольку множество конечное, можно перебрать каждый его элемент и расшифровать исходный текст.

Кроме того, что современные алгоритмы шифрования практически не могут быть взломаны «в лоб» алгоритмом полного перебора, часто возникает проблема, связанная с автоматическим распознаванием нужного исходного текста. Например, если известно, что исходный текст на естественном языке, то может потребоваться проверить миллионы строк — являются ли они строками на естественном языке. Один из стандартных подходов к решению этой задачи — использование таблиц биграмм.

Таблица биграмм – это таблица, каждой строке и каждому столбцу сопоставлен некий символ алфавита, а в ячейке с индексами *[i, j]* хранится вероятность того, что после символа с индексом *i* следует символ с индексом *j*. Это позволяет вычислить вероятность того, что вся строка принадлежит русскому языку по формуле

где *ps(i),s(i+1)*— вероятность, что после символа*s(i)* следует символ *s(i+1)*. Эта формула удобна для теоретического анализа, однако, при практической реализации при большом количестве умножений мантисса переполняется и удобнее вместо произведения использовать, например, сумму.

**Текст задания**

**Задание на лабораторную работу**

С помощью метода полного перебора восстановить исходный текст шифрограммы, зашифрованной шифром Виженера с длиной ключа 3.

**Порядок действий**

1. Сформировать таблицу биграмм для эталонного текста на русском языке.
2. Разработать программу для полного перебора ключей длины 3 в шифре Виженера и оценки вероятности для каждого расшифрованного исходного текста.
3. Найти 10 расшифрованных строк с самой большой оценкой вероятности.
4. Расшифровать шифротекст.

**Пример**

Для некоторого текста на русском языке была получена таблица биграмм. Ниже приведена её часть.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ж** | **3** | **И** | **И** | **К** | **Л** | **М** | **Н** | **О** | **П** | **Р** | **С** | **Т** | **У** | **Ф** | **X** | **Ц** | **Ч** | **Ш** | **Щ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| **А** | 2 | 12 | 35 | 8 | 14 | 7 | 6 | 15 | 7 | 7 | 19 | 27 | 19 | 45 | 3 | 11 | 26 | 31 | 27 | 3 | 1 | 10 | 6 | 7 | 10 | 1 |  |  | 2 | 6 | 9 |
| **Б** | 5 |  |  |  |  | 9 | 1 |  | 6 |  |  | 6 |  | 2 | 21 |  | 8 | 1 |  | 6 |  |  |  |  |  | 1 | 11 |  |  |  | 2 |

Строки таблицы соответствуют первым символам биграмм, столбцы —вторым символам; в ячейках указано количество соответствующих биграмм в тексте. Например, из данной таблицы видно, что сочетание «АВ» встречается 35 раз, а «БО» — 21 раз.

Вероятности для биграмм находятся следующим образом: для каждой строки таблицы считается сумма всех значений и затем каждое значение делится на полученную сумму.

Для данной таблицы сумма значений в первой строке равна 376. Вероятность для сочетания «АА» равна 2/376.

Вероятность P(S) будет равна произведению всех ненулевых вероятностей в таблице.