**Техническое задание**

**Лабораторная работа «Моноалфовитный шифр»**

1. **Общая информация**

Необходимо разработать модуль лабораторной работы «Моноалфовитный шифр».

Окно лабораторной работы должно иметь основное окно и 3 кнопки (см. рисунок 1):

1. теория;
2. пример;
3. выполнить задание.

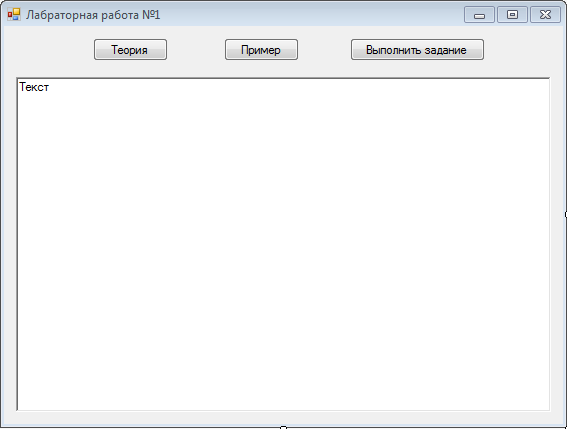


Рисунок 1

Кнопки «Теория» и «Пример» изменяют содержание основного окна на содержимое соответствующих им блоков. Кнопка «Выполнить задание» вызывает окно с текстом задания. В этом окне пользователь видит текст задания, текст, который необходимо расшифровать и кнопка сохранения в файл зашифрованного текста. На этой форме также есть кнопка «Отправить ответ» при нажатии на которую появляется окно, куда пользователь вставляет свой ответ и нажимает кнопку «Проверить ответ». В результате проверки выдаётся сообщение в соответствующем окне.

1. **Блоки «Теория», «Пример»**

Здесь приведено описание блоков теоретического материал и пример выполнения.

**Текст блока «Теория»**

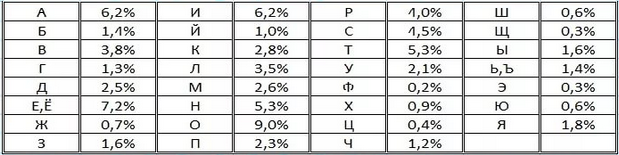
Одним из простейших шифров подстановки является моноалфавитный шифр. Рассмотрим исходное сообщение 𝑀, пусть оно составлено из символов алфавита 𝒜. Тогда моноалфавитным шифром называется отображение 𝒜 → 𝒜. Ключом для этого шифра является отображение 𝒜 → 𝒜.

Особенностью моноалфавитного шифра является сохранение частотных характеристик символов исходного текста в шифротексте. Этим можно воспользоваться для проведения криптоатаки. Предположим, что исходный текст является текстом на естественном языке. В естественных языках частоты встречаемости символов очень неравномерны. Поскольку моноалфавитный шифр не изменяет частот встреч символов, то сопоставляя частотную таблицу для эталонного текста и шифротекста у нас есть возможность сделать предположения о ключе шифра.

Необходимо отметить, что если объем эталонного текста для нас может быть не ограничен, то объем шифротекста всегда ограничен. Поэтому при построении частотной таблицы у нас неизбежно возникают погрешности в вычислении оценок частот встреч букв. При больших частотах встречи букв это будет менее значимо, поскольку статистики будет хватать для верного упорядочивания букв шифротекста, на редковстречаемых символах – ошибка может значительно искажать картину. Поэтому расшифровав самые часто встречаемые буквы с помощью частотного анализа необходимо использовать дополнительную информацию для криптоанализа остального текста.

**Текст блока «Пример»**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Исходный алфавит | Б | В | Е | Й | Н | О | С | \_ |
| Шифрованный | Е | Н | Б | С | \_ | Й | О | В |

Таблица средних частот букв в русском алфавите: 

Самым часто встречаемым символом является «пробел».

Зашифрованный текст:

йойеб\_\_йвнйб\_\_йс

Наш алфавит состоит из 8 символов.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| В | Н | О | Е | Й | С | Б | \_ |
| 1 | 1 | 1 | 1 | 5 | 1 | 2 | 4 |

Чаще всего встречается буква «Й», но «Й» – не пробел, так как пробел не может стоять в начале текста. Самый часто встречаемый символ «О». Следовательно, «Й» переходит в «О».

Второй по встречаемости символ пробел. Этот символ тоже не может быть пробелом. Так как не может быть два подряд стоящих пробела. Две подряд стоящие буквы, это чаще всего «Н». Пробел переходит в «Н».

Третья по встречаемости буква «Б». По частоте это должна быть буква «Е». «Б» переходит в «Е».

Подставим:

о\*о\*енно\*\*оенно\*

о\*о\*енно – похоже на слово особенно. «О» переходит в «С», «Е» переходит в «Б», «Б» переходит в «Е».

Особенно\*\*оенно\*.

Остались буквы «В», «Й» и пробел

\*о\*нно\* - похоже на военный. «Н» переходит в «В», «О» переходит в «Й», «В» переходит в пробел.

Получили:

особенно военной

Расшифрованный текст: особенно военной

**Интерфейс блоков «Теория» и «Пример»:**

Данные блоки имеют одинаковый вид интерфейса –– окно, содержащее текст блока (с картинками). Текстовое окно должно иметь фиксированный размер и бегунок для вмещения содержания, превышающего по размеру само окно. Ввиду того, что содержимое основного окна программы меняется при нажатиях верхних кнопок, то дополнительных элементов для данных трех блоков не требуется.

1. **Блок «Выполнение задания»**

Блок содержит зашифрованный текст, кнопку «Сохранить как …», при нажатии на которую вызывается диалог выбора папки (см. рисунок 2), в которую пользователь желает сохранить задание и кнопку «Отправить ответ» (см. рисунок 3).

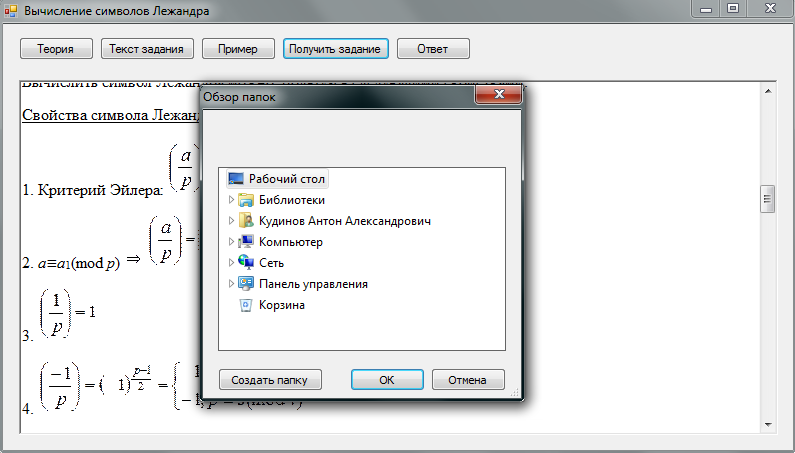


Рисунок 2

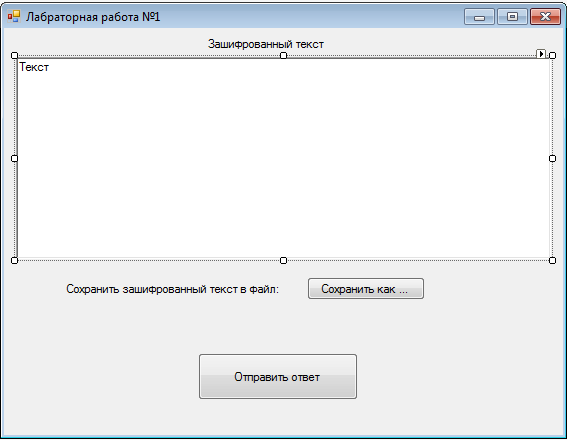


Рисунок 3

Выдаваемое задание должно соответствовать году обучения, семестру и номеру бригады, выбранных в главном меню.

Каждый экземпляр задания должен быть однозначно сгенерирован генератором псевдослучайных чисел на основании года, семестра и номера бригады, чтобы было возможно однозначно восстановить необходимую часть текста для проверки.

Алгоритм генерации содержания каждого экземпляра задания следующий:

1. выбрать случайным образом отрывок текста на русском языке (допустима только кириллица и знак «пробел») из ресурсов проекта, а именно – из файла Sholohov.txt. Отрывок должен быть взят таким образом, чтобы первый символ отрывка был началом слова, а длина отрывка составила 1500 символов + окончание последнего слова;
2. Зашифровать текст с помощью моноалфовитного шифра (заменой символа из алфавита, другим произвольным символом этого же алфавита. Алфавит состоит из 32 букв русского алфавита и пробела).

Символы отрывка и расшифрованного текста должны быть в верхнем регистре.

Заданием, которое выдаётся пользователю, является зашифрованный с помощью шифра Цезаря текст.

## Блок «Проверка ответа»

Блок проверки должен содержать поля для ввода текста, а также кнопку «Проверить» (см. рисунок 4), при нажатии на которую вызывается процедура проверки, после чего пользователь уведомляется о правильности/неправильности ответа.

Ответом задания является расшифрованный текст.

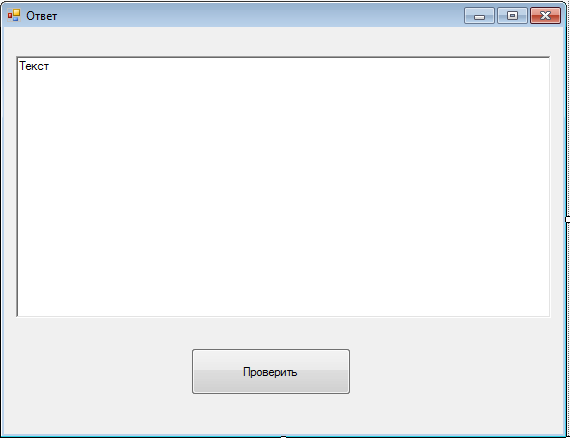


Рисунок 4

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

**Возможные варианты ответов:**

Если количество символов в тексте, которой отправил пользователь больше чем в расшифрованном тексте, то выводим сообщение «Количество введённых символов больше, чем необходимо».

Если количество символов в тексте, которой отправил пользователь меньше чем в расшифрованном тексте, то выводим сообщение «Количество введённых символов меньше, чем необходимо».

Если текст пользователя и исходный текст отличаются более чем на половину, то выводить сообщение «Неверно»

Проверяем первое слово до пробела, если оно совпадает, а остальное нет, то пишет «Все слова кроме первого не совпадают».

Проверяем второе слово до пробела, если первые два слова совпадают, а остальное нет, то пишет «Все слова после второго не совпадают».

Аналогично проверяем последнее и предпоследнее слово и выводим соответственно сообщения: «Все слова кроме последнего не совпадают», «Все слова кроме последних двух не совпадают».

Проверяем первую половину символов, если они все правильные, а во второй половине есть более двух несовпадений выводим сообщение «Вторая половина текста расшифрована неверно».

Проверяем вторую половину символов, если они все правильные, а в первой половине есть более двух несовпадений выводим сообщение «Первая половина текста расшифрована неверно».

Если текст пользователя отличается от исходного на 1 или 2 символа, то выводить сообщение «Верно».

Если есть недопустимые символы, то выводим сообщение «Введены недопустимые символы».

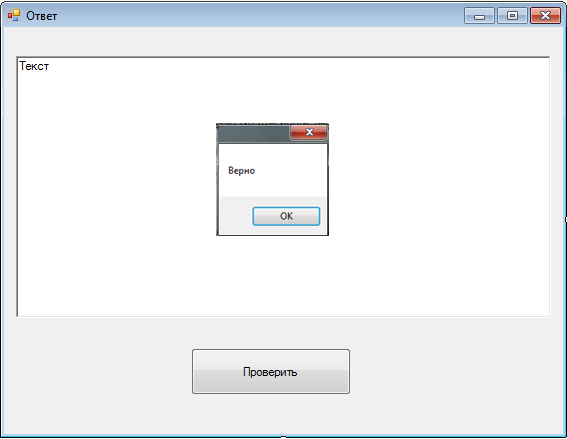


Рисунок 5

1. **Тестирование программы.**

Необходимо протестировать программу на правильность выполнения:

1). Посылаем текст с недопустимыми символами;

2). Посылаем правильно расшифрованный текст;

3). Посылаем текст с несколькими неправильными символами в тексте;

4). Посылаем правильный текст, но с меньшим или с большим количеством символов.

5). Необходимо протестировать, что программа правильно зашифровывает и расшифровывает текст. Для этого необходимо вручную зашифровать и сравнить с тем правильно ли зашифровала программа, а затем расшифровать и проверить правильно ли расшифровала программа текст.