Лабораторная работа № 5

Тема: Криптографические преобразования на основе шифров перестановки.

Цель работы: Освоить построение шифров перестановки, позволяющих осуществлять криптографические преобразования данных

5.1. Краткие теоретические сведения

Шифр, преобразования которого не замещают символы шифруемого текста на другие, а изменяют только порядок их следования, называется *шифром перестановки*.

Тексты, используемые в лабораторной работе, основаны на алфавите, приведенном в табл. 5.1:

Таблица 5.1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Буква | \_ | А | Б | В | Г | Д | Е | Ж | З | И | К | Л | М | Н | О | П |
| Код | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 |
| Буква | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| Код | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |

Все шифры перестановки делятся на два *подкласса*:

– шифры одинарной (простой) перестановки. При шифровании символы перемещаются с исходных позиций в новые один раз;

– шифры множественной (сложной) перестановки. При шифровании символы перемещаются с исходных позиций в новые несколько раз.

К простейшим методам перестановки, которые будут рассматриваться в данной лабораторной работе, относятся:

– маршрутная табличная перестановка;

– вертикальная перестановка с ключом;

– посимвольная векторная перестановка;

– побитовая векторная перестановка.

При использовании метода *маршрутной табличной перестановки* исходный открытый текст вписывают в таблицу по определенному маршруту, а выписывают (получают шифротекст) – по другому. Для данного шифра маршруты вписывания и выписывания, а также размеры таблицы являются ключом. Как правило, открытый текст вписывают построчно слева направо, а шифротекст выписывают по столбцам, начиная с первого.

Алгоритм зашифрования заключается в следующем:

1. Задается количество столбцов *n* – ключ шифрования.

2. Шифруемый открытый текст вписывают построчно слева направо. Если последняя строка оказывается неполной, то она дополняется дополнительными символами (в лабораторных работах – символом «\_» – пробел).

3. Закрытый текст выписывают по столбцам, начиная с первого.

Пример 5.1. Открытый текст «ЗАЩИТА\_ИНФОРМАЦИИ». Пусть число столбцов таблицы шифрования *n* = 5. Тогда таблица шифрования примет вид (табл.5.2):

Таблица 5.2

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| З | А | Щ | И | Т |
| А | \_ | И | Н | Ф |
| О | Р | М | А | Ц |
| И | И | \_ | \_ | \_ |

Шифротекст в этом случае выглядит «ЗАОИА\_РИЩИМ\_ИНА\_ТФЦ\_».

Расшифрование выполняется по следующему алгоритму:

1. Подсчитывают число символов в шифротексте и делят на число столбцов таблицы *n* – ключ шифрования.

2. По столбцам, начиная с первого, вписывают символы шифротекста в количестве, определенном на первом шаге.

3. Выписывают расшифрованный открытый текст по строкам, начиная с первой.

Пример 5.2. Закрытый текст «ЗАОИА\_РИЩИМ\_ИНА\_ТФЦ\_». Общее число символов в нем, равное 20, делим на *n* = 5 (ключ шифрования) и получаем группы по 4 символа, которые вписываем в таблицу (табл. 5.3):

Таблица 5.3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| З | А | Щ | И | Т |
| А | \_ | И | Н | Ф |
| О | Р | М | А | Ц |
| И | И | \_ | \_ | \_ |

Расшифрованный открытый текст будет «ЗАЩИТА\_ИНФОРМАЦИИ\_ \_ \_».

Шифр *вертикальной перестановки с ключом* является разновидностью предыдущего шифра. К особенностям шифра можно отнести следующие:

– ключом является слово или фраза, не содержащее одинаковых символов;

– количество столбцов в таблице фиксируется и определяется длиной ключа.

Зашифрование осуществляется в соответствии со следующим алгоритмом:

1. Выбирается ключевое слово (фраза) с неповторяющимися символами.

2. Шифруемый открытый текст вписывают последовательными строками под символами ключевого слова. Если последняя строка оказывается неполной, то она дополняется специальными символами (в лабораторной работе – символом «\_» - пробел).

3. Зашифрованный текст выписывают по столбцам в той последовательности, в которой располагаются в алфавите буквы ключевого слова (по коду буквы) (или в порядке следования цифр в натуральном ряду, если ключ цифровой).

Пример 5.3. Открытый текст «ЗАЩИТА\_ИНФОРМАЦИИ». Пусть ключевое слово «КРЫША». Получим таблицу шифрования следующего вида (табл.5.4):

Таблица 5.4

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ключ | К | Р | Ы | Ш | А |
| 10 | 16 | 27 | 24 | 01 |
| Текст | З | А | Щ | И | Т |
| А | \_ | И | Н | Ф |
| О | Р | М | А | Ц |
| И | И | \_ | \_ | \_ |

Тогда шифротекст будет «ТФЦ\_ЗАОИА\_РИИНА\_ЩИМ\_».

Расшифрование выполняется в следующем порядке:

1. Подсчитываем число символов в зашифрованном тексте и делим на число символов ключа.

2. Вписываем ключевое слово и под его символами в соответствующей последовательности вписываем символы зашифрованного текста в определенном в п.1 количестве.

3. По строкам таблицы выписываем исходный расшифрованный текст.

Пример 5.4. Закрытый текст «ТФЦ\_ЗАОИА\_РИИНА\_ЩИМ\_». Ключевое слово «КРЫША». Число символов шифротекста равно 20. Делим на число символов ключа, равное 5, и получаем, что шифротекст необходимо разделить на группы по 4 символа. Вписываем эти группы под символами ключа в соответствующем порядке (табл. 5.5)

Таблица 5.5

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ключ | К | Р | Ы | Ш | А |
| 10 | 16 | 27 | 24 | 01 |
| Текст | З | А | Щ | И | Т |
| А | \_ | И | Н | Ф |
| О | Р | М | А | Ц |
| И | И | \_ | \_ | \_ |

и выписываем по строкам исходный текст «ЗАЩИТА\_ИНФОРМАЦИИ\_ \_ \_».

При *посимвольной векторной перестановке* текст делится на блоки *по* *d* символов и в каждом блоке производится одна и та же *перестановка*. Если длина текста не кратна длине блока, последний блок следует дополнить случайным образом взятыми символами (в лабораторной работе – «\_» – пробелами). Правило, по которому производится *перестановка*, является ключом и может быть задано некоторой перестановкой первых *d* натуральных чисел (*вектором перестановки*). Например, для *d* = 5 в качестве ключа перестановки можно взять вектор 43521. Это означает, что в каждом блоке из 5 символов при зашифровании четвертый символ становится на первое место, третий – на второе, пятый – на третье и т.д.

Пример 5.5. Открытый текст «ТЕКСТ\_ДЛЯ\_ШИФРОВАНИЯ». Пусть длина блока символов *d* = 5, и вектор перестановки имеет вид 43521. Количество символов в исходном тексте равно 20, следовательно, текст необходимо разбить на 4 блока: ТЕКСТ \_ДЛЯ\_ ШИФРО ВАНИЯ . Результатом зашифрования будет закрытый текст СКТЕТЯЛ\_Д\_РФОИШИНЯАВ.

При расшифровании в соответствии с заданным ключом вектором перестановки выполняется обратная перестановка символов в блоке, длина которого равна длине вектора. Если задан вектор перестановки 43521, то это означат, что в каждом блоке из пяти символов, на которые разбивается шифротекст, первый символ становится на четвертое место, второй – на третье, третий – на пятое и т.д.

Пример 5.6. Закрытый текст «СКТЕТЯЛ\_Д\_РФОИШИНЯАВ». Если вектор перестановки равен 43521, то разбиваем шифротекст на блоки по пять символов: СКТЕТ ЯЛ\_Д\_ РФОИШ ИНЯАВ и переставляем местами символы в каждом блоке. Тогда расшифрованный текст будет равен «ТЕКСТ \_ДЛЯ\_ ШИФРО ВАНИЯ».

В случае *побитовой векторной перестановки* местами в соответствии с вектором перестановки меняются биты в двоичном эквиваленте кода символа используемого алфавита. При этом следует помнить, что нумерация битов в двоичном числе начинается справа налево, первый бит имеет номер 0. Для букв алфавита, используемого в лабораторной работе, двоичные эквиваленты кодов – пятиразрядные, т.е. вектор перестановки, например, может иметь вид 20431.

Пример 5.7. Открытый текст «ШИФР». Пусть вектор перестановки имеет вид 31042. Тогда при зашифровании получим:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Открытый текст | | | Закрытый текст | | |
| Буква | Код | Двоичный эквивалент | Двоичный эквивалент | Код | Буква |
| Ш | 24 | 11000 | 10010 | 18 | Т |
| И | 09 | 01001 | 10100 | 20 | Ф |
| Ф | 20 | 10100 | 00011 | 03 | В |
| Р | 16 | 10000 | 00010 | 02 | Б |

5.2. Задание на лабораторную работу.

Разработать программу, иллюстрирующую шифрование методами перестановки на примере криптографического алгоритма, заданного преподавателем.

5.3. Краткое описание работы программы

После запуска программы на исполнение открывается окно программы (рис. 5.1).

Меню действий содержит список функций программы: «Файл», «Зашифровать», «Расшифровать», «Справка», «Выход». Предварительно, сразу после запуска программы, рабочая область не содержит никакой информации (либо открытого, либо закрытого текста), поэтому доступными являются только функции «Файл», «Справка», «Выход». Функции «Зашифровать», «Расшифровать» остаются недоступными для выбора. При выборе некоторого действия из этого меню на экране под выбранным объектом появляется дополнительный список действий – выпадающее меню.

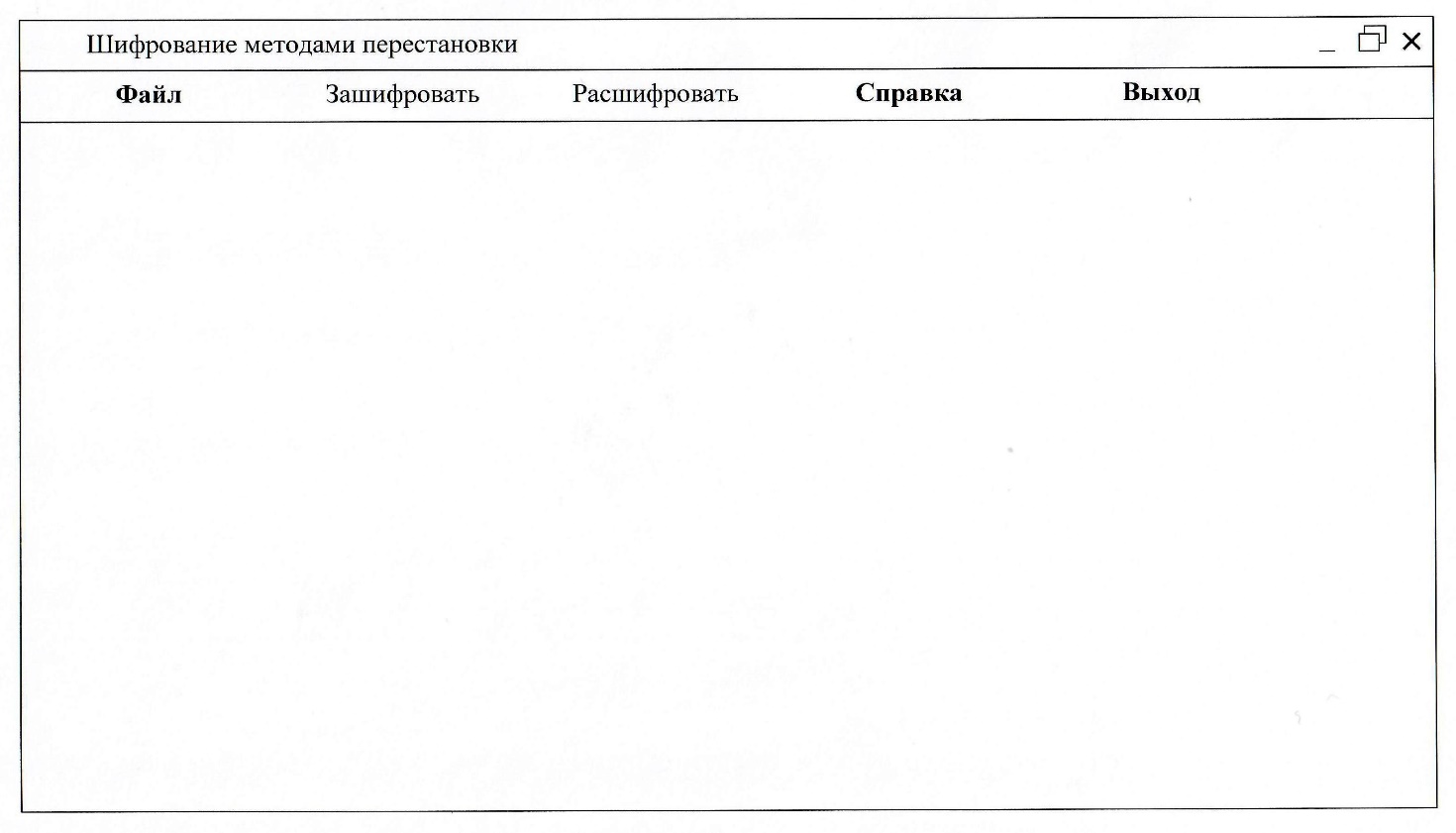


Рис. 5.1.

Пункт меню действий «Файл» (рис. 5.2) содержит подпункты (опции выпадающего меню): «Создать», «Открыть», «Сохранить», «Сохранить как», «Выход».

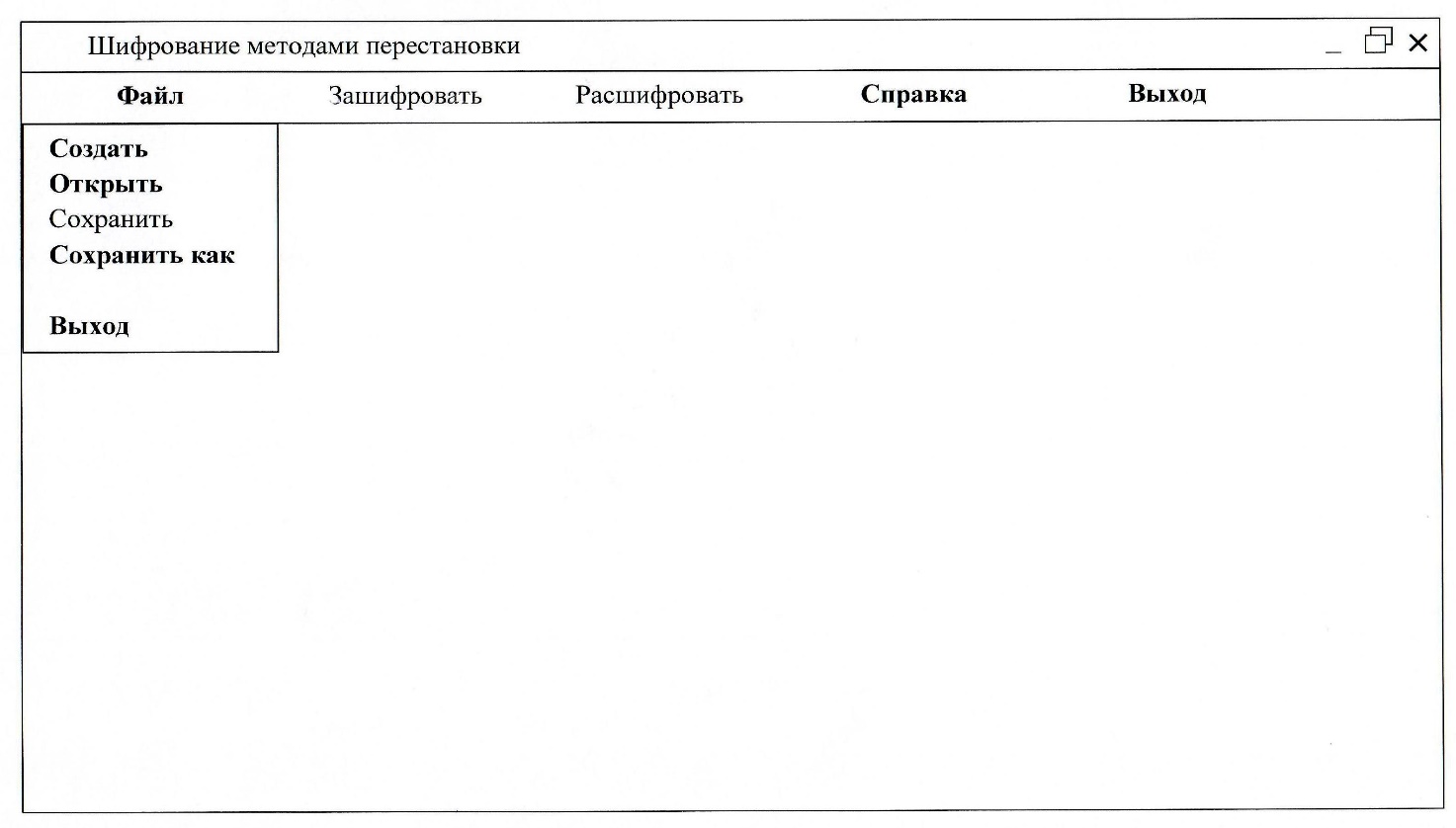


Рис. 5.2.

Создать – данный пункт выпадающего меню предоставляет пользователю право ввести в первую строку рабочей области либо открытый, либо закрытый текст, который впоследствии можно будет использовать при работе с программой, а также дает возможность использовать все недоступные до этого пункты меню действий. При этом длина строки текста не должна превышать 30 символов.

Открыть – при выборе этого пункта появляется диалоговое окно, предоставляющее возможность выбора файла для загрузки. При этом содержимое файла будет отображено в рабочей области окна программы.

Аналогично пункту «Создать» появляется возможность использовать все недоступные до этого пункты меню действий.

Сохранить – при выборе этого пункта содержимое последней строки из рабочей области программы сохраняется в ранее открытом файле (с сохранением имени файла).

Сохранить как – при выборе этого пункта появляется диалоговое окно, позволяющее сохранить на диск содержимое последней строки из рабочей области программы в новом файле.

Выход – выбор этого пункта позволяет выйти из программы.

Пункт меню действий «Справка» (рис. 5.3) содержит подпункты (опции выпадающего меню): «О программе», «Помощь».

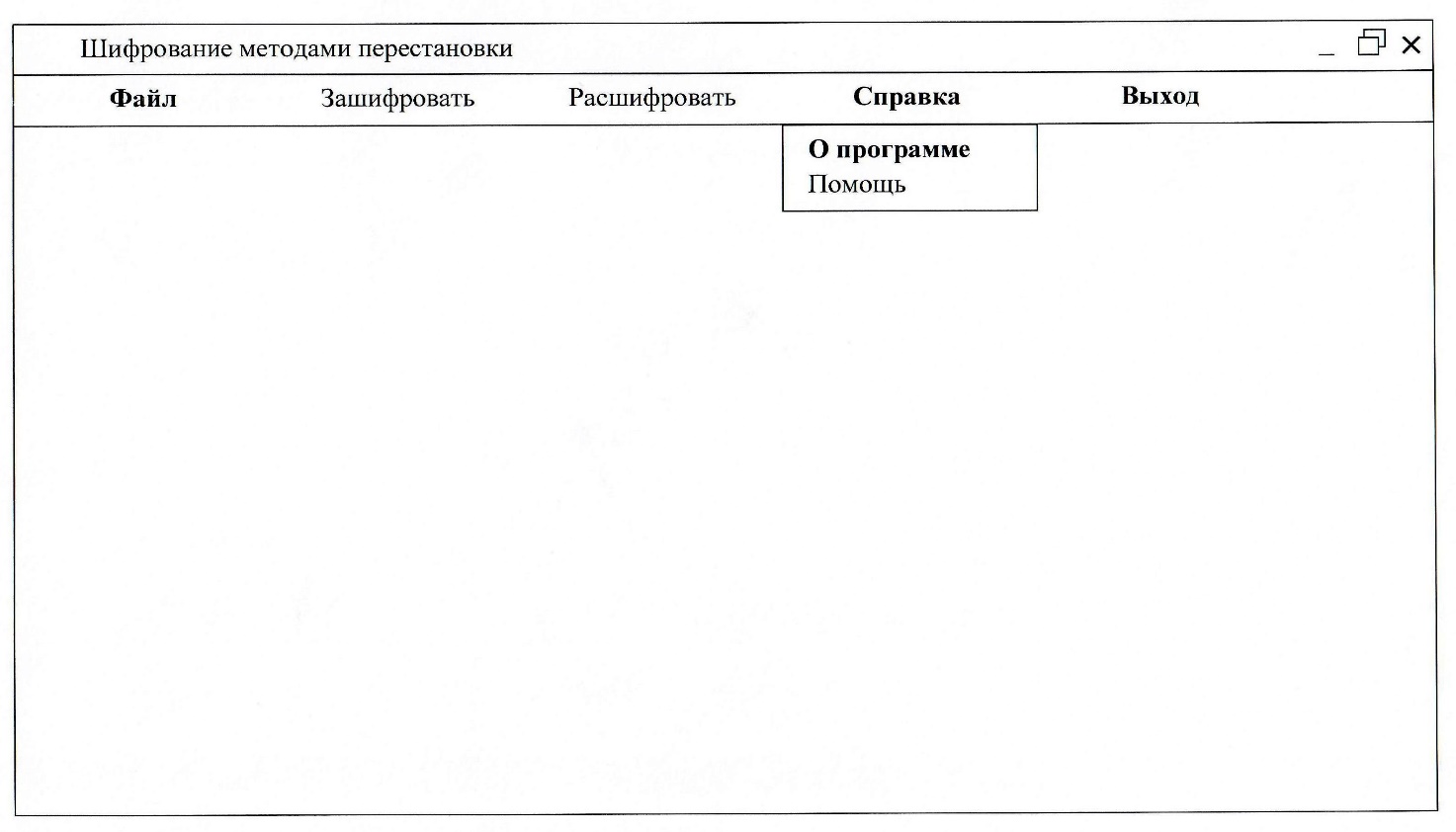


Рис. 5.3.

О программе – при выборе этого пункта появляется всплывающее окно, содержащее *информационное сообщение* о названии и назначении программы и об авторе разработки.

Помощь – выбор этого пункта приводит к появлению всплывающего окна с *информационным сообщением*, содержащим краткую информацию о реализованном методе шифрования. Этот пункт – недоступен до момента заполнения рабочей области окна программы.

Выбор пункта меню действий «Выход» приводит к завершению работы программы.

Пункты меню действий «Зашифровать» или «Расшифровать», доступные при наличии строк текста в рабочей области окна программы, содержат список методов шифрования, рассматриваемых в лабораторной работе (рис.5.4 – 5.5):

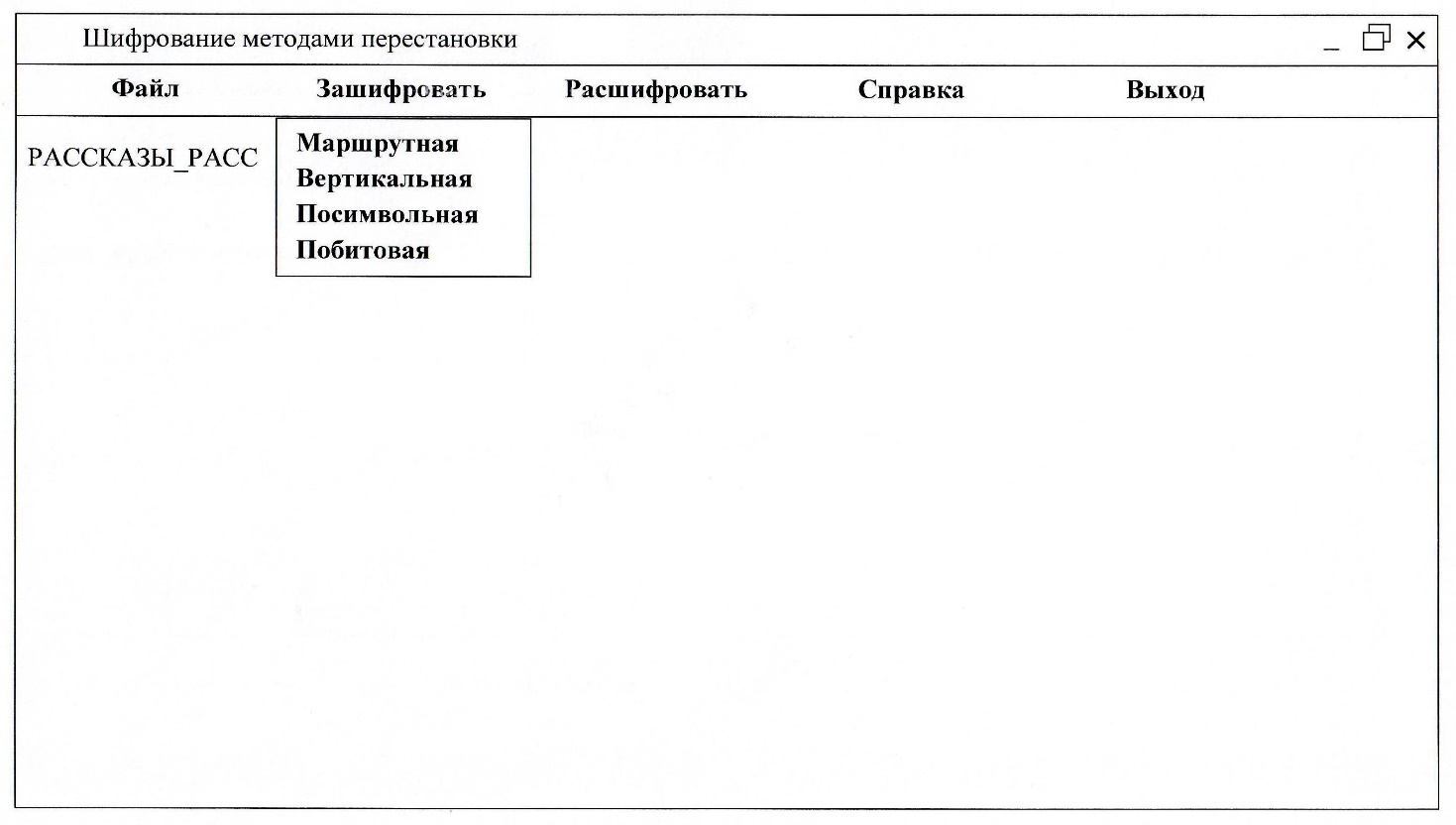


Рис. 5.4.

1. Маршрутная табличная перестановка.

2. Вертикальная перестановка с ключом.

3. Посимвольная векторная перестановка.

4. Побитовая векторная перестановка.

В случае выбора нереализованного согласно заданию на лабораторную работу метода шифрования появляется всплывающее окно, содержащее предупредительное сообщение «Указанный метод не реализован» (рис. 5.6).

Если выбран метод шифрования, реализованный в соответствии с заданием на лабораторную работу, то появляется всплывающее окно, позволяющее задать ключ шифрования и либо подтвердить его значение нажатием клавиши «Ok», либо отказаться от него нажатием клавиши «Esc» (рис. 5.7).

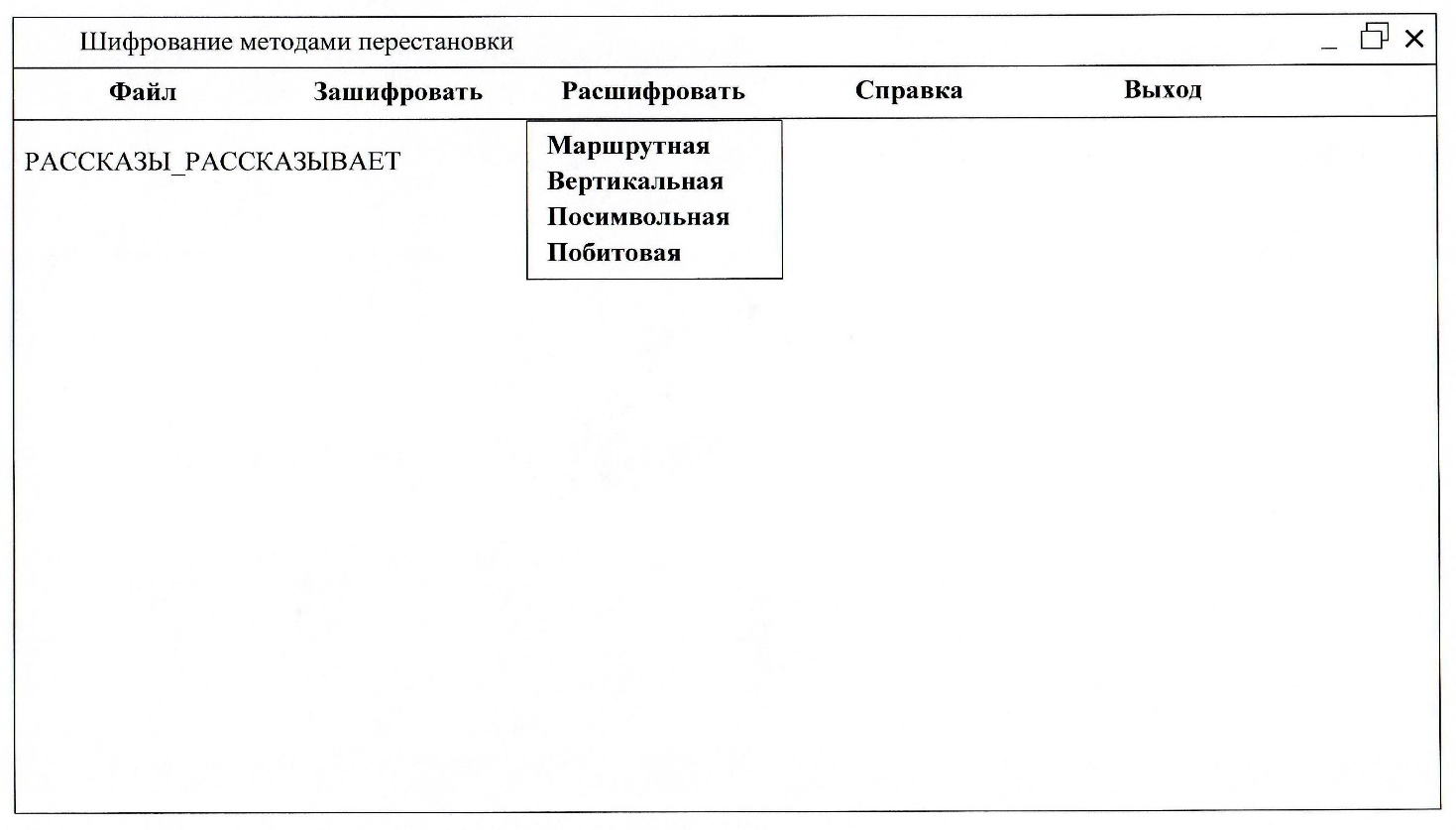


Рис. 5.5.

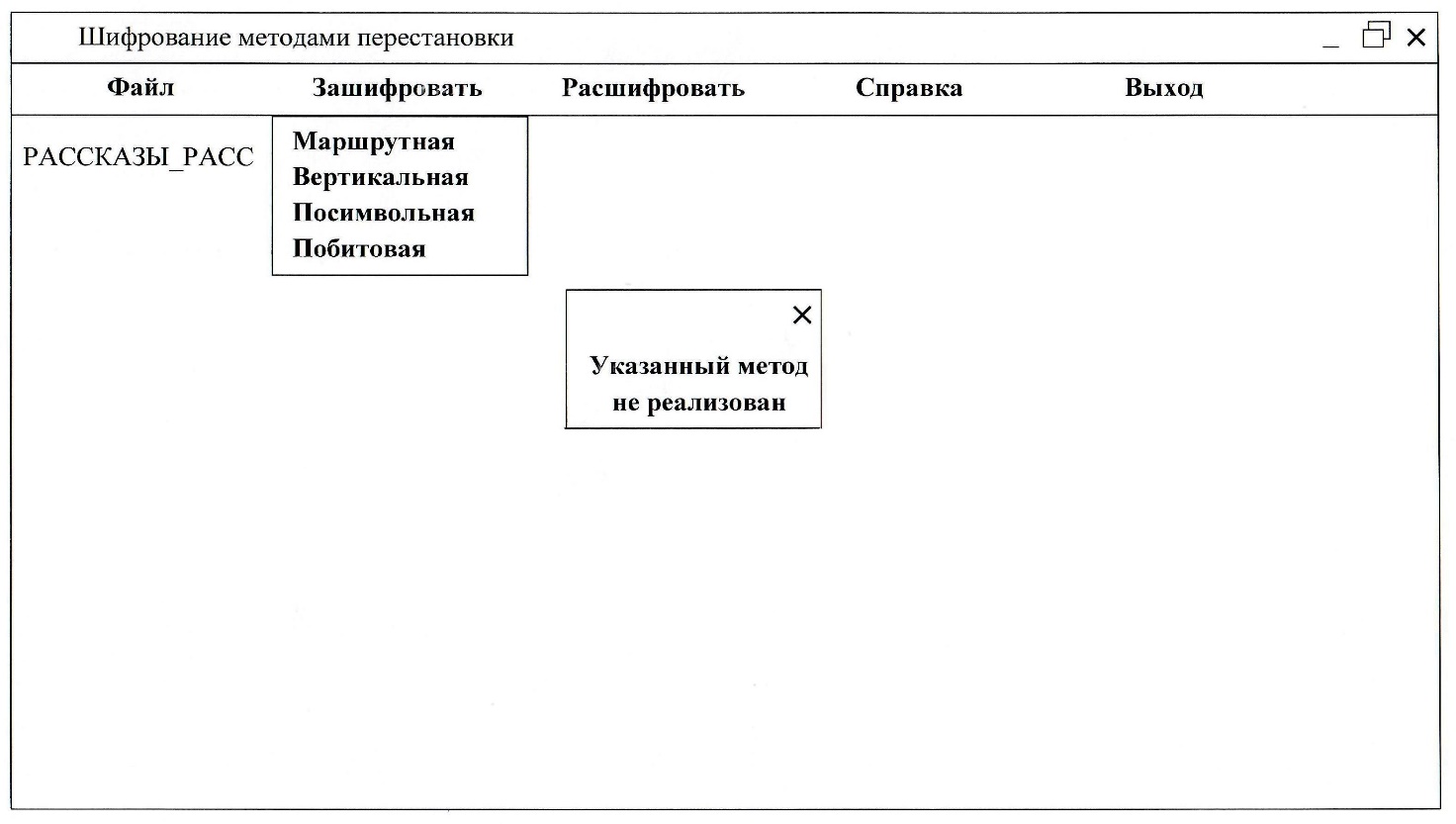


Рис. 5.6.

Если значение ключа подтверждено, но оно содержит ошибку, то появляется всплывающее окно, содержащее критическое сообщение «Значение ключа неправильное» (рис. 5.8). Когда это окно закрывается нажатием в нем клавиши «Ok», очищается окно ввода значения ключа, и ожидается задание нового значения ключа шифрования.

Если подтвержденное значение ключа – правильное, то окно ввода ключа закрывается, реализованный метод шифрования выполняется, и результат (преобразованный текст) отображается в следующей по порядку строке рабочего поля окна программы.

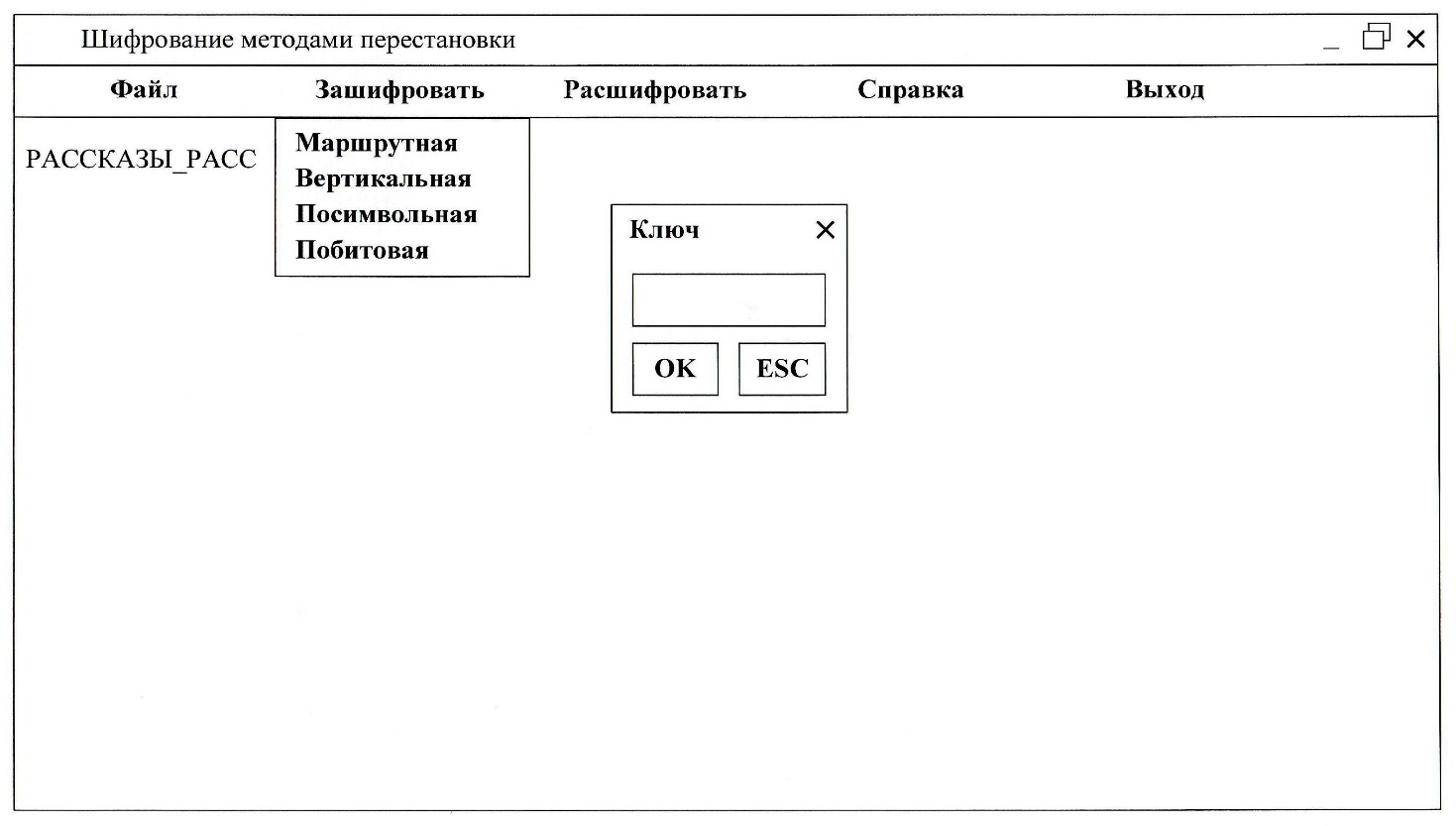


Рис. 5.7.

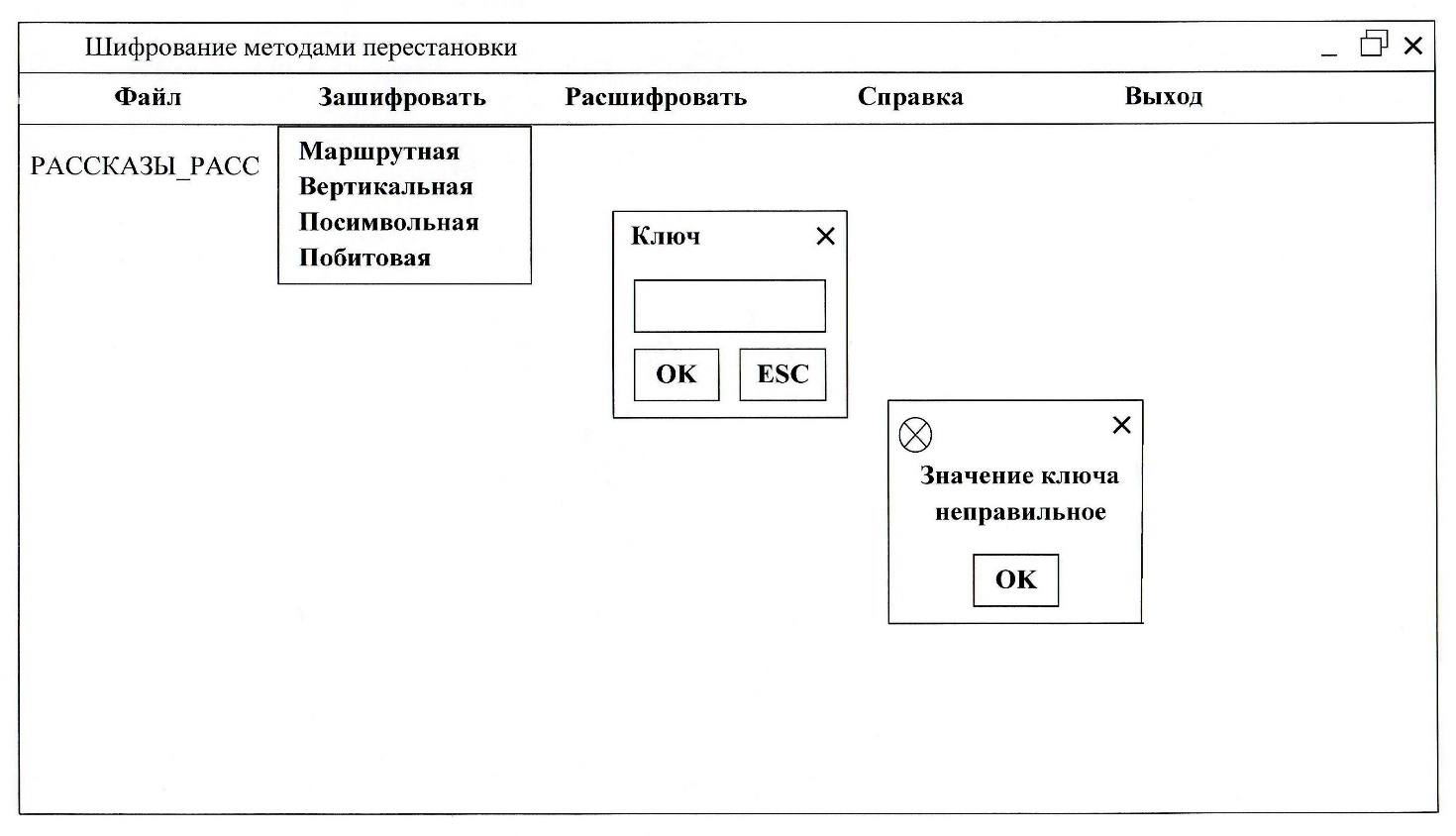


Рис. 5.8.

Если поочередно выполняются действия зашифрование и расшифрование, то при правильном расшифровании полученный текст совпадает с исходным.

5.4. Контрольные вопросы

1. Будет ли увеличиваться длина текста при шифровании методами перестановки?

2. Каким будет шифротекст при зашифровании открытого текста «КРИПТОГРАФИЧЕСКИЕ\_АЛГОРИТМЫ» методом маршрутной перестановки с ключом 5?

3. Каким будет шифротекст при зашифровании открытого текста «КРИПТОГРАФИЧЕСКИЕ\_АЛГОРИТМЫ» методом вертикальной перестановки с ключом «МИЛЯ»?

4. Каким будет шифротекст при зашифровании открытого текста «КРИПТОГРАФИЧЕСКИЕ\_АЛГОРИТМЫ» методом посимвольной перестановки с вектором перестановки «3 4 1 5 6 2»?

5. Каким будет шифротекст при зашифровании открытого текста «КРИПТОГРАФИя» методом побитовой перестановки с вектором перестановки «3 4 1 5 2»?

Лабораторная работа № 6

Тема: Криптографические преобразования на основе методов гаммирования

Цель работы: Освоить шифрование методами гаммирования, позволяющими осуществлять криптографические преобразования данных

6.1. Краткие теоретические сведения

*Гаммирование* – метод криптографического преобразования, заключающийся в том, что символы шифруемого текста складываются с символами некоторой случайной последовательности, называемой гаммой шифра или ключевой гаммой. Стойкость шифрования определяется длиной (периодом) неповторяющейся части гаммы шифра, а также сложностью предугадывания следующих элементов гаммы по предыдущим.

Для создания открытого текста используется алфавит, приведенный в табл. 6.1:

Таблица 6.1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Буква | \_ | А | Б | В | Г | Д | Е | Ж | З | И | К | Л | М | Н | О | П |
| Код | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 |
| Буква | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| Код | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |

Наложение гаммы можно осуществить по формуле

*y* = *x* *XOR* *g* , (6.1)

где *y* , *x* , *g* – коды соответственно зашифрованного символа, исходного символа и гаммы,

*XOR* – побитовая операция «исключающее ИЛИ» (сложение по модулю 2).

Расшифрование текста проводится по аналогичной формуле:

*x* = *y* *XOR* *g*. (6.2)

Гаммирование по модулю 2 в общем случае производится следующим образом:

– коды символов исходного текста и ключа (гамма) представляются в десятичном или двоичном коде и располагаются один под другим, при этом ключ (гамма) записывается столько раз, сколько потребуется;

– каждая пара десятичных чисел складывается, а каждая пара двоичных знаков складывается по модулю два;

– полученная последовательность десятичных или двоичных знаков кодируется символами алфавита в соответствии с выбранным кодом.

Полученный зашифрованный текст является достаточно трудным для рас­крытия в том случае, если гамма шифра не содержит повторяющихся последовательностей. По сути дела гамма шифра должна изменяться случайным образом для каждого шифруемого слова.

Наиболее распространенными гаммами шифра являются:

– псевдослучайная последовательность, вырабатываемая по заданному алгоритму для зашифрования открытых данных и расшифрования зашифрованных данных;

– ключевое слово.

Наиболее доступными являются *псевдослучайные последовательности*, построенные на основе линейного конгруэнтного датчика псевдослучайных чисел (ПСЧ). Он вырабатывает последовательности псевдослучайных чисел T(*i*), описываемые соотношением

*T*(*i*+1) = (*A***·***T*(*i*)+*C*) *mod m*, (6.3)

где *А* и *С* – константы, *Т*(0) – исходная величина, выбранная в качестве порождающего числа. Очевидно, что эти три величины и образуют ключ.

Такой датчик ПСЧ генерирует псевдослучайные числа с определенным периодом повторения, зависящим от выбранных значений А и С. Значение *m* обычно устанавливается равным 2*w* , где *w* – длина машинного слова в битах. Исторически *w* = 16.

Пример 6.1. Открытый текст «ГАММА». Выполнить зашифрование, если значение ключа *А* = *С* = *Т*(0) = 3. Получаем значение гаммы в соответствии с (6.3):

3 12 7 24 11 или в двоичном коде 00011 01100 00111 11000 01011.

При зашифровании будем иметь (табл. 6.2):

Таблица 6.2

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Буква ОТ | Г | А | М | М | А |
| Код | 04 | 01 | 12 | 12 | 01 |
| Двоичный эквивалент | 00100 | 00001 | 01100 | 01100 | 00001 |
| Двоичная гамма | 00011 | 01100 | 00111 | 11000 | 01011 |
| Результат ⊕ | 00111 | 01101 | 01011 | 10100 | 01010 |
| Код | 07 | 13 | 11 | 20 | 10 |
| Буква шифра | Ж | Н | Л | Ф | К |

Т.е. получаем закрытый текст «ЖНЛФК».

Пример 6.2. Закрытый текст «ЖНЛФК». Выполнить расшифрование, если значение ключа *А* = *С* = *Т*(0) = 3. Получаем значение гаммы в соответствии с (6.3):

3 12 7 24 11 или в двоичном коде 00011 01100 00111 11000 01011.

При расшифровании будем иметь (табл. 6.3):

Таблица 6.3

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Буква шифра | Ж | Н | Л | Ф | К |
| Код | 07 | 13 | 11 | 20 | 10 |
| Двоичный эквивалент | 00111 | 01101 | 01011 | 10100 | 01010 |
| Двоичная гамма | 00011 | 01100 | 00111 | 11000 | 01011 |
| Результат ⊕ | 00100 | 00001 | 01100 | 01100 | 00001 |
| Код | 04 | 01 | 12 | 12 | 01 |
| Буква ОТ | Г | А | М | М | А |

Т.е. получаем отрытый текст «ГАММА».

*Гаммирование на основе ключевого слова* поясним следующими примерами.

Пример 6.3. Открытый текст «КРУЖКА». Выполнить зашифрование, если ключевое слово «ПЛОТ». Составим таблицу зашифрования (табл. 6.4):

Таблица 6.4

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Буква ОТ | К | Р | У | Ж | К | А |
| Буква ключа | П | Л | О | Т | П | Л |
| Код буквы ОТ | 10 | 16 | 19 | 07 | 10 | 01 |
| Код буквы ключа | 15 | 11 | 14 | 18 | 15 | 11 |
| Двоичный код  буквы ОТ | 01010 | 10000 | 10011 | 00111 | 01010 | 00001 |
| Двоичный код  буквы ключа | 01111 | 01011 | 01110 | 10010 | 01111 | 01011 |
| Результат ⊕ | 00101 | 11011 | 11101 | 10101 | 00101 | 01010 |
| Код буквы шифра | 05 | 27 | 29 | 21 | 05 | 10 |
| Буква шифра | Д | Ы | Э | Х | Д | К |

Т.е. закрытый текст «ДЫЭХДК».

Пример 6.4. Закрытый текст «ДЫЭХДК». Выполнить расшифрование, если ключевое слово «ПЛОТ». Составим таблицу расшифрования (табл. 6.5):

Таблица 6.5

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Буква ЗТ | Д | Ы | Э | Х | Д | К |
| Буква ключа | П | Л | О | Т | П | Л |
| Код буквы ЗТ | 05 | 27 | 29 | 21 | 05 | 10 |
| Код буквы ключа | 15 | 11 | 14 | 18 | 15 | 11 |
| Двоичный код  буквы ЗТ | 00101 | 11011 | 11101 | 10101 | 00101 | 01010 |
| Двоичный код  буквы ключа | 01111 | 01011 | 01110 | 10010 | 01111 | 01011 |
| Результат ⊕ | 01010 | 10000 | 10011 | 00111 | 01010 | 00001 |
| Код буквы ОТ | 10 | 16 | 19 | 07 | 10 | 01 |
| Буква ОТ | К | Р | У | Ж | К | А |

Т.е. открытый текст «КРУЖКА».

Одним из частных случаев шифра гаммирования является шифр Вижинера, который представляет собой шифр гаммирования с краткопериодической гаммой, т.е. гаммой, которая является повторением некоторого короткого слова – периода.

Отличие от ранее рассмотренных методов гаммирования состоит в том, что зашифрование выполняется путем сложения кодов символов исходного текста и ключа по модулю, равному числу букв в алфавите, т.е. уравнение зашифрования имеет вид:

*yi = (xi + ki)mod n*, (6.4)

где *yi* – код *i* –го символа закрытого текста;

*xi* – код *i* –го символа открытого текста;

*ki* – код *i* –го символа ключа;

*n* = 32 – число букв в алфавите, используемого в лабораторной работе.

Зашифрование осуществляется в соответствии со следующей последовательностью:

– коды символов исходного текста и ключа располагаются один под другим, при этом ключ записывается столько раз, сколько потребуется;

– каждая пара кодов складывается по модулю, равному числу букв в алфавите;

– полученный результат представляет собой код символа закрытого текста;

– выписываются символы закрытого текста в соответствии с полученным кодом.

Пример 6.5. Открытый текст «КРУЖКА». Выполнить зашифрование, если ключевое слово «ПЛОТ». Составим таблицу зашифрования (табл. 6.6):

Таблица 6.6

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Буква ОТ | К | Р | У | Ж | К | А |
| Буква ключа | П | Л | О | Т | П | Л |
| Код буквы ОТ | 10 | 16 | 19 | 07 | 10 | 01 |
| Код буквы ключа | 15 | 11 | 14 | 18 | 15 | 11 |
| Код буквы шифра | 25 | 27 | 01 | 25 | 25 | 12 |
| Буква шифра | Щ | Ы | А | Щ | Щ | М |

Т.е. закрытый текст «ЩЫАЩЩМ».

Уравнение расшифрования имеет вид:

*xi = (n* + *yi* – *ki)mod n*. (6.5)

Расшифрование осуществляется в соответствии со следующей последовательностью:

– коды символов закрытого текста и ключа располагаются один под другим, при этом ключ записывается столько раз, сколько потребуется;

– каждая пара кодов складывается по модулю, равному числу букв в алфавите;

– полученный результат представляет собой код символа открытого текста;

– выписываются символы открытого текста в соответствии с полученным кодом.

Пример 6.6. Закрытый текст «ЩЫАЩЩМ». Выполнить расшифрование, если ключевое слово «ПЛОТ». Составим таблицу расшифрования (табл. 6.7):

Таблица 6.7

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Буква ЗТ | Щ | Ы | А | Щ | Щ | М |
| Буква ключа | П | Л | О | Т | П | Л |
| Код буквы ЗТ | 25 | 27 | 01 | 25 | 25 | 12 |
| Код буквы ключа | 15 | 11 | 14 | 18 | 15 | 11 |
| Код буквы ОТ | 10 | 16 | 19 | 07 | 10 | 01 |
| Буква ОТ | К | Р | У | Ж | К | А |

Т.е. открытый текст «КРУЖКА».

Похожим на шифр Вижинера является *шифр Бофора*, уравнения зашифрования и расшифрования в котором соответственно имеют вид:

*yi = ( n* + *xi* – *ki )mod n*, (6.6)

*xi = ( yi* + *ki )mod n*. (6.7)

Проиллюстрируем работу шифра Бофора следующими примерами.

Пример 6.7. Открытый текст «КРУЖКА». Выполнить зашифрование, если ключевое слово «ПЛОТ». Составим таблицу зашифрования (табл. 6.8):

Таблица 6.8

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Буква ОТ | К | Р | У | Ж | К | А |
| Буква ключа | П | Л | О | Т | П | Л |
| Код буквы ОТ | 10 | 16 | 19 | 07 | 10 | 01 |
| Код буквы ключа | 15 | 11 | 14 | 18 | 15 | 11 |
| Код буквы шифра | 27 | 05 | 05 | 21 | 27 | 22 |
| Буква шифра | Ы | Д | Д | Х | Ы | Ц |

Т.е. закрытый текст «ЫДДХЫЦ».

Пример 6.8. Закрытый текст «ЫДДХЫЦ». Выполнить расшифрование, если ключевое слово «ПЛОТ». Составим таблицу расшифрования (табл. 6.9):

Таблица 6.9

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Буква ЗТ | Ы | Д | Д | Х | Ы | Ц |
| Буква ключа | П | Л | О | Т | П | Л |
| Код буквы ЗТ | 27 | 05 | 05 | 21 | 27 | 22 |
| Код буквы ключа | 15 | 11 | 14 | 18 | 15 | 11 |
| Код буквы ОТ | 10 | 16 | 19 | 07 | 10 | 01 |
| Буква ОТ | К | Р | У | Ж | К | А |

Т.е. открытый текст «КРУЖКА».

6.2. Задание на лабораторную работу.

Разработать программу, иллюстрирующую шифрование методами гаммирования на примере криптографического алгоритма, заданного преподавателем.

6.3. Краткое описание работы программы

После запуска программы на исполнение открывается окно программы (рис. 6.1).

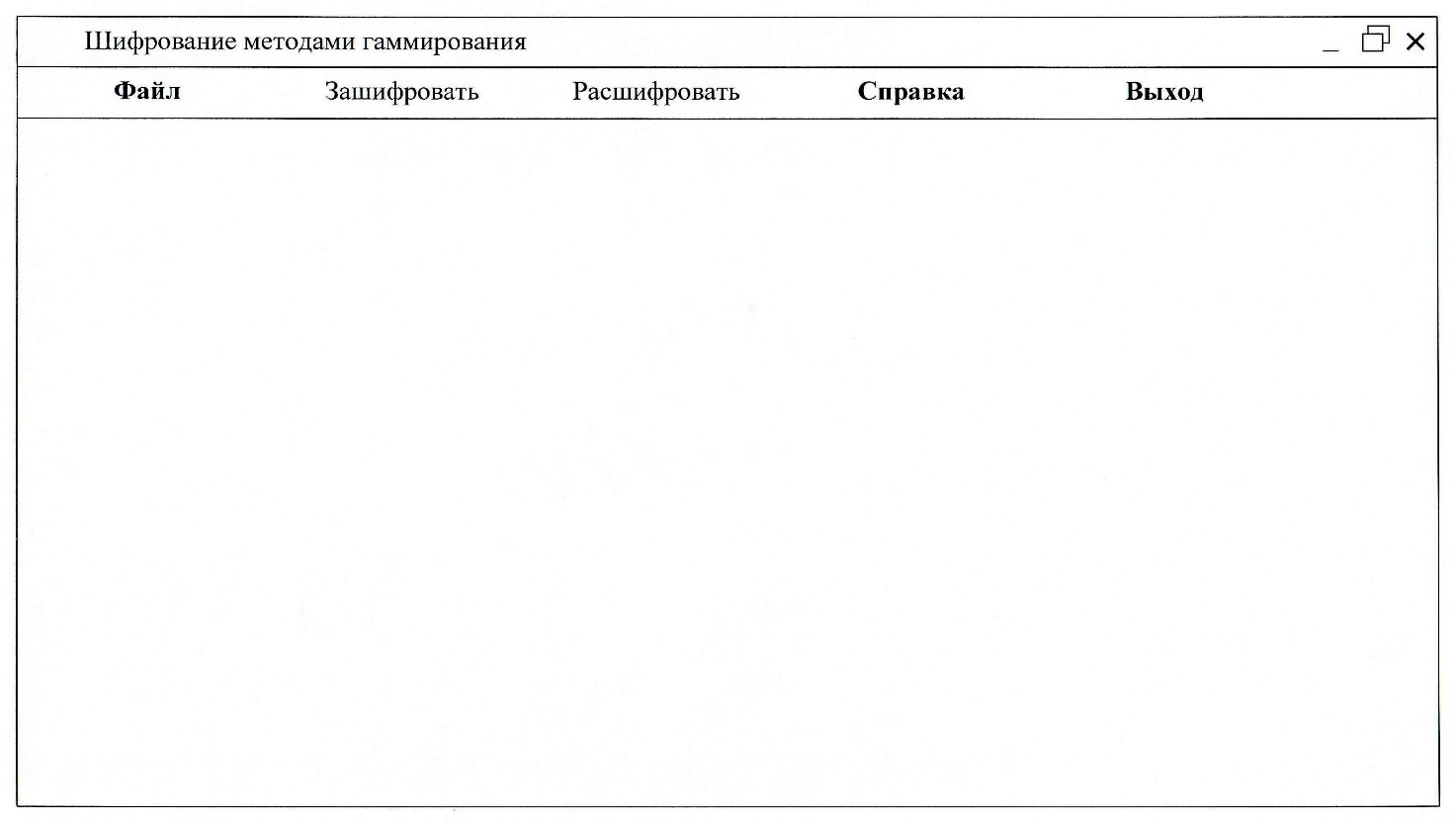


Рис. 6.1.

Меню действий содержит список функций программы: «Файл», «Зашифровать», «Расшифровать», «Справка», «Выход». Предварительно, сразу после запуска программы, рабочая область не содержит никакой информации (либо открытого, либо закрытого текста), поэтому доступными являются только функции «Файл», «Справка», «Выход». Функции «Зашифровать», «Расшифровать» остаются недоступными для выбора. При выборе некоторого действия из этого меню на экране под выбранным объектом появляется дополнительный список действий – выпадающее меню.

Пункт меню действий «Файл» (рис. 6.2) содержит подпункты (опции выпадающего меню): «Создать», «Открыть», «Сохранить», «Сохранить как», «Выход».

Создать – данный пункт выпадающего меню предоставляет пользователю право ввести в первую строку рабочей области либо открытый, либо закрытый текст, который впоследствии можно будет использовать при работе с программой, а также дает возможность использовать все недоступные до этого пункты меню действий. При этом длина строки текста не должна превышать 30 символов.

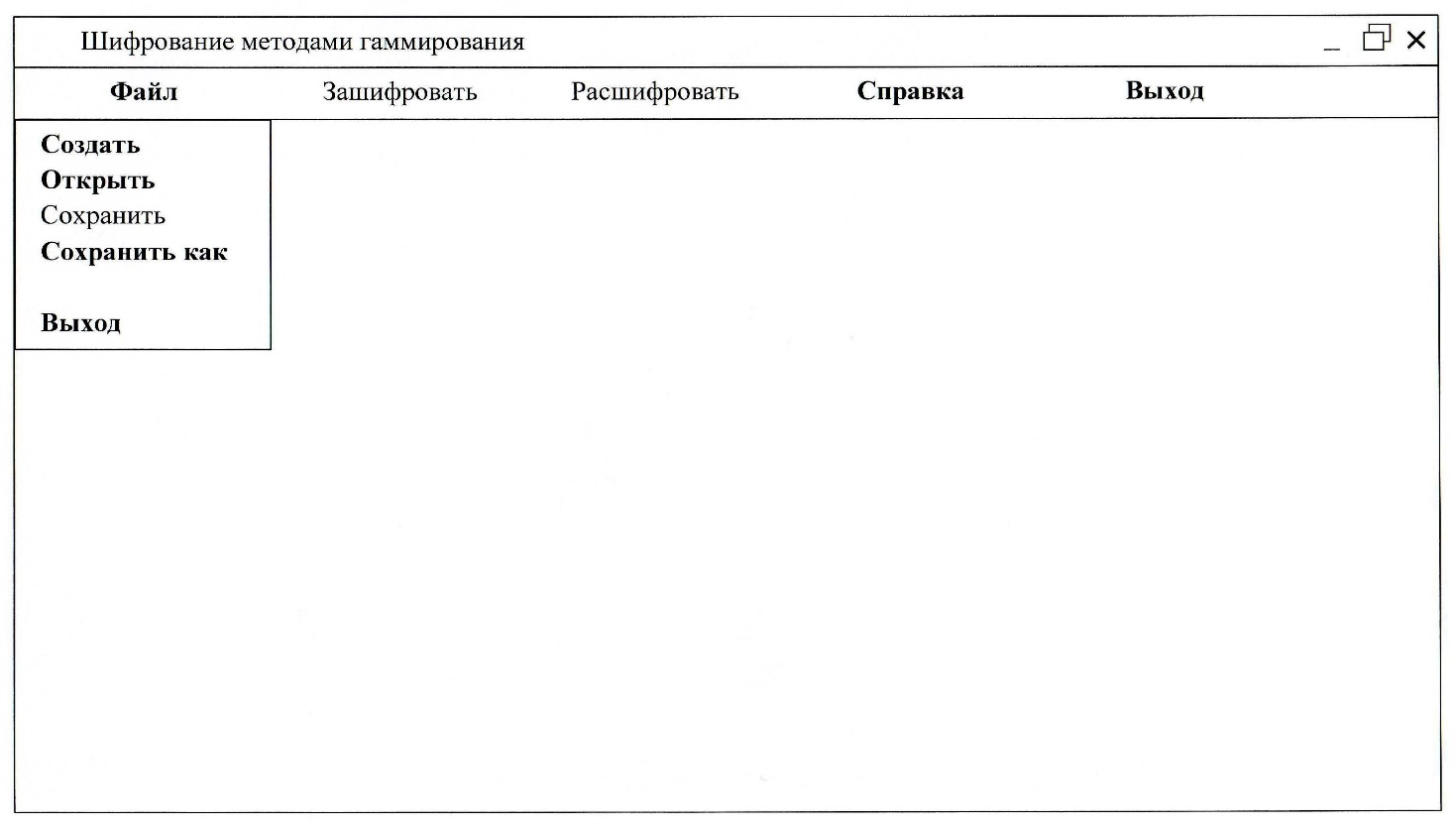


Рис. 6.2.

Открыть – при выборе этого пункта появляется диалоговое окно, предоставляющее возможность выбора файла для загрузки. При этом содержимое файла будет отображено в рабочей области окна программы.

Аналогично пункту «Создать» появляется возможность использовать все недоступные до этого пункты меню действий.

Сохранить – при выборе этого пункта содержимое последней строки из рабочей области программы сохраняется в ранее открытом файле (с сохранением имени файла).

Сохранить как – при выборе этого пункта появляется диалоговое окно, позволяющее сохранить на диск содержимое последней строки из рабочей области программы в новом файле.

Выход – выбор этого пункта позволяет выйти из программы.

Пункт меню действий «Справка» (рис. 6.3) содержит подпункты (опции выпадающего меню): «О программе», «Помощь».

О программе – при выборе этого пункта появляется всплывающее окно, содержащее *информационное сообщение* о названии и назначении программы и об авторе разработки.

Помощь – выбор этого пункта приводит к появлению всплывающего окна с *информационным сообщением*, содержащим краткую информацию о реализованном методе шифрования. Этот пункт – недоступен до момента заполнения рабочей области окна программы.

Выбор пункта меню действий «Выход» приводит к завершению работы программы.

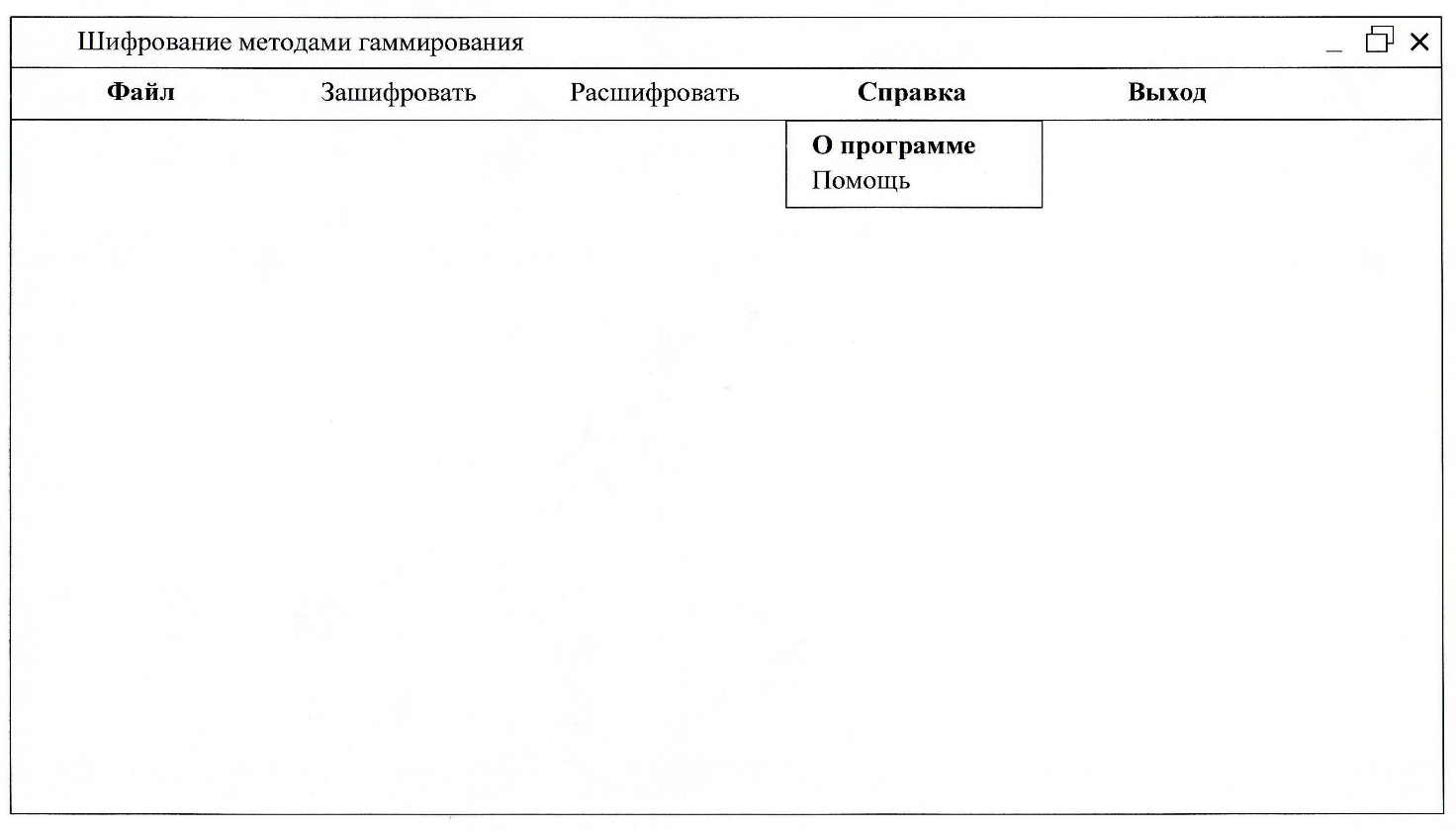


Рис. 6.3.

Пункты меню действий «**Зашифровать**» или «**Расшифровать**», доступные при наличии строк текста в рабочей области окна программы, содержат список методов шифрования, рассматриваемых в лабораторной работе (рис.6.4 – 6.5):

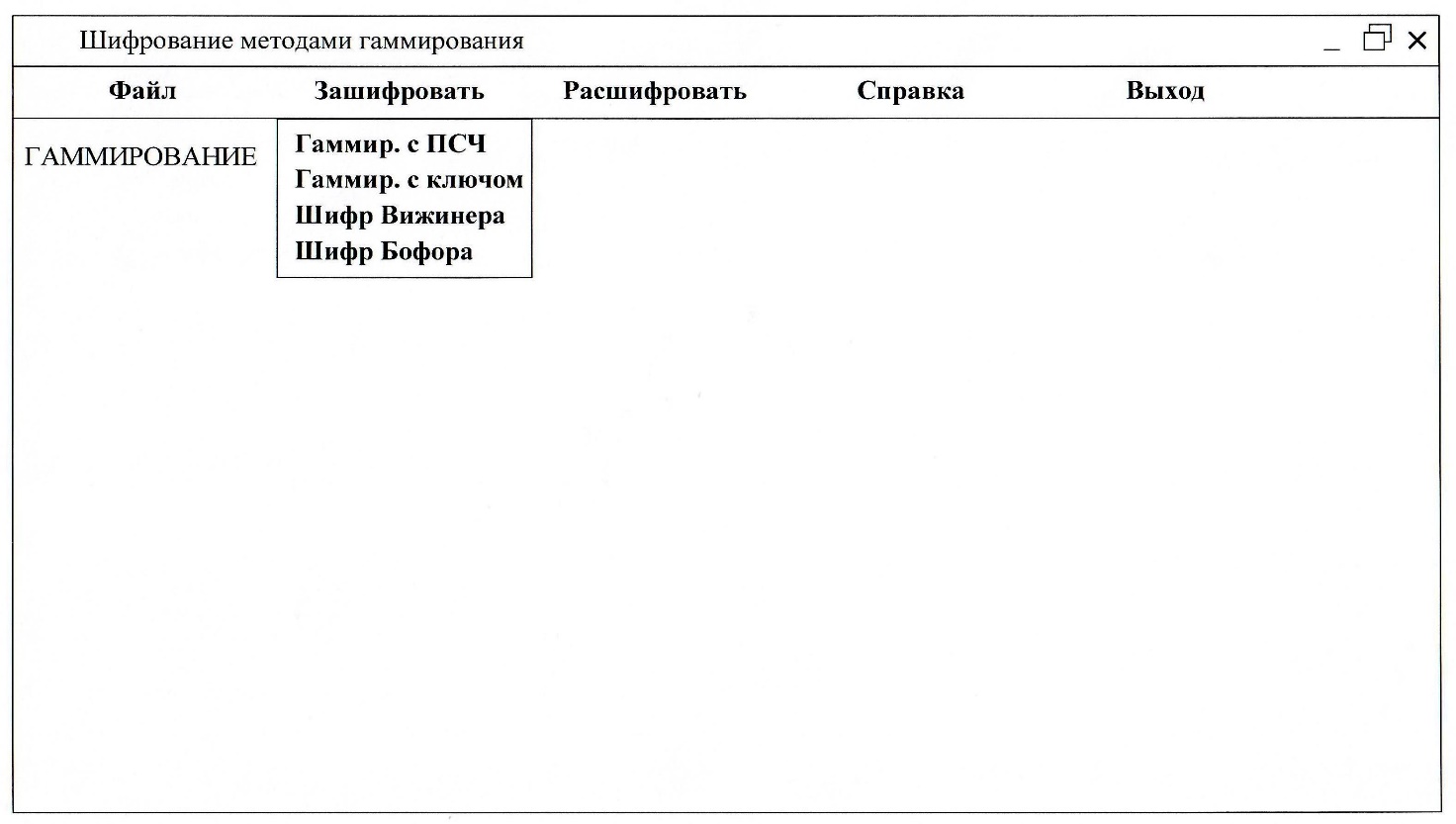


Рис. 6.4.

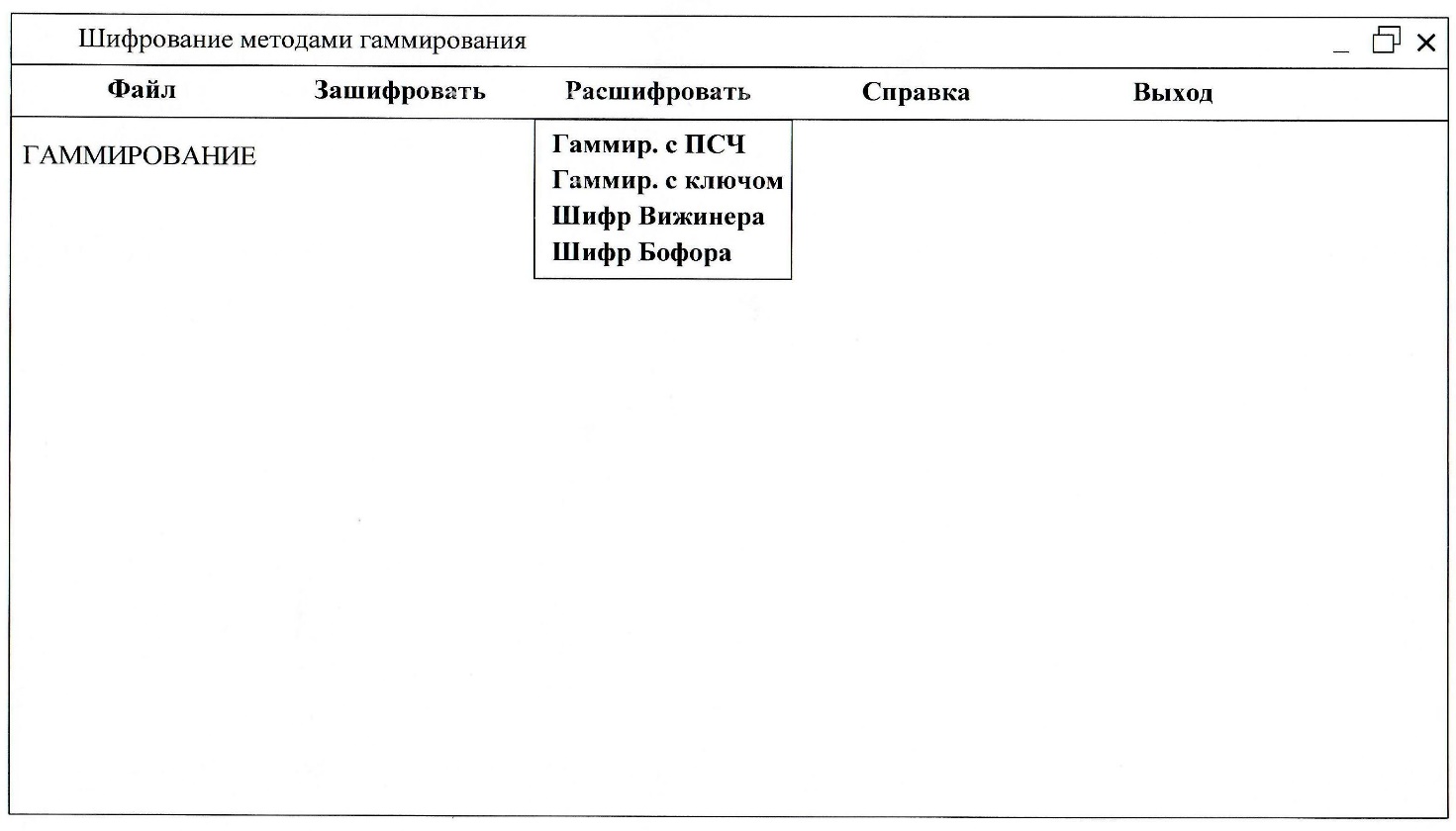


Рис. 6.5.

1. Гаммирование на основе ПСЧ.

2. Гаммирование на основе ключа.

3. Шифр Вижинера.

4. Шифр Бофора.

В случае выбора нереализованного согласно заданию на лабораторную работу метода шифрования появляется всплывающее окно, содержащее предупредительное сообщение «Указанный метод не реализован» (рис. 6.6).

Если выбран метод шифрования, реализованный в соответствии с заданием на лабораторную работу, то появляется всплывающее окно, позволяющее задать ключ шифрования и либо подтвердить его значение нажатием клавиши «Ok», либо отказаться от него нажатием клавиши «Esc» (рис. 6.7).

Если значение ключа подтверждено, но оно содержит ошибку, то появляется всплывающее окно, содержащее критическое сообщение «Значение ключа неправильное» (рис. 6.8). Когда это окно закрывается нажатием в нем клавиши «Ok», очищается окно ввода значения ключа, и ожидается задание нового значения ключа шифрования.

Если подтвержденное значение ключа – правильное, то окно ввода ключа закрывается, реализованный метод шифрования выполняется, и результат (преобразованный текст) отображается в следующей по порядку строке рабочего поля окна программы.

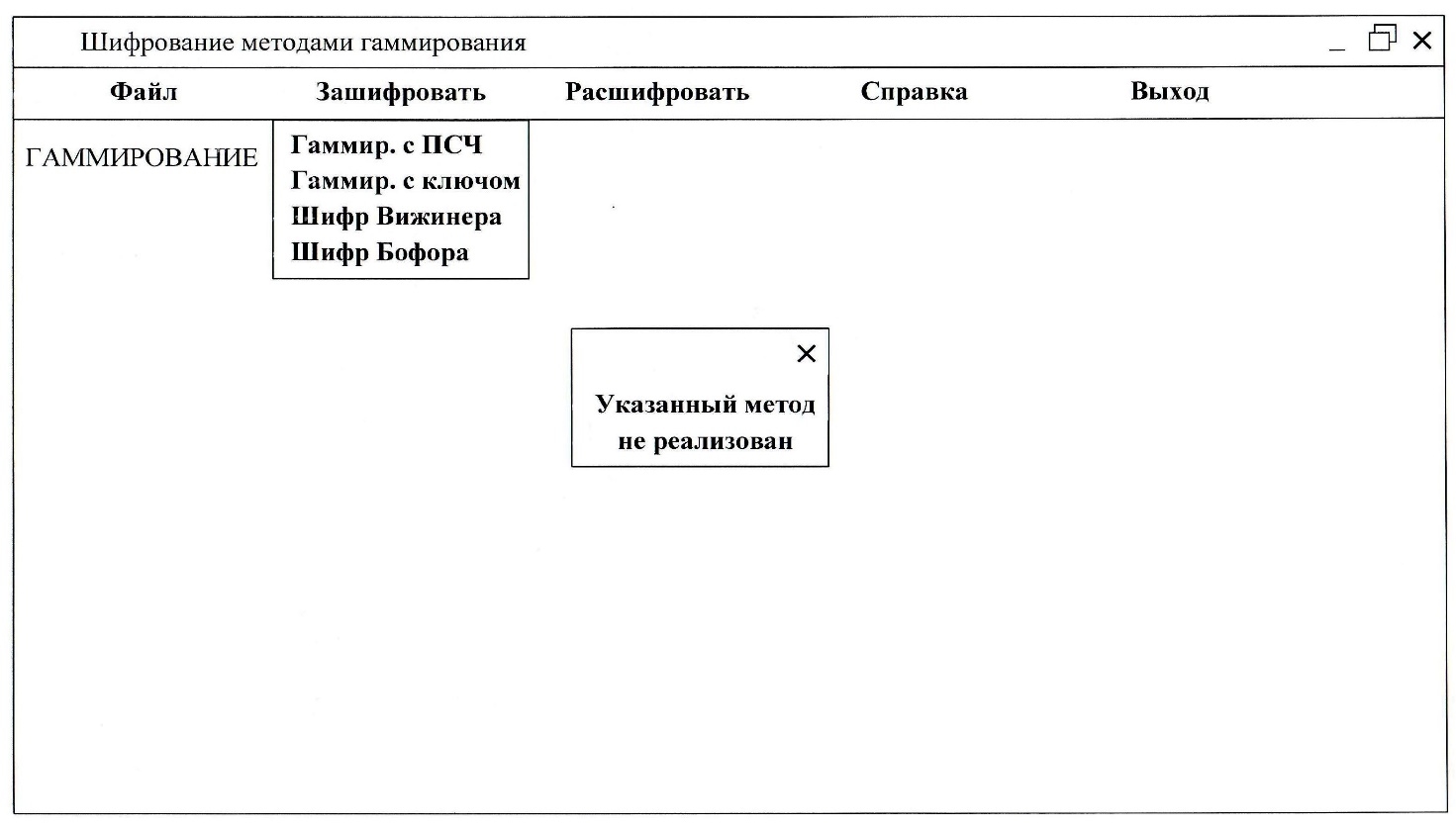


Рис. 6.6.

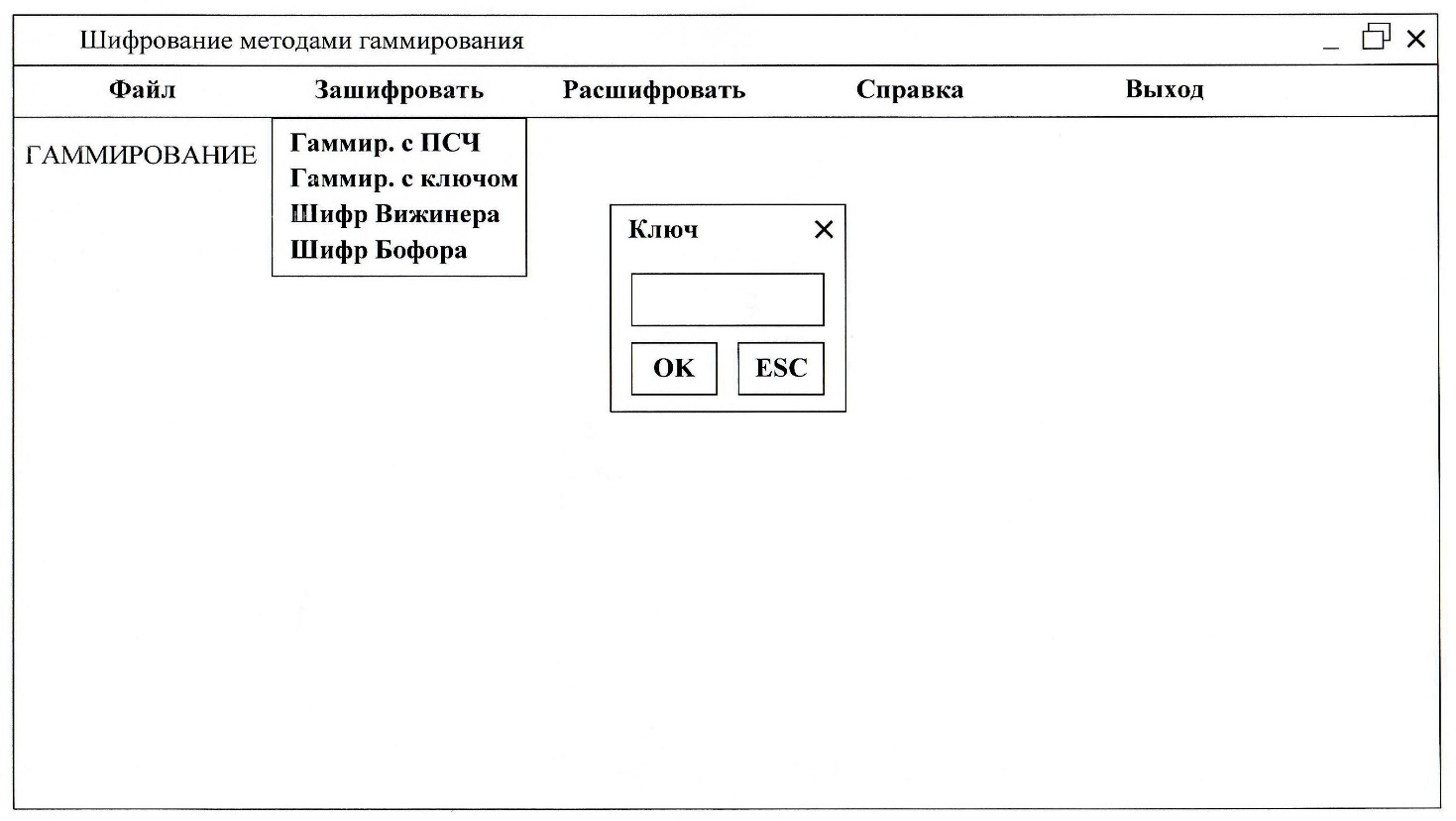


Рис. 6.7.

Если поочередно выполняются действия зашифрование и расшифрование, то при правильном расшифровании полученный текст совпадает с исходным.

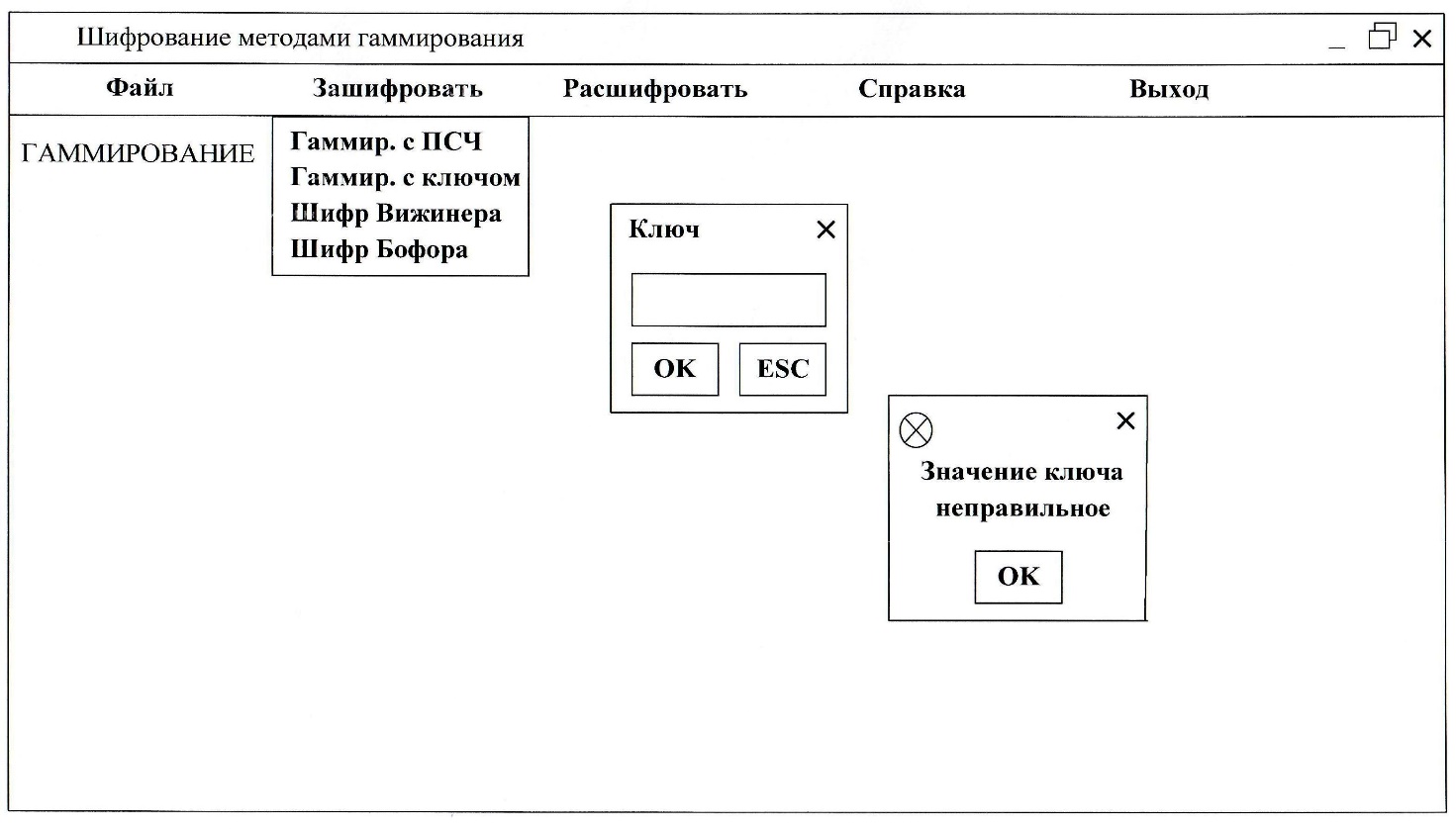


Рис. 6.8.

6.4. Контрольные вопросы

1. В чем заключается гаммирование?

2. Какие псевдослучайные последовательности являются наиболее доступными?

3. Каким будет шифротекст при зашифровании открытого текста «ГАММИРОВАНИЕ» методом гаммирования на основе псевдослучайной последовательности, если значение ключа *А* = 2, *С* = 4, *Т*(0) = 3, *m* = 32?

4. Каким будет шифротекст при зашифровании открытого текста «ГАММИРОВАНИЕ» методом гаммирования на основе ключевого слова «ВОЛЯ»?

5. Каким будет шифротекст при зашифровании открытого текста «ГАММИРОВАНИЕ» методом гаммирования на основе шифра Вижинера, если ключевое слово – «ЗАРЯ»?

6. Каким будет шифротекст при зашифровании открытого текста «ГАММИРОВАНИЕ» методом гаммирования на основе шифра Бофора, если ключевое слово – «ЛЕТО»?