МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ, ИНФОРМАТИКИ И МЕХАНИКИ

КАФЕДРА ТЕХНИЧЕСКОЙ КИБЕРНЕТИКИ И АВТОМАТИЧЕСКОГО РЕГУЛИРОВАНИЯ

**О Т Ч Е Т**

по лабораторной работе № 1

«Система шифрования данных DES»

Выполнил:

студент 4-го курса 4-ой группы

Поляков М.С.

Проверил:

преп. Левицкая Ю.С.

Воронеж

2018

**Содержание**

Постановка задачи……………………………………………………3

Описание алгоритма DES………………………………..…………..6

1. Результаты обучения..…………………………………………11
2. Выявление ошибок в обучающей программе………………..25
3. Принципы работы алгоритма des…………………………
4. Ответы на контрольные вопросы………………………...

Выводы...................................................................................................28

Библиографический список……………………………………….

**Постановка задачи**

1. Ознакомиться с обучающей программой «DES Tutorial».
2. Зафиксировать последовательность этапов и результаты обучения.
3. Провести исследование программы с целью выявления ошибок и недочетов.
4. Сформулировать принципы работы алгоритма DES.
5. Ответить на контрольные вопросы.
6. Составить отчет о проделанной работе.

**1. Описание алгоритма DES**

DES – расшифровать!

Процесс шифрования происходит по алгоритму, использующему схему Фейстеля (рис 1) [1].

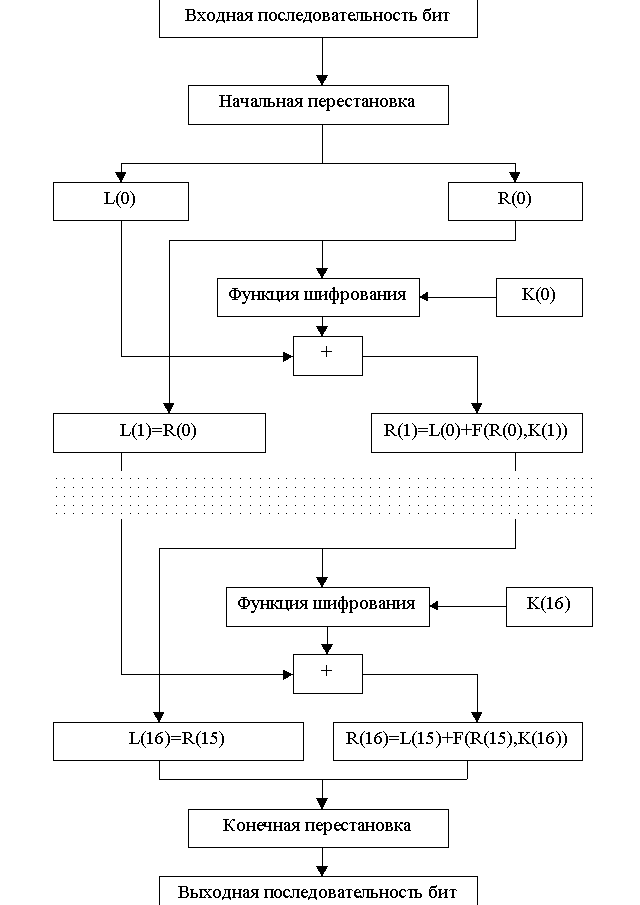


Рис 1. Блок-схема алгоритма шифрования DES

Что такое схема Фейстеля?

На первом шаге 64 битная последовательность перестанавливается в соответствии с таблицей 1.

**Таблица 1. "Начальная перестановка"**

58 50 42 34 26 18 10 2

60 52 44 36 28 20 12 4

62 54 46 38 30 22 14 6

64 56 48 40 32 24 16 8

57 49 41 33 25 17 9 1

59 51 43 35 27 19 11 3

61 53 45 37 29 21 13 5

63 55 47 39 31 23 15 7

Так 58 бит исходной последовательности становится 1, 50 бит становится 2 и т.д. Далее последовательность разбивается на 2 последовательности L(0) (58,50, … ,8) и R(0) (57,49, … ,7) [1]. Затем выполняется процесс шифрования этих последовательностей следующим образом:

L(i)=R(i-1), i=1,2,...,16.

R(i)=L(i-1) + F(R(i-1),K(i)), i=1,2,...,16.

Функция F называется функцией шифрования. Ключ K(i) является 48 битовым и получается в результате преобразования первичного 64 битового ключа. (???) Схема преобразования исходного ключа показана на Рис 2.

Далее выполняется перестановка битов в последовательности C(i)D(i) в соответствие с таблицей 4.

После этого преобразования получаем нужный нам ключ K.

На последнем шаге преобразования получаем последовательности L(16) и R(16). Далее они конкатенируются в последовательность L(16)R(16) и выполняется конечная перестановка битов в этой последовательности согласно таблице 5. Она является обратной к начальной.

**Таблица 5. "Конечная перестановка"**

40 8 48 16 56 24 64 32

39 7 47 15 55 23 63 31

38 6 46 14 54 22 62 30

37 5 45 13 53 21 61 29

36 4 44 12 52 20 60 28

35 3 43 11 51 19 59 27

34 2 42 10 50 18 58 26

33 1 41 9 49 17 57 25

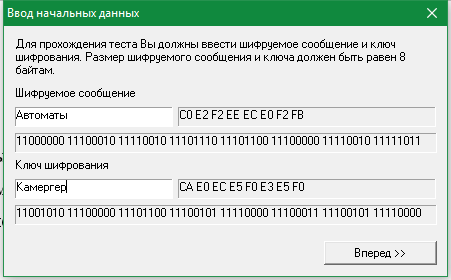
Полученная после этого 64 битная последовательность и будет зашифрованным текстом.

**2. Результаты обучения**

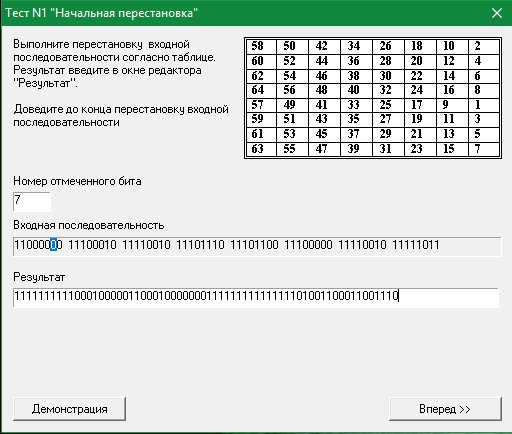
Начальные данные: вариант № 9

Шифруемое сообщение – Автоматы.

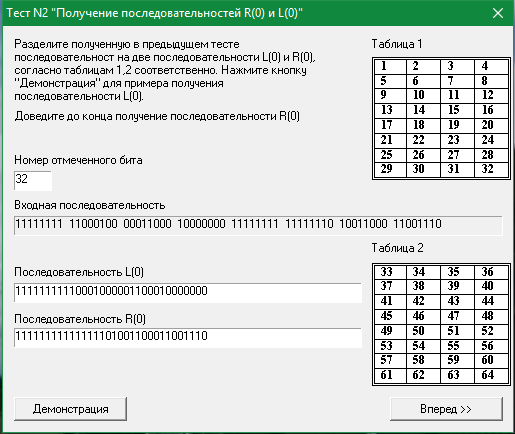
Ключ шифрования – Камергер.

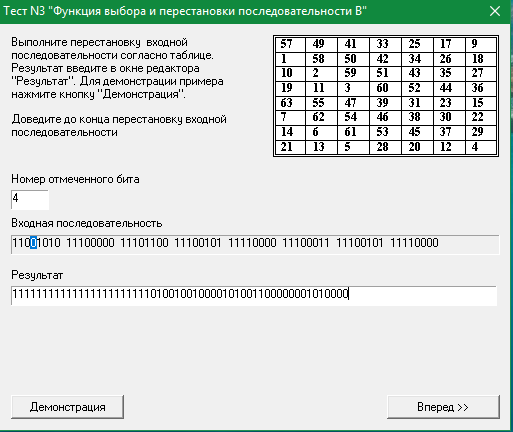


На первом шаге тестирования программы выполняется перестановка битов согласно таблице.

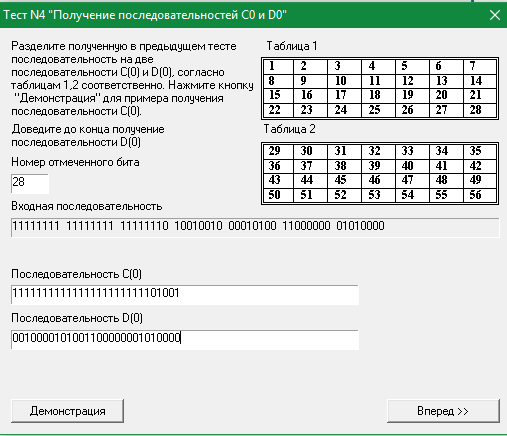


На втором шаге тестирования полученная последовательность бит разделяется на две последовательности: L(0) (биты 58, 50, 42, ..., 8) и R(0) (биты 57, 49, 41, ..., 7), каждая из которых содержит 32 бита.

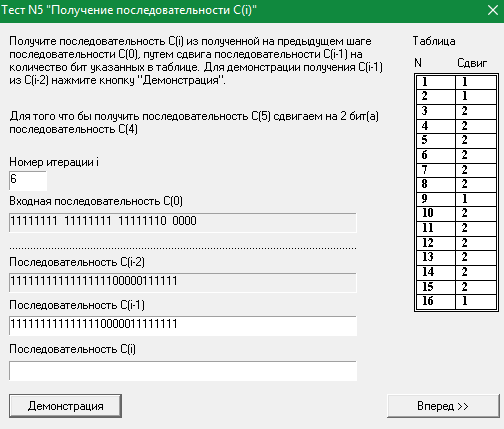


На третьем шаге тестирования программы выполняется перестановка битов в последовательности B согласно таблице.  
 

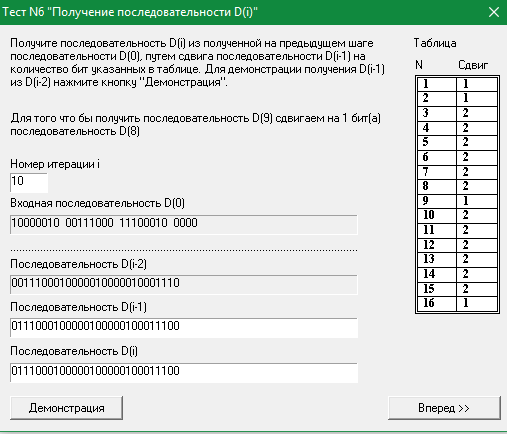
На четвертом шаге из последовательности В с помощью таблиц 1 и 2 получаем последовательности C0 и D0:



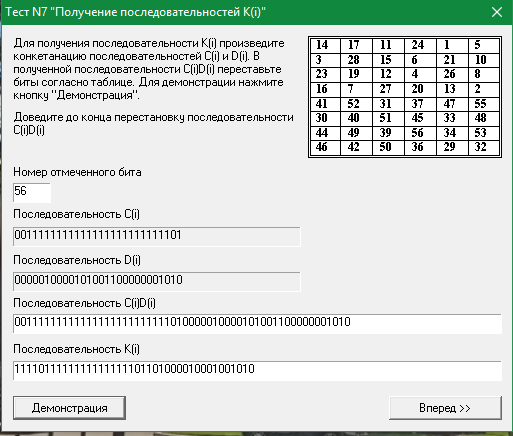
Для получения последовательности С(10) сдвигаем последовательность С(9) влево по кольцу в зависимости от номера шага итерации, указанного в таблице. В данном случае сдвигаем последовательность на 2 бита:



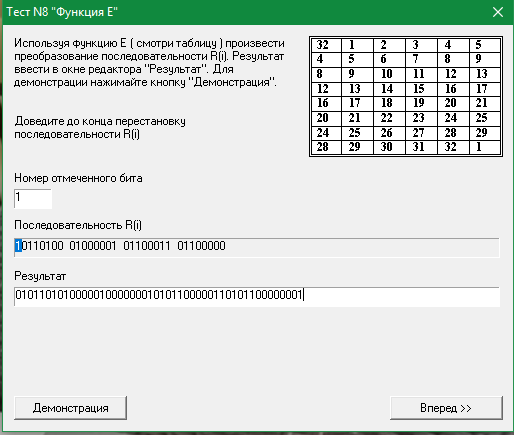
Для получения последовательности D(5) сдвигаем последовательность D(4) влево по кольцу на 2 бита:

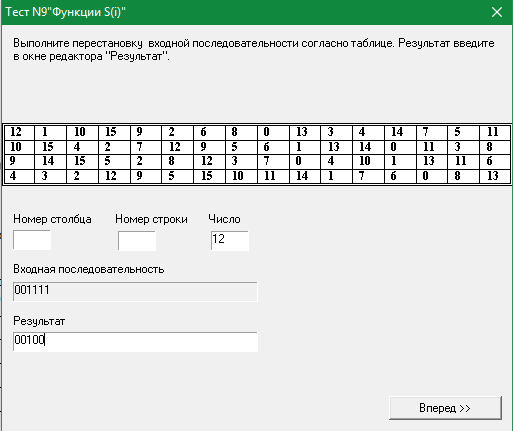


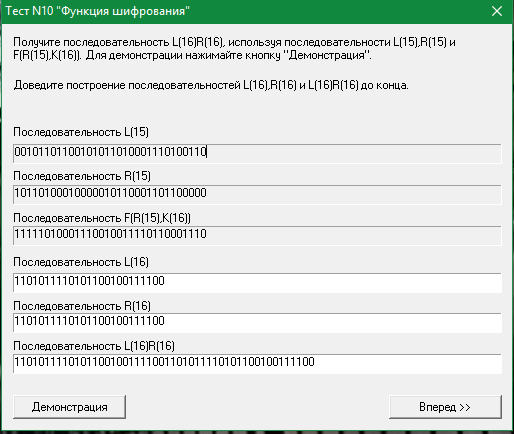
Производим преобразование последовательности R(i), используя функцию Е:

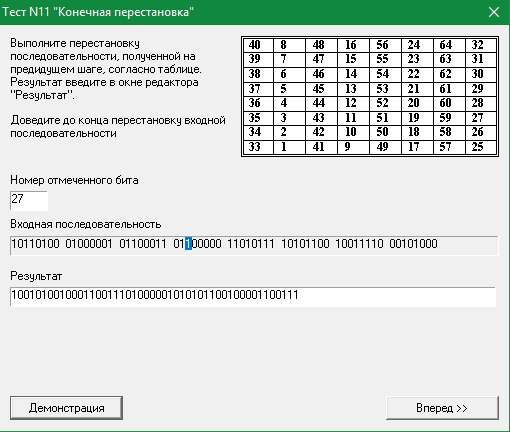


Выполняем перестановку входной последовательности: первый и последний бит - номер строки в двоичной системе, середина – номер столбца в двоичной системе. Нумерация строк и столбцов в таблице начинается с 0. Полученное число переводим в двоичное и получаем результирующую последовательность:

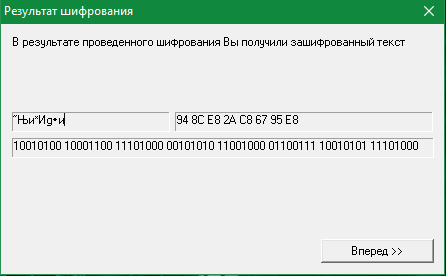


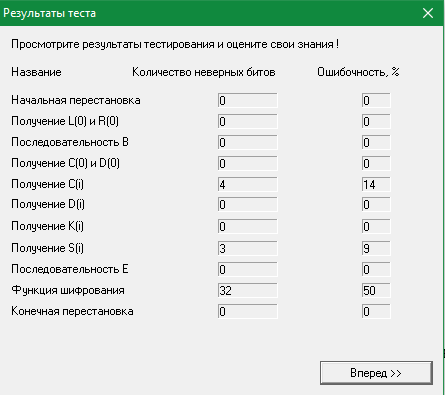




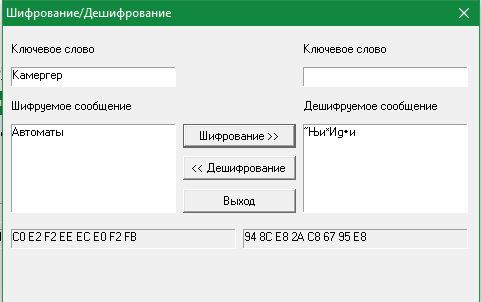
Выполняем перестановку входной последовательности, согласно таблице: 

Результат шифрования:



После нажатия кнопки «Вперед >>» программа проверит введенные ответы на каждом шаге обучения и сверит их с правильными: 

Выполним проверку:



Видим, что результат шифрования совпадает с полученным ранее.

Заметим, что в результате шифрования символ А0 (т.е. с номером 160) не отображается согласно таблице 6 [5].

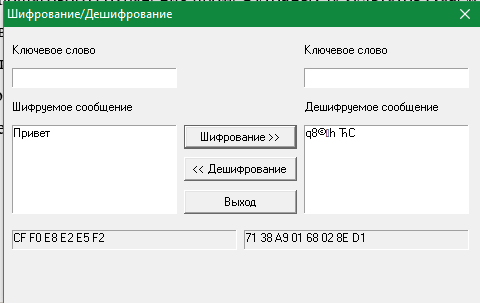
**Таблица 6. "Символы с кодами 128–255 (Кодовая таблица 1251 – MS Windows)"**

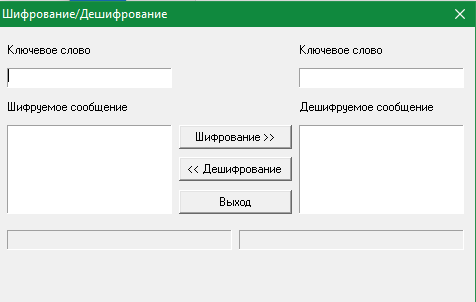
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Код** | **Символ** | **Код** | **Символ** | **Код** | **Символ** | **Код** | **Символ** |
| 128 | Ђ | 160 |  | 192 | А | 224 | а |
| 129 | Ѓ | 161 | Ў | 193 | Б | 225 | б |
| 130 | ‚ | 162 | ў | 194 | В | 226 | в |
| 131 | ѓ | 163 | Ј | 195 | Г | 227 | г |
| 132 | „ | 164 | ¤ | 196 | Д | 228 | д |
| 133 | … | 165 | Ґ | 197 | Е | 229 | е |
| 134 | † | 166 | ¦ | 198 | Ж | 230 | ж |
| 135 | ‡ | 167 | § | 199 | З | 231 | з |
| 136 | € | 168 | Ё | 200 | И | 232 | и |
| 137 | ‰ | 169 | © | 201 | Й | 233 | й |
| 138 | Љ | 170 | Є | 202 | К | 234 | к |
| 139 | ‹ | 171 | « | 203 | Л | 235 | л |
| 140 | Њ | 172 | ¬ | 204 | М | 236 | м |
| 141 | Ќ | 173 | - | 205 | Н | 237 | н |
| 142 | Ћ | 174 | ® | 206 | О | 238 | о |
| 143 | Џ | 175 | Ї | 207 | П | 239 | п |
| 144 | ђ | 176 | ° | 208 | Р | 240 | р |
| 145 | ‘ | 177 | ± | 209 | С | 241 | с |
| 146 | ’ | 178 | І | 210 | Т | 242 | т |
| 147 | “ | 179 | і | 211 | У | 243 | у |
| 148 | ” | 180 | ґ | 212 | Ф | 244 | ф |
| 149 | • | 181 | μ | 213 | Х | 245 | х |
| 150 | – | 182 | ¶ | 214 | Ц | 246 | ц |
| 151 | — | 183 | · | 215 | Ч | 247 | ч |
| 152 | \_ | 184 | ё | 216 | Ш | 248 | ш |
| 153 | ™ | 185 | № | 217 | Щ | 249 | щ |
| 154 | љ | 186 | є | 218 | Ъ | 250 | ъ |
| 155 | › | 187 | » | 219 | Ы | 251 | ы |
| 156 | њ | 188 | ј | 220 | Ь | 252 | ь |
| 157 | ќ | 189 | Ѕ | 221 | Э | 253 | э |
| 158 | ћ | 190 | ѕ | 222 | Ю | 254 | ю |
| 159 | џ | 191 | ї | 223 | Я | 255 | я |

**3. Выявление ошибок в обучающей программе**

В результате тестирования были выявлены следующие недочеты:

1. Невозможно вернуться на предыдущий шаг в режиме обучения.
2. Отсутствие полного описание на некоторых шагах.
3. Множество опечаток как в справке, так и в самой программе.
4. Если в результате шифрования появился символ с кодом 00, то все следующие за ним символы не отображаются, а после расшифровки результат либо не верен, либо полностью отсутствует.
5. На шаге №5 «получение последовательности» программа некорректно отображает информацию к выполнению, например, просит сдвинуть последовательность на 1 бит, а по таблице сдвигать нужно на 2 бита.
6. Если оставить ключевое поле пустым, а ввести только шифруемое сообщение, то приложение зашифрует его неким ключом, который нигде не отображается. С расшифровкой работает аналогично.



1. В режиме Шифрования при нажатии клавиши Enter программа закрывается в любом случае. 

**4. Принципы работы алгоритма DES**

DES (Data Encryption Standard) – стандарт шифрования данных.

1. Алгоритм DES является блочным, поточным , или и то и другое? Что это означает?

2. Алгоритм DES является симметричным или нет? Что это означает?.

3. Какова длина ключа? Вся ли она используется при шифровании и расшифровании? Как связана с криптостойкостью?

4. Алгоритм реализует 16 шагов шифрования для получения достаточной случайности (чего?).

5. Основные методы шифрования, используемые в данном алгоритме.

6. Что такое схема Фейстеля? Как она используется в алгоритме?

7. Используется 12 (???) таблиц перестановок. Все таблицы перестановок являются фиксированными.

8. Начальная и конечная перестановки являются обратимыми. Для расшифрования необходимо проделать те же шаги но в обратном порядке (???).

9. Каким образом обеспечивается нелинейность преобразований и зачем она нужна?

10. Как происходит расшифрование? Каким образом обеспечивается взаимная обратимость шифрования и расшифрования?

**5. Ответы на контрольные вопросы**

1. Перечислите режимы работы обучающей программы DES Tutorial.

Система позволяет пользователю работать в двух режимах (а может в трех?):

1) режим тестирования – программа вместе с пользователем проводит процесс шифрования данных. В этом режиме программа поэтапно выполняет шифрование данных и просит пользователя закончить за нее работу на том или ином этапе;

2) режим шифрования/расшифрования – программа шифрует и расшифровывает текстовые строки, используя введенный ключ[1].

1. В чем состоит основная идея шифрования данных?

Основная идея шифрования – скрытие смысла передаваемого сообщения [3].

1. Для решения каких задач используется кодирование информации?

Кодирование используется в случаях, когда необходимо представить открытый текст в более удобном виде для передачи по телекоммуникационным каналам, для уменьшения длины сообщения (архивация), для повышения помехоустойчивости (обнаружение и исправление ошибок) [3].

1. Опишите упрощенную схему симметричного шифрования.

1) Исходные данные разбиваются на блоки фиксированной длины, может осуществляться начальная перестановка данных в каждом блоке.

2) Данные преобразуются использованием ключа шифрования (сам ключ шифрования также предварительно преобразовывается).

3) Преобразование производится определенное число раз (раундов), после каждого преобразования может производиться перестановка данных; в качестве исходного результата для преобразования используется результат предыдущего преобразования и перестановки.

4) После определенного числа раундов производится финальная перестановка, полученный после этого результат становится шифртекстом [4].

Упрощенная схема симметричного шифрования приведена на рис 3.

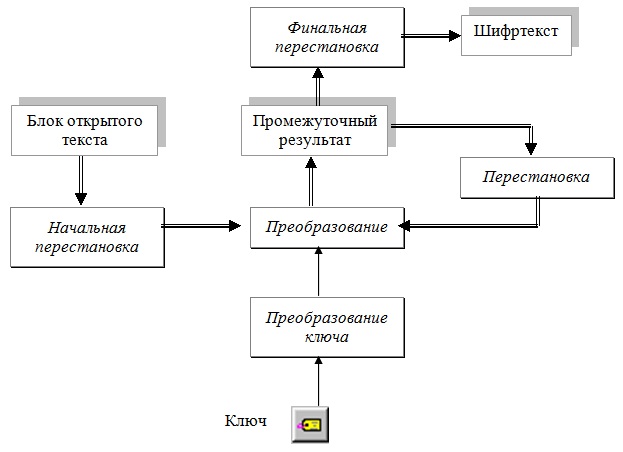


Рис 3. Подпись под рисунком !!!

1. Что означает фраза "процесс расшифрования данных является инверсным по отношению к процессу шифрования"?

(???) Это означает, что все действия должны быть выполнены в обратном порядке, т.е. расшифровываемые данные сначала переставляются в соответствии с таблицей 1, а затем над последовательностью бит R(16)L(16) выполняется те же действия, что и в процессе шифрования, но в обратном порядке [1].

ВЫВОДЫ

В результате ознакомления с обучающей программой «DES Tutorial», изучен криптографический алгоритма DES, сформулированы принципы его работы, зафиксированы последовательность этапов и итоги обучения. Также проведено исследование программы (тестирование) и выявлены ошибки и недочеты, которые показали …. Приведенные ответы на контрольные вопросы позволили расширить представление об особенностях симметричного шифрования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кабанов Е. В. Программа обучения алгоритму шифрования DES / Е. В. Кабанов, М. В. Прокопов [электронный ресурс], 2001г. – (URL: [http://blackw.des.ru](http://blackw.des.ru/) ([blackwolf@mail.ru](mailto:blackwolf@mail.ru), [nexus@mail.ru](mailto:nexus@mail.ru)) (дата обращения: 23.10.2011)
2. ???Основы криптографии: учебное пособие / А. П. Алферов [и др.]. – М.: Гелиос АРВ, 2001. – 480 с.
3. ???Воронков Б. Н. Методическое пособие по разработке средств защиты информации в вычислительных сетях / Б. Н. Воронков, В. И. Тупота. – Воронеж: ВГУ, 2000. – 112 с.
4. Панасенко С. П. Криптографические методы защиты информации / С. П. Панасенко [текст], 2006. –

(URL: <http://www.panasenko.ru/Articles/102/102.html>) (дата обращения: 23.10.2011)

1. Таблицы кодов ASCII – [сайт]. – (URL: [http://ascii.org.ru](http://ascii.org.ru/)) (дата обращения: 25.11.2011)