# **Лабораторная работа 1А**

**“Изучение и ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ПРОСТЕЙШИХ МЕТОДОВ ШИФРОВАНИЯ ДАННЫХ В РУЧНОМ РЕЖИМЕ”**

**(часть 1)**

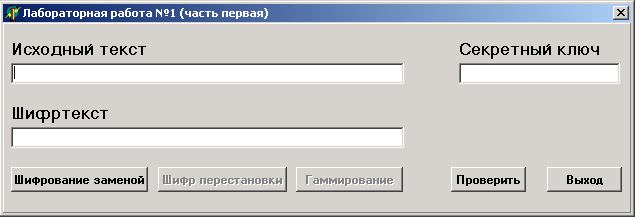
**Цель работы:** Приобретение первичных практических навыков “ручного” шифрования на примере простейших алгоритмов преобразования данных.

**Контрольное программное обеспечение:**

* Программа LR1\_1, реализующая простейшие виды перестановок, подстановок и гаммирования, а также позволяющая проверять результаты ручного шифрования, выполняемого обучаемым;

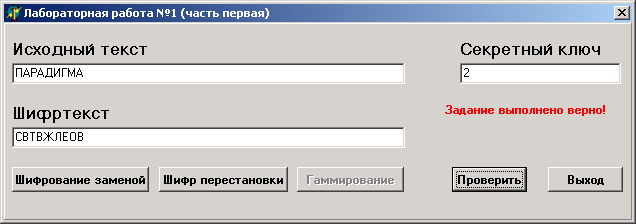
# Порядок выполнения работы

При запуске программы LR1\_1 появляется главное меню лабораторной работы:

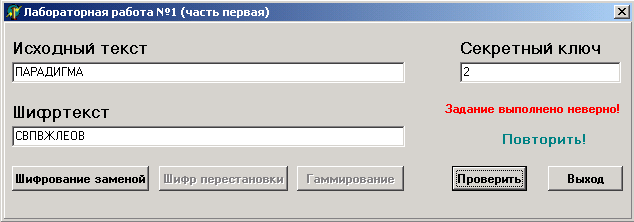


При выполнении работы предлагается три варианта задания, которые обучаемые выполняют последовательно.

**1. Режим шифрования методом простой замены.** В окно *Исходный текст* вводится открытый текст длиной не более 40 букв русского алфавита и пробелов. В окно *Секретный ключ* вводится ключ k, имеющий значение от 0 до 31. Каждой букве присваивается числовое значение от 0 до 31. После этого в соответствии с алгоритмом простой замены yi=(xi+k) mod 32, обучаемый самостоятельно вычисляет криптограмму. Содержание криптограммы вводится в окно *Шифртекст*. Проверка правильности выполнения шифрования осуществляется путем нажатия на кнопку *Проверить*. Если задание выполнено правильно, тогда в левом нижнем углу появляется сообщение *Задание выполнено верно* и активируется кнопка, соответствующая второму пункту работы:

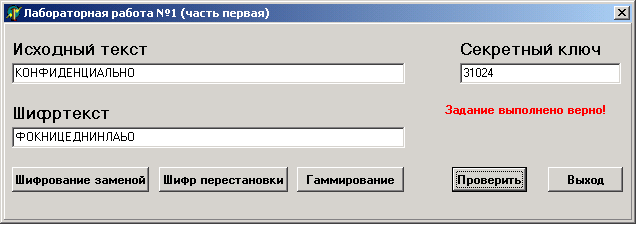


В ином случае появляется сообщение *Задание выполнено неверно* и предлагается повторить выполнение задания:



Переход к следующему пункту возможен только при правильно выполненном задании.

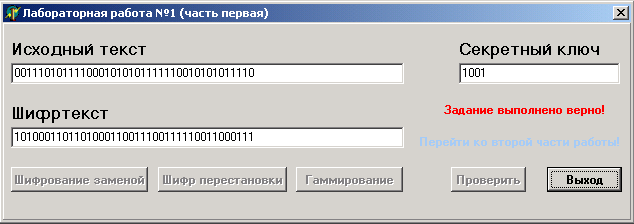
**2. Режим шифрования методом перестановок.** В окно *Исходный текст* вводится открытый текст длиной не более 40 (кратно 5) любых символов. В окно *Секретный ключ* вводится ключ перестановки внутри пятисимвольного блока, например, 31024. После этого в соответствии с данным ключом, задающим конкретную перестановку, обучаемый самостоятельно вычисляет криптограмму. Ключ используется циклически до конца открытого текста. Содержание криптограммы вводится в окно *Шифртекст*. Проверка правильности выполнения шифрования осуществляется путем нажатия на кнопку *Проверить*. Если задание выполнено правильно, тогда в левом нижнем углу появляется сообщение *Задание выполнено верно* и активируется кнопка, соответствующая третьему пункту работы:



В ином случае появляется сообщение *Задание выполнено неверно* и предлагается повторить выполнение задания.

Переход к следующему пункту возможен только при правильно выполненном задании.

**3. Режим шифрования методом гаммирования.** В окно *Исходный текст* вводится, предварительно преобразованный обучаемым к двоичному виду в соответствии с таблицей ASCII кодов, открытый текст длиной не более 40 двоичных символов (0 и 1). В окно *Секретный ключ* вводится ключ (гамма) длиной не более 16 двоичных символов. После этого обучаемый вычисляет криптограмму путем сложения по модулю 2 открытого текста и гаммы: *yi*=(*xi*+*ki*) mod 2. Ключ используется циклически до конца открытого текста. Полученное содержание криптограммы вводится в окно *Шифртекст*. Проверка правильности выполнения шифрования осуществляется путем нажатия на кнопку *Проверить*. Если задание выполнено правильно, тогда в левом нижнем углу появляется сообщение *Задание выполнено верно,* а также сообщение *Перейти ко второй части работы* (выполнению лабораторной работы №1):



В ином случае появляется сообщение *Задание выполнено неверно* и предлагается повторить выполнение задания.

**Контрольные вопросы**

1. Перечислить задачи, решаемые криптографическими системами.
2. Перечислить классы шифров по стойкости.
3. Дать определение безусловно стойкого шифра.
4. Дать определение вычислительно стойкого шифра.
5. Указать класс стойкости шифра в отчёте (по выбору преподавателя).
6. Перечислить достаточные условия безусловной стойкости шифра.
7. Объяснить, каким образом из указанного преподавателем шифра создать безусловно стойкий шифр.

# Содержание отчета

1. Результаты шифрования.
2. Ответы на контрольные вопросы.

При защите отчёта решить задачу по указанию преподавателя. №№ задач 1 – 26 из сборника задач.