Лабораторная работа №1.

Часть 1.

1. С клавиатуры вводится 32-х разрядное целое число a в двоичной системе счисления.
   1. Вывести k −ый бит числа a. Номер бита предварительно запросить у пользователя.
   2. Установить/снять k −ый бит числа a.
   3. Поменять местами i −ый и j −ый биты в числе a. Числа i и j предварительно запросить у пользователя.
   4. Обнулить младшие m бит.
2. А) «Склеить» первые i битов с последними i битами из целого числа длиной len битов. *Пример.* Пусть есть 12-ти разрядное целое число, представленное в двоичной системе счисления 100011101101. «Склеим» первые 3 и последние 3 бита, получим 100101.
   В) Получить биты из целого числа длиной len битов, находящиеся между первыми i битами и последними i битами. *Пример.* Пусть есть 12-ти разрядное целое число, представленное в двоичной системе счисления 100011101101. Получим биты находящиеся между первыми 3 и последними 3 битами: 011101.
3. Поменять местами байты в заданном 32-х разрядном целом числе. Перестановка задается пользователем.

Часть 2.

4. Найти максимальную степень 2, на которую делится данное целое число. *Примечание.* Операторами цикла пользоваться нельзя.
5. Пусть x целое число. Найти такое p, что $2^p \leq x \leq 2^{p+1}$.
6. Дано 2^p разрядное целое число. «Поксорить» все биты этого числа друг с другом. *Пример.*$101110001 \rightarrow 1;\ 11100111 \rightarrow 0$.
7. Написать макросы циклического сдвига в 2^p разрядном целом числе на n бит влево и вправо.
8. Дано n битовое данное. Задана перестановка бит $(1, 8, 23, 0, 16, \dots)$. Написать функцию, выполняющую эту перестановку. Пример. $\overset{7}{1}\overset{6}{0}\overset{5}{1}\overset{4}{0}\overset{3}{1}\overset{2}{1}\overset{1}{1}\overset{0}{0} \rightarrow 11110001$. Биты, переставлены в соответствии с перестановкой $(5, 3, 7, 1, 4, 0, 6, 2)$.

Часть 3.

9. Разработайте алгоритм шифрования на основе замены последовательности битов. Например, определите таблицу, в которой задано правило замены 4 бит на какую-то другую последовательность бит. Разработайте консольное приложение, шифрующее и дешифрующее файл, используя ваш алгоритм.
10. Разработать приложение, шифрующее и дешифрующее файл с помощью алгоритма Вернама.
11. Разработайте приложение, обеспечивающее безопасность данных на основе алгоритма DES. **Примечание.** В приложении необходимо реализовать возможность выбора режима работы алгоритма. Выполните сравнительный анализ эффективности вашей реализации алгоритма DES. Воспользуйтесь какой-либо готовой реализацией алгоритма и выполните множественное шифрование и дешифрование данных вашей реализацией и готовым решением. Постройте графики скорости шифрования данных ($v = v(s), s$ −размер шифруемых данных).
12. Реализуйте алгоритм RC4.

Внимание. Запрещается реализовывать задания в виде консольных приложений. Обязательно наличие типичных элементов управления: меню, строки состояния, древовидного элемента управления. В ваших программах для демонстрации алгоритма необходимо шифровать файлы. Рекомендуемые языки программирования и технологии: C#/WPF, ado .net, C++/QT, python, PyQt, js.