**Задание для лабораторной работы №5**

**Реализация исторических алгоритмов шифрования**

Написать программу, реализующую два исторических примера алгоритмов шифрования. Продумать интерфейс, руководство пользователя и описание работы алгоритмов (их историей и криптоустойчивостью), для демонстрации алгоритмов пользователю со встроенными примерами текстов (шифруем и дешифруем), а также с возможностью ввода произвольного текста с его шифровкой дешифровкой.

Вариант получается из номера N студента по списку группы по следующей формуле (N%10)+1.

Необходимо реализовать следующие этапы для каждого своего алгоритма:

1. Краткое описание алгоритма шифрования.

2. Определение ограничений на решаемую задачу.

3. Реализация данного алгоритма в виде программного кода.

4. Реализация и описание графического интерфейса.

5. Оформление отчета (включает описание выше и нижеизложенных пунктов со скриншотами работы программы и результатов)

*Для защиты программы необходимо предложить несколько (3-4) различных текстов, в которых используется различное количество символов, например: может быть дан текст в котором встречаются много раз только три-четыре буквы, или текст где все буквы сообщения различные, а также вариативность текстов может быть русско-английская.*

**Варианты (подробные описания шифрования ищите в сети Интернет):**

1. Вариант: 1 и 11

2. Вариант: 2 и 12

3. Вариант: 3 и 13

4. Вариант: 4 и 14

5. Вариант: 5 и 15

6. Вариант: 6 и 16

7. Вариант: 7 и 17

8. Вариант: 8 и 18

9. Вариант: 9 и 19

10. Вариант: 10 и 20

**Соответствие номеров алгоритмам шифрования:**

1. Шифр Цезаря

2. Шифровка последовательностей нулей и единиц

3. «Табличная шифровка»

4. «Матричная шифровка»

5. «Шифровка решеткой»

6. «Шифровка зафиксированной перестановкой»

7. Шифр Гронсфельда

8. Шифровка с помощью квадрата Полибия

9. Шифр Хилла (с длиной блока = 2)

10. Шифр Атбаш

11. Шифр Вижинера (для латинских букв)

12. Шифр Вижинера (для русских букв)

13. Шифр Плейфера

14. Шифр с использованием кодового слова

15. Шифр перестановки "скитала"

16. Простая табличная перестановка

17. Табличная шифровка с ключевым словом

18. Двойная табличная перестановка

19. Шифровка с помощью магического квадрата

20. Шифровка «тарабарская грамота» (весь алфавит)

Для каждого алгоритма шифрования необходимо написать программу (можно написать одну с меню-выбором из двух заданных алгоритмов), которая работает в двух режимах: шифрования и дешифрования. При любом из режимов программа считывает исходный текст из окна или файла, шифрует или дешифрует его и записывает или отображает в окно или в другой файл.

Креативность приветствуется!