

РАЗРАБОТКА ПРОГРАММЫ С КЛАССИЧЕСКИМ КРИПТОАЛГОРИТМОМ ДЛЯ ЗАЩИТЫ ТЕКСТОВОЙ ИНФОРМАЦИИ.

Цель работы: на практике реализовать один из классических вариантов криптографического алгоритма

Теоретическая часть: такая же, как и для лабораторной №1 и содержится в файле ЛР_1_ИБ_САПР.pdf

Программное обеспечение: Си++, C#, Delphi и т.д.

Задание:

1. Выдаются по вариантам (Таблица 1) и соответствуют номеру студента в журнале.
2. Программа должна иметь графический пользовательский интерфейс.
3. Программа должна уметь правильно шифровать текстовую информацию, согласно алгоритму, указанному в задании.
4. Программа должна уметь правильно расшифровать текстовую информацию, согласно алгоритму, указанному в задании.
5. Программа должна содержать справочную информацию по алгоритму шифрования
6. Источник входных и выходных данных указан в задании.
7. Программа должна корректно обрабатывать ошибки ввода(работать только с допустимыми входными значениями)
8. Отчет по лабораторной работе должен содержать: титульный лист, вариант задания, код работы алгоритма шифрования и блок-схему алгоритма, принтскрины результатов работы программы, показывающие все возможные варианты ее функционирования.

Таблица 1. Варианты задания для лабораторной работы 1

Вариант	Алгоритм шифрования	Символы, с которыми работает алгоритм	Входные данные	Выходные данные	Синхронный вывод*
1	Одноалфавитный метод (с фиксированным смещением).	Символы русского языка(без учета регистра букв) и знак пробела	Клавиатура и файл	На экран	Да, при введение текста с клавиатуры
2	Одноалфавитный метод с задаваемым смещением (от 2 до 20).	Символы русского языка(без учета регистра букв) и знак пробела, цифры, знаки препинания	Клавиатура и файл	На экран, в файл**	Нет
3	Перестановка символов.	Символы русского языка(без учета регистра букв) и знак пробела	Клавиатура и файл	На экран	Нет
4	По дополнению до 255 (инверсный метод)	Символы русского языка(без учета регистра букв) и знак пробела, цифры, знаки препинания	Клавиатура и файл	На экран, в файл	Нет
5	Многоалфавитный метод (с фиксированным ключом).	Символы русского язык(без учета регистра букв) и знак пробела	Клавиатура и файл	На экран	Да, при введение текста с клавиатуры
6	Метод гаммирования	Символы русского языка(без учета регистра букв) и знак пробела, цифры, знаки препинания	Клавиатура и файл	На экран, в файл	Нет
7	Таблицы	Символы русского языка	Клавиатура и	На экран	Да, при

	Виженера		файл		введение текста с клавиатуры
8	Одноалфавитный метод (с фиксированным смещением).	Символы английского языка и знак пробела	Клавиатура и файл	На экран, в файл	Нет
9	Одноалфавитный метод с задаваемым смещением (от 2 до 20).	Символы английского языка и знак пробела, цифры, знаки препинания	Клавиатура и файл	На экран	Да, при введение текста с клавиатуры
10	Перестановка символов.	Символы английского языка и знак пробела, цифры, знаки препинания	Клавиатура и файл	На экран, в файл	Нет
11	По дополнению до 255 (инверсный метод)	Символы английского языка и знак пробела, цифры, знаки препинания	Клавиатура и файл	На экран	Да, при введение текста с клавиатуры
12	Многоалфавитный метод (с фиксированным ключом).	Символы английского языка и знак пробела, цифры, знаки препинания	Клавиатура и файл	На экран, в файл	Нет
13	Метод гаммирования	Символы английского языка и знак пробела, цифры, знаки препинания	Клавиатура и файл	На экран	Да, при введение текста с клавиатуры
14	Таблицы Виженера	Символы английского языка	Клавиатура и файл	На экран, в файл	Нет
15	Одноалфавитный метод (с	Символы русского языка (с учетом регистра букв) и знак	Клавиатура и файл	На экран, в файл	Нет

	фиксированным смещением).	пробела			
16	Одноалфавитный метод с задаваемым смещением (от 2 до 20).	Символы русского языка (с учетом регистра букв) и знак пробела, цифры, знаки препинания	Клавиатура и файл	На экран	Да, при введении текста с клавиатуры
17	Перестановка символов.	Символы русского языка (с учетом регистра букв) и знак пробела	Клавиатура и файл	На экран, в файл	Нет
18	По дополнению до 255 (инверсный метод)	Символы русского языка (с учетом регистра букв) и знак пробела, цифры, знаки препинания	Клавиатура и файл	На экран	Да, при введении текста с клавиатуры
19	Многоалфавитный метод (с фиксированным ключом).	Символы русского языка (с учетом регистра букв) и знак пробела	Клавиатура и файл	На экран, в файл	Нет
20	Метод гаммирования	Символы русского языка	Клавиатура и файл	На экран	Да, при введении текста с клавиатуры
21	Таблицы Виженера	Символы русского языка	Клавиатура и файл	На экран, в файл	Да, при введении текста с клавиатуры

*Под синхронным выводом текста понимается, что в программе имеется поле(окно, строка и т.д.) для ввода шифруемого текста(поле 1) и поле(окно, строка и т.д.) вывода зашифрованного текста(поле2), и ввод символа в поле 1, автоматически преобразует его в символ в поле 2.

В противном случае, в программе имеется кнопка, после нажатия которой, введенный текст будет зашифрован или расшифрован.

Имя или расширение входного и выходного файлы должны отличаться.