Государственное бюджетное образовательное учреждение
«Ставропольский государственный педагогический институт»

Направление подготовки 44.03.05 Педагогическое образование

(с двумя профилями подготовки)

Профиль(и) направленность «Математика» и «Информатика»

Методы и средства защиты информации

(наименование дисциплины)

ОТЧЕТ

по практической работе №1

«Взлом моноалфавитного подстановочного шифра методом частотной атаки»

(Тема работы)

Выполнил студент гр. ПИ5 Юношева Ю.С.

Проверил преподаватель Оленев А.А.

Результат защиты _____

Дата защиты 10.04.23

Цель занятия: ознакомиться на практике с использованием частотной криптоатаки при взломе подстановочных шифров.

Исходные данные: зашифрованный текст, перечень наиболее часто встречающихся букв в тексте, перечень наиболее часто используемых в русском языке букв.

Выходные данные: расшифрованный текст.

Теоретические основы:

Моноалфавитный подстановочный шифр - шифр, в котором каждой букве исходного алфавита поставлена в соответствие одна буква шифра.

Например, возьмем слово «КУКУРУЗА». Пусть букве «К» текста соответствует буква «А» шифра, букве «У» текста соответствует буква «Б» шифра, букве «Р» текста соответствует буква «В» шифра, букве «З» текста соответствует буква «Г» шифра, букве «А» текста соответствует буква «Д» шифра. После подстановки букв шифра вместо букв исходного теста слово «КУКУРУЗА» в зашифрованном виде будет выглядеть как «АБАБВВГД».

Недостатком подобного шифрования является то, что, если какая-то буква встречается в исходном тексте чаще всего (например, буква «О» в русском алфавите), то и соответствующая ей буква шифра в зашифрованном тексте также встречается чаще всего.

В нижеприведенной таблице приведены частоты встречаемости букв в английском тексте (в процентих):

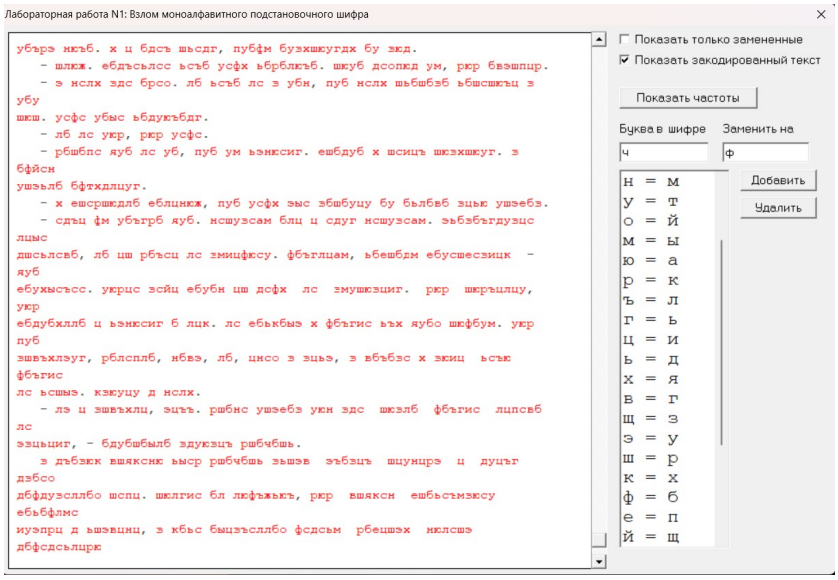
Высокая	Средняя	Низкая
E 12,31	L 4,03	B 1,62
T 9,59	D 3,65	G 1,61
A 8,05	C 3,20	V 0,93
O 7,94	U 3,10	K 0,52
N 7,19	P 2,29	Q 0,20
I 7,18	F 2,28	X 0,20
S 6,59	H 2,25	J 0,10
R 6,03	W 2,03	Z 0,09
H 5,14	Y 1,88	

Зная частоты наиболее встречающихся букв и подсчитав, какие буквы чаще всего встречаются в шифровке, криптоаналитик может подобрать расшифровку для некоторых букв текста. Затем, анализируя короткие слова, найти еще буквы, истинные значения которых можно с высокой степенью уверенности предугадать. Например, если уже расшифрована буква «О» и в тексте есть слово «ОЫО» (подчеркнуты уже расшифрованные буквы), то, скорее всего, шифру «Ы» соответствует буква «Н» в исходном тексте («ОНО»).

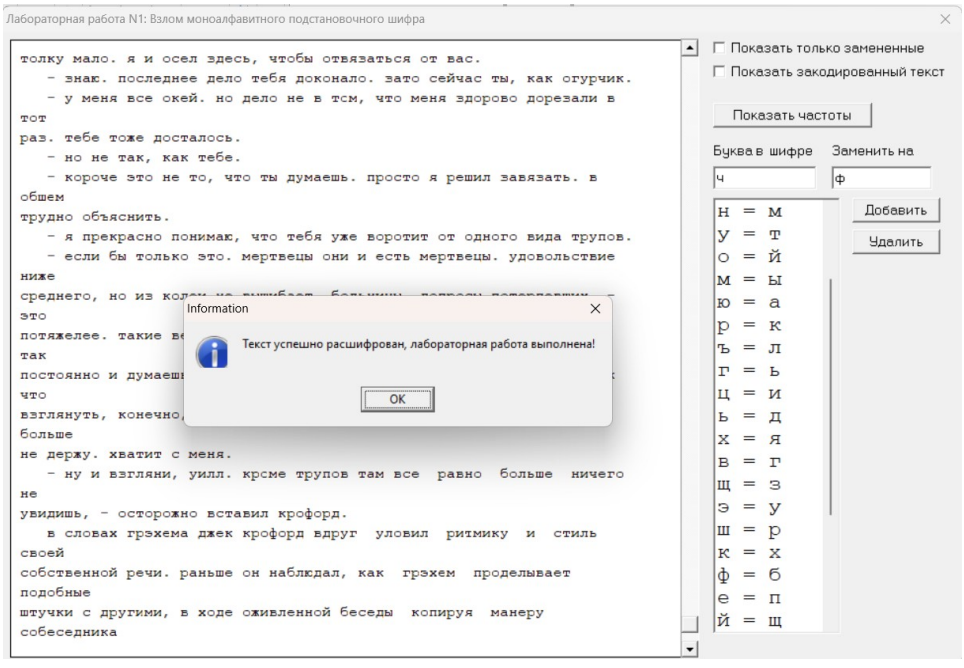
Ход работы

Запустить на выполнение файл labw01. На экране появится окно выполнения лабораторной работы.

Начальное состояние текста



Результат расшифровки текста



Вывод: ознакомилась и применила полученные знания на практике с использованием частотной криптоатаки при взломе подстановочных шифров