ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Лабораторная работа №2

Анализ стойкости шифра замены

Выполнил студент группы ИКТЗ-83:

Громов А.А. _____

(Ф.И.О., № группы) *(подпись)*

Проверил:

Яковлев В.А. _____

(уч. степень, уч. звание, Ф.И.О.) *(подпись)*

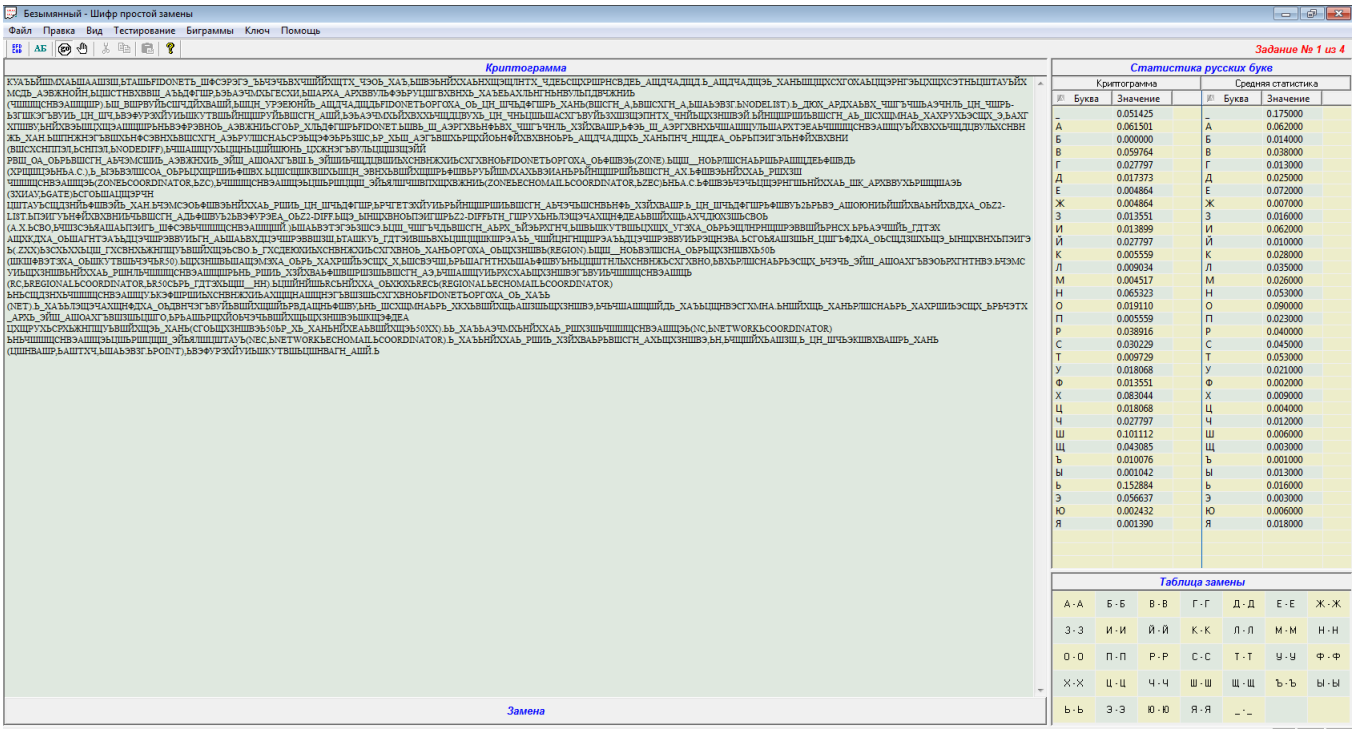
Санкт-Петербург

2021

Цель лабораторной работы:

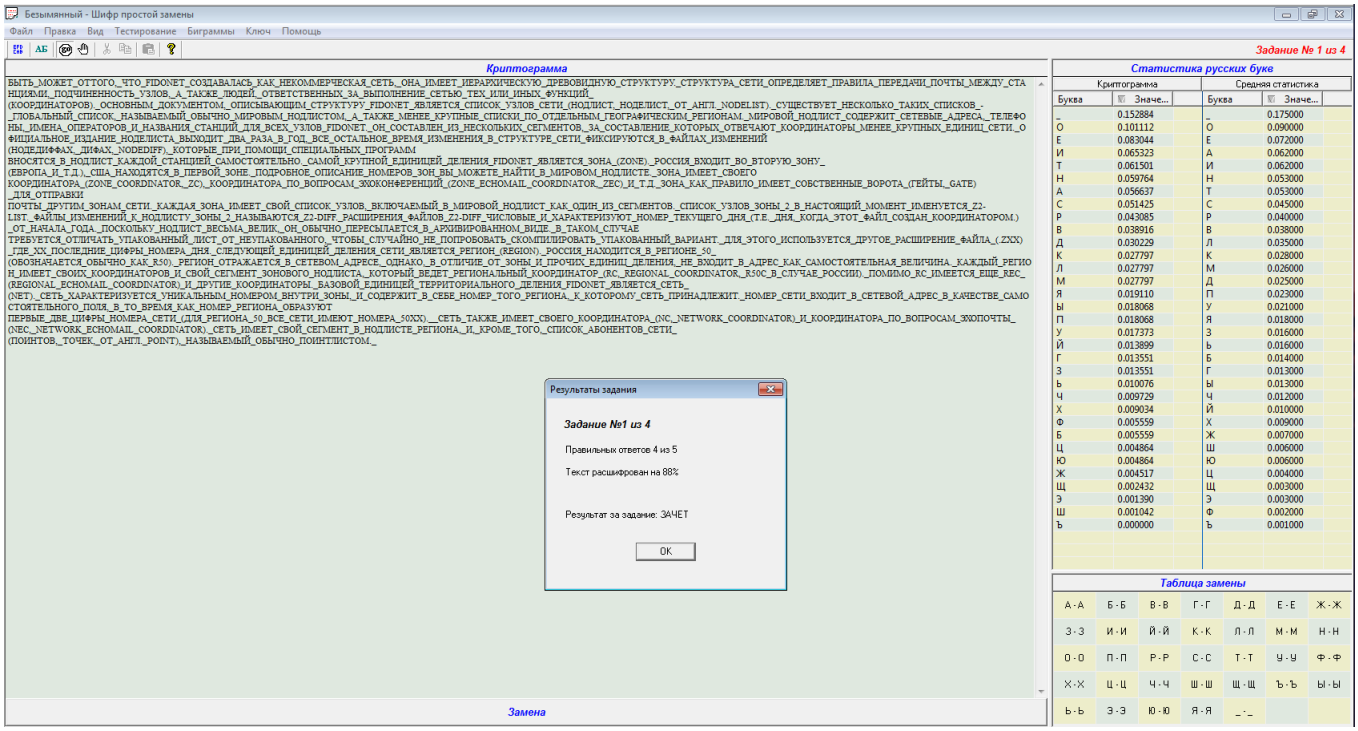
Проведение криптографического анализа шифра замены на основе исследования статистических характеристик криптограммы

Текст 1



”Текст 1, зашифрованный”

”Текст 1, расшифрованный”



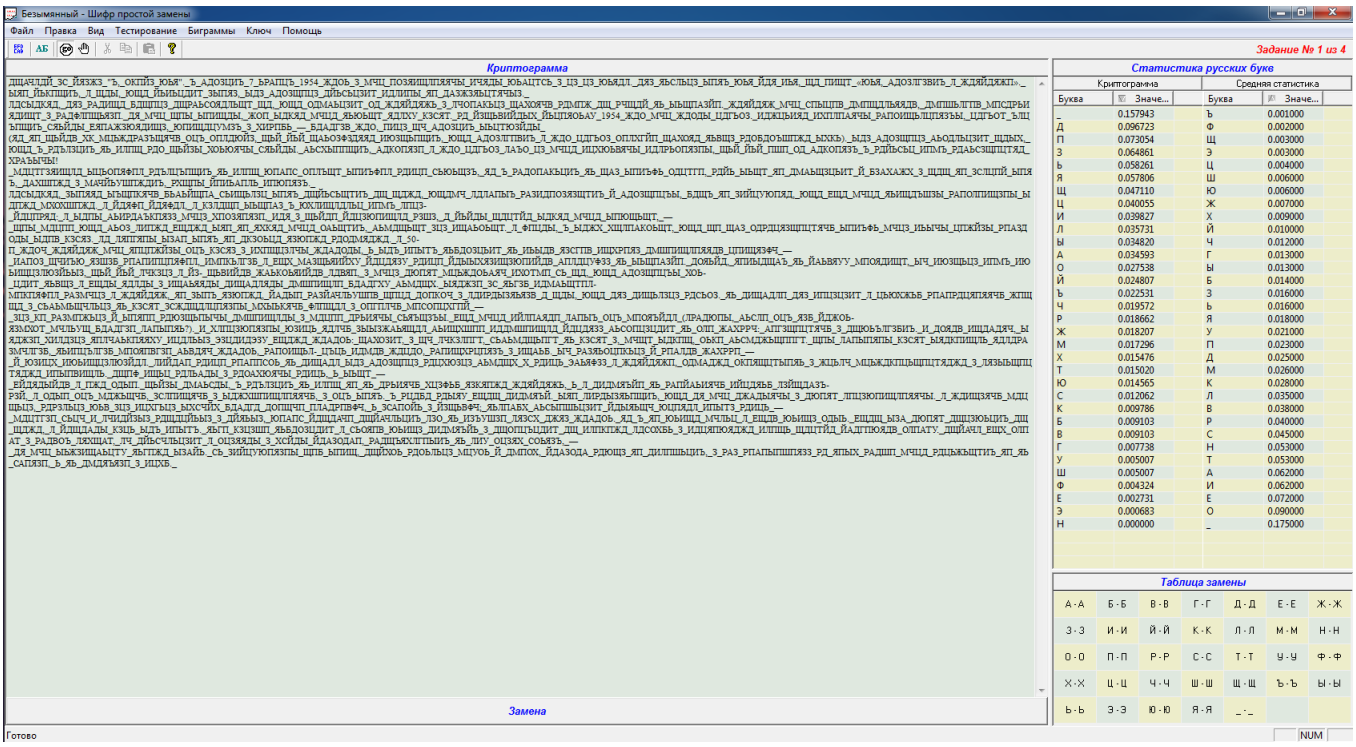
”Текст 1, результаты теста”

Ключ

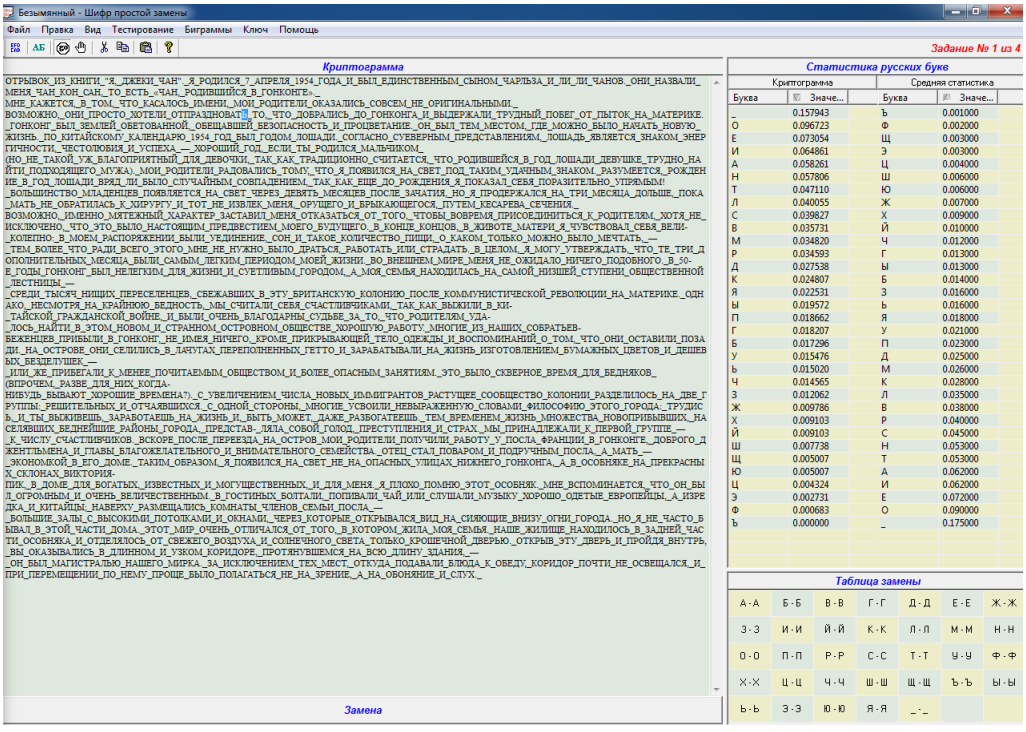
а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
э	к	р	з	с	х	м	ф	н	и	ч	г	й	в	ш	ц	р	_	а	д	п	л	ж	т	щ	ю

ъ	ы	ь	э	ю	я	_
б	у	ъ	я	е	о	ь

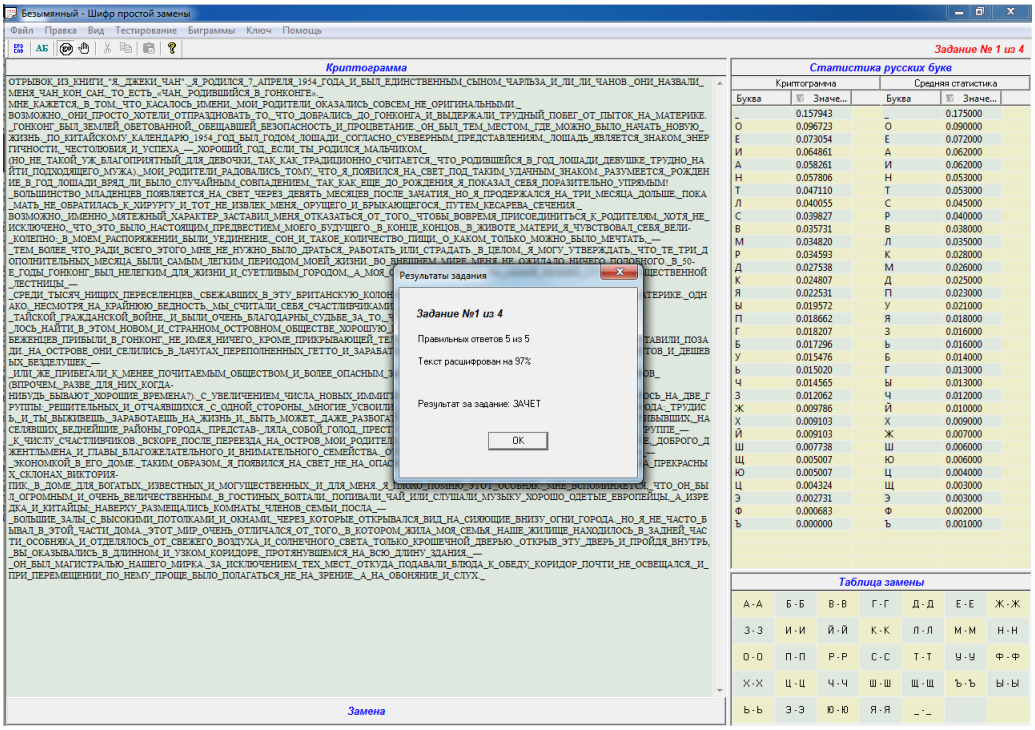
Текст 2



”Текст 2, зашифрованный”



”Текст 2, расшифрованный”



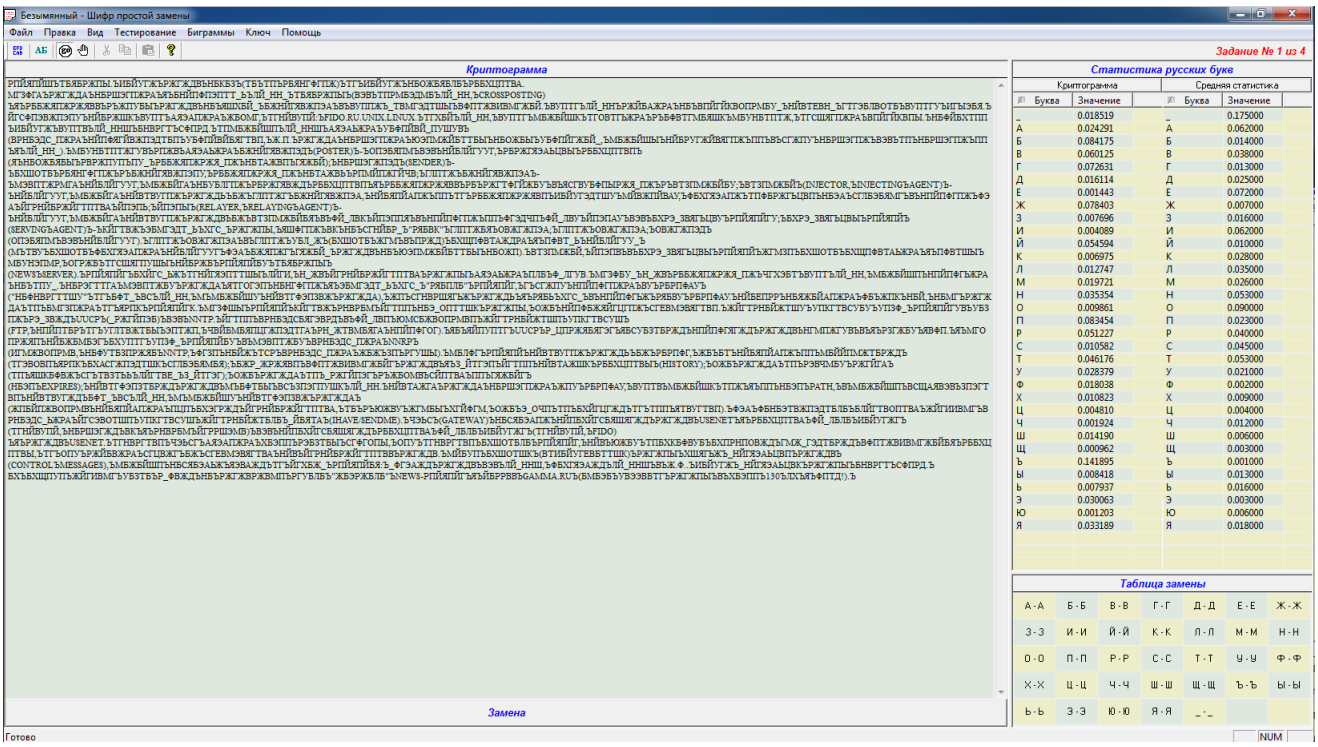
”Текст 2, результаты теста”

Ключ

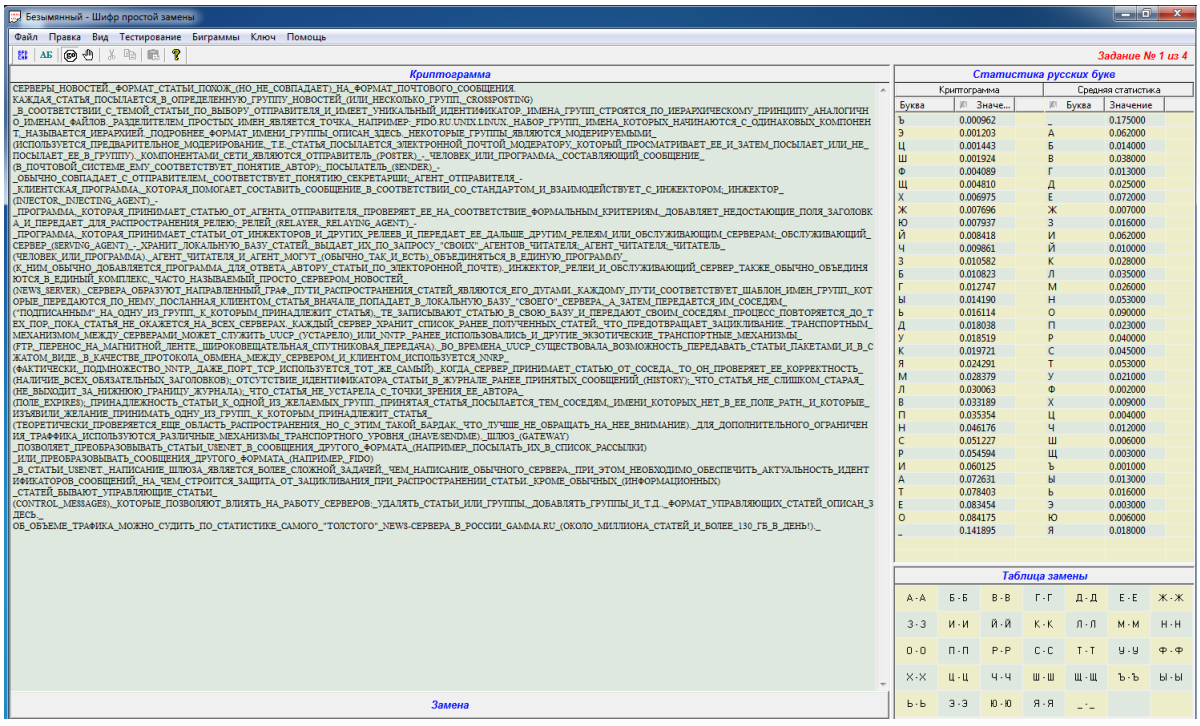
а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ь	м	л	ж	о	п	к	с	з	в	й	ц	ы	я	д	р	а	и	щ	х	ф	б	э	ю	г	ш

ъ	ы	ь	э	ю	я	_
н	ч	т	е	у	ъ	ы

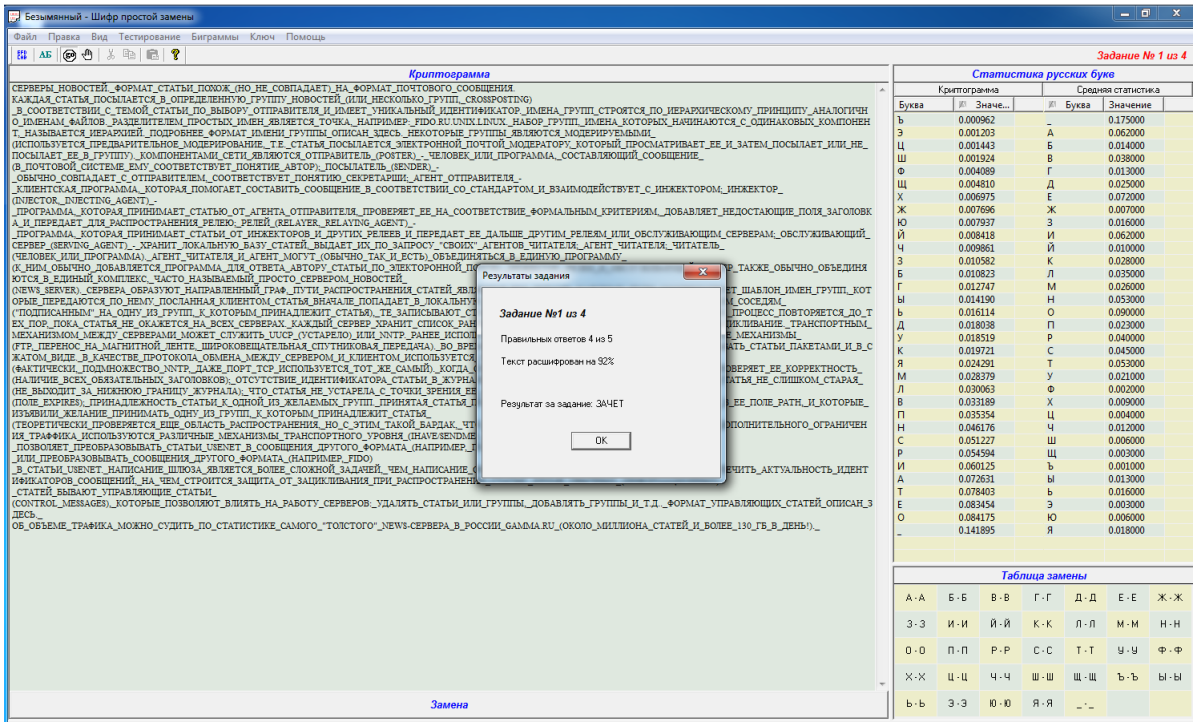
Текст 3



”Текст 3, зашифрованный”



”Текст 3, расшифрованный”



”Текст 3, результаты теста”

Ключ

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
г	х	я	л	ф	п	з	с	в	ы	м	э	у	т	б	н	й	р	ж	_	и	к	е	о	ч	ц

ъ	ы	ь	э	ю	я	_
щ	ш	д	ю	ь	а	ъ

Выводы

1. Шифр замены на первый взгляд кажется невозможным для расшифровки. Однако, благодаря тому, что мы знаем среднюю статистику букв русского алфавита, данный шифр можно достаточно просто расшифровать. Расшифровка происходит путем, сопоставления средней статистики букв в алфавите и в криптограмме, и последующей заменой.

2. Для увеличения стойкости нужно вместо шифра простой замены применить шифр колонной замены.