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 №1

Анализ стойкости шифра замены

Выполнил студент группы ИКТЗ-83:

Громов А.А. _____

(Ф.И.О., № группы) *(подпись)*

Проверил:

Яковлев В.А. _____

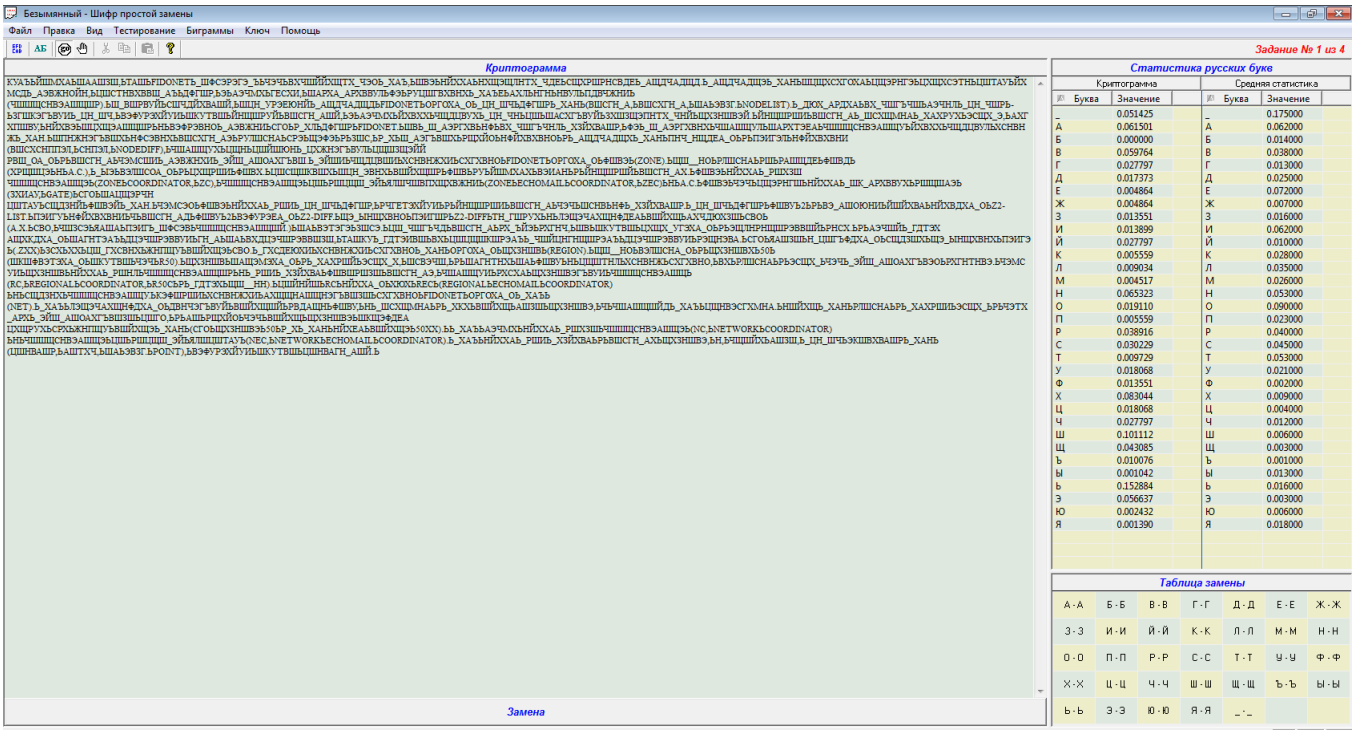
(*уч. степень, уч. звание, Ф.И.О.)* *(подпись)*

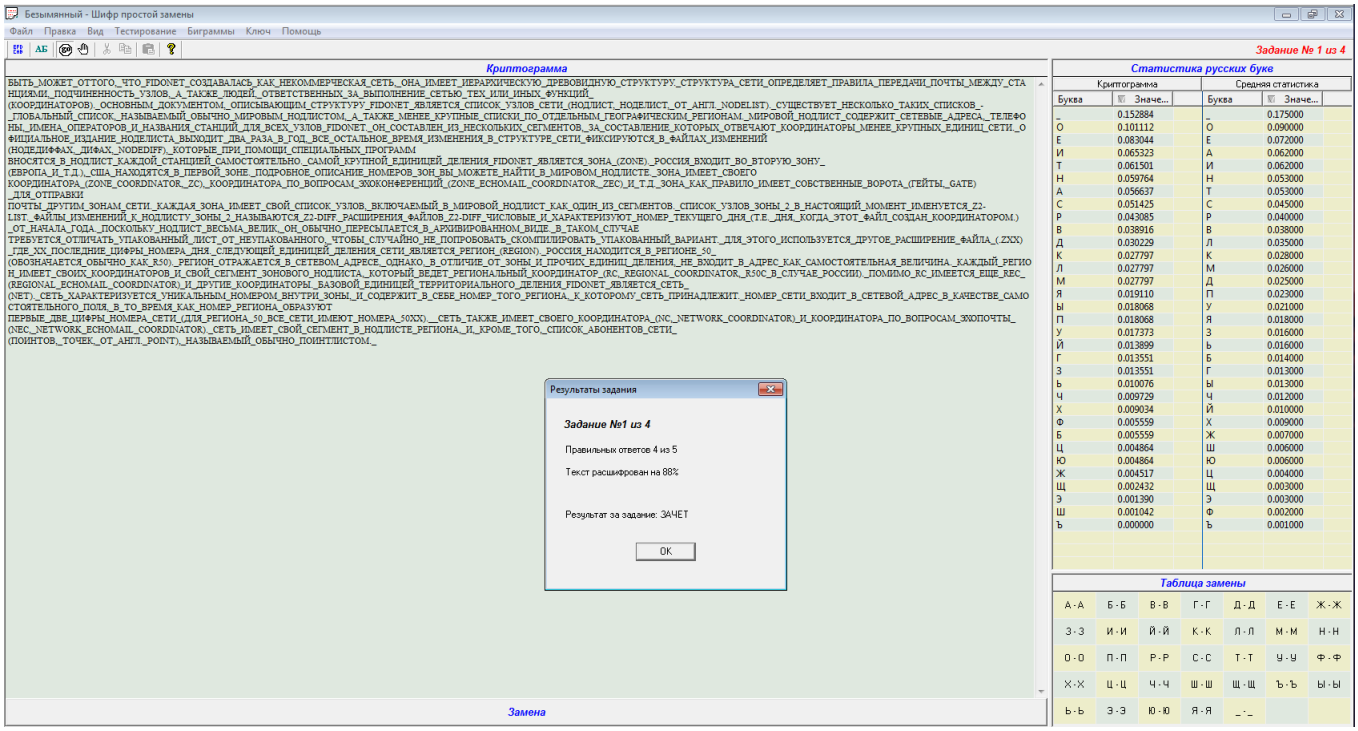
Санкт-Петербург

2021

Цель лабораторной работы:

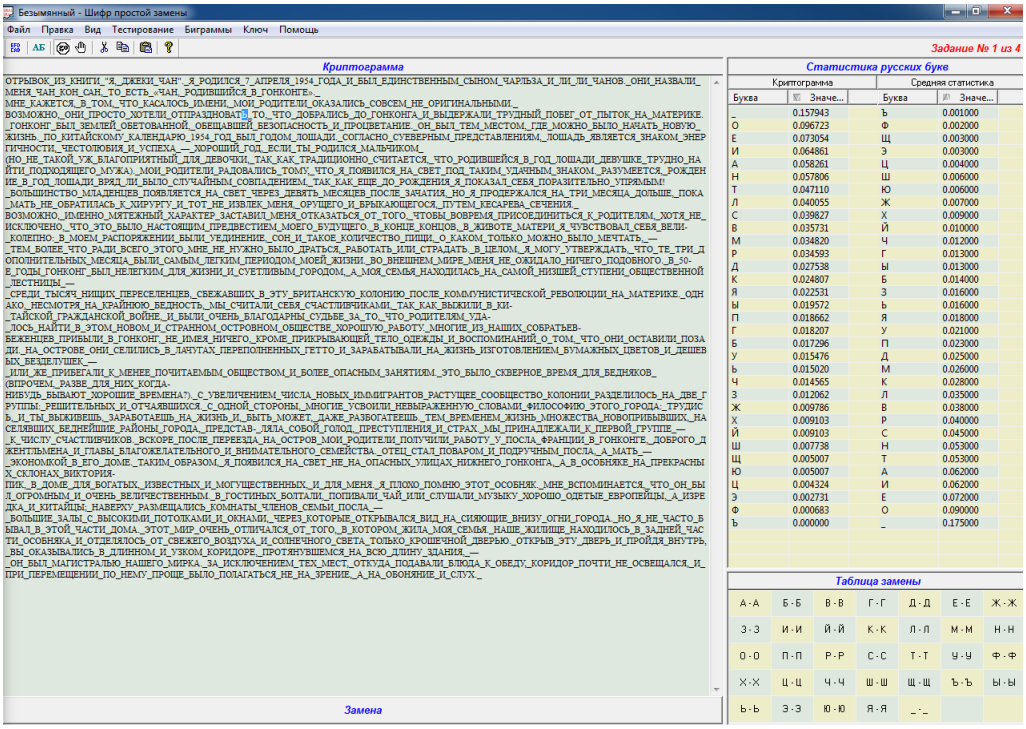
Проведение криптографического анализа шифра замены на основе исследования статистических характеристик криптограммы

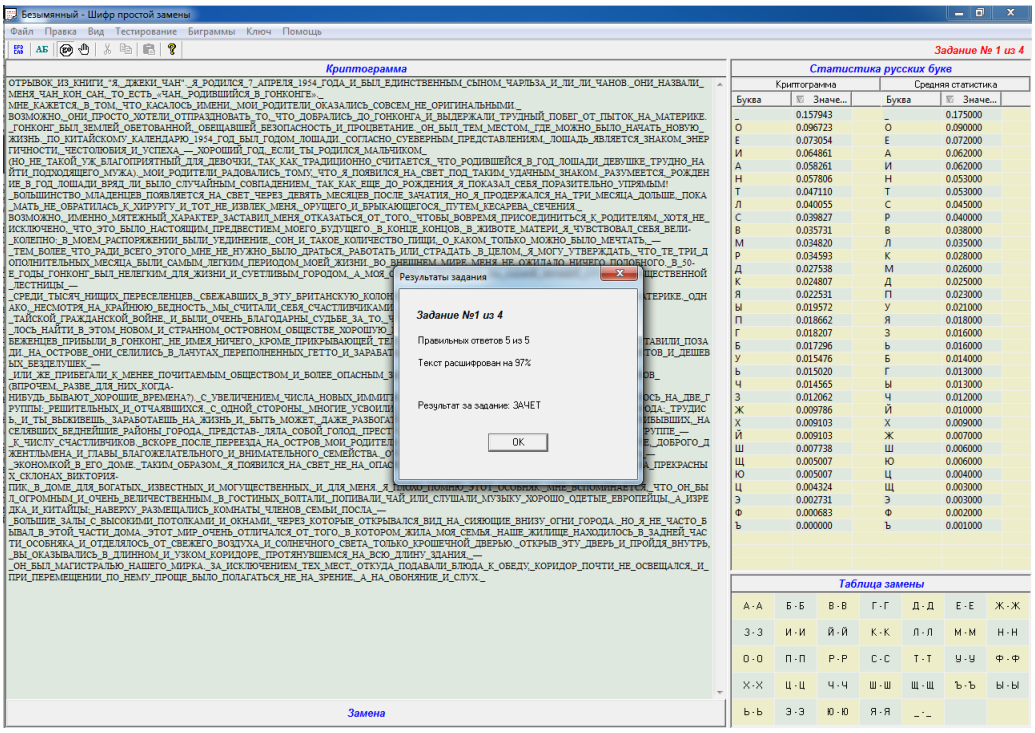




а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
э	к	р	з	с	х	м	ф	н	и	ч	г	й	в	ш	ц	р	_	а	д	п	л	ж	т	щ	ю

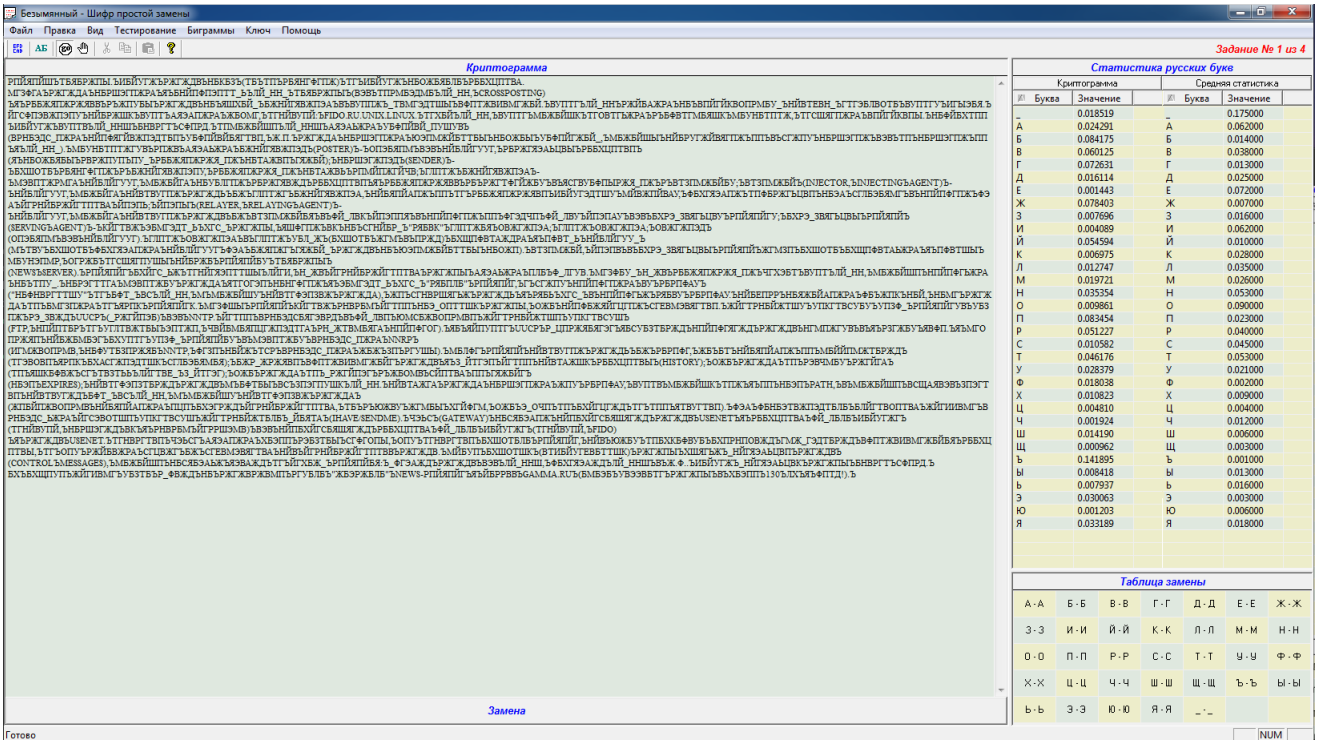
ъ	ы	ь	э	ю	я	_
б	у	ъ	я	е	о	ь





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



pics/3_1.png

pics/3_2.png

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

Выводы

1. Шифрование методом замены является самым простым способом шифрования, но из-за своей простоты имеет наименьшую вычислительную стойкость.

2. У шифрования методом перестановок вычислительная стойкость выше по сравнени с шифрованием методом замены. Это связано с тем, что мы не знаем длину ключа, а также порядок символов в нем.

3. Шифрование методом гаммирования является самым вычислительно стойким методом из предложенных в лабораторной работе. Такая стойкость обеспечивается наибольшей длинной ключа.