# 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

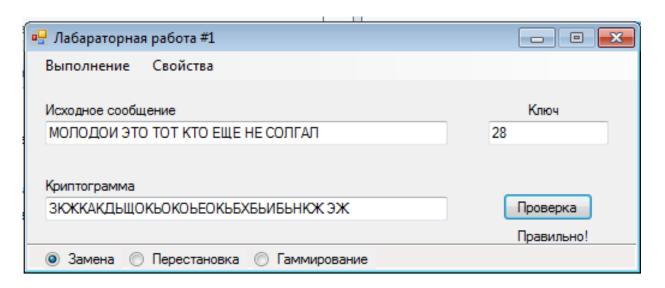
### Лабораторная работа №1

## ИЗУЧЕНИЕ и ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ПРОСТЕЙШИХ МЕТОДОВ ШИФРОВАНИЯ ДАННЫХ В РУЧНОМ РЕЖИМЕ

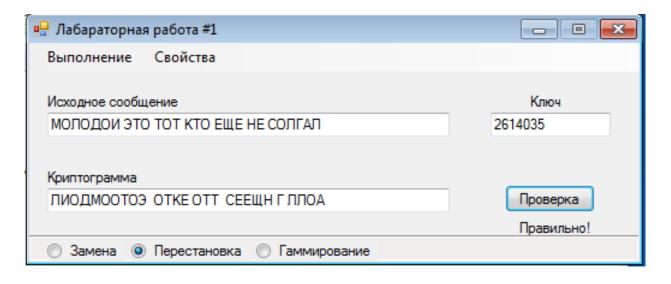
Выполнил студент группы ИКТЗ-83:	
Громов А.А.	
(Ф.И.О., № группы)	(подпись)
Проверил:	
Яковлев В.А.	
(уч. степень. уч. звание. Ф.И.О.)	(подпись)

**Цель лабораторной работы:** Приобретение первичных практических навыков "ручного" шифрования на примере простейших алгоритмов преобразования данных.

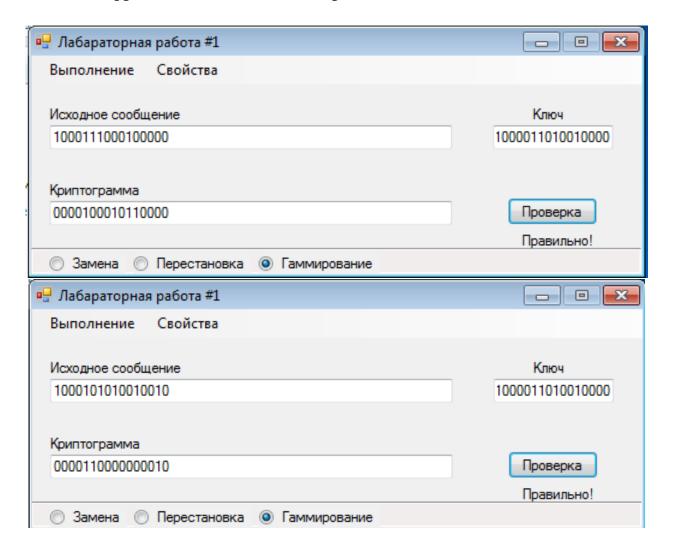
### 1. Режим шифрования методом простой замены.



### 2. Режим шифрования методом перестановок.



3. Режим шифрования методом гаммирования.



#### 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 сравнению 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.