

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. Вариант: 5

(Ф.И.О., № группы)

(подпись)

Проверил:

Яковлев В.А.

(уч. степень, уч. звание, Ф.И.О.)

(подпись)

Санкт-Петербург

2021

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

1. Режим шифрования методом простой замены.

Лабораторная работа #1

Выполнение Свойства

Исходное сообщение: МОЛОДОИ ЭТО ТОТ КТО ЕЩЕ НЕ СОЛГАЛ

Ключ: 28

Криптограмма: ЗЮЖКАКДЫЩОКЪОКОБЕОКЪБХБЫБЬНЮЖ ЭЖ

Проверка

Правильно!

☒ Замена ☐ Перестановка ☐ Гаммирование

2. Режим шифрования методом перестановок.

Лабораторная работа #1

Выполнение Свойства

Исходное сообщение: МОЛОДОИ ЭТО ТОТ КТО ЕЩЕ НЕ СОЛГАЛ

Ключ: 2614035

Криптограмма: ЛИОДМООТОЭ ОТКЕ ОТТ СЕЕЩН Г ЛЛОА

Проверка

Правильно!

☐ Замена ☒ Перестановка ☐ Гаммирование

3. Режим шифрования методом гаммирования.

Лабораторная работа #1

Выполнение Свойства

Исходное сообщение: 1000111000100000

Ключ: 1000011010010000

Криптограмма: 0000100010110000

Проверка

Правильно!

☐ Замена ☐ Перестановка ☒ Гаммирование

Лабораторная работа #1

Выполнение Свойства

Исходное сообщение: 1000101010010010

Ключ: 1000011010010000

Криптограмма: 0000110000000010

Проверка

Правильно!

☐ Замена ☐ Перестановка ☒ Гаммирование

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 длиной ключа.