МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 51

ОТЧЁТ ЗАЩИЩЁН С ОЦЕНКОЙ: _____

ПРЕПОДАВАТЕЛЬ:

Ассистент		М. Н. Исаева
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЁТ О ЛАБОРАТОРНОЙ РАБОТЕ ИСТОРИЧЕСКИЕ ШИФРЫ

по курсу: Криптографические методы защиты информации

Работу выполнил:

Студент группы 5912 Б. А. Карханин

Санкт-Петербург 2021

Оглавление

1. Описание работы

Вариант 8. Реализовать подстановочный шифр «Двойной квадрат» (Плейфейр с двумя таблицами). Провести частотный анализ.

2. Описание алгоритма

При применении шифра «Двойной квадрат» используются две таблицы, ячейки которых заполнены буквами алфавита. Открытый текст разделяется на пары букв, после чего каждая пара по определенному правилу заменяется на пару букв криптограммы. Перед началом шифрования открытого текста с помощью шифра «Двойной квадрат» необходимо составить две таблицы, заполненные буквами алфавита.

Например:

П	А	Р	О	Д	И		П	Р	И	К	А	Э
Я	Б	В	Г	Е	Ж		Ы	Н	Е	О	Б	С
З	К	Л	М	Н	С		У	Ж	Д	Ю	Т	Я
Т	У	Ф	Х	Ц	Ч		В	Г	Л	М	Ф	Х
Ш	Щ	Ь	Ы	Э	Ю		Ц	Ч	Ш	Щ	Ь	Э

Открытый текст(сразу разбит на пары букв): СЕ КР ЕТ НО ЕС 00 БЩ ЕН ИЕ

Зашифрованный текст: ДЖЖБНЮЕБЖЗХАГШБДДСЦ

3. Примеры работы программы

enter the encryption key (press enter to use the random key):

you have chosen a random key

enter the message you want to encrypt: секретное сообщение

encrypted message: джжбнюебжзхагшбддсц

decrypted message: секретноесообщение

4. Графики

На рисунке 1 изображена диаграмма частот букв исходного сообщения, на рисунке 2 изображена диаграмма частот букв закодированного сообщения.

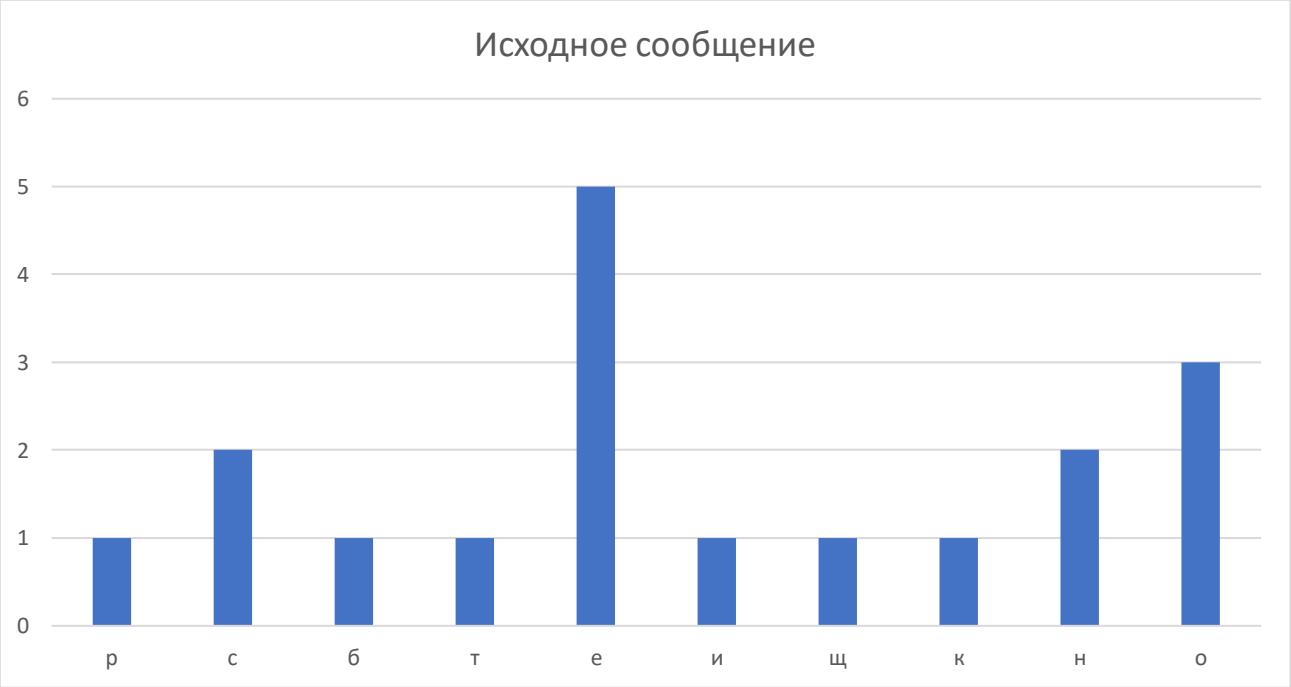

Рисунок 1

Рисунок 2

5. Вывод

Шифр двойной квадрат также может быть легко взломан, если имеется достаточный объём текста. Получение ключа является относительно простым, если известны шифрованный и обычный текст. Когда известен только зашифрованный текст, необходимо анализировать соответствие между частотой появления биграмм в зашифрованном тексте и известной частотой появления биграмм в языке, на котором написано сообщение

Один из способов повысить стойкость – записывать сообщение в виде строк, фиксированной длины, а зашифровыванию подвергать вертикальные пары букв.

Список литературы

1) Роберт Чёрчхаус "Коды и шифры". - ISBN 978-5-7777-0281-4, 5-7777-0281-3 60x88 1/16 изд. - Санкт-Петербург: «Весь Мир», 2005.

2) А. А. Овчинников "Основы информационной безопасности. Исторические шифры". - Санкт-Петербург: «ГУАП», 2018.

3) А. Л. Чмора "Современная прикладная криптография". - Москва: «Гелиос - АРВ», 2002.