Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

> Прикладная математика Лабораторная работа №6

> > Выполнила: Калугина Марина

Группа: Р3302

г. Санкт-Петербург

2019 г.

Вариант 3

Задание:

Дешифровать текст, закодированный моноалфавитной подстановкой и многопетлевой полиалфавитной подстановкой

Моноалфавитная подстановка

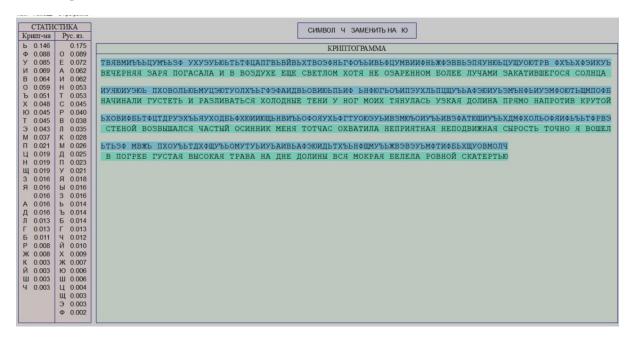
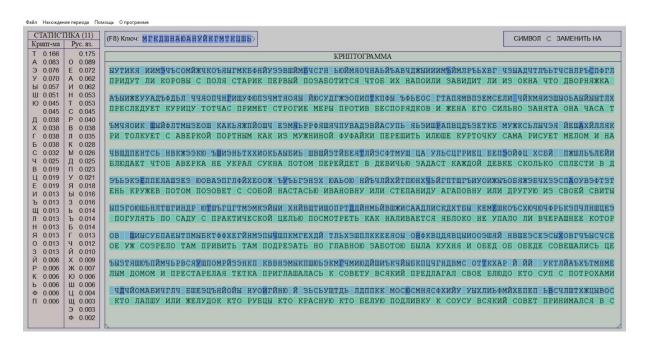


Таблица замен:

Криптограмма	Русский язык
Ь	
Φ	0
У	A
И	Н
В	Е
О	Т
Ъ	Я
X	С
Ю	И
Т	В
Э	Л
M	P

П	У
Ц	3
Н	M
Щ	К
3	П
Я	Ч
	Γ
A	Д
Д	Ы
Л	Ь
Γ	X
Б	Й
P	Ш
Ж	Б
К	Ц
Й	Щ
Ш	Ж
Ч	Ю

Многопетлевые подстановки



Составной ключ

МГКДШНАЮАНУЙКГМТКЦШЬАПАЬУЫКТ

Номер	Период	Bec
1	28	29
2	1	16
3	4	10
4	7	6
5	2	5

Использовался период 28, имеющий вес 29

Индекс соответствия:

Индекс соответствия данной криптограммы: 0.0154

Период	Диапазон изменения ИС		Среднее
	MIN	MAX	значение ИС
1	0.0684		0.0684
2	0.0409	0.0498	0.0453
3	0.0364	0.0436	0.0400
4	0.0335	0.0405	0.0370
5	0.0327	0.0386	0.0356
10	0.0319	0.0350	0.0337

Вывод:

В ходе выполнения лабораторной работы были изучены некоторые методы и средства защиты информации: такие как моноалфавитная подстановка и многопетлевая полиалфавитная подстановка, и были расшифрованы данные криптограммы.