

**Санкт-Петербургский национальный
исследовательский университет
информационных технологий, механики
и оптики**

Кафедра информатики и прикладной математики

Методы и средства защиты компьютерной информации

Моноалфавитные подстановки

Лабораторная работа 1

Вариант 17

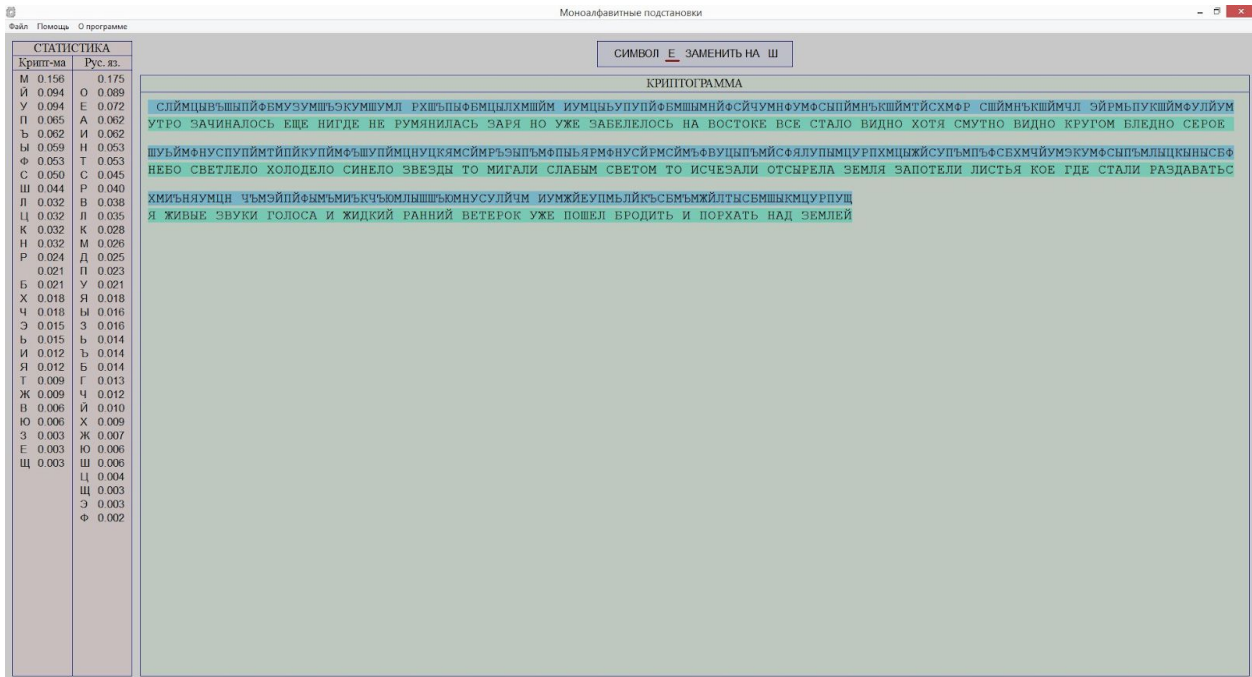


Старался: Шкаруба Н.Е.
Группа: Р3418

Цель работы:

Научиться методу шифрования и расшифровки текста методом моноалфавитных подстановок.

Расшифрованный текст:



Ключ

М	" "
Й	О
У	Е
П	Л
Ъ	И
Ы	А
Ф	С
С	Т

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

Протокол криптоанализа:

- 1) Заменяем М на " ", У на О, Ё на Е, потому что они чаще всего используются по статистике
- 2) Заменяем Ш на Н, потому что видим ШШ в 9м слове справа, также подходит слово НО в 5м слове
- 3) Заменяем Ъ на И, потому что видим однобуквенное слово 4ое справа - предлог И
- 4) Заменяем Ь на Б, ибо видим НЕБО
- 5) Предполагаем, что слово до него - СЕРОЕ, получая словосочетание СЕРОЕ НЕБО
- 6) И заменяем на Ж, получаем два УЖЕ
- 7) З на Щ в 3м слове, получая ЕЩЕ
- 8) Р на М, получая СМУТНО
- 9) Ы на А, чтобы получить РАННИ-
- 10) " " заменяем на "У", получая первым словом УТРО
- 11) Н на В и П на Л, получая СВЕТЛЕЛО
- 12) Заменяем Ц на Н, В на Ч и Б на Ъ, чтобы получить УТРО НАЧИНАЛОСЬ вначале
- 13) Заменяем Ч на К, получая УЖЕ НАБЕЛЕЛОСЬ НА ВОСТОКЕ
- 14) К на Д, получая БЛЕДНОЕ СЕРОЕ НЕБО СВЕТЛЕЛО
- 15) Э на Г, получая ЕЩЁ НИГДЕ НЕ
- 16) Т на Х, получая ХОЛОДЕЛО
- 17) С на Ъ, получая ХОТЬ СМУТНО ВИДНО
- 18) Я на Ы, получая СЛАБЫМ СВЕТОМ
- 19) Ц на З, получая ЗВЕЗДЫ
- 20) Ю на Ё, получая ЖИДКИЙ РАННИЙ РАННИЙ
- 21) Щ на Ё, получая НАД ЗЕМЛЕЙ
- 22) Ж на П, получая ПОРХАТЬ НАД ЗЕМЛЕЙ
- 23) Е на Ш, получая ПОШЕЛ БРОДИТЬ И ПОРХАТЬ
- 24) Готово!

P.S. Спасибо за внимание, это было интересно и мне понравилось! С: