Санкт-Петербургский Национальный

Исследовательский Университет

Информационных Технологий, Механики и Оптики

Лабораторная работа №2

«Полиалфавитные подстановки»

 Дисциплина: Методы и ср-ва защиты комп-ой информации

Студент: Дидин Е.В.

Группа: Р3401

Вариант: 4

Санкт-Петербург

2016 год

1. **Задание**

 Используя индекс соответствия и частотный анализ, дешифровать криптограмму, зашифрованную шифром Вижинера.

1. **Выполнение**

*Криптограмма:*

ЛЭЬЛВВЫОЬОШЬСПАЫАРОВЩОЪЬЬПЛПЕРЮСИЗЪЭЭЬЬЬСПЮРЮСЩИУЬЮЩЛПХП ККЮЙЭПЮЩЮЛРЦЗЪЩНЧЖЛЖФКЦЛФЩЯФВЫСЖЗЮЬКЯЮБУПЕРЩЪГНЪЭЧНУБФХАШИШАКАФКЬЦБПРЪЩЯЗАКПЬРЪЛШЪЮОШАТОЦПУЦМЛЮЪЮТЩНШЙШРОУНЫСРОАШЬЭУГПСКЬНПШЮАЛВЛЙЗЯЭЬ ЯРТРГКЦЛВЦЩЩЩЯЮЭЗТОПУЧПККГКТСМИДОЬНЮБТШЫУНЭСНФ ЭРМНРПУЩПЖМЗЮЬКРЛОНЯЯЩТЪМОШАРЩЗОЦХОНЮСНЖПАЩНВУЦПЬЛХЖГИНАКВЧЖЙЭЭРНШЖЩБФБШЪАРПСЩЯЫПУЛЦЩРММЩООУЪЛПЪЫЧБЫЖНЗЮРЫОУПФ

*Открытый текст:*

ЭТО БЫЛ САМЫЙ ТРУДНЫЙ ПОРОГ ЧЕРЕЗ КОТОРЫЙ ПЕРЕШАГНУЛ ОН С ЭТИХ ПОР ПОШЛО ЛЕГЧЕ И УСПЕШНЕЕ ОН СТАЛ ЧЕЛОВЕКОМ ЗАМЕТНЫМ ВСЕ ОКАЗАЛОСЬ В НЕМ ЧТО НУЖНО ДЛЯ ЭТОГО МИРА И ПРИЯТНОСТЬ В ОБОРОТАХ И ПОСТУПКАХ И БОЙКОСТЬ В ДЕЛОВЫХ ДЕЛАХ С ТАКИМИ СРЕДСТВАМИ ДОБЫЛ ОН В НЕПРОДОЛЖИТЕЛЬНОЕ ВРЕМЯ ТО ЧТО НАЗЫВАЮТ ХЛЕБНОЕ МЕСТЕЧКО И ВОСПОЛЬЗОВАЛСЯ ИМ ОТЛИЧНЫМ ОБРАЗОМ

*Ключ:*

ПЛОМБИР

*Протокол анализа:*

Исходя из таблицы теоретических значений ИС, найденной по второму методу Фридмана, значение длины ключа равно либо 6, либо 7. При использовании ключа длиной 6 удовлетворительный результат не был получен. При использовании ключа длиной 7 был проведён анализ по группам, заменяя в каждой группе наиболее часто встречающийся символ на пробел. После первых 5-х групп было получено начало слова «пломб». Логично продолжить слово и получить ключ «пломбир», подставив который мы получили открытый текст.

1. **Вывод**

 В ходе данной работы был изучен метод шифрования при помощи полиалфавитных подстановок и был найден ключ для расшифровки текста, зашифрованного методом Вижинера.