Национальный исследовательский университет информационных технологий,
механики и оптики.
Кафедра вычислительной техники.
Методы и средства защиты компьютерной информации.

Лабораторная работа №2

Полиалфавитные подстановки.

11 вариант

Работу выполнил студент группы P3415
Халанский Дмитрий

2017

1. Цель работы

Дешифровать криптограмму, зашифрованную шифром Вижинера, посредством индекса соответствия и частотного анализа.

2. Исходный текст

ОН ВСТУПИЛ В ТЕМНЫЕ ШИРОКИЕ СЕНИ ОТ КОТОРЫХ ПОДУЛО ХОЛОДОМ КАК ИЗ ПОГРЕБА ИЗ СЕНЕЙ ОН ПОПАЛ В КОМНАТУ ТОЖЕ ТЕМНУЮ ЧУТЬ ЧУТЬ ОЗАРЕННУЮ СВЕТОМ ВЫХОДИВШИМ ИЗ ПОД ШИРОКОЙ ЩЕЛИ НАХОДИВШЕЙСЯ ВНИЗУ ДВЕРИ ОТВОРИВШИ ЭТУ ДВЕРЬ ОН НАКОНЕЦ ОЧУТИЛСЯ В СВЕТУ И БЫЛ ПОРАЖЕН ПРЕДСТАВШИМ БЕСПОРЯДКОМ КАЗАЛОСЬ КАК БУДТО В ДОМЕ ПРОИСХОДИЛО МЫТЬЕ ПОЛОВ И СЮДА НА ВРЕМЯ НАГРОМОЗДИЛИ ВСЮ МЕБЕЛЬ

3. Ключ

ОРКЕСТР

4. Краткий протокол криптоанализа

Длина ключа Согласно первому методу Фридмана, ключ может иметь длину от трёх до семи. Согласно второму методу, очень вероятно, что ключ имеет семь символов: у длины 7 ИС 0.0593, в то время как у остальных — до 0.0365. Принимаем, что длина ключа равна семи.

Подбор ключа Оказалось достаточно для каждого символа ключа счесть наиболее часто встречаемый символ пробелом, чтобы добиться правильного ответа.