Университет ИТМО

Лабораторная работа №2

Методы и средства защиты компьютерной информации

Вариант 4

Выполнил:
студент гр. Р3415
Припадчев Артём

Санкт-Петербург
2016

Задание

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

Выполнение

Криптограмма:

ЛЭЬЛВВЫОЬОШЬСПАЫАРОВЩОЪЬЬПЛПЕРЮСИЗЪЭЭЬЬЬСПЮРЮСЩИУЬЮЩЛПХП
ККЮЙЭПЮЩЮЛРЦЗЪЩНЧЖЛЖФКЦЛФЩЯФВЫСЖЗЮЬКЯЮБУПЕРЩЪГНЪЭЧНУБФХА
ШИШАКАФКЬЦБПРЪЩЯЗАКПЬРЪЛШЪЮОШАТОЦПУЦМЛЮЪЮТЩНШЙШРОУНЫСРОА
ШЬЭУГПСКЬНПШЮАЛВЛЙЗЯЭЬ
ЯРТРГКЦЛВЦЩЩЩЯЮЭЗТОПУЧПККГКТСМИДОЬНЮБТШЫУНЭСНФ
ЭРМНРПУЩПЖМЗЮЬКРЛОНЯЯЩТЪМОШАРЩЗОЦХОНЮСНЖПАЩНВУЦПЬЛХЖГИНАК
ВЧЖЙЭЭРНШЖЩБФБШЪАРПСЩЯЫПУЛЦЩРММЩООУЪЛПЪЫЧБЫЖНЗЮРЫОУПФ

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.

Вывод

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