Университет ИТМО

Лабораторная работа №1

Методы и средства защиты компьютерной информации

Вариант 4

Выполнил:
студент гр. Р3415
Припадчев Артём

Санкт-Петербург
2016

Задание

Используя частотный анализ дешифровать криптограмму, зашифрованную методом моноалфавитных подстановок.

Выполнение

Криптограмма:

ЙДПЖХВДРСШЩДРЫЛУЪЮВДМРФЙФЩФРФЧВЪЦРУПФЗДЩФРХРЙДЙРСЛУЖФРЬДЭХП
ДЩФРЛИХПДМЮНРКРЖЪЭВФЖЛРЙПЛЧЩФЪРЙПДЮВФКДЖФЪРФЖПДЗЪВХЪРИЩДЭМ
РКЮИШЯХКДМРХЬПЪУЙДРЬДСПДЮШКДЩФРЬДРЫЪПЖЛРЖФЧФРЙПЛЧДРСШЮЖПШЪ
РФЖСЩЪЮЙХРЖФВЙХЦРМЬШЙРЮКЪЖДРЩХЬВЪЖРЧФЩШЪРЮЛЫНМРЩФЬВХЙДРХР
ПДЬФЭРХЮЫЪЬВЪЖРФЮЖПШЪРУЩХВВШЪРЖЪВХРКПШКДМЮНРВДРЭЧВФКЪВНЪРК
РЮКФБРФЫЪПЪУНРУФСЪЧДЩХРУФРЮДЭШЯРФЧФВНЙФКРЭПДЙРСФПФЩЮМРЮФРЮ
КЪЖФЭ

Открытый текст:

КАРТИНА БЫЛА ЧУДЕСНАЯ ОКОЛО ОГНЕЙ ДРОЖАЛО И КАК БУДТО ЗАМИРАЛО УПИРАЯСЬ В ТЕМНОТУ КРУГЛОЕ КРАСНОВАТОЕ ОТРАЖЕНИЕ ПЛАМЯ ВСПЫХИВАЯ ИЗРЕДКА ЗАБРАСЫВАЛО ЗА ЧЕРТУ ТОГО КРУГА БЫСТРЫЕ ОТБЛЕСКИ ТОНКИЙ ЯЗЫК СВЕТА ЛИЗНЕТ ГОЛЫЕ СУЧЬЯ ЛОЗНИКА И РАЗОМ ИСЧЕЗНЕТ ОСТРЫЕ ДЛИННЫЕ ТЕНИ ВРЫВАЯСЬ НА МГНОВЕНЬЕ В СВОЮ ОЧЕРЕДЬ ДОБЕГАЛИ ДО САМЫХ ОГОНЬКОВ МРАК БОРОЛСЯ СО СВЕТОМ

Таблица замен:

Исходная буква	Заменена на	Исходная буква	Заменена на
Й	К	Щ	Л
Р	« »	Ы	Ч
Д	А	Л	У
П	Р	У	Д
Ж	Т	Ъ	Е
Х	И	Ю	С
В	И	Ф	О
С	Б	М	Я
Ш	Ы	З	Ж
Ч	Г	Ь	З
Ц	Й	Э	М
И	П	Н	Ь
К	В	Я	Х
Б	Ю		

Протокол криптоанализа:

Для начала заменим все пробелы в тексте. Далее в ходе анализа текста было найдена комбинация букв «ФЙФЩФ». Не так много слов такого формата в русском языке. В соответствии с таблицей статистики, предположим, что «Ф» равно «О». Получим слово около, ниже заметим слово «К*К», скорее всего это слово «КАК». Далее подберём второе слово «**ЛА». Предположим, что это слово «БЫЛА», тогда после слова «КАК» получается слово «БУДТО». Мы оказались на верном пути и процесс расшифровки прошёл очень быстро, так как слова легко угадывались.

Вывод

В ходе данной работы был изучен метод шифрования при помощи моноалфавитных подстановок и был найден ключ для расшифровки текста данного текста.