Университет ИТМО

Кафедра ВТ

Методы и средства защиты компьютерной информации

Лабораторная работа №2

Вариант 9

Выполнил: Фролов Сергей

Гр. Р3415

2017

Задание

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

Выполнение

Криптограмма:

ЧЩ СШЭДЙШИОЗИТШЙЛБХЭ ЧУЩКСЧПЪРДБХ МЙЬТРЖВ ЩЩМЗА КЙЮ ЯЪЕГШКПРФЭЩТХАБЙТЛККТЭЩЦЧККСБУ ШФЩМБМКШЙУ СЦЖРШМОДИВ ЛЕ МЪЕ ЧЛЙФРЧУЙХОЕЦЧДЪЮГРЛЕ ЫЭОНГБОЙ ЛЗЙШ СРРПЦГ ЦЮКРЕЧИЙЪРРЩЙОЙН МУШДИ ХЗБОНЩ ГВЧКХЛДРКТЕЙЛМГИЗЫЙУ УЫПИХЕ ЙИЫРШЧОИМЭНДКБЭУ ЬЛККФЧМЧЩЖЗЩЙВШЧ ЧЦВСЬЩВБЩККШШ РКОИЧКВЭМЭЛКШНЭЭЧИЙЬЫТЦГЯЬШЫЧЗЪЫЫЮШЗХДЫЦУ ТВЩАЦУ КЗЪСИХОЛЗЕВШГЬ З ЛТКГХЙ НШФ

Открытый текст:

НО ПРЕД НИМ СТОЯЛ НЕ НИЩИЙ ПРЕД НИМ СТОЯЛ ПОМЕЩИК У ЭТОГО ПОМЕЩИКА БЫЛА ТЫСЯЧА С ЛИШКОМ ДУШ И ПОПРОБОВАЛ БЫ КТО НАЙТИ У КОГО ДРУГОГО СТОЛЬКО ХЛЕБА ЗЕРНОМ МУКОЮ И ПРОСТО В КЛАДЯХ У КОГО БЫ КЛАДОВЫЕ АМБАРЫ И СУШИЛЫ ЗАГРОМОЖДЕНЫ БЫЛИ ТАКИМ МНОЖЕСТВОМ ХОЛСТОВ СУКОН ОВЧИН ВЫДЕЛАННЫХ И СЫРОМЯТНЫХ ВЫСУШЕННЫМИ РЫБАМИ И ВСЯКОЙ ОВОЩЬЮ ИЛИ ГУБИНОЙ

Ключ:

КЛАВИША

Протокол анализа:

По второму методу Фридмана предположим, что длина ключа ровна 7. В первой группе заменяем Й на « ». Во второй Щ на « » менять нет смысла так как нет слова «н». Меняем Щ на О. Далее меняем « » на « ». В следующей группе замена Р на « » не дала результатов, тогда меняем на О. Далее угадывается ключ «клавиша» и остальные буквы в криптограмме.