Университет ИТМО

Кафедра ВТ

Методы и средства защиты компьютерной информации

Лабораторная работа №1

Вариант 9

Выполнил: Фролов Сергей

Гр. Р3415

2017

**Задание**

Используя частотный анализ дешифровать криптограмму, зашифрованную методом моноалфавитных подстановок.

**Выполнение**

*Криптограмма:*

ШВБВЦЙВРЫ МБЙНФВРЫБЬЭИМВРЫБЫШГЦСКБЕШБГЮЮБЫШГЦСКБУЦТШИЦЫЦБЙШЫШЬШЧБЬУЬНЫЦ КБВЦБСЭЪЭБЪЗШ НЫЦ КБЬБ ИШЗШВРБНБШИСЦЬНЫЦБШСВШЧБ ШЪЦФЮБЫЦЕРБ ШЪЦФЦБЕЗШВУНИЮЫКВШБУЦЬНУОЦЫЦБПЮЗИШЕДЦВШЬБУЦФНЕЮЫБУЦГНЕЮЫБРСЦЗНЫБЫШГЦСКБФРЫЦФШТБЕШБЙШЫШЬЮБТЮОСРБРГЦТНБЪЭ ИЗЮЮБТШЫВННБ Ш ФШПНЫБВЦУЮТКБШ ТШИЗЮЫБЫЦЕРБРБ ШЪЦФНБЕШЕЫЮЬЦЫБВЦБЗЦВРБЕНДВРЫБЮЮБВШЙШЩБЬБЪШФБПИШЪЭБШВЦБВЮБЕНЖЦЫЦБРЛЮЕНЫ МБУЦБДШЫФРБНБЬСЮЫБВШЙРБЬБ ИЗЮТМ

*Открытый текст:*

ОН НАГНУЛСЯ ГИКНУЛ ВЫТЯНУЛ ЛОШАДЬ ПО ШЕЕ ЛОШАДЬ ЗАМОТАЛА ГОЛОВОЙ ВЗВИЛАСЬ НА ДЫБЫ БРОСИЛАСЬ В СТОРОНУ И ОТДАВИЛА ОДНОЙ СОБАКЕ ЛАПУ СОБАКА ПРОНЗИТЕЛЬНО ЗАВИЗЖАЛА ЧЕРТОПХАНОВ ЗАКИПЕЛ ЗАШИПЕЛ УДАРИЛ ЛОШАДЬ КУЛАКОМ ПО ГОЛОВЕ МЕЖДУ УШАМИ БЫСТРЕЕ МОЛНИИ СОСКОЧИЛ НАЗЕМЬ ОСМОТРЕЛ ЛАПУ У СОБАКИ ПОПЛЕВАЛ НА РАНУ ПИХНУЛ ЕЕ НОГОЮ В БОК ЧТОБЫ ОНА НЕ ПИЩАЛА УЦЕПИЛСЯ ЗА ХОЛКУ И ВДЕЛ НОГУ В СТРЕМЯ

*Таблица замен:*

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

*Протокол криптоанализа:*

Сначала расставим пробелы заменив Б на пробелы. Затем заменим Ш на О в соответствии со статистикой. Предположим, что первое слово «он», заменяем В на Н. Предположим что слово ШВЦ – слово «она», заменяем Ц на А. Видим слова заканчивающиеся на юю. Скорее всего необходима замена Ю на Е. Есть слово ГЮЮ. Так как Н уже занято, то ГЮЮ скорее всего слово «шее». Кроме того есть слова заканчивающиеся на НН и вероятнее всего это ИИ, то есть заменяем Н на И. Перед шее скорее всего предлог по, замена Е на П. В тексте есть 3 слова с ОША посередине. Предположим, что это слово лошадь и делаем соответствующие замены. Остальные слова уже довольно легко угадывались.