МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ Федеральное государственное автономное образовательное учреждение высшего образования

«Новосибирский национальный исследовательский государственный университет» (Новосибирский государственный университет, НГУ)

Структурное подразделение Новосибирского государственного университета

Высший колледж информатики Университета (ВКИ НГУ)

КАФЕДРА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ЛАБОРАТОРНАЯ РАБОТА

ОТЧЕТ ПО ”Игре в шпионов”

Руководитель Родионова О.К.

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_2018 г.

Студент 3 курса Гайдучик В.В.

гр. 503а1

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2018 г.

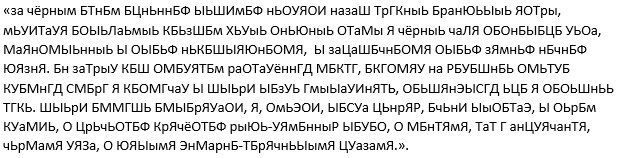
Новосибирск

2018

Был получен зашифрованный текст от Пестовой М.А.. Текст был перенесён в Microsoft Word. Известно, что первое словосочетание «ЧЪ ВЩЁАНЖ» является ключевым, которое дешифруется как «ЗА ЧЁРНЫМ». Всего знаков в тексте – 485.

«ЧЪ ВЩЁАНЖ БТАБЖ БЦАЬААБФ ЫЬШИЖБФ АЬОУЯОИ АЪЧЪШ ТЁГКАНЬ БЁЪАЮЬЫНЬ ЯОТЁН, ЖЬУИТЪУЯ БОЫЬЛЪЬЖНЬ КБЬЧШБЖ ХЬУНЬ ОАЬЮАНЬ ОТЪМН Я ВЩЁАНЬ ВЪЛЯ ОБОАБЫБЦБ УЬОЪ, МЪЯАОМЫЬААНЬ Ы ОЫБЬФ АЬКБШЫЯЮАБОМЯ, Ы ЧЪЦЪШБВАБОМЯ ОЫБЬФ ЧЯЖАЬФ АБВАБФ ЮЯЧАЯ. БА ЧЪТЁНУ КБШ ОМБУЯТБЖ ЁЪОТЪУЩААГД МБКТГ, БКГОМЯУ АЪ РБУБШАБЬ ОМЬТУБ КУБМАГД СМБЁГ Я КБОМГВЪУ Ы ШЫЬЁИ ЫБЧУЬ ГЖНЫЪУИАЯТЬ, ОБЬШЯАЭЫСГД ЬЦБ Я ОБОЬШАЬЬ ТГКЬ. ШЫЬЁИ БММГШЬ БМЫБЁЯУЪОИ, Я, ОЖЬЭОИ, ЫБСУЪ ЦЬАЁЯР, БВЬАИ ЫНОБТЪЭ, Ы ОЬЁБЖ КУЪМИЬ, О ЦЁЬВЬОТБФ КЁЯВЩОТБФ ЁНЮЬ-УЯЖБААНР ЫБУБО, О МБАТЯЖЯ, ТЪТ Г ЪАЦУЯВЪАТЯ, ВЬЁМЪЖЯ УЯЗЪ, О ЮЯЫНЖЯ ЭАМЪЁАБ-ТБЁЯВАЬЫНЖЯ ЦУЪЧЪЖЯ.».

ШАГ 1: Буквы, которые являются частью зашифрованного текста, будут малого размера. А буквы, которые были заменены, будут большого размера. Производим замену букв «Ч Ъ В Щ Ё А Н Ж» на «з а ч ё р н ы м» соответственно.



ШАГ 2: Так как ключ известен, составляется таблица дешифровки (Таблица 1.1).

*Таблица 1.1 – Таблица дешифровки:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шифровка | Дешифровка | Шифровка | Дешифровка | Шифровка | Дешифровка |
| **А** | Н | **Л** |  | **Ч** | З |
| **Б** |  | **М** |  | **Ш** |  |
| **В** | Ч | **Н** | Ы | **Щ** | Ё |
| **Г** |  | **О** |  | **Ъ** | А |
| **Д** |  | **П** |  | **Ы** |  |
| **Е** |  | **Р** |  | **Ь** |  |
| **Ё** | Р | **С** |  | **Э** |  |
| **Ж** | М | **Т** |  | **Ю** |  |
| **З** |  | **У** |  | **Я** |  |
| **И** |  | **Ф** |  |  |  |
| **Й** |  | **Х** |  |  |  |
| **К** |  | **Ц** |  |  |  |

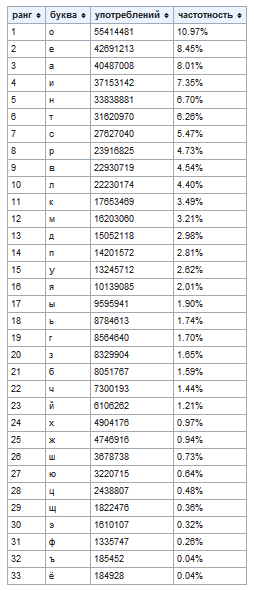
ШАГ 3: На основе статистических данных составляется таблица частоты встречаемости символов в зашифрованном тексте (Таблица 2.1).

*Таблица 2.1 – Таблица частоты встречаемости символов:*

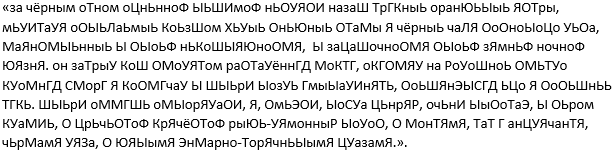
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Буква | Кол-во в тексте | Встречаемость | Буква | Кол-во в тексте | Встречаемость | Буква | Кол-во в тексте | Встречаемость |
| **А** | *42* | 0.086 | **Л** | *2* | 0.004 | **Ч** | *9* | 0.018 |
| **Б** | *53* | 0.109 | **М** | *19* | 0.039 | **Ш** | *12* | 0.024 |
| **В** | *12* | 0.024 | **Н** | *17* | 0.035 | **Щ** | *4* | 0.008 |
| **Г** | *12* | 0.024 | **О** | *33* | 0.068 | **Ъ** | *30* | 0.061 |
| **Д** | *3* | 0.006 | **П** | *0* | 0 | **Ы** | *23* | 0.047 |
| **Е** | *0* | 0 | **Р** | *3* | 0.006 | **Ь** | *46* | 0.094 |
| **Ё** | *19* | 0.039 | **С** | *3* | 0.006 | **Э** | *4* | 0.008 |
| **Ж** | *17* | 0.035 | **Т** | *20* | 0.041 | **Ю** | *6* | 0.012 |
| **З** | *1* | 0.002 | **У** | *23* | 0.047 | **Я** | *34* | 0.070 |
| **И** | *10* | 0.020 | **Ф** | *8* | 0.016 |  |  |  |
| **Й** | *0* | 0 | **Х** | *1* | 0.002 |  |  |  |
| **К** | *11* | 0.022 | **Ц** | *8* | 0.016 |  |  |  |

ШАГ 4: Берётся таблица встречаемости символов (Таблица 3.1).

*Таблица 3.1 – Таблица встречаемости символов:*



ШАГ 5: Следуя значениям вышеуказанной таблицы (Таблица 3.1), производится замена самой встречаемой буквы «Б» (см. в Таблицу 2.1) на букву «о».

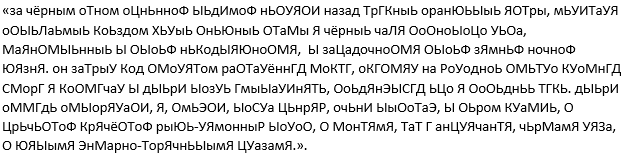


ШАГ 6: На основе предыдущего шага, обновляются данные таблицы дешифровки (Таблица 1.2).

*Таблица 1.2 – Таблица дешифровки:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шифровка | Дешифровка | Шифровка | Дешифровка | Шифровка | Дешифровка |
| **А** | Н | **Л** |  | **Ч** | З |
| **Б** | О | **М** |  | **Ш** |  |
| **В** | Ч | **Н** | Ы | **Щ** | Ё |
| **Г** |  | **О** |  | **Ъ** | А |
| **Д** |  | **П** |  | **Ы** |  |
| **Е** |  | **Р** |  | **Ь** |  |
| **Ё** | Р | **С** |  | **Э** |  |
| **Ж** | М | **Т** |  | **Ю** |  |
| **З** |  | **У** |  | **Я** |  |
| **И** |  | **Ф** |  |  |  |
| **Й** |  | **Х** |  |  |  |
| **К** |  | **Ц** |  |  |  |

ШАГ 7: Слово текста «АЪЧЪШ» можно дешифровать, как слово «НАЗАД», так как других аналогов в этом случае – просто нет. Ввиду этого производится замена буквы «Ш» шифрованного текста на букву «д».

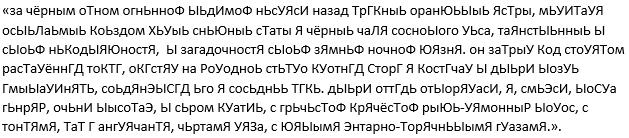


ШАГ 8: На основе предыдущего шага, обновляются данные таблицы дешифровки (Таблица 1.3).

*Таблица 1.3 – Таблица дешифровки:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шифровка | Дешифровка | Шифровка | Дешифровка | Шифровка | Дешифровка |
| **А** | Н | **Л** |  | **Ч** | З |
| **Б** |  | **М** |  | **Ш** | Д |
| **В** | Ч | **Н** | Ы | **Щ** | Ё |
| **Г** |  | **О** |  | **Ъ** | А |
| **Д** |  | **П** |  | **Ы** |  |
| **Е** |  | **Р** |  | **Ь** |  |
| **Ё** | Р | **С** |  | **Э** |  |
| **Ж** | М | **Т** |  | **Ю** |  |
| **З** |  | **У** |  | **Я** |  |
| **И** |  | **Ф** |  |  |  |
| **Й** |  | **Х** |  |  |  |
| **К** |  | **Ц** |  |  |  |

ШАГ 9: Можно предположить, что слово «ЧЪЦЪШБВАБОМЯ» дешифруется как «ЗАГАДОЧНОСТ . » (точка указывает на отсутствующую букву). Последнюю букву, трудно сразу разгадать, так как тут есть 2 варианта дешифровки: «ЗАГАДОЧНОСТЬ» или «ЗАГАДОЧНОСТИ». Таким образом, мы производим замену букв «М О Ц» зашифрованного текста на «т с г» соответственно.

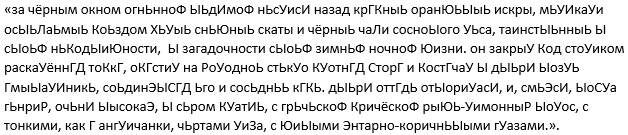


ШАГ 10: На основе предыдущего шага, обновляются данные таблицы дешифровки (Таблица 1.4).

*Таблица 1.4 – Таблица дешифровки:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шифровка | Дешифровка | Шифровка | Дешифровка | Шифровка | Дешифровка |
| **А** | Н | **Л** |  | **Ч** | З |
| **Б** | О | **М** | Т | **Ш** | Д |
| **В** | Ч | **Н** | Ы | **Щ** | Ё |
| **Г** |  | **О** | С | **Ъ** | А |
| **Д** |  | **П** |  | **Ы** |  |
| **Е** |  | **Р** |  | **Ь** |  |
| **Ё** | Р | **С** |  | **Э** |  |
| **Ж** | М | **Т** |  | **Ю** |  |
| **З** |  | **У** |  | **Я** |  |
| **И** |  | **Ф** |  |  |  |
| **Й** |  | **Х** |  |  |  |
| **К** |  | **Ц** | Г |  |  |

ШАГ 11: Предполагаем, что слова шифрованного текста «БТАБЖ» и «ЯОТЁН» можно дешифровать, как «ОКНОМ» и «ИСКРЫ». Ввиду этого предположения, выполняется замена букв «Т Я» на «к и» соответственно.

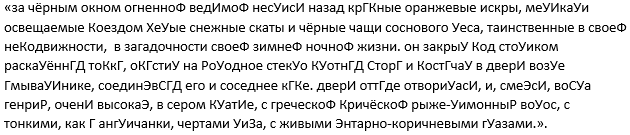


ШАГ 12: На основе предыдущего шага, обновляются данные таблицы дешифровки (Таблица 1.5).

*Таблица 1.5 – Таблица дешифровки:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шифровка | Дешифровка | Шифровка | Дешифровка | Шифровка | Дешифровка |
| **А** | Н | **Л** |  | **Ч** | З |
| **Б** | О | **М** | Т | **Ш** | Д |
| **В** | Ч | **Н** | Ы | **Щ** | Ё |
| **Г** |  | **О** | С | **Ъ** | А |
| **Д** |  | **П** |  | **Ы** |  |
| **Е** |  | **Р** |  | **Ь** |  |
| **Ё** | Р | **С** |  | **Э** |  |
| **Ж** | М | **Т** | К | **Ю** |  |
| **З** |  | **У** |  | **Я** | И |
| **И** |  | **Ф** |  |  |  |
| **Й** |  | **Х** |  |  |  |
| **К** |  | **Ц** | Г |  |  |

ШАГ 13: Предполагается, что слова «МЪЯАОМЫЬААНЬ», «БЁЪАЮЬЫНЬ» и «БОЫЬЛЪЬЖНЬ» шифрованного текста – дешифруются, как «ТАИНСТВЕННЫЕ», «ОРАНЖЕВЫЕ» и «ОСВЕЩАЕМЫЕ», так как это прилагательные с окончанием на «ЫЕ». Таким образом, производится замена букв «Ы Ь Л Ю» на «в е щ ж» соответственно.

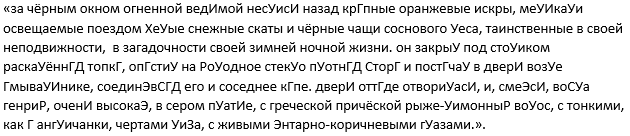


ШАГ 14: На основе предыдущего шага, обновляются данные таблицы дешифровки (Таблица 1.6).

*Таблица 1.6 – Таблица дешифровки:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шифровка | Дешифровка | Шифровка | Дешифровка | Шифровка | Дешифровка |
| **А** | Н | **Л** | Щ | **Ч** | З |
| **Б** | О | **М** | Т | **Ш** | Д |
| **В** | Ч | **Н** | Ы | **Щ** | Ё |
| **Г** |  | **О** | С | **Ъ** | А |
| **Д** |  | **П** |  | **Ы** | В |
| **Е** |  | **Р** |  | **Ь** | Е |
| **Ё** | Р | **С** |  | **Э** |  |
| **Ж** | М | **Т** | К | **Ю** | Ж |
| **З** |  | **У** |  | **Я** | И |
| **И** |  | **Ф** |  |  |  |
| **Й** |  | **Х** |  |  |  |
| **К** |  | **Ц** | Г |  |  |

ШАГ 15: Предполагается, что словосочетание: «Ы ОЫБЬФ АЬКБШЫЯЮАБОМЯ» зашифрованного текста дешифруется, как «В СВОЕЙ НЕПОДВИЖНОСТИ». Ввиду этого предположения, производится замена букв «Ф К» на «й п» соответственно.

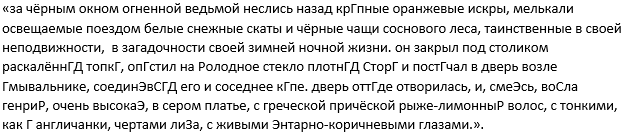


ШАГ 16: На основе предыдущего шага, обновляются данные таблицы дешифровки (Таблица 1.7).

*Таблица 1.7 – Таблица дешифровки:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шифровка | Дешифровка | Шифровка | Дешифровка | Шифровка | Дешифровка |
| **А** | Н | **Л** | Щ | **Ч** | З |
| **Б** | О | **М** | Т | **Ш** | Д |
| **В** | Ч | **Н** | Ы | **Щ** | Ё |
| **Г** |  | **О** | С | **Ъ** | А |
| **Д** |  | **П** |  | **Ы** | В |
| **Е** |  | **Р** |  | **Ь** | Е |
| **Ё** | Р | **С** |  | **Э** |  |
| **Ж** | М | **Т** | К | **Ю** | Ж |
| **З** |  | **У** |  | **Я** | И |
| **И** |  | **Ф** | Й |  |  |
| **Й** |  | **Х** |  |  |  |
| **К** | П | **Ц** | Г |  |  |

ШАГ 17: Предполагается, что такие слова, как «ЧЪТЁНУ», «ХЬУНЬ» и «ЖЬУИТЪУЯ» шифрованного текста – дешифруются, как «ЗАКРЫЛ», «БЕЛЫЕ» и «МЕЛЬКАЛИ». Таким образом, производится замена букв «У И Х» на «Л Ь Б» соответственно.

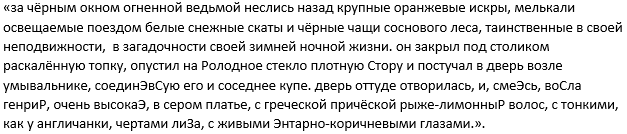


ШАГ 18: На основе предыдущего шага, обновляются данные таблицы дешифровки (Таблица 1.8).

*Таблица 1.8 – Таблица дешифровки:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шифровка | Дешифровка | Шифровка | Дешифровка | Шифровка | Дешифровка |
| **А** | Н | **Л** | Щ | **Ч** | З |
| **Б** | О | **М** | Т | **Ш** | Д |
| **В** | Ч | **Н** | Ы | **Щ** | Ё |
| **Г** |  | **О** | С | **Ъ** | А |
| **Д** |  | **П** |  | **Ы** | В |
| **Е** |  | **Р** |  | **Ь** | Е |
| **Ё** | Р | **С** |  | **Э** |  |
| **Ж** | М | **Т** | К | **Ю** | Ж |
| **З** |  | **У** | Л | **Я** | И |
| **И** | Ь | **Ф** | Й |  |  |
| **Й** |  | **Х** | Б |  |  |
| **К** | П | **Ц** | Г |  |  |

ШАГ 19: Предполагается, что слова «ТЁГКАНЬ» и «ЁЪОТЪУЩААГД» зашифрованного текста – дешифруются, как «КРУПНЫЕ» и «РАСКАЛЁННУЮ». Ввиду этого предположения, производится замена букв «Г Д» на «у ю».

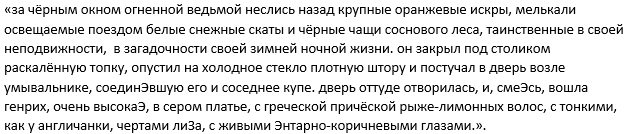


ШАГ 20: На основе предыдущего шага, обновляются данные таблицы дешифровки (Таблица 1.9).

*Таблица 1.9 ­– Таблица дешифровки:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шифровка | Дешифровка | Шифровка | Дешифровка | Шифровка | Дешифровка |
| **А** | Н | **Л** | Щ | **Ч** | З |
| **Б** | О | **М** | Т | **Ш** | Д |
| **В** | Ч | **Н** | Ы | **Щ** | Ё |
| **Г** | У | **О** | С | **Ъ** | А |
| **Д** | Ю | **П** |  | **Ы** | В |
| **Е** |  | **Р** |  | **Ь** | Е |
| **Ё** | Р | **С** |  | **Э** |  |
| **Ж** | М | **Т** | К | **Ю** | Ж |
| **З** |  | **У** | Л | **Я** | И |
| **И** | Ь | **Ф** | Й |  |  |
| **Й** |  | **Х** | Б |  |  |
| **К** | П | **Ц** | Г |  |  |

ШАГ 21: Предполагается, что слова «РБУБШАБЬ» и «СМБЁГ» зашифрованного текста дешифруются, как «ХОЛОДНОЕ» и «ШТОРУ». Таким образом, производится замена букв «Р С» на «х ш».

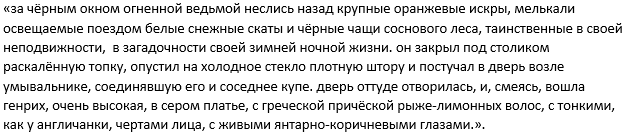


ШАГ 22: На основе предыдущего шага, обновляются данные таблицы дешифровки (Таблица 1.10).

*Таблица 1.10 – Таблица дешифровки:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шифровка | Дешифровка | Шифровка | Дешифровка | Шифровка | Дешифровка |
| **А** | Н | **Л** | Щ | **Ч** | З |
| **Б** | О | **М** | Т | **Ш** | Д |
| **В** | Ч | **Н** | Ы | **Щ** | Ё |
| **Г** | У | **О** | С | **Ъ** | А |
| **Д** | Ю | **П** |  | **Ы** | В |
| **Е** |  | **Р** | Х | **Ь** | Е |
| **Ё** | Р | **С** | Ш | **Э** |  |
| **Ж** | М | **Т** | К | **Ю** | Ж |
| **З** |  | **У** | Л | **Я** | И |
| **И** | Ь | **Ф** | Й |  |  |
| **Й** |  | **Х** | Б |  |  |
| **К** | П | **Ц** | Г |  |  |

ШАГ 23: Предполагается, что такие слова, как «ОЖЬЭОИ» и «УЯЗЪ» зашифрованного текста можно перевести, как «СМЕЯСЬ» и «ЛИЦА». Ввиду этого предположения, производится замена букв «Э З» на «я ц» соответственно.



ШАГ 24: На основе предыдущего шага, обновляются данные таблицы дешифровки (Таблица 1.11).

*Таблица 1.11 – Таблица дешифровки:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Шифровка | Дешифровка | Шифровка | Дешифровка | Шифровка | Дешифровка |
| **А** | Н | **Л** | Щ | **Ч** | З |
| **Б** | О | **М** | Т | **Ш** | Д |
| **В** | Ч | **Н** | Ы | **Щ** | Ё |
| **Г** | У | **О** | С | **Ъ** | А |
| **Д** | Ю | **П** | - | **Ы** | В |
| **Е** | - | **Р** | Х | **Ь** | Е |
| **Ё** | Р | **С** | Ш | **Э** | Я |
| **Ж** | М | **Т** | К | **Ю** | Ж |
| **З** | Ц | **У** | Л | **Я** | И |
| **И** | Ь | **Ф** | Й |  |  |
| **Й** | - | **Х** | Б |  |  |
| **К** | П | **Ц** | Г |  |  |

ВЫВОД: Текст был расшифрован за 24 шага. Расшифровка текста производилась визуальным и статистическим методом.