1. **Задание №1: Расшифровать фразу, зашифрованную столбцовой перестановкой**

ПКЕЕРРПО\_ЙУСТ\_ИТПСУТЛЯЕИН

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. Известно, что шифрование производилось по столбцам, следовательно, расшифрование следует проводить, меняя порядок столбцов.

П К Е Е Р

Р П О \_ Й

У С Т \_ И

Т П С У Т

Л Я Е И Н

ПЕ-15

ПЕ-15

ПР-41

КП-2

КЕ-4

КЕ-4

КР-10

ЕП-16

ЕК-13

ЕЕ-7

ЕР-39

РП-2

РК-3

РЕ-37

РЕ-37

1. **Задание №2: Расшифровать фразу, зашифрованную двойной перестановкой (сначала были переставлены столбцы, затем строки)**

П\_БИРДЛЬНЕВ\_ОП\_ОПЗДЕВЫГЕА

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| П | Д | В | О | В |
| - | Л | - | П | Ы |
| Б | Ь | О | З | Г |
| И | Н | П | Д | Е |
| Р | Е | - | Е | А |

ПО-46

ДП-3

ДВ-3

ДО-22

ДВ-3

ВП-6

ВД-3

ВО-58

ВВ-5

ОП-18

ОД-47

ОВ-84

ОВ-84

1. Задание №3: Расшифровать текст. Каждой букве алфавита соответствует двузначное число.

22 10 75 62 47 10 74 10 24 88 47 39 35 66 15 75 58 10 47 64 53 53 85 66

35 10 69 62 28 10 24 53 66 49 53 47 47 10 49 64 10 58 39 28 22 88 17 10 79 47 88

15 47 66 22 53. 44 47 10 85 17 10 28 53 24 75 44 35 51 66 75 58 53 47 53

64 88. 35 10 35 72 62 28 10 24 66 47 88 17 10 69, 44 66 80 37 80 10 24 69

49 88 75 39 37 74 53 17 66 58 28 66 17 88 47 53 88 53 85 66 35 66 15, 22 37

28 75 58 28 10, 35 66 58 66 17 62 88 53 75 85 62 58 62 28 10 88 79 39, 66 35 10 69

10 28 79 53 75 39 28 49 10 28 47 66 69 47 10 35 66 74 62 42 74 88 75 58 10

42. 79 53 17 66 35 53 88 28 66 17 66 58 10 72 62 24 53 17 10 75 85 10 42 47 37

58 62, 37 75 10 49 39 72 10 37 58 66 47 37 24 10 28 75 37 74 88 17 35 10

42. 44 28 66 79 88 24 28 42 66 24 24, 51 49 88 58 37 74 10 47 47 62

88 69 88 17 35 10 24 10 69 62 72 35 66 66 58 17 10 31 10 24 53 64 28

88 58 62 53 49 88 58 10 24 53 53 47 58 88 17 39 88 17 10. 37 49 53 28 53

58 88 24 39 47 66, 47 66 42 66 69 44 53 47 47 88 37 69 47 10 24 74 88 47 44.

66 47 85 17 66 58 44 47 37 24 17 88 51 53 75 58 17 10 64 53 66 47 47 37 97 35 47

53 51 37. 44 28 69 44 24 17 37 22 35 37, 66 72 7 41 03 54 73 7 24 85 88 17 66

28 72 17 66 47 69 66 28 37 97 22 88 17 47 53 24 39 47 53 64 37 53, 75

35 24 66 47 53 28 79 53 75 39 47 10 49 17 10 75 35 17 62 58 62 74 53 75 58 17

10 47 53 64 10 74 53, 75 58 66 24 35 47 37 24 75 44 75 85 88 17 28 66 15 53

69 74 47 66 31 88 75 58 28 10 47 88 66 31 53 49 10 47 47 66 75 58 88 15, 35

66 58 66 17 62 88 85 66 49 75 58 88 17 88 51 10 24 53 74 88 47 44 25 58 66 15

47 66 22 39 97. 74 66 88 53 74 44, 42 66 17 42 88 24 37 53 75 72 66 17

42 88 75, 72 62 24 66 47 10 22 88 17 58 10 47 66 28 35 47 53 51 88, 53 22

88 17 47 53 24 10 88 80 88 47 88 37 75 85 88 24 53 28 62 75 66 42 47 37 58 39.

Часы на маленькой станции показывали одиннадцать вчерашней ночи. Я
направился к гостинице. Как бывало не раз, я ощущал здесь умиротворение и покой, чувства, которые испытываешь, оказавшись в давно знакомых местах. Широкие ворота были распахнуты, усадьба утонула в сумерках. Я вошел в холл, где туманные зеркала зыбко отражали цветы и детали интерьера. Удивительно, но хозяин не узнал меня. Он протянул регистрационную книгу. Я взял ручку, обмакнул перо в бронзовую чернильницу и, склонившись над раскрытыми страницами, столкнулся с первой из множества неожиданностей, которые подстерегали меня этой ночью. Мое имя, Хорхе Луис Борхес, было начертано в книге, и чернила еще не успели высохнуть.

1. Задание №4: Расшифруйте текст с известной длиной ключа (пробел является частью алфавита).

Длина ключа: 3

yexiwpnbjfzhcnpmswkorthnngaefltepxnkknpmswgeeywomnqucawnzqooxnxwswm

hjywjlnombkywjlnxsrwkwomwjlnpmswrboynsnraxcnjo\_etkw\_wttwmhjywjlnexnbtkdzapn

acewjisainpmopewoejdfgwyvaejkwrwmhjywjlnqxhxqzue\_afaoewjepnngxnawkbtmhjywjl

nstegxnhnyaegdnfwfncwbqunkknljblqswtawmbnxsoernjfojrwnawjwcmgajapmnzjapzeuee

eiwjlnzqbpmsoeeeiswfekza\_ejeyvwfnlfqgebberklfwavasnpmswibcxnlnqgehlegdjnohsjynk

knxetkbnot\_agb\_cnyqbsxnxevkwawfa\_egdjawibcxndteojfwfa\_eeeisnxnxqzwhvxxswyvaet

kbnkkgasnpmswkbteuayfwfjxcnyzgwntwsbpegdjn\_tuoeuaynptneynyjtkwswyvaevqsgawf

wfa\_egafewngwybwuwahsoeooelkzninudynczsoxnesnxeqkzapwlwttwfaerohezk\_snxnsms

njnitfpecatchjndfiaezeyghjnabcawwasqaebbegdjndfeomsneeafzeywaxnkknjfgqwswkbtmhj

ywjlnexnoyeksuhcnkuckxs\_epuefkrswuskuzaegdjnhjoczswfuxnaoynzwhaqnoubnyfwaojyf

wngwro\_jneqzaloheojinpmswhoiuoelawmooepajawxgafreqlwnapjaontunac

**1. ШИФР СТОЛБЦОВОЙ ПЕРЕСТАНОВКИ**

При решении заданий на криптоанализ шифров перестановки необходимо восстановить начальный порядок следования букв текста. Для этого используется анализ совместимости символов, в чем может помочь таблица сочетаемости.

Таблица 1. Сочетаемость букв русского языка

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Г** | **С** | **Слева** |  | **Справа** | **Г** | **С** |
| 3 | 97 | л, д, к, т, в, р, н | **А** | л, н, с, т, р, в, к, м | 12 | 88 |
| 80 | 20 | я, е, у, и, а, о | **Б** | о, ы, е, а, р, у | 81 | 19 |
| 68 | 32 | я, т, а, е, и, о | **В** | о, а, и, ы, с, н, л, р | 60 | 40 |
| 78 | 22 | р, у, а, и, е, о | **Г** | о, а, р, л, и, в | 69 | 31 |
| 72 | 28 | р, я, у, а, и, е, о | **Д** | е, а, и, о, н, у, р, в | 68 | 32 |
| 19 | 81 | м, и, л, д, т, р, н | **Е** | н, т, р, с, л, в, м, и | 12 | 88 |
| 93 | 17 | р, е, и, а, у, о | **Ж** | е, и, д, а, н | 71 | 29 |
| 98 | 11 | о, е, а, и | **З** | а, н, в, о, м, д | 51 | 49 |
| 27 | 73 | р, т, м, и, о, л, н | **И** | с, н, в, и, е, м, к, з | 25 | 75 |
| 55 | 45 | ь, в, е, о, а, и, с | **К** | о, а, и, р, у, т, л, е | 73 | 27 |
| 77 | 23 | г, в, ы, и, е, о, а | **Л** | и, е, о, а, ь, я, ю, у | 75 | 25 |
| 80 | 20 | я, ы, а, и, е, о | **М** | и, е, о, у, а, н, п, ы | 73 | 27 |
| 55 | 45 | д, ь, н, о, а, и, е | **Н** | о, а, и, е, ы, н, у | 80 | 20 |
| 11 | 89 | р, п, к, в, т, н | **О** | в, с, т, р, и, д, н, м,  | 15 | 85 |
| 65 | 35 | в, с, у, а, и, е, о | **П** | о, р, е, а, у, и, л | 68 | 32 |
| 55 | 45 | и, к, т, а, п, о, е | **Р** | а, е, о, и, у, я ,ы, н | 80 | 20 |
| 69 | 31 | с, т, в, а, е, и, о | **С** | т, к, о, я, е, ь, с, н | 32 | 68 |
| 57 | 43 | ч, у, и, а, е, о, с | **Т** | о, а, е, и, ь, в, р, с | 63 | 37 |
| 15 | 85 | п, т, к, д, н, м, р | **У** | т, п, с, д, н, ю, ж | 16 | 84 |
| 70 | 30 | н, а, е, о, и | **Ф** | и, е, о, а, е, о, а | 81 | 19 |
| 90 | 10 | у, е, о, а, ы, и | **Х** | о, и, с, н, в, п, р | 43 | 57 |
| 69 | 31 | е, ю, н, а, и | **Ц** | и, е, а, ы | 93 | 7 |
| 82 | 18 | е, а, у, и, о | **Ч** | е, и, т, н | 66 | 34 |
| 67 | 33 | ь, у, ы, е, о, а, и, в | **Ш** | е, и, н, а, о, л | 68 | 32 |
| 84 | 16 | е, б, а, я, ю | **Щ** | е, и, а | 97 | 3 |
| 0 | 100 | м, р, т, с, б, в, н | **Ы** | л, х, е, м, и, в, с, н | 56 | 44 |
| 0 | 100 | н, с, т, л | **Ь** | н, к, в, п, с, е, о, и | 24 | 76 |
| 14 | 86 | с, ы, м, л, д, т, р, н | **Э** | н, т, р, с, к | 0 | 100 |
| 58 | 42 | ь, о, а, и, л, у | **Ю** | д, т, щ, ц, н, п | 11 | 89 |
| 43 | 57 | о, н, р, л, а, и, с | **Я** | в, с, т, п, д, к, м, л | 16 | 84 |

Таблица 2. Сочетаемость букв английского языка

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Г** | **С** | **Слева** |  | **Справа** | **Г** | **С** |
| 19 | 81 | l,c,d,m,n,s,w,t,r,e,h  | **A** | n,t,s,r,l,d,c,m | 6 | 94 |
| 55 | 45 | y,b,n,t,u,d,o,s,a,e  | **В** | e,l,u,o,a,y,b,r | 70 | 30 |
| 61 | 39 | u,o,s,n,a,i,l,e  | **С** | h,o,e,a,i,t,r,l,k | 59 | 41 |
| 52 | 48 | r,i,l,a,n,e  | **D** | e,i,t,a,o,u | 54 | 46 |
| 8 | 92 | c,b,e,m,v,d,s,l,n,t,r,h  | **E** | r,d,s,n,a,t,m,e,c,o | 21 | 79 |
| 69 | 31 | s,n,f,d,a,i,e,o  | **F** | t,o,e,i,a,r,f,u | 52 | 48 |
| 36 | 64 | o,d,u,r,i,e,a,n  | **G** | e.h.o.r.a.t.f.w.i.s | 42 | 58 |
| 7 | 93 | g,e,w,s,c,t  | **H** | e,a,i,o | 90 | 10 |
| 13 | 87 | f,m,w,e,n,l,d,s,r,h,t  | **I** | n,t,s,o,c,r,e,m,a,l | 17 | 83 |
| 28 | 72 | y,w,t,s,n,e,c,b,a,c  | **J** | u,o,a,e,m,w | 88 | 12 |
| 53 | 47 | y,u,i,n,a,r,o,c  | **К** | e,i,n,a,t,s | 68 | 32 |
| 52 | 48 | m,p,t,i,b,u,o,e,l,a  | **L** | e,i,y,o,a,d,u | 65 | 35 |
| 69 | 31 | s,d,m,r,i,a,o,e  | **M** | e,a,o,i,p,m | 71 | 29 |
| 89 | 11 | u,e,o,a,i  | **N** | d,t,g,e,a,s,o,i,c | 32 | 68 |
| 21 | 79 | o,d,l,p,h,n,e,c,f,s,i,r,t  | **О** | n,f,r,u,t,m,l,s,w,o | 18 | 82 |
| 47 | 53 | r,l,t,n,i,p,m,a,o,u,e,s  | **P** | o,e,a,r,l,u,p,t,i,s | 59 | 41 |
| 20 | 80 | o,n,l,e,d,r,s  | **Q** | u | 100 | 0 |
| 70 | 30 | p,i,u,t,a,o,e  | **R** | e,o,a,t,i,s,y | 61 | 39 |
| 48 | 52 | d,t,o,u,r,n,s,i,a,e  | **S** | t,e,o,i,s,a,h,p,u | 41 | 59 |
| 43 | 57 | u,o,d,t,f,e,i,n,s.a  | **Т** | h,i,o,e,a,t,r | 38 | 62 |
| 35 | 65 | p,f,t,l,b,d,s,o  | **U** | n,s,t,r,l,p,b,c | 8 | 92 |
| 88 | 12 | r,u,o,a,i,e  | **V** | e,i,o,a | 99 | 1 |
| 48 | 52 | g,d,y,n,s,t,o,e  | **W** | a,h,i,e,o,n | 80 | 20 |
| 95 | 5 | u,n,i,e  | **X** | p,t,i,a,u,c,k,o | 38 | 62 |
| 24 | 76 | b,n,a,t,e,r,l  | **Y** | a,o,s,t,w,h,i,e,d,m | 38 | 62 |
| 88 | 12 | o,n,a,i  | **Z** | e,i,w | 86 | 14 |

При анализе сочетаемости букв друг с другом следует иметь в виду зависимость появления букв в открытом тексте от значительного числа предшествующих букв. Для анализа этих закономерностей используют понятие условной вероятности.

Систематически вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А.А.Марковым (1856 — 1922). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В связи с этим А. А. Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Им были подсчитаны частоты встречаемости биграмм вида гласная-гласная (*г,г*), гласная-согласная (*г,с*), согласная-гласная (*с,г*), согласная-согласная (*с,с*) в русском тексте длиной в 105 знаков. Результаты подсчета отражены в следующей таблице:

Таблица 3. Чередование гласных и согласных

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Г** | **С** | **Всего** |
| **Г** | 6588 | 38310 | 44898 |
| **С** | 38296 | 16806 | 55102 |

**Пример решения:**

Дан шифр-текст: СВПООЗЛУЙЬСТЬ\_ЕДПСОККАЙЗО

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. Известно, что шифрование производилось по столбцам, следовательно, расшифрование следует проводить, меняя порядок столбцов.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **С** | **В** | **П** | **О** | **О** |
| **З** | **Л** | **У** | **Й** | **Ь** |
| **С** | **Т** | **Ь** | **\_** | **Е** |
| **Д** | **П** | **С** | **О** | **К** |
| **К** | **А** | **Й** | **З** | **О** |

Необходимо произвести анализ совместимости символов (Таблица сочетаемости букв русского и английского алфавита, а также таблицы частот биграмм представлена выше). В первом и третьем столбце сочетание СП является крайне маловероятным для русского языка, следовательно, такая последовательность столбцов быть не может. Рассмотрим другие запрещенные и маловероятные сочетания букв: ВП (2,3 столбцы), ПС (3,1 столбцы), ПВ (3,2 столбцы). Перебрав их все, получаем наиболее вероятные сочетания биграмм по столбцам:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **В** | **О** | **С** | **П** | **О** |
| **Л** | **Ь** | **З** | **У** | **Й** |
| **Т** | **Е** | **С** | **Ь** | **\_** |
| **П** | **О** | **Д** | **С** | **К** |
| **А** | **З** | **К** | **О** | **Й** |

Получаем осмысленный текст: ВОСПОЛЬЗУЙТЕСЬ\_ПОДСКАЗКОЙ

**2. ШИФР ДВОЙНОЙ ПЕРЕСТАНОВКИ**

**Пример решения:**

Дан шифр-текст: ЫОЕЧТТОУ\_СНСОРЧТРНАИДЬН\_Е

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. известно, что шифрование производилось сначала по столбцам, а затем по строкам, следовательно, расшифрование следует проводить тем же способом.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ы** | **О** | **Е** | **Ч** | **Т** |
| **Т** | **О** | **У** | **\_** | **С** |
| **Н** | **С** | **О** | **Р** | **Ч** |
| **Т** | **Р** | **Н** | **А** | **И** |
| **Д** | **Ь** | **Н** | **\_** | **Е** |

Производим анализ совместимости символов. Если в примере столбцовой перестановки можно было легко подобрать нужную комбинацию путем перебора, то здесь лучше воспользоваться таблицей частот букв русского языка (см. приложение). Для оптимизации скорости выполнения задания можно проверить все комбинации букв только в первой строке. Получаем ОЕ-15, ОЧ-12, ЕТ-33, ТЕ-31, ЧО-х, ЕО-7, ЧЫ-х, ОЫ-х, ТЫ-11, ТЧ-1, ЧЕ-23 (где х-запрещенная комбинация).

Из полученных результатов можно предположить следующую комбинацию замены столбцов **2 4 3 5 1:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **О** | **Ч** | **Е** | **Т** | **Ы** |
| **О** | **\_** | **У** | **С** | **Т** |
| **С** | **Р** | **О** | **Ч** | **Н** |
| **Р** | **А** | **Н** | **И** | **Т** |
| **Ь** | **\_** | **Н** | **Е** | **Д** |

Теперь необходимо переставить строки в нужном порядке. **3 2 4 5 1:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **С** | **Р** | **О** | **Ч** | **Н** |
| **О** | **\_** | **У** | **С** | **Т** |
| **Р** | **А** | **Н** | **И** | **Т** |
| **Ь** | **\_** | **Н** | **Е** | **Д** |
| **О** | **Ч** | **Е** | **Т** | **Ы** |

Получаем осмысленный текст:

СРОЧНО\_УСТРАНИТЬ\_НЕДОЧЕТЫ

**3. ШИФР ПРОСТОЙ ЗАМЕНЫ**

|  |  |  |  |
| --- | --- | --- | --- |
| -0,175 | О0,090 | Е,Ё0,072 | А0,062 |
| И0,062 | Т0,053 | Н0,053 | С0,045 |
| Р0,040 | В0,038 | Л0,035 | К0,028 |
| М0,026 | Д0,025 | П0,023 | У0,021 |
| Я0,018 | Ы0,016 | 30,016 | Ь,Ъ0,014 |
| Б0,014 | Г0,013 | Ч0,012 | Й0,010 |
| Х0,009 | Ж0,007 | Ю0,006 | Ш0,006 |
| Ц0,004 | Щ0,003 | Э0,003 | Ф0,002 |

Криптоанализ шифра простой замены основан на использовании статистических закономерностей языка. Так, например, известно, что в русском языке частоты букв распределены следующим образом:

Таблица 4. Частоты букв русского языка
(в 32-буквенном алфавите со знаком пробела)

 Рисунок 6. Диаграмма частот букв русского языка

Для получения более точных сведений об открытых текстах можно строить и анализировать таблицы k-грамм при k>2, однако для учебных целей вполне достаточно ограничиться биграммами. Неравновероятность k -грамм (и даже слов) тесно связана с характерной особенностью открытого текста – наличием в нем большого числа повторений отдельных фрагментов текста: корней, окончаний, суффиксов, слов и фраз. Так, для русского языка такими привычными фрагментами являются наиболее частые биграммы и триграммы:

СТ, НО, ЕН, ТО, НА, ОВ, НИ, РА, ВО,
 КО, СТО, ЕНО, НОВ, ТОВ, ОВО, ОВА

Полезной является информация о сочетаемости букв, то есть о предпочтительных связях букв друг с другом, которую легко извлечь из таблиц частот биграмм.

Имеется в виду таблица, в которой слева и справа от каждой буквы расположены наиболее предпочтительные "соседи" (в порядке убывания частоты соответствующих биграмм). В таких таблицах обычно указывается также доля гласных и согласных букв (в процентах), предшествующих (или следующих за) данной букве.

Таблица 5. Таблица частот биграмм русского языка

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ж** | **3** | **И** | **И** | **К** | **Л** | **М** | **Н** | **О** | **П** | **Р** | **С** | **Т** | **У** | **Ф** | **X** | **Ц** | **Ч** | **Ш** | **Щ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| **А** | 2 | 12 | 35 | 8 | 14 | 7 | 6 | 15 | 7 | 7 | 19 | 27 | 19 | 45 | 3 | 11 | 26 | 31 | 27 | 3 | 1 | 10 | 6 | 7 | 10 | 1 |  |  | 2 | 6 | 9 |
| **Б** | 5 |  |  |  |  | 9 | 1 |  | 6 |  |  | 6 |  | 2 | 21 |  | 8 | 1 |  | 6 |  |  |  |  |  | 1 | 11 |  |  |  | 2 |
| **В** | 35 | 1 | 5 | 3 | 3 | 32 |  | 2 | 17 |  | 7 | 10 | 3 | 9 | 58 | 6 | 6 | 19 | 6 | 7 |  | 1 | 1 | 2 | 4 | 1 | 18 | 1 | 2 |  | 3 |
| **Г** | 7 |  |  |  | 3 | 3 |  |  | 5 |  | 1 | 5 |  | 1 | 50 |  | 7 |  |  | 2 |  |  |  |  |  |  |  |  |  |  |  |
| **Д** | 25 |  | 3 | 1 | 1 | 29 | 1 | 1 | 13 |  | 1 | 5 | 1 | 13 | 22 | 3 | 6 | 8 | 1 | 10 |  |  | 1 | 1 | 1 |  | 5 | 1 |  |  | 1 |
| **Е** | 2 | 9 | 18 | 11 | 27 | 7 | 5 | 10 | 6 | 15 | 13 | 35 | 24 | 63 | 7 | 16 | 39 | 37 | 33 | 3 | 1 | 8 | 3 | 7 | 3 | 3 |  |  | 1 | 1 | 2 |
| **Ж** | 5 | 1 |  |  | 6 | 12 |  |  | 5 |  |  |  |  | 6 |  |  |  | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **3** | 35 | 1 | 7 | 1 | 5 | 3 |  |  | 4 |  | 2 | 1 | 2 | 9 | 9 | 1 | 3 | 1 |  | 2 |  |  |  |  |  |  | 4 |  |  |  | 4 |
| **И** | 4 | 6 | 22 | 5 | 10 | 21 | 2 | 23 | 19 | 11 | 19 | 21 | 20 | 32 | 8 | 13 | 11 | 29 | 29 | 3 | 1 | 17 | 3 | 11 | 1 | 1 |  |  | 1 | 3 | 17 |
| **И** | 1 | 1 | 4 | 1 | 3 |  | 1 | 2 | 4 |  | 5 | 1 | 2 | 7 | 9 | 7 | 3 | 10 | 2 |  |  |  | 1 | 3 | 2 |  |  |  |  |  |  |
| **К** | 24 | 1 | 4 | 1 |  | 4 | 1 | 1 | 26 |  | 1 | 4 | 1 | 2 | 66 | 2 | 10 | 3 | 7 | 10 |  |  | 1 |  |  |  |  |  |  |  |  |
| **Л** | 25 | 1 | 1 | 1 | 1 | 33 | 2 | 1 | 36 |  | 1 | 2 | 1 | 8 | 30 | 2 |  | 3 | 1 | 6 |  | 4 |  | 1 |  |  | 2 | 30 |  | 4 | 9 |
| **М** | 18 | 2 | 4 | 1 | 1 | 21 | 1 | 2 | 23 |  | 3 | 1 | 3 | 7 | 19 | 5 | 2 | 5 | 3 | 9 | 1 |  |  | 2 |  |  | 5 | 1 | 1 |  | 3 |
| **Н** | 54 | 1 | 2 | 3 | 3 | 34 |  |  | 58 |  | 3 |  | 1 | 24 | 67 | 2 | 1 | 9 | 9 | 7 | 1 |  | 5 | 2 |  |  | 36 | 3 |  |  | 5 |
| **О** | 1 | 28 | 84 | 32 | 47 | 15 | 7 | 18 | 12 | 29 | 19 | 41 | 38 | 30 | 9 | 18 | 43 | 50 | 39 | 3 | 2 | 5 | 2 | 12 | 4 | 3 |  |  | 2 | 3 | 2 |
| **П** | 7 |  |  |  |  | 15 |  |  | 4 |  |  | 9 |  | 1 | 46 |  | 41 | 1 |  | 6 |  |  |  |  |  |  | 2 |  |  |  | 2 |
| **Р** | 55 | 1 | 4 | 4 | 3 | 37 | 3 | 1 | 24 |  | 3 | 1 | 3 | 7 | 56 | 2 | 1 | 5 | 9 | 16 |  | 1 | 1 | 1 | 2 |  | 8 | 3 |  |  | 5 |
| **С** | 8 | 1 | 7 | 1 | 2 | 25 |  |  | 6 |  | 40 | 13 | 3 | 9 | 27 | 11 | 4 | 11 | 82 | 6 |  | 1 | 1 | 2 | 2 |  | 1 | 8 |  |  | 17 |
| **Т** | 35 | 1 | 27 | 1 | 3 | 31 |  | 1 | 28 |  | 5 | 1 | 1 | 11 | 56 | 4 | 26 | 18 | 2 | 10 |  |  |  | 1 |  |  | И | 21 |  |  | 4 |
| **У** | 1 | 4 | 4 | 4 | 11 | 2 | 6 | 3 | 2 |  | 8 | 5 | 5 | 5 | 1 | 5 | 7 | 14 | 7 |  |  | 1 |  | 8 | 3 | 2 |  |  |  | 9 | 1 |
| **Ф** | 2 |  |  |  |  | 2 |  |  | 2 |  |  |  |  |  | 1 |  | 1 | 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Х** | 4 | I | 4 | 1 | 3 | 1 |  | 2 | 3 |  | 4 | 3 | 3 | 4 | 18 | 5 | 3 | 4 | 2 | 2 | 1 |  |  | 1 |  |  |  |  |  |  |  |
| **Ц** | 3 |  |  |  |  | 7 |  |  | 10 |  | 2 |  |  |  | 1 |  |  |  |  | 1 |  |  |  |  |  |  | 1 |  |  |  |  |
| **Ч** | 12 |  |  |  |  | 23 |  |  | 13 |  | 2 |  |  | 6 |  |  |  |  | 7 | 1 |  |  |  |  | 1 |  |  | 1 |  |  |  |
| **Ш** | 5 |  |  |  |  | 11 |  |  | 14 |  | 1 | 2 |  | 2 | 2 |  |  |  |  | 1 |  |  |  |  |  |  |  | 1 |  |  |  |
| **Щ** | 3 |  |  |  |  | 8 |  |  | 6 |  |  |  |  | 1 |  |  |  |  |  | 1 |  |  |  |  |  |  |  |  |  |  |  |
| **Ы** |  | 1 | 9 | 1 | 3 | 12 |  | 2 | 4 | 7 | -3 | 6 | 6 | 3 | 2 | 10 | 3 | 9 | 4 | 1 |  | 16 |  | 1 | 2 |  |  |  |  |  |  |
| **Ь** |  | 2 | 4 | 1 | 1 | 2 |  | 2 | 2 |  | 6 |  | 3 | 13 | 2 | 4 | 1 | 11 | 3 |  |  |  |  | 1 | 4 |  |  |  | 1 | 3 | 1 |
| **Э** |  |  |  |  |  |  |  |  |  |  | 1 |  |  | 1 |  |  |  | 1 | 9 |  |  |  |  |  |  |  |  |  |  |  |  |
| **Ю** |  | 2 | 1 | 2 | 1 |  |  | 3 | 1 |  | 1 |  | 1 | 1 | 1 | 3 | 1 | 1 | 7 |  |  |  | 1 | 1 |  | 4 |  |  |  |  |  |
| **Я** | 1 | 3 | 9 | 1 | 3 | 3 | 1 | 5 | 3 | 2 | 3 | 3 | 4 | 6 | 3 | 6 | 3 | 6 | 10 |  |  | 2 | 1 | 4 | 1 | 1 |  |  | 1 | 1 | 1 |

Таблица 6. Таблица частот биграмм английского языка

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **А** | **В** | **С** | **D** | **Е** | **F** | **G** | **Н** | **I** | **J** | **К** | **L** | **М** | **N** | **О** | **Р** | **Q** | **R** | **S** | **Т** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| **А** | 4 | 20 | 28 | 52 | 2 | 11 | 28 | 4 | 32 | 4 | 6 | 62 | 23 | 167 | 2 | 14 | 0 | 83 | 76 | 127 | 7 | 25 | 8 | 1 | 9 | 1 |
| **В** | 13 | 0 | 0 | 0 | 55 | 0 | 0 | 0 | 8 | 2 | 0 | 22 | 0 | 0 | 11 | 0 | 0 | 15 | 4 | 2 | 13 | 0 | 0 | 0 | 15 | 0 |
| **С** | 32 | 0 | 7 | 1 | 69 | 0 | 0 | 33 | 17 | 0 | 10 | 9 | 1 | 0 | 50 | 3 | 0 | 10 | 0 | 28 | 11 | 0 | 0 | 0 | 3 | 0 |
| **D** | 40 | 16 | 9 | 5 | 65 | 18 | 3 | 9 | 56 | 0 | 1 | 4 | 15 | 6 | 16 | 4 | 0 | 21 | 18 | 53 | 19 | 5 | 15 | 0 | 3 | 0 |
| **Е** | 84 | 20 | 55 | 125 | 51 | 40 | 19 | 16 | 50 | 1 | 4 | 55 | 54 | 146 | 35 | 37 | 6 | 191 | 149 | 65 | 9 | 26 | 31 | 12 | 5 | 0 |
| **F** | 19 | 3 | 5 | 1 | 19 | 21 | 1 | 3 | 30 | 2 | 0 | 11 | 1 | 0 | 51 | 0 | 0 | 26 | 8 | 47 | 6 | 3 | 3 | 0 | 2 | 0 |
| **G** | 20 | 4 | 3 | 2 | 35 | 1 | 3 | 15 | 18 | 0 | 0 | 5 | 1 | 4 | 21 | 1 | 1 | 20 | 9 | 21 | 9 | 0 | 5 | 0 | 1 | 0 |
| **Н** | 101 | 1 | 3 | 0 | 270 | 5 | 1 | 6 | 57 | 0 | 0 | 0 | 3 | 2 | 44 | 1 | 0 | 3 | 10 | 18 | 6 | 0 | 5 | 0 | 3 | 0 |
| **I** | 40 | 7 | 51 | 23 | 25 | 9 | 11 | 3 | 0 | 0 | 2 | 38 | 25 | 202 | 56 | 12 | 1 | 46 | 79 | 117 | 1 | 22 | 0 | 4 | 0 | 3 |
| **J** | 3 | 0 | 0 | 0 | 5 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 |
| **К** | 1 | 0 | 0 | 0 | 11 | 0 | 0 | 0 | 13 | 0 | 0 | 0 | 0 | 2 | 2 | 0 | 0 | 0 | 6 | 2 | 1 | 0 | 2 | 0 | 1 | 0 |
| **L** | 44 | 2 | 5 | 12 | 62 | 7 | 5 | 2 | 42 | 1 | 1 | 53 | 2 | 2 | 25 | 1 | 1 | 2 | 16 | 23 | 9 | 0 | 1 | 0 | 33 | 0 |
| **М** | 52 | 14 | 1 | 0 | 64 | 0 | 0 | 3 | 37 | 0 | 0 | 0 | 7 | 1 | 17 | 18 | 1 | 2 | 12 | 3 | 8 | 0 | 1 | 0 | 2 | 0 |
| **N** | 42 | 10 | 47 | 122 | 63 | 19 | 106 | 12 | 30 | 1 | 6 | 6 | 9 | 7 | 54 | 7 | 1 | 7 | 44 | 124 | 6 | 1 | 15 | 0 | 12 | 0 |
| **О** | 7 | 12 | 14 | 17 | 5 | 95 | 3 | 5 | 14 | 0 | 0 | 19 | 41 | 134 | 13 | 23 | 0 | 91 | 23 | 42 | 55 | 16 | 28 | 0 | 4 | 1 |
| **Р** | 19 | 1 | 0 | 0 | 37 | 0 | 0 | 4 | 8 | 0 | 0 | 15 | 1 | 0 | 27 | 9 | 0 | 33 | 14 | 7 | 6 | 0 | 0 | 0 | 0 | 0 |
| **Q** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 17 | 0 | 0 | 0 | 0 | 0 |
| **R** | 83 | 8 | 16 | 23 | 169 | 4 | 8 | 8 | 77 | 1 | 10 | 5 | 26 | 16 | 60 | 4 | 0 | 24 | 37 | 55 | 6 | 11 | 4 | 0 | 28 | 0 |
| **S** | 65 | 9 | 17 | 9 | 73 | 13 | 1 | 47 | 75 | 3 | 0 | 7 | 11 | 12 | 56 | 17 | 6 | 9 | 48 | 116 | 35 | 1 | 28 | 0 | 4 | 0 |
| **Т** | 57 | 22 | 7 | 1 | 76 | 5 | 2 | 330 | 126 | 1 | 0 | 14 | 10 | 6 | 79 | 7 | 0 | 49 | 50 | 56 | 21 | 2 | 27 | 0 | 24 | 0 |
| **U** | 11 | 5 | 9 | 6 | 9 | 1 | 6 | 0 | 9 | 0 | 1 | 19 | 5 | 31 | 1 | 15 | 0 | 47 | 39 | 31 | 0 | 3 | 0 | 0 | 0 | 0 |
| **V** | 7 | 0 | 0 | 0 | 72 | 0 | 0 | 0 | 28 | 0 | 0 | 0 | 0 | 0 | 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 |
| **W** | 36 | 1 | 1 | 0 | 38 | 0 | 0 | 33 | 36 | 0 | 0 | 4 | 1 | 8 | 15 | 0 | 0 | 0 | 4 | 2 | 0 | 0 | 1 | 0 | 0 | 0 |
| **X** | 1 | 0 | 2 | 0 | 0 | 1 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 1 | 5 | 0 | 0 | 0 | 3 | 0 | 0 | 1 | 0 | 0 | 0 |
| **Y** | 14 | 5 | 4 | 2 | 7 | 12 | 2 | 6 | 10 | 0 | 0 | 3 | 7 | 5 | 17 | 3 | 0 | 4 | 16 | 30 | 0 | 0 | 5 | 0 | 0 | 0 |
| **Z** | 1 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Пример криптоанализа шифра замены**

Известно, что зашифровано стихотворение Р. Киплинга в переводе С.Я. Маршака. Шифрование заключалось в замене каждой буквы на двузначное число. Отдельные слова разделены несколькими пробелами, знаки препинания сохранены. Таблица частот букв русского языка приведена выше.

29 15 10 17 29 22 25 31 15 33 35 41 43 45 35 57 45 25 17 59 15 10 25 41 25

69, 59 78 29 82 25 78 25 17 15 10 88 90 78 25 62 25 22 10 57 73 79 35 67 78 90

88 29 45 35 29, 54 57 90 31 90 73 22 88 15 88 29 15 17 69 41 25 15, 70 17 90 57 43

59 15 78 15 62 22 25 17 57 25 69 88 15 82 17 25 88 29 45 35…

Подсчитаем частоты шифрообразований:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | 29 | 15 | 10 | 17 | 22 | 25 | 31 | 33 | 35 | 41 | 43 | 45 | 57 |
| Количество | 7 | 10 | 4 | 7 | 4 | 12 | 2 | 1 | 5 | 3 | 2 | 4 | 5 |
| Обозначение | 59 | 69 | 78 | 82 | 88 | 90 | 62 | 73 | 79 | 67 | 54 | 70 |
| Количество | 3 | 3 | 4 | 2 | 6 | 5 | 1 | 2 | 1 | 1 | 1 | 1 |

Из таблица частот букв русского языка видно, что чаще всего встречается буква О, на втором месте Е. В нашем шифротексте чаще всего встречается обозначение 25 (12 раз), на втором месте идет обозначение 15 (10 раз), остальные обозначения им существенно уступают. Поэтому можем выдвинуть гипотезу: 25=О, 15=Е. Однако, текст у нас не очень большой, поэтому закономерности русского языка проявляются в нем не обязательно в строгом соответствии с таблицей частот букв русского языка. Поэтому возможен и вариант: 25=Е, 15=О. Но тогда последнее слово в третьей строке имеет окончание ЕО, что возможно, но все же более вероятный вариант ОЕ. Итак, будем работать с текстом, считая, что 25=О, 15=Е.

Теперь нам поможет знак препинания: «29, …». Крайне маловероятно, чтобы запятая стояла после согласной. Итак, 29 – гласная, причем вероятнее всего 29=И или 29=А, т.к. гласные Я, Ю, Э, У встречаются в осмысленных текстах на русском языке намного реже, чем И и А, что не противоречит таблице частот шифротекста.

В последней строке: 88 15, но 15=Е, следовательно, 88 – согласная, причемнаиболее вероятные значения – это Н и Т. Итак, 25=О, 15=Е, 29=А, 88= *Н*

Теперь третье слово в третьей строке имеет 4 варианта:

* + 29=И, 88=Н: 22 Н Е Н И Е
	+ 29=И, 88=Т: 22 Т Е Т И Е
	+ 29=А, 88=Н: 22 Н Е Н А Е
	+ 29=А, 88=Т: 22 Т Е Т А Е

Из рассмотренных вариантов лишь один является осмысленным, и он позволяет найти значение 22. Имеем: 22=М и третье слово в третье строке М Н Е Н И Е.

Теперь рассмотрим второе слово в первой строке. Е 10 17 И, причем 10 и 17 – согласные, и это не М и не Н. Наиболее вероятное слово Е С Л И, т.е. 10=С, 17=Л. Конечно, если мы, продолжая работать с текстом, вдруг получим «нечитаемое» слово, то придется вернуться к этому этапу и рассмотреть другие варианты. Однако, это маловероятно, поскольку вряд ли в стихотворении были слова наподобие Е Р Т И, Е В Л И и т.п.

Далее, первое слово второй строки: 59 78 И, причем 59 и 78 – согласные, и это не С, не Л, не М и не Н. Так что это слово П Р И, т.е. 59=П, 78=Р. Тогда шестое слово первой строки 45 О Л П Е, что дает значение 45=Т и тогда при 57=В получаем фрагмент «…В Т О Л П Е…». Также второе слово последней строки П Е Р Е 62 дает нам значение 62=Д.

Далее рассмотрим начало второй строки: «П Р И 82 О Р О Л Е С Н 90 Р О Д О М …». Из него следует, что 82=К и 90=А.

Зная, что 82=К, посмотрим на самое последнее слово К Л О Н И Т 35, откуда станет ясно, что 35=Ь.

Перед последней атакой выпишем текст, заменяя известные обозначения буквами.

И Е С Л И М О 31 Е 33 Ь 41 43 Т Ь В Т О Л П Е С О 41 О 69,

П Р И К О Р О Л Е С Н А Р О Д О М С В 73 79 Ь 67 Р А Н И Т Ь

И, 54 В А 31 А 73 М Н Е Н И Е Л 69 41 О Е,

70 Л А В 43 П Е Р Е Д М О Л В О 69 Н Е К Л О Н И Т Ь…

Из последней строки: 69=Ю, тогда слова Л Ю 41 О Е и С О 41 О Ю определяют 41: 41=Б. Теперь из четвертого слова первой строки Б 43 Т Ь получаем, что 43=Ы. А первое слово из последней строки 70 Л А В Ы – это Г Л А В Ы. Слово в первой строке М О 31 Е 33 Ь угадывается из контекста: М О Ж Е Ш Ь, т.е. 31=Ж, 33=Ш. Теперь второе слово в третьей строке запишется как 54 В А Ж А 73, откуда, с учетом контекста: 54=У, 73=Я. После этого окончание второй строки имеет вид «… С В Я 79 Ь 67 Р А Н И Т Ь». Легко определяются буквы 79=З, 67=Х.

**Ответ:**И Е С Л И М О Ж Е Ш Ь Б Ы Т Ь В Т О Л П Е С О Б О Ю,
П Р И К О Р О Л Е С Н А Р О Д О М С В Я З Ь Х Р А Н И Т Ь И,
У В А Ж А Я М Н Е Н И Е Л Ю Б О Е, Г Л А В Ы П Е Р Е Д
М О Л В О Ю Н Е К Л О Н И Т Ь…

**4. ШИФР ВИЖЕНЕРА**

**Теория криптоанализа шифра Виженера**

Рассмотрим шифр модульного гаммирования с уравнением
**bi = (ai+ yi) mod n**, для которого гамма является периодической последовательностью знаков алфавита. Такая гамма обычно получается периодическим повторением некоторого ключевого слова. Например, ключевое слово KEY дает гамму KEYKEYKEY... . Рассмотрим задачу вскрытия такого шифра по тексту одной криптограммы достаточной длины.

Пусть μ - длина ключевого слова. Обычно криптоанализ шифра Виженера проводится в два этапа. На первом этапе определяется число μ, на втором этапе — само ключевое слово.

Для определения числа μ применяется так называемый тест Казиски, названный в честь Ф. Казиски, применившего его в 1863 г. Тест основан на простом наблюдении о том, что два одинаковых отрезка открытого текста, отстоящих друг от друга на расстоянии, кратном μ, будут одинаково зашифрованы. В силу этого в шифр-тексте ищутся повторения длины, не меньшей трех, и расстояния между ними. Обратим внимание на то, что случайно такие одинаковые отрезки могут появиться в тексте с достаточно малой вероятностью.

Пусть d1,d2,... — найденные расстояния между повторениями и d — наибольший общий делитель этих чисел. Тогда μ должно делить d. Чем больше повторений имеет текст, тем более вероятно, что μ совпадает с d. Для уточнения значения μ, можно использовать так называемый индекс совпадения, введенный в практику У. Фридманом в 1920 г.

Для строки х = (x1,...,,xm) длины т, составленной из букв алфавита А, индексом совпадения в х, обозначаемым Ic(х) будем называть вероятность того, что две случайно выбранные буквы из х совпадают.

Пусть A = { ai,..., an }. Будем отождествлять буквы алфавита с числами, так что a1 ≡ 0,..., an-1 ≡ n - 2, аn = n -1.

Теорема. Индекс совпадения в х вычисляется по формуле



где fi — число вхождений буквы ai в х, I *Є* Zn.

Доказательство. Будем вычислять Iс(х) как отношение числа благоприятных исходов к общему числу исходов. Благоприятным является исход, при котором на выбранных двух позициях в х расположены одинаковые буквы. Общее число исходов равно, очевидно, С2m . Число благоприятных исходов есть



В самом деле, переупорядочим буквы в х таким образом, чтобы сначала шли fa1 букв а1 затем — fa2 букв *а2* и т.д.(4):



Теперь заметим, что при случайном выборе мест (*i* и *j)* в строке *х* благоприятными являются следующие исходы:



В случае (*а1*) мы можем выбрать пару букв а, из набора (3) *С2fa*1 способами, в случае (*а2*) пару букв *а2* из (3) — *С2fa*2способами и т. д.

Таким образом, общее число благоприятных исходов выражается величиной (2), а индекс совпадения в *х* — формулой



и, следовательно, формулой (1).

Пусть *х* — строка осмысленного текста (например, английского). Допустим, как и ранее, что буквы в *х* появляются на любом месте текста с соответствующими вероятностями *р0,...,рn-1* независимо друг от друга, где *рi* — вероятность появления буквы *i* в осмысленном тексте, i Є Zn В такой модели открытого текста вероятность того, что две случайно выбранные буквы из *х* совпадают с *i* Є Zn равна *p2i* следовательно,



Взяв за основу значения вероятностей *рi* для открытых текстов на английском языке, получаем приближение . Тем самым для английских текстов *х* можно пользоваться следующим приближением для индекса совпадения: *Ic(x) ≈* 0,066.

Аналогичные приближения можно получить и для других языков. Так, для русского языка получаем приближение: *Iс(x) ≈* 0,053.

Приведем значения индексов совпадения для ряда европейских языков:

Таблица 7. Индексы совпадения европейских языков

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Язык | Русский | Англ | Франц | Нем | Итал | Испан |
| *Ic(x) ≈* | 0,0529 | 0,0662 | 0,0778 | 0,0762 | 0,0738 | 0,0775 |

Рассуждения, использованные при выводе формулы (4), остаются, очевидно, справедливыми и в случае, когда *х* результат зашифрования некоторого открытого текста простой заменой. В этом случае вероятности *рi* переставляются местами, но сумма остается неизменной.

Предположим, что *х* — реализация независимых испытаний случайной

величины, имеющей равномерное распределение на Z*n*. Тогда индекс совпадения вычисляется по формуле



Вернемся к вопросу об определении числа μ. Пусть y = *y1* y*2* …y*n* — данный шифр-текст. Выпишем его с периодом μ:



и обозначим столбцы получившейся таблицы через *Y↓1,..., Y↓μ*. Если *μ* это

истинная длина ключевого слова, то каждый столбец *Y↓i, i Є 1, μ*, представляет собой участок открытого текста, зашифрованный простой заменой, определяемой подстановкой



для некоторого s *Є* 0, n-l (числа берутся по модулю n).

В силу сказанного выше, (для английского языка) *Iс(Y↓i) ≈* 0,066 при любом *i*. С другой стороны, если *μ* отлично от длины ключевого слова, то столбцы *Y↓i* будут более "случайными", поскольку они являются результатом зашифрования фрагментов открытого текста некоторым многоалфавитным шифром. Тогда *Iс(Y↓i)* будет ближе (для английского языка) к числу 1/28 ≈ 0,038

Заметная разница значений *Iс(x)* для осмысленных открытых текстов и случайных последовательностей букв (для английского языка — 0,066 и 0,038, для русского языка — 0,053 и 0,030) позволяет в большинстве случаев установить точное значение *μ.*

Предположим, что на первом этапе мы нашли длину ключевого слова *μ.* Рассмотрим теперь вопрос о нахождении самого ключевого слова. Для его нахождения можно использовать так называемый *взаимный индекс совпадения.*

Пусть *х = (х1 ,...,хп),у = (у1,...,ут)*— две строки букв алфавита А. Взаимным индексом совпадения *х и у,* обозначаемым *МIс(х, у),* называется вероятность того, что случайно выбранная буква из *х* совпадает со случайно выбранной буквой из *у.*

Пусть *f0 f1 …fn* и *f10 f11* …*f1n-1* — числа вхождений букв алфавита в *х и у* соответственно.

**Теорема.** *Взаимный индекс совпадения в х и у вычисляется по формуле* (эта теорема доказывается точно так же, как и предыдущая теорема.)

**

Пусть k = (*k1*,..., *kμ*,) — истинное ключевое слово. Попытаемся оценить индексы *MIc(Y↓i, Y↓j)*

Для этого напомним, что *Y↓3* является результатом зашифрования фрагмента открытого текста простой заменой, определяемой подстановкой (5) при некотором *s.* Вероятность того, что *Y↓i* и *Y↓j* произвольная пара букв равна 0, имеет вид *pn-si\*pn-sj* (где *ра* — вероятность появления буквы а в открытом тексте); вероятность того, что обе буквы есть 1, равна
*pn-si+1\*pn-sj+1* и так далее. На основании этого получаем:



Заметим, что сумма в правой части последнего равенства зависит только от разности *(si – sj)mod n ,* которую назовем *относительным сдвигом Y↓i* и *Y↓j*. Заметим также, что



поэтому *Y↓i* и *Y↓j* с относительными сдвигами *s* и *п-s* имеют одинаковые взаимные индексы совпадения. Приведем таблицу значений сумм (7) для английского языка:

Таблица 8. Взаимный индекс совпадения при сдвиге *s*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ***Сдвиг s*** | ***0*** | ***1*** | ***2*** | ***3*** | ***4*** | ***5*** | ***6*** |
| ***MI*** *c***(*x*, *y*) ≈** | 0,066 | 0,039 | 0,032 | 0,034 | 0,044 | 0,033 | 0,036 |
| ***Сдвиг s*** | *7* | *8* | *9* | *10* | *11* | *12* | *13* |
| ***MI*** *c***(*x*, *y*) ≈** | 0,039 | 0,034 | 0,034 | 0,038 | 0,045 | 0,039 | 0,043 |

Обратим внимание на то, что ненулевые "сдвиги" дают взаимные индексы совпадения, изменяющиеся в пределах от 0,032 до 0,045, в то время как при нулевом сдвиге индекс *MIc(x,y)* близок к 0,066. Это наблюдение позволяет определить величины относительных сдвигов *si – sj* столбцов *Y↓i* и *Y↓j*. Для этого заметим, что при некотором значении *s(i,j)Є*0, n-1столбец *Ys(i,j)↓j*, полученный из *Y↓j* прибавлением к каждому его элементу числа *S(i,j)* (по модулю *n*), имеет нулевой относительный сдвиг с *Y↓j*.

Пусть *Y0↓j , Y1↓j,…, Yn-1↓j* – результаты зашифрования *Y↓j* каждой из простых замен (5). Несложно вычислить взаимные индексы

**

(всего, таким образом, имеется *С2μn* значений). Для этого воспользуемся формулой, полученной из (6):

**

Если *s* равно *si – sj* - (относительному сдвигу *Y↓i* и *Y↓j*), то взаимный индекс впадения должен быть (для английского языка) близок к 0,066, так как относительный сдвиг *Y↓i* и *Y↓j* равен нулю. Если же s не равно *si – sj* то взаимный индекс совпадения должен колебаться в пределах 0,032 - 0,045.

Используя изложенный метод, мы сможем связать системой уравнений относительные сдвиги различных пар столбцов *Y↓i* и *Y↓j*. В результате останется 26 (для английского языка) вариантов для ключевого слова, из которых можно выбрать наиболее предпочтительный вариант (если ключевое слово является осмысленным).

Следует отметить, что предложенный метод будет эффективным для не слишком больших значений μ. Это объясняется тем, что для хороших сближений индексов совпадения требуются тексты достаточно большой длины.

**Пример криптоанализа текста:**

Задан некоторый текст зашифрованный шифром Виженера, требуется определить ключевое слово и прочитать открытый текст.

Шифрованный текст:

влцдутжбюцхъяррмшбрхцэооэцг**брь**цмйфктъъюьмшэсяцпунуящэйтаьэдкци**брь**цгбрпачкъуцпъбьсэгкцъгуущарцёэвърюуоюэкааэбрняфукабъарпяъафкъиьжяффнйояфывбнэнфуюг**брь**сшьжэтбэёчюъюръегофкбьчябашвёэуъъюаднчжчужцёэвлрнчулбюпцуруньъшсэюъзкцхъяррнрювяспэмасчкпэужьжыатуфуярюравртубурьпэщлафоуфбюацмнубсюкйтаьэдйюнооэгюожбгкбрънцэпотчмёодзцвбцшщвщепчдчдръюьскасэгъппэгюкдойрсрэвоопчщшоказръббнэугнялёкьсрбёуыэбдэулбюасшоуэтъшкрсдугэфлбубуъчнчтртпэгюкиугюэмэгюккъъпэгяапуфуэзьрадзьжчюрмфцхраююанчёчюъыхьъцомэфъцпоирькнщпэтэузуябащущбаыэйчдфрпэцъьрьцъцпоилуфэдцойэдятррачкубуфнйтаьэдкцкрннцюабугюуубурьпйюэъжтгюркующоъуфъэгясуоичщщчдцсфырэдщэъуяфшёчцюйрщвяхвмкршрпгюопэуцчйтаьэдкци**брь**цыяжтюрбуэтэбдуящэубъибрювъежагибрбагбрымпуноцшяжцечкфодщоъчжшйуъцхчщвуэбдлдъэгясуахзцэбдэулькнъщбжяцэьрёдъьвювлрнуяфуоухфекьгцчччгэъжтанопчынажпачкъуъмэнкйрэфщэъьбудэндадъярьеюэлэтчоубъцэфэвлнёэгфдсэвэёкбсчоукгаутэыпуббцчкпэгючсаъбэнэфъркацхёваетуфяепьрювържадфёжбьфутощоявьъгупчршуитеачйчирамчюфчоуяюонкяжыкгсцбрясшчйотъъжрсщчл

Для определения числа букв в данном ключевом слове применяется так называемый тест Казиски. Тест основан на простом наблюдении о том, что два одинаковых отрезка открытого текста, отстоящих друг от друга на расстоянии, кратном μ (количество букв в слове), будут одинаково зашифрованы. В силу этого в шифротексте ищутся повторения длины, не меньшей трех, и расстояния между ними. Необходимо обратить внимание на то, что случайно такие одинаковые отрезки могут появиться в тексте с достаточно малой вероятностью.

В данном тексте обнаружено четырехкратное повторение буквосочетания «брь». Выясним расстояние между ними и найдем наибольший общий делитель этих расстояний.

В результате получаем: 35, 85, 510

НОД = 5;

Следовательно, с определенной долей вероятности можно заключить, что длина кодового слова равна 5.

Для подтверждения гипотезы воспользуемся математической статистикой для определения длины ключевого слова. Для этого запишем шифр-текст в таблицу с 5 столбцами, предполагая, что длина ключевого слова равна 5.

Вычислим взаимные индексы совпадения *IC(x)* букв в каждом из столбцов таблицы, для достоверного установления длины ключевого слова. Для этого посчитаем частоту повторения букв в каждом столбце. Таблица состоит из 5 столбцов, так как на предыдущем этапе нами было установлено, что ключевое слово по НОД может состоять из 5 букв.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Y1** | **Y2** | **Y3** | **Y4** | **Y5** |
| **В** | л | ц | д | у |
| **Т** | ж | б | ю | ц |
| **Х** | ъ | я | р | р |
| **М** | ш | б | р | х |
| **Ц** | э | о | о | э |
| **Ц** | г | б | р | ь |
| **Ц** | м | й | ф | к |
| **Т** | ъ | ъ | ю | ь |
| **М** | ш | э | с | я |
| **Ц** | п | у | н | у |
| **Я** | щ | э | й | т |
| **А** | ь | э | д | к |
| **Ц** | и | б | р | ь |
| **Ц** | г | б | р | п |
| **А** | ч | к | ъ | у |
| **Ц** | п | ъ | б | ь |
| **С** | э | г | к | ц |
| **Ъ** | г | у | у | щ |
| **А** | р | ц | ё | э |
| **В** | ъ | р | ю | у |
| **О** | ю | э | к | а |
| **А** | э | б | р | н |
| **Я** | ф | у | к | а |
| **Б** | ъ | а | р | п |
| **Я** | ъ | а | ф | к |
| **Ъ** | и | ь | ж | я |
| **Ф** | ф | н | й | о |
| **Я** | ф | ы | в | б |
| **Н** | э | н | ф | у |
| **Ю** | г | **б** | **р** | **ь** |
| **С** | ш | ь | ж | э |
| **Т** | б | э | ё | ч |
| **Ю** | ъ | ю | р | ъ |
| **Е** | г | о | ф | к |
| **Б** | ь | ч | я | б |
| **А** | ш | в | ё | э |
| **У** | ъ | ъ | ю | а |
| **Д** | н | ч | ж | ч |
| **У** | ж | ц | ё | э |
| **В** | л | р | н | ч |
| **У** | л | б | ю | п |
| **Ц** | у | р | у | н |
| **Ь** | ъ | ш | с | э |
| **Ю** | ъ | з | к | ц |
| **Х** | ъ | я | р | р |
| **Н** | р | ю | в | я |
| **С** | п | э | м | а |
| **С** | ч | к | п | э |
| **У** | ж | ь | ж | ы |
| **А** | т | у | ф | у |
| **Я** | р | ю | р | а |
| **В** | р | т | у | б |
| **У** | р | ь | п | э |
| **Щ** | л | а | ф | о |
| **У** | ф | б | ю | а |
| **Ц** | м | н | у | б |
| **С** | ю | к | й | т |
| **А** | ь | э | д | й |
| **Ю** | н | о | о | э |
| **Г** | ю | о | ж | б |
| **Г** | к | б | р | ъ |
| **Н** | ц | э | п | о |
| **Т** | ч | м | ё | о |
| **Д** | з | ц | в | б |
| **Ц** | ш | щ | в | щ |
| **Е** | п | ч | д | ч |
| **Д** | р | ъ | ю | ь |
| **С** | к | а | с | э |
| **Г** | ъ | п | п | э |
| **Г** | ю | к | д | о |
| **Й** | р | с | р | э |
| **В** | о | о | п | ч |
| **Щ** | ш | о | к | а |
| **З** | р | ъ | б | б |
| **Н** | э | у | г | н |
| **Я** | л | ё | к | ь |
| **С** | р | б | ё | у |
| **Ы** | э | б | д | э |
| **У** | л | б | ю | а |
| **С** | ш | о | у | э |
| **Т** | ъ | ш | к | р |
| **С** | д | у | г | э |
| **Ф** | л | б | у | б |
| **У** | ъ | ч | н | ч |
| **Т** | р | т | п | э |
| **Г** | ю | к | и | у |
| **Г** | ю | э | м | э |
| **Г** | ю | к | к | ъ |
| **Ъ** | п | э | г | я |
| **А** | п | у | ф | у |
| **Э** | з | ь | р | а |
| **Д** | з | ь | ж | ч |
| **Ю** | р | м | ф | ц |
| **Х** | р | а | ю | ю |
| **А** | н | ч | ё | ч |
| **Ю** | ъ | ы | х | ь |
| **Ъ** | ц | о | м | э |
| **Ф** | ъ | ц | п | о |
| **И** | р | ь | к | н |
| **Щ** | п | э | т | э |
| **У** | з | у | я | б |
| **А** | щ | у | щ | б |
| **А** | ы | э | й | ч |
| **Д** | ф | р | п | э |
| **Ц** | ъ | ь | р | ь |
| **Ц** | ъ | ц | п | о |
| **И** | л | у | ф | э |
| **Д** | ц | о | й | э |
| **Д** | я | т | р | р |
| **А** | ч | к | у | б |
| **У** | ф | н | й | т |
| **А** | ь | э | д | к |
| **Ц** | к | р | н | н |
| **Ц** | ю | а | б | у |
| **Г** | ю | у | у | б |
| **У** | р | ь | п | й |
| **Ю** | э | ъ | ж | т |
| **Г** | ю | р | к | у |
| **Ю** | щ | о | ъ | у |
| **Ф** | ъ | э | г | я |
| **С** | у | о | и | ч |
| **Щ** | щ | ч | д | ц |
| **С** | ф | ы | р | э |
| **Д** | щ | э | ъ | у |
| **Я** | ф | ш | ё | ч |
| **Ц** | ю | й | р | щ |
| **В** | я | х | в | м |
| **К** | р | ш | р | п |
| **Г** | ю | о | п | э |
| **У** | ц | ч | й | т |
| **А** | ь | э | д | к |
| **Ц** | и | **б** | **р** | **ь** |
| **Ц** | ы | я | ж | т |
| **Ю** | р | б | у | э |
| **Т** | э | б | д | у |
| **Я** | щ | э | у | б |
| **Ъ** | и | б | р | ю |
| **В** | ъ | е | ж | а |
| **Г** | и | б | р | б |
| **А** | г | б | р | ы |
| **М** | п | у | н | о |
| **Ц** | ш | я | ж | ц |
| **Е** | ч | к | ф | о |
| **Д** | щ | о | ъ | ч |
| **Ж** | ш | й | у | ъ |
| **Ц** | х | ч | щ | в |
| **У** | э | б | д | л |
| **Д** | ъ | э | г | я |
| **С** | у | а | х | з |
| **Ц** | э | б | д | э |
| **У** | л | ь | к | н |
| **Ъ** | щ | б | ж | я |
| **Ц** | э | ь | р | ё |
| **Д** | ъ | ь | в | ю |
| **В** | л | р | н | у |
| **Я** | ф | у | о | у |
| **Х** | ф | е | к | ь |
| **Г** | ц | ч | ч | ч |
| **Г** | э | ъ | ж | т |
| **А** | н | о | п | ч |
| **Ы** | н | а | ж | п |
| **А** | ч | к | ъ | у |
| **Ъ** | м | э | н | к |
| **Й** | р | э | ф | щ |
| **Э** | ъ | ь | б | у |
| **Д** | э | н | д | а |
| **Д** | ъ | я | р | ь |
| **Е** | ю | э | л | э |
| **Т** | ч | о | у | б |
| **Ъ** | ц | э | ф | э |
| **В** | л | н | ё | э |
| **Г** | ф | д | с | э |
| **В** | э | ё | к | б |
| **С** | ч | о | у | к |
| **Г** | а | у | т | э |
| **Ы** | п | у | б | б |
| **Ц** | ч | к | п | э |
| **Г** | ю | ч | с | а |
| **Ъ** | б | э | н | э |
| **Ф** | ъ | р | к | а |
| **Ц** | х | ё | в | а |
| **Е** | т | у | ф | я |
| **Е** | п | ь | р | ю |
| **В** | ъ | р | ж | а |
| **Д** | ф | ё | ж | б |
| **Ь** | ф | у | т | о |
| **Щ** | о | я | в | ь |
| **Ъ** | г | у | п | ч |
| **Р** | ш | у | и | т |
| **Е** | а | ч | й | ч |
| **И** | р | а | м | ч |
| **Ю** | ф | ч | о | у |
| **Я** | ю | о | н | к |
| **Я** | ж | ы | к | г |
| **С** | ц | б | р | я |
| **С** | ш | ч | й | о |
| **Т** | ъ | ъ | ж | р |
| **С** | щ | ч | л |  |

Частота повторения букв в столбцах:

1 столбец (общее количество букв m=198)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | а | б | в | г | д | е | ё | ж | з | и | й | к | л |
| Количество | 17 | 2 | 10 | 16 | 14 | 7 | 0 | 1 | 1 | 3 | 2 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| Количество | 3 | 4 | 1 | 0 | 1 | 16 | 9 | 14 | 5 | 5 | 23 | 0 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | щ | ъ | ы | ь | э | ю | я |
| Количество | 5 | 10 | 3 | 2 | 2 | 10 | 11 |



2 столбец (общее количество букв m=198)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | а | б | в | г | д | е | ё | ж | з | и | й | к | л |
| Количество | 2 | 2 | 0 | 7 | 1 | 0 | 0 | 4 | 4 | 5 | 0 | 3 | 11 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| Количество | 3 | 5 | 2 | 10 | 18 | 0 | 2 | 3 | 14 | 2 | 7 | 9 | 11 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | щ | ъ | ы | ь | э | ю | я |
| Количество | 9 | 26 | 2 | 5 | 14 | 15 | 2 |



3 столбец (общее количество букв m=198)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | а | б | в | г | д | е | ё | ж | з | и | й | к | л |
| Количество | 9 | 24 | 1 | 1 | 1 | 2 | 4 | 0 | 1 | 0 | 3 | 10 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| Количество | 2 | 6 | 17 | 1 | 9 | 1 | 3 | 19 | 0 | 1 | 6 | 14 | 4 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | щ | ъ | ы | ь | э | ю | я |
| Количество | 1 | 8 | 4 | 14 | 23 | 3 | 6 |

4 столбец (общее количество букв m=198)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | а | б | в | г | д | е | ё | ж | з | и | й | к | л |
| Количество | 0 | 5 | 8 | 5 | 13 | 0 | 9 | 16 | 0 | 3 | 9 | 15 | 2 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| Количество | 4 | 9 | 4 | 14 | 27 | 5 | 3 | 13 | 13 | 2 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | щ | ъ | ы | ь | э | ю | я |
| Количество | 2 | 5 | 0 | 0 | 0 | 9 | 2 |



5 столбец (общее количество букв m=197)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | а | б | в | г | д | е | ё | ж | з | и | й | к | л |
| Количество | 15 | 18 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 2 | 9 | 1 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| Количество | 1 | 6 | 11 | 5 | 5 | 0 | 8 | 19 | 0 | 1 | 6 | 17 | 0 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | щ | ъ | ы | ь | э | ю | я |
| Количество | 4 | 4 | 2 | 13 | 33 | 4 | 9 |



По полученным индексам совпадения можно сказать, что длина ключевого слова выбрана верно и равна 5.

После того как мы нашли длину ключевого слова произведем поиск его истинного значения. Для его нахождения можно использовать так называемый взаимный индекс совпадения
 *., где*

*fi, fi* 1 *-* частота буквы i в столбцах *Yi, Yi1* соответственно;

m, m` - число букв в столбцах , *Yi, Yi1* соответственно;

Так как каждый из столбцов таблицы является результатом зашифрования фрагмента открытого текста простой заменой, определяемой подстановкой, то попытаемся оценить взаимные индексы совпадения.

Взаимный индекс совпадения значения ключевого слова для русского языка должен находиться в приделах 0,053 – 0,07. И для его вычисления предварительно необходимо определить относительный сдвиг всех столбцов относительно первого.

Сдвиг 2-го столбца на 6 позиций

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | а | б | в | г | д | е | ё | ж | з | и | й | к | л |
| Количество | 26 | 2 | 5 | 14 | 15 | 2 | 2 | 2 | 0 | 7 | 1 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| Количество | 4 | 4 | 5 | 0 | 3 | 11 | 3 | 5 | 2 | 10 | 18 | 0 | 2 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | щ | ъ | ы | ь | э | ю | я |
| Количество | 3 | 14 | 2 | 7 | 9 | 11 | 9 |

*MIc(Y1,Y26)=* 0.05494

Сдвиг 3-го столбца на 3 позиции

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | а | б | в | г | д | е | ё | ж | з | и | й | к | л |
| Количество | 23 | 3 | 6 | 9 | 24 | 1 | 1 | 1 | 2 | 4 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| Количество | 3 | 10 | 0 | 2 | 6 | 17 | 1 | 9 | 1 | 3 | 19 | 0 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | щ | ъ | ы | ь | э | ю | я |
| Количество | 6 | 14 | 4 | 1 | 8 | 4 | 14 |

*MIc(Y1,Y33)=* 0.5798

Сдвиг 4-го столбца на 16 позиций

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | а | б | в | г | д | е | ё | ж | з | и | й | к | л |
| Количество | 27 | 5 | 3 | 13 | 13 | 2 | 0 | 1 | 0 | 2 | 5 | 0 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| Количество | 0 | 9 | 2 | 0 | 5 | 8 | 5 | 13 | 0 | 9 | 16 | 0 | 3 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | щ | ъ | ы | ь | э | ю | я |
| Количество | 9 | 15 | 2 | 4 | 9 | 4 | 14 |

*MIc(Y1,Y416)=* 0.06068

Сдвиг 5-го столбца на 3 позиции

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | а | б | в | г | д | е | ё | ж | з | и | й | к | л |
| Количество | 33 | 4 | 9 | 15 | 18 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| Количество | 2 | 9 | 1 | 1 | 6 | 11 | 5 | 5 | 0 | 8 | 19 | 0 | 1 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Обозначение | щ | ъ | ы | ь | э | ю | я |
| Количество | 6 | 17 | 0 | 4 | 4 | 2 | 13 |

*MIc(Y1,Y53)=* 0.06045

По взаимным индексам совпадения можно судить что **с**двиги между столбцами выбраны верно.

Составим уравнения для определения ключевого слова:

g[1]-g[2]=6 g[1]=g[2] + 6 g[2]=g[1] - 6

g[1]-g[3]=3 g[1]=g[3] + 3 g[3]=g[1] - 3

g[1]-g[4]=16 g[1]=g[4] + 16 g[4]=g[1] - 16

g[1]-g[5]=3 g[1]=g[5] + 3 g[5]=g[1] - 3

Теперь только необходимо вычислить значение g[1]

g[l]=1: быюсю g[l]=2: вьятя g[l]=3: гэауа

g[l]=4: дюбфб g[l]=5: еявхв g[l]=6: ёагцг

g[l]=7: жбдчд g[l]=8: звеше g[l]=9: игёщё

g[l]=10: йджъж g[l]=ll: кезыз g[l]=12: лёиьи

g[lj=13: мжйэй g[l]=14: нзкюк g[l]=15: оилял

g[l]=16: пймам g[l]=17: pкнбн g[l]=18: «**словоｻ**

g[l]=19: тмпгп g[l]=20: унрдр g[l]=21: фосес

g[l]=22: xптёт g[l]=23: цружу g[l]=24: чсфзф

g[l]=25: штхих g[l]=26: щуцйц g[l]=27: ъфчкч

g[l]=28: ыхшлш g[l]=29: ьцщмщ g[l]=30: эчънъ

g[l]=31: юшыоы g[l]=32: ящьпь

Найдено одно ключевое слово «СЛОВО»

Расшифруем зашифрованный текст:

Развебытьздоровымтожесамоечтонебытьбольнымопределенноздоровьеэтонечтобольшеедлянасфизическоездоровьеэтоисостояниеиспособностьиэнергиязаниматьсятемчтонамнеобходимополучатьприэтомудовольствиеивыздоравливатьбезвсякойпомощиздоровьепарадоксальновынеможетенепосредственнозаставитьсебястатьздоровымвамостаетсятольконаблюдатьзатемкакудивительнаяспособностьвашегоорганизмаисцелятьсебяначинаетдействоватьсамасобойивашебогатствоилибедностьжестокостьилидобродетельностьнеимеютздесьповидимомуникакогозначенияздоровьеэтонечтопозитивноеононеозначаетотказотудовольствияздоровьеявляетсяестественнымследствиемнашегообразажизнивзаимоотношенийдиетыокружающейобстановкиздоровьеэтонепредметсобственностиэтопроцессэтоточтомыделаемрезультатнашихмыслейичувствэтообразсуществованияинтересночтонаправлениемедицинскихисследованийвсебольшеибольшеотклоняетсявсторонутойобластикотораядосихпорсчиталасьсферойдеятельностипсихологовисейчасужетруднопровестичеткиеразграничениямеждуфизическимииментальнымифакторамизаболеваний

**Вывод:** Ключевое слово верное, текст читается