*Агафонова Ирина Витальевна,*
*Дмитриева Оксана Михайловна*

# ЭВОЛЮЦИЯ ШИФРОВ ЗАМЕНЫ: ИДЕИ И МЕХАНИЗМЫ. ЧАСТЬ 1.

Две задачи из области криптографии веками решаются параллельно: как зашифровать сообщение, чтобы его мог прочитать только тот, кому оно адресовано, и как прочесть чужое зашифрованное сообщение. Вторую задачу – взлом шифра – требовалось решать хотя бы для того, чтобы быть уверенным, что надежен твой собственный шифр.

В книгах [1]–[3] можно узнать много интересного о шифрах и приспособлениях для шифрования, изобретенных в разные годы в разных странах. Наш рассказ посвящен только одному классу шифров, известному с древнейших времен – шифрам замены или подстановочным.

Приведенные примеры используют либо 26-буквенный латинский алфавит, иногда усеченный, либо 32-буквенный русский, где отсутствует буква «ё» (заменена на «е»).

## ОПИСАНИЕ ОДНОАЛФАВИТНОЙ ЗАМЕНЫ

При таком шифровании каждая буква алфавита заменяется другой по некоторой фиксированной схеме, например, как в таблице 1.

Тогда сообщение «secret» кодируется как «vjlwju»

Здесь и отправитель, и получатель должны знать таблицу кодов, и, если получатель ее не знает, отправитель должен найти способ передать ему эту таблицу.

Вот один из таких шифров, предложенный еще во II веке до н.э. греческим историком Полибием (таблица 2). В квадрат 5×5 вписаны 25 букв алфавита. Каждая буква шифруется той, которая стоит в квадрате сразу под ней, а если буква находится в последней строке, то она шифруется буквой того же столбца из первой строки.

То же сообщение «secret» кодируется как «xkhwky».

Еще один и, видимо, самый знаменитый вариант шифра замены, связывают с именем Юлия Цезаря. Каждая буква алфа-

**Таблица 2.** Квадрат Полибия

| | | | | |
|---|---|---|---|---|
| a | b | c | d | e |
| f | g | h | i | k |
| l | m | n | o | p |
| q | r | s | t | u |
| v | w | x | y | z |

**Таблица 1.** Шифр замены

| Буква | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Код | n | m | l | k | j | i | h | g | f | e | d | c | b | a | z | y | x | w | v | u | t | s | r | q | p | o |

**Таблица 3.** Шифр Цезаря

| буква | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| код | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c |

вита заменяется другой буквой, стоящей в алфавите правее на фиксированное число позиций. В таблице 3 приведен шифр Цезаря со сдвигом на три позиции.

Сообщение «secret» кодируется как «vhfuhw».

Если получатель знает, что применялся шифр Цезаря со сдвигом, равным 3, то он восстановит текст.

А если мы не знаем величину сдвига? В этом случае шифр все равно недостаточно защищен. Взломаем шифр Цезаря с помощью следующего простого приема. Взглянув на достаточно длинный набор каких–либо букв (например, из десяти букв), мы можем сказать, является ли этот набор частью осмысленного текста. Возьмем с десяток вертикальных полосок, на которых написан алфавит, и рассмотрим некоторое зашифрованное сообщение.

*...как прочесть чужое зашифрованное сообщение.*

Пусть это сообщение написано на русском языке и начинается с текста «юзшвцчхиптп».

Приложим вертикальные полоски друг к другу так, чтобы в каком-то выбранном нами ряду по горизонтали получалось начало текста. Читая горизонтальные ряды букв, находим среди беспорядочных сочетаний букв единственное, которое имеет смысл (таблица 4).

Понятно, что такому взлому поддаются только шифры сдвига. Но и остальные шифры простой замены не очень сложно вскрыть. Метод, который используется для расшифровки, называют частотным анализом.

## ЧАСТОТНЫЙ АНАЛИЗ

Этот метод изобрел арабский криптоаналитик Аль-Кинди (Al-Kindi). Метод основан на наблюдении, что одни буквы алфавита встречаются в текстах чаще, чем другие. Например, в английском алфавите чаще всего встречается буква «е».

**Таблица 4.** Вскрытие шифра Цезаря

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ц | я | р | ъ | о | п | н | а | з | к | з |
| ч | а | с | ы | п | р | о | б | и | л | и |
| ш | б | т | ь | р | с | п | в | й | м | й |
| щ | в | у | э | с | т | р | г | к | н | к |
| ъ | г | ф | ю | т | у | с | д | л | о | л |
| ы | д | х | я | у | ф | т | е | м | п | м |
| ь | е | ц | а | ф | х | у | ж | н | р | н |
| э | ж | ч | б | х | ц | ф | з | о | с | о |
| **ю** | **з** | **ш** | **в** | **ц** | **ч** | **х** | **и** | **п** | **т** | **п** |
| я | и | щ | г | ч | ш | ц | й | р | у | р |
| а | й | ъ | д | ш | щ | ч | к | с | ф | с |

Приведем таблицы среднестатистических частот употреблений букв в английском и русском языке.

Конечно, эти таблицы заполнены без учета знаков препинания, цифр и других символов, которые могут встретиться в тексте. Сумма процентов в последней таблице меньше 100, так как при ее составлении учитывались промежутки между словами, которым и принадлежит оставшаяся доля. В русском тексте промежуток – это самая частая «буква».

В тексте достаточно большого объема эти статистические закономерности будут проявляться, но в небольшом отрывке они не обязательно соблюдаются.

Тем не менее, как, может быть, помнит читатель, Шерлоку Холмсу в рассказе «Плясущие человечки» удалось разгадать шифр, состоящий, казалось, из детских рисунков (см. рисунок 1).

Великий сыщик догадался, что имеет дело с шифром простой замены, где роль кодовых символов играют рисунки: каждая буква сообщения кодируется особой фигуркой человечка, а последняя буква слова отмечается флажком в его руке. Имелось пять шифрованных посланий, подобных приведенному на рисунке 1. К успеху Холмса привел частотный анализ и верное предположение, что два из пяти посланий начинаются с имени женщины Илси.

Другой литературный герой, Вильям Легран из рассказа Эдгара По «Золотой жук», столкнулся с непонятным текстом из цифр и других символов и тоже пришел к выводу, что имеет дело с шифром простой замены. Вот этот текст:

53##+305))6*;4826)4#.)4#);806*;48+8||60))85;;]8*;:#*8+83(88)5*+;46(;88*96*?;8)*#(;485);5*+2:*#(;4956*2(5*=4)8||8*;4069285);)6+8)4##;1#9;48081;8:8#1;48+85;4)485+528806*81(#9;48;(88;4(#?34;48)4#;161;:188;#?;

Легран имел дополнительную информацию, позволявшую считать исходный текст написанным на английском языке. И, хотя в

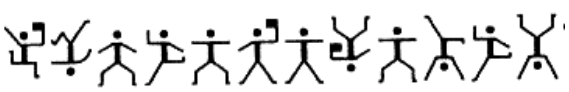


**Рисунок 1.**

*Приложим вертикальные полоски друг к другу...*

его тексте отсутствовали пробелы, он выделил самый распространенный знак 8, встречающийся 34 раза, и, в согласии с таблицей частот, решил, что это буква «е». Затем Легран отыскал целых 7 трехсимвольных сочетаний

;48

и резонно предположил, что это самое частое слово английского языка – артикль the. Дальнейшие рассуждения Леграна привели его к полной расшифровке текста и зарытым сокровищам.

Заметим, что упорядоченность букв английского текста по частоте, которую приводит Эдгар По в этом рассказе, не вполне соответствует таблице 5, но бук-

**Таблица 5.** Частотность букв английского языка

| Буква | Процентное содержание | Буква | Процентное содержание | Буква | Процентное содержание |
|---|---|---|---|---|---|
| a | 8,2 | j | 0,1 | s | 6,3 |
| b | 1,5 | k | 0,8 | t | 9,0 |
| c | 2,8 | l | 4,0 | u | 2,8 |
| d | 4,2 | m | 2,4 | v | 1,0 |
| e | 12,7 | n | 6,7 | w | 2,4 |
| f | 2,2 | o | 7,5 | x | 0,1 |
| g | 2,0 | p | 1,9 | y | 2,0 |
| h | 6,1 | q | 0,1 | z | 0,1 |
| i | 7,0 | r | 6,0 | | |

*Попробуем и мы при помощи частотного анализа дешифровать фрагмент художественного текста.*

ва «е» неизменно лидирует с большим отрывом.

Попробуем и мы при помощи частотного анализа дешифровать фрагмент художественного текста. Мы не ожидаем, что в нем в точности проявятся приведенные в таблице 6 частотные закономерности, тем более что фрагмент этот невелик. Но мы можем, как герои Конан Дойля и По, привлекать к разгадыванию кое-какие дополнительные предположения.

**Таблица 6.** Частотность букв русского языка

| Буква | Процентное содержание | Буква | Процентное содержание | Буква | Процентное содержание |
|---|---|---|---|---|---|
| а | 6,2 | л | 3,5 | ц | 0,4 |
| б | 1,4 | м | 2,6 | ч | 1,2 |
| в | 3,8 | н | 5,3 | ш | 0,6 |
| г | 1,3 | о | 9,0 | щ | 0,3 |
| д | 2,5 | п | 2,3 | ы | 1,6 |
| е,ё | 7,2 | р | 4,0 | ъ,ь | 1,4 |
| ж | 0,7 | с | 4,5 | э | 0,3 |
| з | 1,6 | т | 5,3 | ю | 0,6 |
| и | 6,2 | у | 2,1 | я | 1,8 |
| й | 1,0 | ф | 0,2 | | |
| к | 2,8 | х | 0,2 | | |

Итак, вот текст:

*шч счкх бьш зьш лех чкщшхпшч пнш нпъшу чш м зьэ цтчэьэ чкщшхпшч фкскхый пцэ ыьшхж цкхпчжфтц чтбьшрчец бпхшмпфшц м ыъкмчпчттт ы ьпц бьш ъштыяшотхш ьпщпъж цпроэ пнш оэвшу т зьтц меышфтц лпыфшчпбчец чплшц ы лпнэгтцт щш чпц шлххфкцт пцэ лехш ышмпъвпччш мып ъкмчш м зьэ цтчэьэ фьш ле чт ыьшйх чко чтц бьш ле чт ншмшътх шл чпц шч ъко лех ышхжфш ьшцэ бьш шыькчшмтхтыж чко чтц хиот т рпххх ышхжфш бьшл зьт хиот щшцшнхт пцэ т мшсмъкьтхт ле пнш ф ртсчт фшьшъкй фкскххкыж пцэ ыьшхж щъпфъкычши щшьшцэ бьш шч ькф тчкбп щшчтцкх пп ьпщпъж шч ышлъкх мып ымшт ытхе бьшле щшвпмпхтьжый т щъштсмпыьт фкфшу чтлэож смэф шч ыххклш щшвпмпхтх чшнши т щъштсмпх ыкцшнш пнш ъксркхшлтмвту ыхклеу лшхпсчпччеу ыьшч*

У нас есть основания считать, исходя из используемого алфавита, что исходный текст написан на русском языке.

Как видим, в тексте отсутствуют заглавные буквы и абзацы. Отсутствуют также знаки препинания и другие небуквенные символы. Пробелы сохранены, и это сделает дешифровку возможной, хотя размер этого фрагмента слишком мал для уверенного частотного анализа.

Мы предположим, что использовался шифр простой замены, и проведем частотный анализ текста. Ограничимся списком из десяти самых частых букв (таблица 7).

Нам будет удобно выделять в тексте как прописные те буквы, которые получаются в результате расшифровки.

**Таблица 7.** Частоты десяти букв

| В данном тексте | *ш* | *т* | *п* | *ч* | *х* | *ь* | *к* | *ц* | *ы* | *м* |
|---|---|---|---|---|---|---|---|---|---|---|
| Доля % | 11,3 | 6,6 | 6,5 | 6,3 | 5,3 | 4,8 | 4,5 | 4,0 | 3,8 | 3,1 |
| Стандарт по таблице 6 | О | Е | А | И | Н | Т | С | Р | В | Л |
| Доля % | 9 | 7,2 | 6,2 | 6,2 | 5,3 | 5,3 | 4,5 | 4,0 | 3,8 | 3,5 |

Уже по той причине, что текст содержит отдельные слова *чш* и *шч*, видно, что порядок частот в исследуемом тексте не соответствует стандарту. Тем не менее, стандартный список позволяет начать расшифровку.

По частоте заметно выделяется буква *ш*, и мы предполагаем, что *ш* = О. Заметим также, что отдельное слово *пп* (третья по частоте буква) может означать только ЕЕ, так что *п* = Е. (Мы выделяем расшифрованные буквы, записав их заглавными).

*Оч счкх бьО зьО лех чкщОхЕОч ЕнО нЕъОу чО м зьэ цтчэьэ чкщОхЕОч фкскхый Ецэ ыьОхж цкхЕчжфтц чтбьОрчец бЕхОмЕфОц м ыъкмчЕчтт ы ьЕц бьО ъОтыяОотхО ьЕщЕъж цЕроэ ЕнО оэвОу т зьтц меыОфтц лЕыфОчЕбчец чЕлОц ы лЕнэгтцт щО чЕц Олхкфкцт Ецэ лехО ыОмЕъвЕччО мыЕ ъкмчО м зьэ цтчэьэ фьО ле чт ыьОйх чко чтц бьО ле чт нОмОътх Ол чЕц Оч ъко лех ьОхжфО ьОцэ бьО ОыькчОмтхтыж чко чтц хиот т рЕхкх ьОхжфО бьОл зьт хиот щОцОнхт Ецэ т мОсмъкьтхт ле ЕнО ф ртсчт фОьОъкй фкскхкыж Ецэ ыьОхж щъЕфъкычОи щОьОцэ бьО Оч ькф тчкбЕ щОчтцкх ЕЕ ьЕщЕъж Оч ыОлъкх мыЕ ымОт ытхе бьОле щОвЕмЕхтьжый т щъОтсмЕыьт фкфОу чтлэож смэф Оч ыхклО щОвЕмЕхтх чОнОи т щъОтсмЕх ыкцОнО ЕнО ъксркхОлтмвту ыхклеу лОхЕсчЕччеу ыьОч*

Теперь в тексте четырежды встречается *ЕнО*, причем буква *н* не из самых частых. Подходит только вариант *ЕГО*, то есть *н=Г*.

*Оч счкх бьО зьО лех чкщОхЕОч ЕГО ГЕъОу чО м зьэ цтчэьэ чкщОхЕОч фкскхый Ецэ ыьОхж цкхЕчжфтц чтбьОрчец бЕхОмЕфОц м ыъкмчЕчтт ы ьЕц бьО ъОтыяОотхО ьЕщЕъж цЕроэ ЕГО оэвОу т зьтц меыОфтц лЕыфОчЕбчец чЕлОц ы лЕГэгтцт щО чЕц Олхкфкцт Ецэ лехО ыОмЕъвЕччО мыЕ ъкмчО м зьэ цтчэьэ фьО ле чт ыьОйх чко чтц бьО ле чт ГОмОътх Ол чЕц Оч ъко лех ьОхжфО ьОцэ бьО ОыькчОмтхтыж чко чтц хиот т рЕхкх ьОхжфО бьОл зьт хиот щОцОГхт Ецэ т мОсмъкьтхт ле ЕГО ф ртсчт фОьОъкй фкскхкыж Ецэ ыьОхж щъЕфъкычОи щОьОцэ бьО Оч ькф тчкбЕ щОчтцкх ЕЕ ьЕщЕъж Оч ыОлъкх мыЕ ымОт ытхе бьОле щОвЕмЕхтьжый т щъОтсмЕыьт фкфОу чтлэож смэф Оч ыхклО щОвЕмЕхтх чОГОи т щъОтсмЕх ыкцОГО ЕГО ъксркхОлтмвту ыхклеу лОхЕсчЕччеу ыьОч*

Четвертая по частоте буква Ч, судя по *Оч* и *чО*, согласная, это, очевидно, *Н* или *Т*. Подстановка *Т* вместо *ч* в слово *чОГОи* не дает осмысленного результата, а подстановка *Н* допускает расшифровку *НОГОЙ* или *НОГОЮ*, так что *ч=Н*.

*ОН сНкх бьО зьО лех НкщОхЕОН ЕГО ГЕъОу НО м зьэ цтНэьэ НкщОхЕОН фкскхый Ецэ ыьОхж цкхЕНжфтц НтбьОрНец бЕхОмЕфОц м ыъкмНЕНтт ы ьЕц бьО ъОтыяОотхО ьЕщЕъж цЕроэ ЕГО оэвОу т зьтц меыОфтц лЕыфОНЕбНец НЕлОц ы лЕГэгтцт щО НЕц Олхкфкцт Ецэ лехО ыОмЕъвЕННО мыЕ ъкмНО м зьэ цтНэьэ фьО ле Нт ыьОйх Нко Нтц бьО ле Нт ГОмОътх Ол НЕц ОН ъко лех ьОхжфО ьОцэ бьО ОыькНОмтхтыж Нко Нтц хиот т рЕхкх ьОхжфО бьОл зьт хиот щОцОГхт Ецэ т мОсмъкьтхт ле ЕГО ф ртсНт фОьОъкй фкскхкыж Ецэ ыьОхж щъЕфъкыНОи щОьОцэ бьО ОН ькф тНкбЕ щОНтцкх ЕЕ ьЕщЕъж ОН ыОлъкх мыЕ ымОт ытхе бьОле щОвЕмЕхтьжый т щъОтсмЕыьт фкфОу Нтлэож смэф ОН ыхклО щОвЕмЕхтх НОГОи т щъОтсмЕх ыкцОГО ЕГО ъксркхОлтмвту ыхклеу лОхЕсНЕННеу ыьОН*

Вторая по частоте *т*, как видно из *Нт*, гласная, причем по частоте это *А* или *И*. Слово *ыъкмНЕНтт* едва ли оканчивается на два *А*, в то время как окончание *ИИ* весьма распространено. Делаем вывод: *т* = *И*. Для буквы *А* тоже можем найти код, так как из оставшихся букв самые частые *х* (но это не *А*, судя по *НкщОхЕОН*), *ь* (но это не *А*, судя по *ьЕщЕъж*) и *к*. В последнем случае противоречий не выявлено, полагаем *к* = *А*.

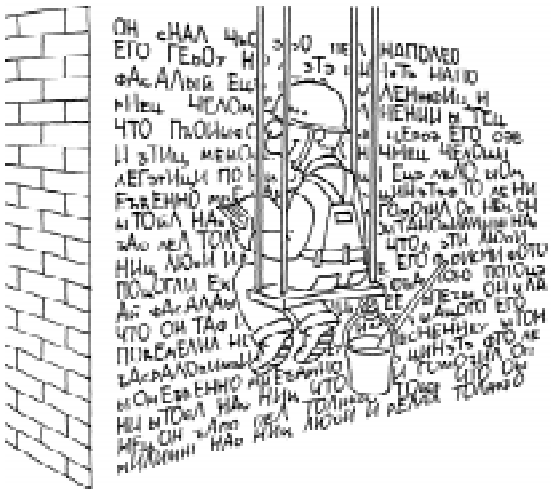
*ОН сНАх бьО зьО лех НАщОхЕОН ЕГО ГЕъОу НО м зьэ цИНэьэ НАщОхЕОН фАсАхый Ецэ ыьОхж цАхЕНжфИц НИбьОрНец бЕхОмЕфОц м ыъАмНЕНИИ ы ьЕц бьО ъОИыяОоИхО ьЕщЕъж цЕроэ ЕГО оэвОу И зьИц меыОфИц лЕыфОНЕбНец НЕлОц ы лЕГэгИцИ щО НЕц ОлхАфАцИ Ецэ лехО ыОмЕъвЕННО мыЕ ъАмНО м зьэ цИНэьэ фьО ле НИ ыьОйх НАо НИц бьО ле НИ ГОмОъИх Ол НЕц ОН ъАо лех ьОхжфО ьОцэ бьО ОыьАНОмИхИыж НАо НИц хиоИ И рЕхАх ьОхжфО бьОл зьИ хиоИ щОцОГхИ Ецэ И мОсмъАьИхИ ле ЕГО ф рИсНИ фОьОъАй фАсАхАыж Ецэ ыьОхж щъЕфъАыНОи щОьОцэ бьО ОН ьАф ИНАбЕ щОНИцАх ЕЕ ьЕщЕъж ОН ыОлъАх мыЕ ымОИ ыИхе бьОле щОвЕмЕхИьжый И щъОИсмЕыьИ фАфОу НИлэож смэф ОН ыхАлО*

*щОвЕмЕхИх НОГОи И щъОИсмЕх ыАцОГО ЕГО ъАсрАхОлИмвИу ыхАлеу лОхЕсНЕННеу ыьОН*

Теперь уже можно прочесть слово *НАщОхЕОН* как *НАПОЛЕОН*, никакая другая пара букв вместо *щ* и *х* не подходит, и мы сразу получаем *щ = П*, *х = Л*:

*ОН сНАЛ бьО зьО леЛ НАПОЛЕОН ЕГО ГЕъОу НО м зьэ цИНэьэ НАПОЛЕОН фАсАЛый Ецэ ыьОЛж цАЛЕНжфИц НИбьОрНец бЕЛОмЕфОц м ыъАмНЕНИИ ы ьЕц бьО ъОИыяОоИЛО ьЕПЕъж цЕроэ ЕГО оэвОу И зьИц меыОфИц лЕыфОНЕбНец НЕлОц ы лЕГэгИцИ ПО НЕц ОлЛАфАцИ Ецэ леЛО ыОмЕъвЕННО мыЕ ъАмНО м зьэ цИНэьэ фьО ле НИ ыьОйЛ НАо НИц бьО ле НИ ГОмОъИЛ Ол НЕц ОН ъАо леЛ ьОЛжфО ьОцэ бьО ОыьАНОмИЛИыж НАо НИц ЛиоИ И рЕЛАЛ ьОЛжфО бьОл зьИ ЛиоИ ПОцОГЛИ Ецэ И мОсмъАьИЛИ ле ЕГО ф рИсНИ фОьОъАй фАсАЛАыж Ецэ ыьОЛж ПъЕфъАыНОи ПОьОцэ бьО ОН ьАф ИНАбЕ ПОНИцАЛ ЕЕ ьЕПЕъж ОН ыОлъАЛ мыЕ ымОИ ыИЛе бьОле ПОвЕмЕЛИьжый И ПъОИсмЕыьИ фАфОу НИлэож смэф ОН ыЛАлО ПОвЕмЕЛИЛ НОГОи И ПъОИсмЕЛ ыАцОГО ЕГО ъАсрАЛОлИмвИу ыЛАлеу лОЛЕсНЕННеу ыьОН*

В слове *НОГОи* теперь можно расшифровать последнюю букву *и*; из двух подходящий вариантов *и = Й* или *и = Ю*, как подсказывает слово *ЛиоИ*, надо брать *и = Ю*. Слово *ИНАбЕ* дает подстановку *б=Ч*.



*Закончить расшифровку этого отрывка, взятого из романа Л.Н. Толстого «Война и мир», предоставляется читателю.*

*ОН сНАЛ ЧьО зьО леЛ НАПОЛЕОН ЕГО ГЕъОу НО м зьэ цИНэьэ НАПОЛЕОН фАсАЛый Ецэ ыьОЛж цАЛЕНжфИц НИЧьОрНец ЧЕЛОмЕфОц м ыъАмНЕНИИ ы ьЕц ЧьО ПъОИыяОоИЛО ьЕПЕъж цЕроэ ЕГО оэвОу И зьИц меыОфИц лЕыфОНЕЧНец НЕлОц ы лЕГэгИцИ ПО НЕц ОлЛАфАцИ Ецэ леЛО ыОмЕъвЕННО мыЕ ъАмНО м зьэ цИНэьэ фьО ле НИ ыьОйЛ НАо НИц ЧьО ле НИ ГОмОъИЛ Ол НЕц ОН ъАо леЛ ьОЛжфО ьОцэ ЧьО ОыьАНОмИЛИыж НАо НИц ЛЮоИ И рЕЛАЛ ьОЛжфО ЧьОл зьИ ЛЮоИ ПОцОГЛИ Ецэ И мОсмъАьИЛИ ле ЕГО ф рИсНИ фОьОъАй фАсАЛАыж Ецэ ыьОЛж ПъЕфъАыНОЮ ПОьОцэ ЧьО ОН ьАф ИНАЧЕ ПОНИцАЛ ЕЕ ьЕПЕъж ОН ыОлъАЛ мыЕ ымОИ ыИЛе ЧьОле ПОвЕмЕЛИьжый И ПъОИсмЕыьИ фАфОу НИлэож смэф ОН ыЛАлО ПОвЕмЕЛИЛ НОГОЮ И ПъОИсмЕЛ ыАцОГО ЕГО ъАсрАЛОлИмвИу ыЛАлеу лОЛЕсНЕННеу ыьОН*

Слово *ЧьО*, подкрепленное сравнением частот, приводит к подстановке *ь = Т*.

*ОН сНАЛ ЧТО зТО леЛ НАПОЛЕОН ЕГО ГЕъОу НО м зТэ цИНэТэ НАПОЛЕОН фАсАЛый Ецэ ыТОЛж цАЛЕНжфИц НИЧТОрНец ЧЕЛОмЕфОц м ыъАмНЕНИИ ы ТЕц ЧТО ПъОИыяОоИЛО ТЕПЕъж цЕроэ ЕГО оэвОу И зТИц меыОфИц лЕыфОНЕЧНец НЕлОц ы лЕГэгИцИ ПО НЕц ОлЛАфАцИ Ецэ леЛО ыОмЕъвЕННО мыЕ ъАмНО м зТэ цИНэТэ фТО ле НИ ыТОйЛ НАо НИц ЧТО ле НИ ГОмОъИЛ Ол НЕц ОН ъАо леЛ ТОЛжфО ТОцэ ЧТО ОыТАНОмИЛИыж НАо НИц ЛЮоИ И рЕЛАЛ ТОЛжфО ЧТОл зТИ ЛЮоИ ПОцОГЛИ Ецэ И мОсмъАТИЛИ ле ЕГО ф рИсНИ фОТОъАй фАсАЛАыж Ецэ ыТОЛж ПъЕфъАыНОЮ ПОТОцэ ЧТО ОН ТАф ИНАЧЕ ПОНИцАЛ ЕЕ ТЕПЕъж ОН ыОлъАЛ мыЕ ымОИ ыИЛе ЧТОле ПОвЕмЕЛИТжый И ПъОИсмЕыТИ фАфОу НИлэож смэф ОН ыЛАлО ПОвЕмЕЛИЛ НОГОЮ И ПъОИсмЕЛ ыАцОГО ЕГО ъАсрАЛОлИмвИу ыЛАлеу лОЛЕсНЕННеу ыТОН*

Закончить расшифровку этого отрывка, взятого из романа Л.Н.Толстого «Война и мир», предоставляется читателю.

Предложим в заключение для расшифровки интересный текст, полученный простой заменой 32 букв русского алфавита на числа. Это олимпиадная задача, взятая из [4]. В тексте сохранены промежутки между словами и знаки препинания. Зашифровано четверостишие В.Высоцкого:

12 2 24 5 3 21 6 29 28 2 20 18 20 21 5 10 27 17 2 11 2 16 –
19 2 27 5 8 29 12 31 22 2 16, 19 2 19 5 17 29 8 29 6 29 16:
8 2 19 19 29 10 19 29 14 19 29 29 19 10 2 24 2 11 2 16
10 14 18 21 17 2 20 2 28 29 16 21 29 28 6 29 16.

Желаем успеха!

*(Окончание следует)*

Литература

1. Введение в криптографию/ Под ред. *В.В. Ященко*. СПб.: Питер, 2001.

2. *Черчхаус Р.* Коды и шифры. Юлий Цезарь, «Энигма» и Интернет. М.: Весь Мир, 2005.

3. Математический клуб «Кенгуру», выпуск № 14. Шифры и математика, автор *Н.А. Жарковская* // СПб.: 2006.

4. *Зубов А.Ю. и др.* Олимпиады по криптографии и математике для школьников. М.: МЦНМО, 2006.

***Агафонова Ирина Витальевна, кандидат физико-математических наук, доцент кафедры исследования операций Санкт-Петербургского государственного университета,***

***Дмитриева Оксана Михайловна, кандидат физико-математических наук, доцент кафедры математики Санкт-Петербургского государственного университета Телекоммуникаций.***