**Задача 5.**

Астраханцев Роман, СКБ-171

**Обозначения.**

*A* – алфавит открытого текста (=*Z­­33* для русского текста)  
*n* =*|A|* - мощность алфавита  
*X* – множество открытых текстов  
*Y* – множество шифрованных текстов  
*K* – множество ключей  
*E­­k*– алгоритм зашифрования на ключе *k*   
*D­­k*– алгоритм расшифрования на ключе *k*

**Использование гаммы короткого периода**

Метод вскрытия на основе индекса совпадения и взаимного индекса совпадения основывается на вычислении вероятности того, что два случайных элемента текста совпадут. Эту вероятность называют индексом совпадений. Уильям Фридман показал, что значения индекса совпадений существенно отличаются для текстов различной природы. Это позволяет сначала определить длину ключа шифра. Длина ключа задаёт количество используемых алфавитов и период шифрования этими алфавитами. Поэтому на этом этапе исследуется периодичность шифртекста. Затем ищется сам ключ. Для нахождения этого вычисляют относительные сдвиги используемых алфавитов, а затем подбирают ключ перебором.

Рассмотрим текст, написанный на некотором языке. Алфавит данного языка будем полагать состоящим из n символов. Рассмотрим строку из m>n символов. Индексом совпадения называют вероятность совпадения двух произвольных символов в строке. Если — количество i-го символа алфавита в строке, то индекс совпадения вычисляется по формуле:

Допустим, строка является открытым текстом либо получена из него простой перестановкой. В этом случае индекс совпадений удобно выразить через вероятности появления i - го символа. Обозначим их . Тогда получим следующую формулу:

|  |  |
| --- | --- |
| Язык |  |
| Русский | 0,055 |
| Английский | 0,066 |
| Французский | 0,078 |
| Итальянский | 0,074 |

На основе экспериментально подсчитанных данных о частотах встречаемости знаков в различных языках получаем следующие значения для индекса совпадения:

Если случайная строка, тогда

С помощью индекса совпадения вычисляют точное значение длины периода следующим образом.

Пусть − выборка с шагом из исходного шифртекста . Если истинная длина периода, то отрезок представляет собой соответствующий отрезок открытого текста, зашифрованный шифром простой замены. При этом, к примеру, для русского языка при любом выполнено .

Если же опробуемое значение ложно, то

Отличное от значения индекса совпадения для осмысленных открытых текстов и для случайных последовательностей букв алфавита, как правило, позволяет найти точное значение периода.

После нахождения периода восстановление ключевой гаммы проводится на основе взаимного индекса совпадения – вероятность совпадения случайно выбранной буквы в строке со случайно выбранной буквой в строке .

Формула взаимного индекса совпадения:

Таким образом, взаимный индекс совпадения зависит только от разности гамм, которая называется относительным сдвигом отрезков и .

Пример взаимного индекса совпадения в зависимости от относительного сдвига для русского языка:

|  |  |
| --- | --- |
|  |  |
| 0 | 0,055 |
| 1 | 0,037 |
| 2 | 0,035 |
| 3 | 0,04 |
| 4 | 0,034 |
| 5 | 0,036 |
| 6 | 0,033 |
| 7 | 0,024 |
| 8 | 0,029 |
| 9 | 0,032 |
| 10 | 0,027 |
| 11 | 0,025 |
| 12 | 0,024 |
| 13 | 0,029 |
| 14 | 0,032 |
| 15 | 0,024 |
| 16 | 0,025 |

Из приведенных данных видно, что ненулевые сдвиги отвечают взаимным индексам совпадения, лежащим в диапазоне от 0.024 до 0.04. При нулевом значении взаимный индекс равен 0.055. Это позволяет найти величины относительных сдвигов (путем опробования из значения) для отрезков и , . После этого останется опробовать n вариантов ключевого слова (которое будет однозначно задаваться значением гаммы )

1. 5 примеров шифрования для «слов-лозунгов»:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | н | о | я | д | р | у | г | о | м | у | о | т | д | а | н | а | я | б | у | д | у | в | е | к | е | м | у | в | е | р | н | а |
|  | 14 | 15 | 32 | 4 | 17 | 20 | 3 | 15 | 13 | 20 | 15 | 19 | 4 | 0 | 14 | 0 | 32 | 1 | 20 | 4 | 20 | 2 | 5 | 11 | 5 | 13 | 20 | 2 | 5 | 17 | 14 | 0 |
|  | а | н | я | а | н | я | а | н | я | а | н | я | а | н | я | а | н | я | а | н | я | а | н | я | а | н | я | а | н | я | а | н |
| γ*i* | 0 | 14 | 32 | 0 | 14 | 32 | 0 | 14 | 32 | 0 | 14 | 32 | 0 | 14 | 32 | 0 | 14 | 32 | 0 | 14 | 32 | 0 | 14 | 32 | 0 | 14 | 32 | 0 | 14 | 32 | 0 | 14 |
| *yi* | 14 | 29 | 31 | 4 | 31 | 19 | 3 | 29 | 12 | 20 | 29 | 18 | 4 | 14 | 13 | 0 | 13 | 0 | 20 | 18 | 19 | 2 | 19 | 10 | 5 | 27 | 19 | 2 | 19 | 16 | 14 | 14 |
|  | н | ь | ю | д | ю | т | г | ь | л | у | ь | с | д | н | м | а | м | а | у | с | т | в | т | й | е | ъ | т | в | т | п | н | н |

а) женское имя из 3-х букв: «Аня»

б) мужское имя из 4-х букв: «Рома»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | н | о | я | д | р | у | г | о | м | у | о | т | д | а | н | а | я | б | у | д | у | в | е | к | е | м | у | в | е | р | н | а |
|  | 14 | 15 | 32 | 4 | 17 | 20 | 3 | 15 | 13 | 20 | 15 | 19 | 4 | 0 | 14 | 0 | 32 | 1 | 20 | 4 | 20 | 2 | 5 | 11 | 5 | 13 | 20 | 2 | 5 | 17 | 14 | 0 |
|  | р | о | м | а | р | о | м | а | р | о | м | а | р | о | м | а | р | о | м | а | р | о | м | а | р | о | м | а | р | о | м | а |
| γ*i* | 17 | 15 | 13 | 0 | 17 | 15 | 13 | 0 | 17 | 15 | 13 | 0 | 17 | 15 | 13 | 0 | 17 | 15 | 13 | 0 | 17 | 15 | 13 | 0 | 17 | 15 | 13 | 0 | 17 | 15 | 13 | 0 |
| *yi* | 31 | 30 | 12 | 4 | 1 | 2 | 16 | 15 | 30 | 2 | 28 | 19 | 21 | 15 | 27 | 0 | 16 | 16 | 0 | 4 | 4 | 17 | 18 | 11 | 22 | 28 | 0 | 2 | 22 | 32 | 27 | 0 |
|  | ю | э | л | д | б | в | п | о | э | в | ы | т | ф | о | ъ | а | п | п | а | д | д | р | с | к | х | ы | а | в | х | я | ъ | а |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | н | о | я | д | р | у | г | о | м | у | о | т | д | а | н | а | я | б | у | д | у | в | е | к | е | м | у | в | е | р | н | а |
|  | 14 | 15 | 32 | 4 | 17 | 20 | 3 | 15 | 13 | 20 | 15 | 19 | 4 | 0 | 14 | 0 | 32 | 1 | 20 | 4 | 20 | 2 | 5 | 11 | 5 | 13 | 20 | 2 | 5 | 17 | 14 | 0 |
|  | с | р | е | д | а | с | р | е | д | а | с | р | е | д | а | с | р | е | д | а | с | р | е | д | а | с | р | е | д | а | с | р |
| γ*i* | 18 | 17 | 5 | 4 | 0 | 18 | 17 | 5 | 4 | 0 | 18 | 17 | 5 | 4 | 0 | 18 | 17 | 5 | 4 | 0 | 18 | 17 | 5 | 4 | 0 | 18 | 17 | 5 | 4 | 0 | 18 | 17 |
| *yi* | 32 | 32 | 4 | 8 | 17 | 5 | 20 | 20 | 17 | 20 | 0 | 3 | 9 | 4 | 14 | 18 | 16 | 6 | 24 | 4 | 5 | 19 | 10 | 15 | 5 | 31 | 4 | 7 | 9 | 17 | 32 | 17 |
|  | я | я | д | з | р | е | у | у | р | у | а | г | и | д | н | с | п | ё | ч | д | е | т | й | о | е | ю | д | ж | и | р | я | р |

в) день недели: «среда»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | н | о | я | д | р | у | г | о | м | у | о | т | д | а | н | а | я | б | у | д | у | в | е | к | е | м | у | в | е | р | н | а |
|  | 14 | 15 | 32 | 4 | 17 | 20 | 3 | 15 | 13 | 20 | 15 | 19 | 4 | 0 | 14 | 0 | 32 | 1 | 20 | 4 | 20 | 2 | 5 | 11 | 5 | 13 | 20 | 2 | 5 | 17 | 14 | 0 |
|  | л | е | т | о | л | е | т | о | л | е | т | о | л | е | т | о | л | е | т | о | л | е | т | о | л | е | т | о | л | е | т | о |
| γ*i* | 12 | 5 | 19 | 15 | 12 | 5 | 19 | 15 | 12 | 5 | 19 | 15 | 12 | 5 | 19 | 15 | 12 | 5 | 19 | 15 | 12 | 5 | 19 | 15 | 12 | 5 | 19 | 15 | 12 | 5 | 19 | 15 |
| *yi* | 26 | 20 | 18 | 19 | 29 | 25 | 22 | 30 | 25 | 25 | 1 | 1 | 16 | 5 | 0 | 15 | 11 | 6 | 6 | 19 | 32 | 7 | 24 | 26 | 17 | 18 | 6 | 17 | 17 | 22 | 0 | 15 |
|  | щ | у | с | т | ь | ш | х | э | ш | ш | б | б | п | е | а | о | к | ё | ё | т | я | ж | ч | щ | р | с | ё | р | р | х | а | о |

г) время года: «лето»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | н | о | я | д | р | у | г | о | м | у | о | т | д | а | н | а | я | б | у | д | у | в | е | к | е | м | у | в | е | р | н | а |
|  | 14 | 15 | 32 | 4 | 17 | 20 | 3 | 15 | 13 | 20 | 15 | 19 | 4 | 0 | 14 | 0 | 32 | 1 | 20 | 4 | 20 | 2 | 5 | 11 | 5 | 13 | 20 | 2 | 5 | 17 | 14 | 0 |
|  | и | ю | л | ь | и | ю | л | ь | и | ю | л | ь | и | ю | л | ь | и | ю | л | ь | и | ю | л | ь | и | ю | л | ь | и | ю | л | ь |
| γ*i* | 9 | 31 | 12 | 29 | 9 | 31 | 12 | 29 | 9 | 31 | 12 | 29 | 9 | 31 | 12 | 29 | 9 | 31 | 12 | 29 | 9 | 31 | 12 | 29 | 9 | 31 | 12 | 29 | 9 | 31 | 12 | 29 |
| *yi* | 23 | 13 | 11 | 0 | 26 | 18 | 15 | 11 | 22 | 18 | 27 | 15 | 13 | 31 | 26 | 29 | 8 | 32 | 32 | 0 | 29 | 0 | 17 | 7 | 14 | 11 | 32 | 31 | 14 | 15 | 26 | 29 |
|  | ц | м | к | а | щ | с | о | к | х | с | ъ | о | м | ю | щ | ь | з | я | я | а | ь | а | р | ж | н | к | я | ю | н | о | щ | ь |

д) название месяца: «июль»

1. Для одного из примеров (первые 12 вариантов отвечают случаю, когда слово-лозунг является названием месяца, следующие 7 вариантов соответствуют дням недели) проводится подробный алгоритм вскрытия на основе перебора вариантов слова-лозунга, снятия гаммы с шифртекста и проверки полученного текста на «осмысленность».

Шифртекст:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | я | я | д | з | р | е | у | у | р | у | а | г | и | д | н | с | п | ё | ч | д | е | т | й | о | е | ю | д | ж | и | р | я | р |

«понедельник»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | п | р | ц | г | м | а | з | ч | г | к | х | у | ъ | ц | и | н | к | ъ | ы | ц | ь | з | ъ | а | ч | щ | а | в | э | ф | с | з |
|  | 16 | 17 | 23 | 3 | 13 | 0 | 8 | 24 | 3 | 11 | 22 | 20 | 27 | 23 | 9 | 14 | 11 | 27 | 28 | 23 | 29 | 8 | 27 | 0 | 24 | 26 | 0 | 2 | 30 | 21 | 18 | 8 |
|  | п | о | н | е | д | е | л | ь | н | и | к | п | о | н | е | д | е | л | ь | н | и | к | п | о | н | е | д | е | л | ь | н | и |
| γ*i* | 16 | 15 | 14 | 5 | 4 | 5 | 12 | 29 | 14 | 9 | 11 | 16 | 15 | 14 | 5 | 4 | 5 | 12 | 29 | 14 | 9 | 11 | 16 | 15 | 14 | 5 | 4 | 5 | 12 | 29 | 14 | 9 |
| *yi* | 32 | 32 | 4 | 8 | 17 | 5 | 20 | 20 | 17 | 20 | 0 | 3 | 9 | 4 | 14 | 18 | 16 | 6 | 24 | 4 | 5 | 19 | 10 | 15 | 5 | 31 | 4 | 7 | 9 | 17 | 32 | 17 |
|  | я | я | д | з | р | е | у | у | р | у | а | г | и | д | н | с | п | ё | ч | д | е | т | й | о | е | ю | д | ж | и | р | я | р |

«вторник»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | э | м | х | ч | г | ь | и | с | ю | е | п | х | а | щ | л | я | б | х | й | ы | ъ | р | ч | а | ф | р | ы | ь | ж | ю | р | а |
|  | 30 | 13 | 22 | 24 | 3 | 29 | 9 | 18 | 31 | 5 | 16 | 22 | 0 | 26 | 12 | 32 | 1 | 22 | 10 | 28 | 27 | 17 | 24 | 0 | 21 | 17 | 28 | 29 | 7 | 31 | 17 | 0 |
|  | в | т | о | р | н | и | к | в | т | о | р | н | и | к | в | т | о | р | н | и | к | в | т | о | р | н | и | к | в | т | о | р |
| γ*i* | 2 | 19 | 15 | 17 | 14 | 9 | 11 | 2 | 19 | 15 | 17 | 14 | 9 | 11 | 2 | 19 | 15 | 17 | 14 | 9 | 11 | 2 | 19 | 15 | 17 | 14 | 9 | 11 | 2 | 19 | 15 | 17 |
| *yi* | 32 | 32 | 4 | 8 | 17 | 5 | 20 | 20 | 17 | 20 | 0 | 3 | 9 | 4 | 14 | 18 | 16 | 6 | 24 | 4 | 5 | 19 | 10 | 15 | 5 | 31 | 4 | 7 | 9 | 17 | 32 | 17 |
|  | я | я | д | з | р | е | у | у | р | у | а | г | и | д | н | с | п | ё | ч | д | е | т | й | о | е | ю | д | ж | и | р | я | р |

«среда»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | н | о | я | д | р | у | г | о | м | у | о | т | д | а | н | а | я | б | у | д | у | в | е | к | е | м | у | в | е | р | н | а |
|  | 14 | 15 | 32 | 4 | 17 | 20 | 3 | 15 | 13 | 20 | 15 | 19 | 4 | 0 | 14 | 0 | 32 | 1 | 20 | 4 | 20 | 2 | 5 | 11 | 5 | 13 | 20 | 2 | 5 | 17 | 14 | 0 |
|  | с | р | е | д | а | с | р | е | д | а | с | р | е | д | а | с | р | е | д | а | с | р | е | д | а | с | р | е | д | а | с | р |
| γ*i* | 18 | 17 | 5 | 4 | 0 | 18 | 17 | 5 | 4 | 0 | 18 | 17 | 5 | 4 | 0 | 18 | 17 | 5 | 4 | 0 | 18 | 17 | 5 | 4 | 0 | 18 | 17 | 5 | 4 | 0 | 18 | 17 |
| *yi* | 32 | 32 | 4 | 8 | 17 | 5 | 20 | 20 | 17 | 20 | 0 | 3 | 9 | 4 | 14 | 18 | 16 | 6 | 24 | 4 | 5 | 19 | 10 | 15 | 5 | 31 | 4 | 7 | 9 | 17 | 32 | 17 |
|  | я | я | д | з | р | е | у | у | р | у | а | г | и | д | н | с | п | ё | ч | д | е | т | й | о | е | ю | д | ж | и | р | я | р |

«четверг»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | з | ъ | с | ё | л | ф | р | ь | л | б | ю | ю | ш | б | ц | м | э | д | т | у | в | ы | е | ь | г | щ | у | д | с | л | м | о |
|  | 8 | 27 | 18 | 6 | 12 | 21 | 17 | 29 | 12 | 1 | 31 | 31 | 25 | 1 | 23 | 13 | 30 | 4 | 19 | 20 | 2 | 28 | 5 | 29 | 3 | 26 | 20 | 4 | 18 | 12 | 13 | 15 |
|  | ч | е | т | в | е | р | г | ч | е | т | в | е | р | г | ч | е | т | в | е | р | г | ч | е | т | в | е | р | г | ч | е | т | в |
| γ*i* | 24 | 5 | 19 | 2 | 5 | 17 | 3 | 24 | 5 | 19 | 2 | 5 | 17 | 3 | 24 | 5 | 19 | 2 | 5 | 17 | 3 | 24 | 5 | 19 | 2 | 5 | 17 | 3 | 24 | 5 | 19 | 2 |
| *yi* | 32 | 32 | 4 | 8 | 17 | 5 | 20 | 20 | 17 | 20 | 0 | 3 | 9 | 4 | 14 | 18 | 16 | 6 | 24 | 4 | 5 | 19 | 10 | 15 | 5 | 31 | 4 | 7 | 9 | 17 | 32 | 17 |
|  | я | я | д | з | р | е | у | у | р | у | а | г | и | д | н | с | п | ё | ч | д | е | т | й | о | е | ю | д | ж | и | р | я | р |

«пятница»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | п | а | с | ъ | з | о | у | д | с | б | т | ъ | т | д | ю | т | э | ш | о | н | е | г | н | ь | ч | х | н | ж | щ | с | м | г |
|  | 16 | 0 | 18 | 27 | 8 | 15 | 20 | 4 | 18 | 1 | 19 | 27 | 19 | 4 | 31 | 19 | 30 | 25 | 15 | 14 | 5 | 3 | 11 | 29 | 24 | 22 | 14 | 7 | 26 | 18 | 13 | 3 |
|  | п | я | т | н | и | ц | а | п | я | т | н | и | ц | а | п | я | т | н | и | ц | а | п | я | т | н | и | ц | а | п | я | т | н |
| γ*i* | 16 | 32 | 19 | 14 | 9 | 23 | 0 | 16 | 32 | 19 | 14 | 9 | 23 | 0 | 16 | 32 | 19 | 14 | 9 | 23 | 0 | 16 | 32 | 19 | 14 | 9 | 23 | 0 | 16 | 32 | 19 | 14 |
| *yi* | 32 | 32 | 4 | 8 | 17 | 5 | 20 | 20 | 17 | 20 | 0 | 3 | 9 | 4 | 14 | 18 | 16 | 6 | 24 | 4 | 5 | 19 | 10 | 15 | 5 | 31 | 4 | 7 | 9 | 17 | 32 | 17 |
|  | я | я | д | з | р | е | у | у | р | у | а | г | и | д | н | с | п | ё | ч | д | е | т | й | о | е | ю | д | ж | и | р | я | р |

«суббота»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | н | л | г | ж | в | т | у | в | э | т | я | ф | ц | д | ь | ю | о | е | и | с | е | б | ц | н | д | п | с | ж | ч | э | ю | п |
|  | 14 | 12 | 3 | 7 | 2 | 19 | 20 | 2 | 30 | 19 | 32 | 21 | 23 | 4 | 29 | 31 | 15 | 5 | 9 | 18 | 5 | 1 | 23 | 14 | 4 | 16 | 18 | 7 | 24 | 30 | 31 | 16 |
|  | с | у | б | б | о | т | а | с | у | б | б | о | т | а | с | у | б | б | о | т | а | с | у | б | б | о | т | а | с | у | б | б |
| γ*i* | 18 | 20 | 1 | 1 | 15 | 19 | 0 | 18 | 20 | 1 | 1 | 15 | 19 | 0 | 18 | 20 | 1 | 1 | 15 | 19 | 0 | 18 | 20 | 1 | 1 | 15 | 19 | 0 | 18 | 20 | 1 | 1 |
| *yi* | 32 | 32 | 4 | 8 | 17 | 5 | 20 | 20 | 17 | 20 | 0 | 3 | 9 | 4 | 14 | 18 | 16 | 6 | 24 | 4 | 5 | 19 | 10 | 15 | 5 | 31 | 4 | 7 | 9 | 17 | 32 | 17 |
|  | я | я | д | з | р | е | у | у | р | у | а | г | и | д | н | с | п | ё | ч | д | е | т | й | о | е | ю | д | ж | и | р | я | р |

«воскресенье»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | э | р | т | э | а | а | в | о | г | ч | ы | б | ъ | т | г | б | к | ф | т | ц | и | н | з | а | у | у | у | в | ч | л | с | ф |
|  | 30 | 17 | 19 | 30 | 0 | 0 | 2 | 15 | 3 | 24 | 28 | 1 | 27 | 19 | 3 | 1 | 11 | 21 | 19 | 23 | 9 | 14 | 8 | 0 | 20 | 20 | 20 | 2 | 24 | 12 | 18 | 21 |
|  | в | о | с | к | р | е | с | е | н | ь | е | в | о | с | к | р | е | с | е | н | ь | е | в | о | с | к | р | е | с | е | н | ь |
| γ*i* | 2 | 15 | 18 | 11 | 17 | 5 | 18 | 5 | 14 | 29 | 5 | 2 | 15 | 18 | 11 | 17 | 5 | 18 | 5 | 14 | 29 | 5 | 2 | 15 | 18 | 11 | 17 | 5 | 18 | 5 | 14 | 29 |
| *yi* | 32 | 32 | 4 | 8 | 17 | 5 | 20 | 20 | 17 | 20 | 0 | 3 | 9 | 4 | 14 | 18 | 16 | 6 | 24 | 4 | 5 | 19 | 10 | 15 | 5 | 31 | 4 | 7 | 9 | 17 | 32 | 17 |
|  | я | я | д | з | р | е | у | у | р | у | а | г | и | д | н | с | п | ё | ч | д | е | т | й | о | е | ю | д | ж | и | р | я | р |