**Задача 3.**

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*

**Неравновероятная гамма**

В случае использования малого числа знаков гаммы, суммарная вероятность которых близка к единице, возможно восстановление открытого текста с помощью зигзагообразного чтения в колонках. Для этого в каждой колонке выписывают возможные значения знака открытого текста (вычитанием возможных значений гаммы) и затем, выбирая по одному знаку из каждой колонки, получают открытый текст. Выбор производится с учетом запрещенных в языке открытого текста символов. Метод чтения в колонках представляет собой так называемый метод бесключевого чтения. В примерах ниже для упрощения гамма принимает только два (три) значения, а остальные значения не принимает.

1. Пример алгоритма дешифрования для шифра:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | р | у | в | и | х | ц | ё | у | с | ц | с | х | ж | г | е | д | д | ё | ш | и | ш | е | з | н | й | с | ц | е | й | у | р | г |
|  | 17 | 20 | 2 | 9 | 22 | 23 | 6 | 20 | 18 | 23 | 18 | 22 | 7 | 3 | 19 | 5 | 2 | 6 | 25 | 9 | 25 | 5 | 8 | 14 | 10 | 18 | 23 | 5 | 10 | 20 | 17 | 3 |
|  | н | о | я | ё | т | у | г | р | о | у | о | т | д | а | п | в | я | г | х | ё | х | в | е | к | ж | о | у | в | ж | р | н | а |
|  | л | о | э | д | р | с | б | о | м | с | м | р | в | ю | н | а | э | б | у | д | у | а | г | и | е | м | с | А | е | о | л | ю |
| γ*i* | 3 | 5 | 3 | 5 | 5 | 3 | 3 | 5 | 5 | 3 | 3 | 3 | 3 | 3 | 5 | 5 | 3 | 5 | 5 | 5 | 5 | 3 | 3 | 3 | 5 | 5 | 3 | 3 | 5 | 3 | 3 | 3 |
| *xi* | 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 |
|  | 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 |

Для дешифровки выпишем всевозможные сочетания из первых 4 букв и выберем наиболее подходящие варианты исходя из правил языка и осмысленности текста:

|  |  |  |  |
| --- | --- | --- | --- |
| нояё | нояд | ноэё | ноэд |
| нояё | нояд | ноэё | ноэд |
| лояё | лояд | лоэё | лоэд |
| лояё | лояд | лоэё | лоэд |

Теперь выпишем все следующие варианты четверок и будем комбинировать их с отобранными на прошлом этапе четверками по смыслу и языковым особенностям:

|  |  |  |  |
| --- | --- | --- | --- |
| тугр | туго | тубр | тубо |
| тсгр | тсго | тсбр | тсбо |
| ругр | руго | рубр | рубо |
| рсгр | рсго | рсбр | рсбо |

|  |  |  |  |
| --- | --- | --- | --- |
| оуот | оуор | оумт | оумр |
| осот | осор | осмт | осмр |
| муот | муор | мумт | мумр |
| мсот | мсор | мсмт | мсмр |

Совмещаем подходящие друг другу куски текста и получаем фрагмент «ноядругомуот». Повторяя процедуру, получаем исходный открытый текст.

1. Пример алгоритма дешифрования для шифра:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | р | ф | в | ж | ц | ъ | ё | х | у | ц | ф | х | ж | ё | р | ж | ё | д | щ | к | ъ | з | з | н | л | п | щ | е | л | у | р | ж |
|  | 17 | 21 | 2 | 7 | 23 | 27 | 6 | 22 | 20 | 23 | 21 | 22 | 7 | 6 | 17 | 7 | 6 | 4 | 26 | 11 | 27 | 8 | 8 | 14 | 12 | 16 | 26 | 5 | 12 | 20 | 17 | 7 |
|  | н | с | я | д | у | ч | г | т | р | у | с | т | д | г | н | д | г | б | ц | з | ч | е | е | к | и | м | ц | в | и | р | н | д |
|  | к | о | ь | б | р | ф | а | п | н | р | о | п | б | а | к | б | а | ю | у | е | ф | в | в | з | ё | й | у | я | ё | н | к | б |
|  | й | н | ы | а | п | у | я | о | м | п | н | о | а | я | й | а | я | э | т | д | у | б | б | ж | е | и | т | ю | е | м | й | а |
| γ*i* | 3 | 6 | 3 | 3 | 6 | 7 | 3 | 7 | 7 | 3 | 6 | 3 | 3 | 6 | 3 | 7 | 7 | 3 | 6 | 7 | 7 | 6 | 3 | 3 | 7 | 3 | 6 | 3 | 7 | 3 | 3 | 7 |
| *xi* | 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 |
|  | 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 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| нся | нсь | нсы | ноя | ноь | ноы | ння | ннь | нны |
| кся | ксь | ксы | коя | коь | коы | кня | кнь | кны |
| йся | йсь | йсы | йоя | йоь | йоы | йня | йнь | йны |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| дуч | дуф | дуу | дрч | дрф | дру | дпч | дпф | дпу |
| буч | буф | буу | брч | брф | бру | бпч | бпф | бпу |
| ауч | ауф | ауу | арч | арф | ару | апч | апф | апу |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| гтр | гтн | гтм | гпр | гпн | гпм | гор | гон | гом |
| атр | атн | атм | апр | апн | апм | аор | аон | аом |
| ятр | ятн | ятм | япр | япн | япм | яор | яон | яом |

Совмещаем подходящие друг другу куски текста и получаем фрагмент «ноядругом». Повторяя процедуру, получаем исходный открытый текст.