**Задача 4.**

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*

**Перекрытие гаммы**

Перекрытие гаммы основано на том, что тексты могут быть зашифрованы с помощью одинаковой гаммы, результате чего есть возможность воспользоваться методом протяжки вероятного слова.

Чтобы воспользоваться методом протяжки вероятного слова, нужно сделать предположение о слове или фразе, которая находится в одном из открытых текстов. Затем, выбирая место подбором, можно вычитать из шифротекста символы предполагаемого слова. Если место выбрано верно, то, используя полученную гамму на других шифротекстах в том же месте, должны получиться осмысленные тексты, не противоречащие правилам языка открытого текста.

После того, как вероятное слово было протянуто верно, необходимо на основе других шифротекстов достроить открытый текст во всех шифротекстах, основываясь на правилах грамматики.

1. 3 примера использования одной и той же гаммы для шифрования двух разных открытых текстов

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| (1) | н | о | я | д | р | у | г | о | м | у | о | т | д | а | н | а |
| *xi*(1) | 14 | 15 | 32 | 4 | 17 | 20 | 3 | 15 | 13 | 20 | 15 | 19 | 4 | 0 | 14 | 0 |
| (2) | я | б | у | д | у | в | е | к | е | м | у | в | е | р | н | а |
| *xi*(2) | 32 | 1 | 20 | 4 | 20 | 2 | 5 | 11 | 5 | 13 | 20 | 2 | 5 | 17 | 14 | 0 |
| γ*i* | 25 | 15 | 28 | 18 | 12 | 3 | 15 | 16 | 25 | 0 | 9 | 5 | 8 | 32 | 8 | 23 |
| (1) | 6 | 30 | 27 | 22 | 29 | 23 | 18 | 31 | 5 | 20 | 24 | 24 | 12 | 32 | 22 | 23 |
| (1) | ё | э | ъ | х | ь | ц | с | ю | е | у | ч | ч | л | я | х | ц |
| (2) | 24 | 16 | 15 | 22 | 32 | 5 | 20 | 27 | 30 | 13 | 29 | 7 | 13 | 16 | 22 | 23 |
| (2) | ч | п | о | х | я | е | у | ъ | э | м | ь | ж | м | п | х | ц |
|  | 18 | 19 | 21 | 0 | 3 | 15 | 2 | 29 | 25 | 26 | 5 | 16 | 1 | 17 | 0 | 0 |

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| (1) | м | а | т | е | м | а | т | и | к | а | ц | а | р | и | ц | а | н | а | у | к |
| *xi*(1) | 13 | 0 | 19 | 5 | 13 | 0 | 19 | 9 | 11 | 0 | 23 | 0 | 17 | 9 | 23 | 0 | 14 | 0 | 20 | 11 |
| (2) | а | л | г | е | б | р | а | ц | а | р | и | ц | а | а | н | а | л | и | з | а |
| *xi*(2) | 0 | 12 | 3 | 5 | 1 | 17 | 0 | 23 | 0 | 17 | 9 | 23 | 0 | 0 | 14 | 0 | 12 | 9 | 8 | 0 |
| γ*i* | 25 | 15 | 28 | 18 | 12 | 3 | 15 | 16 | 25 | 0 | 9 | 5 | 8 | 32 | 8 | 23 | 1 | 32 | 1 | 19 |
| (1) | 5 | 15 | 14 | 23 | 25 | 3 | 1 | 25 | 3 | 0 | 32 | 5 | 25 | 8 | 31 | 23 | 15 | 32 | 21 | 30 |
| (1) | е | о | н | ц | ш | г | б | ш | г | а | я | е | ш | з | ю | ц | о | я | ф | э |
| (2) | 25 | 27 | 31 | 23 | 13 | 20 | 15 | 6 | 25 | 17 | 18 | 28 | 8 | 32 | 22 | 23 | 13 | 8 | 9 | 19 |
| (2) | ш | ъ | ю | ц | м | у | о | ё | ш | р | с | ы | з | я | х | ц | м | з | и | т |
|  | 20 | 12 | 17 | 0 | 21 | 17 | 14 | 14 | 22 | 17 | 19 | 23 | 16 | 24 | 24 | 0 | 31 | 9 | 21 | 22 |

1. Для одного из примеров (выбор по согласованию с преподавателем) проводится подробный алгоритм вскрытия на основе протяжки известного фрагмента открытого текста I=i1i2…iS, S=10-15 знаков. При этом проводится «привязка» начала фрагмента I к позиции в открытом тексте, вычисляется соответствующий фрагмент во втором открытом тексте и анализируется возможность его присутствия как части смыслового текста

Возьмем для дешифрования третий пример.

Шифртекст1: еонцшгбшгаяешзюцояфэ

Шифртекст2: шъюциуоёшрсызяхцмзит

Предположим, что сообщение 2 содержит имя “царица”, тогда сделаем протяжку это слова так, чтобы при дешифровании 1 шифртекста получился осмысленный текст:

|  |  |
| --- | --- |
| Сдвиг от начала | Расшифрованный текст |
| 0 | гфаиёп |
| 1 | кпршёт |
| 2 | ёаашит |
| 3 | ёпгыбп |
| 4 | ётгуён |
| 5 | итышдй |
| 6 | икацар |
| 7 | бпютжи |
| 8 | ёнъщяи |
| 9 | дйбсяа |
| 10 | арщсцв |
| 11 | жищишч |
| 12 | яиркнл |
| 13 | яатавк |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| (1) |  |  |  |  |  |  |  | и | к | а | ц | а | р |  |  |  |  |  |  |  |
| *xi*(1) |  |  |  |  |  |  |  | 9 | 11 | 0 | 23 | 0 | 17 |  |  |  |  |  |  |  |
| (2) |  |  |  |  |  |  |  | ц | а | р | и | ц | а |  |  |  |  |  |  |  |
| *xi*(2) |  |  |  |  |  |  |  | 23 | 0 | 17 | 9 | 23 | 0 |  |  |  |  |  |  |  |
| γ*i* |  |  |  |  |  |  |  | 16 | 25 | 0 | 9 | 5 | 8 |  |  |  |  |  |  |  |

Видно, что во втором тексте также встречается «ика» (типичное окончание слова) и «цар» (начало слов «царь», «царица», «царство»). Предположим, что в 1ом шифртексте также встречается слово «царица». Тогда получим следующее.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| (1) |  |  |  |  |  |  |  | и | к | а | ц | а | р | и | ц | а |  |  |  |  |
| *xi*(1) |  |  |  |  |  |  |  | 9 | 11 | 0 | 23 | 0 | 17 | 9 | 23 | 0 |  |  |  |  |
| (2) |  |  |  |  |  |  |  | ц | а | р | и | ц | а | а | н | а |  |  |  |  |
| *xi*(2) |  |  |  |  |  |  |  | 23 | 0 | 17 | 9 | 23 | 0 | 0 | 14 | 0 |  |  |  |  |
| γ*i* |  |  |  |  |  |  |  | 16 | 25 | 0 | 9 | 5 | 8 | 32 | 8 | 23 |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| (1) |  |  |  |  |  |  |  | и | к | а | ц | а | р | и | ц | а | н | а | у | к |
| *xi*(1) |  |  |  |  |  |  |  | 9 | 11 | 0 | 23 | 0 | 17 | 9 | 23 | 0 | 14 | 0 | 20 | 11 |
| (2) |  |  |  |  |  |  |  | ц | а | р | и | ц | а | а | н | а | л | и | з | а |
| *xi*(2) |  |  |  |  |  |  |  | 23 | 0 | 17 | 9 | 23 | 0 | 0 | 14 | 0 | 12 | 9 | 8 | 0 |
| γ*i* |  |  |  |  |  |  |  | 16 | 25 | 0 | 9 | 5 | 8 | 32 | 8 | 23 | 1 | 32 | 1 | 19 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| (1) | м | а | т | е | м | а | т | и | к | а | ц | а | р | и | ц | а | н | а | у | к |
| *xi*(1) | 13 | 0 | 19 | 5 | 13 | 0 | 19 | 9 | 11 | 0 | 23 | 0 | 17 | 9 | 23 | 0 | 14 | 0 | 20 | 11 |
| (2) | а | л | г | е | б | р | а | ц | а | р | и | ц | а | а | н | а | л | и | з | а |
| *xi*(2) | 0 | 12 | 3 | 5 | 1 | 17 | 0 | 23 | 0 | 17 | 9 | 23 | 0 | 0 | 14 | 0 | 12 | 9 | 8 | 0 |
| γ*i* | 25 | 15 | 28 | 18 | 12 | 3 | 15 | 16 | 25 | 0 | 9 | 5 | 8 | 32 | 8 | 23 | 1 | 32 | 1 | 19 |

Получили, что следующее слово начинается на «ана». Это может быть либо что-то в именительном падеже «анархия», либо в что-то в родительном падеже «ананаса». Перебирая различные варианты приходим к выводу, что это слово «анализа».

Получили осмысленный текст. Из его содержания понятно, что конструкция 1 шифртекста имеет вид «что-то – царица наук». Науки, чьё название заканчивается на «ика» — это «инфморматика», «математика», «арифметика» и другие. Перебирая различные варианты получаем, что подходит «математика», а итоговая расшифровка выглядит следующим образом: