**Задача 1.**

Астраханцев Роман, СКБ-171

**Обозначения.**

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

В шифре Цезаря и шифре Хилла зашифрование происходит побуквенно. Каждой букве алфавита открытого текста ставится числовой эквивалент – порядковый номер буквы в алфавите. Исходя из этого для русского алфавита *X=Y=A*.

* 1. **Шифр Цезаря.**

Шифр Цезаря является примером шифра простой замены и в качестве ключа использует фиксированный сдвиг порядковых номеров букв алфавита открытого текста, то есть *k* ∈ *K= Z­­33*\{0} – фиксированный сдвиг.

Алгоритм зашифрования *E­­k* выглядит следующим образом.

*n* =*|A|* - мощность алфавита

Нетрудно понять, что алгоритм расшифрования *D­­k* выглядит следующим образом.

*n* =*|A|* - мощность алфавита

Легко видеть, что распределение букв алфавита открытого текста сохраняется при зашифровании. Это связанно с тем, что каждая буква исходного текста шифруется одинаково вне зависимости от позиции в тексте. Таким образом имея шифртекст большого объёма и распределение букв исходного алфавита можно провести частотный анализ букв шифртекста, найти сопоставить частоты наиболее встречающихся букв алфавитов открытого текста и шифртекста и восстановить сообщения исходя из правил языка и запретных комбинаций.

Ниже приведены примеры использования шифра Цезаря (k=3). В таблицах указан исходный текст, шифртекст и их численное представление.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Н | о | я | д | р | у | г | о | м | у | о | т | д | а | н | а |
| 14 | 15 | 32 | 4 | 17 | 20 | 3 | 15 | 13 | 20 | 15 | 19 | 4 | 0 | 14 | 0 |
| 17 | 18 | 2 | 7 | 20 | 23 | 6 | 18 | 16 | 23 | 18 | 22 | 7 | 3 | 17 | 3 |
| Р | с | в | ж | у | ц | ё | с | п | ц | с | х | ж | г | р | г |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Я | б | у | д | у | в | е | к | е | м | у | в | е | р | н | а |
| 32 | 1 | 20 | 4 | 20 | 2 | 5 | 11 | 5 | 13 | 20 | 2 | 5 | 17 | 14 | 0 |
| 2 | 4 | 23 | 7 | 23 | 5 | 8 | 14 | 8 | 16 | 23 | 5 | 8 | 20 | 17 | 3 |
| В | д | ц | ж | ц | е | з | н | з | п | ц | е | з | у | р | г |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Т | в | о | р | и | б | о | л | ь | ш | о | е | д | о | б | р | о | г | о |
| 19 | 2 | 15 | 17 | 9 | 1 | 15 | 12 | 29 | 25 | 15 | 5 | 4 | 15 | 1 | 17 | 15 | 3 | 15 |
| 22 | 5 | 18 | 20 | 12 | 4 | 18 | 15 | 32 | 28 | 18 | 8 | 7 | 18 | 4 | 20 | 18 | 6 | 18 |
| Х | е | с | у | л | д | с | о | я | ы | с | з | ж | с | д | у | с | ё | с |

* 1. **Шифр Хилла.**

Шифр Хилла так же является примером шифра простой замены. В качестве ключа для алфавита мощности используются пара ∈ *K*={(, ): , ∈*Z­­33*, НОД(, )=1} фиксированный сдвиг порядковых номеров букв алфавита открытого текста, то есть *k* ∈ *K= Z­­33*\{0} – фиксированный сдвиг.

Алгоритм зашифрования *E­­k* на ключе выглядит следующим образом.

*n* =*|A|* - мощность алфавита

Нетрудно понять, что алгоритм расшифрования *D­­k* выглядит следующим образом.

*n* =*|A|* - мощность алфавита

Точно так же, как и с шифром Цезаря, шифр Хилла кодирует каждую одинаково и независимо от других. Это делает такой шифр так же уязвимым к частотному анализу. Отличием этих шифров будет мощность ключевого множества и временем перебора всех вариантов этого множества.

Ниже приведены примеры использования шифра Хилла (a=4, b=5). В таблицах указан исходный текст, шифртекст и их численное представление.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Н | о | я | д | р | у | г | о | м | у | о | т | д | а | н | а |
| 14 | 15 | 32 | 4 | 17 | 20 | 3 | 15 | 13 | 20 | 15 | 19 | 4 | 0 | 14 | 0 |
| 28 | 32 | 1 | 21 | 7 | 19 | 17 | 32 | 24 | 19 | 32 | 15 | 21 | 5 | 28 | 5 |
| ﻿Ы | я | б | ф | ж | т | р | я | ч | т | я | о | ф | е | ы | е |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Я | б | у | д | у | в | е | к | е | м | у | в | е | р | н | а |
| 32 | 1 | 20 | 4 | 20 | 2 | 5 | 11 | 5 | 13 | 20 | 2 | 5 | 17 | 14 | 0 |
| 1 | 9 | 19 | 21 | 19 | 13 | 25 | 16 | 25 | 24 | 19 | 13 | 25 | 7 | 28 | 5 |
| ﻿Б | и | т | ф | т | м | ш | п | ш | ч | т | м | ш | ж | ы | е |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Т | в | о | р | и | б | о | л | ь | ш | о | е | д | о | б | р | о | г | о |
| 19 | 2 | 15 | 17 | 9 | 1 | 15 | 12 | 29 | 25 | 15 | 5 | 4 | 15 | 1 | 17 | 15 | 3 | 15 |
| 15 | 13 | 32 | 7 | 8 | 9 | 32 | 20 | 22 | 6 | 32 | 25 | 21 | 32 | 9 | 7 | 32 | 17 | 32 |
| ﻿О | м | я | ж | з | и | я | у | х | ё | я | ш | ф | я | и | ж | я | р | я |