**Лабораторная работа №3**

**Тема:** Шифр Виженера.

**Задание:** Разработать программу для шифрации и дешифрации по методу Виженера.

**Пояснения:** *Шифр Виженера.*

Одна из возможностей усовершенствования простого моноалфавитного шрифта заключается в использовании нескольких моноалфавитных подстановок, применяемых в ходе шифрования открытого текста в зависимости от определенных условий. Семейство шрифтов, основанных на применении таких методов шифрования, называется *полиалфавитными шифрами.* Подобные методы шифрования обладают следующими общими свойствами.

1. Используется набор связанных моноалфавитных подстановок.
2. Имеется некоторый ключ, по которому определяется, какое конкретное преобразование должно применяться для шифрования на данном этапе.

Самым широко известным и одновременно самым простым алгоритмом такого рода является шифр Виженера (Vigenure). Этот шифр базируется на наборе правил моно алфавитной подстановки, представленных 26 шифрами Цезаря со сдвигом от 0 до 25 (для латинского алфавита). Каждый из таких шифров можно обозначить ключевой буквой, являющейся буквой шифрованного текста, соответствующего букве A открытого текста. Например, шифр Цезаря, для которого смещение равно 3, обозначается ключевой буквой D.

Для облегчения понимания и применения этой схемы была предложена матрица, названная «табло Виженера» (см. табл. 3). Все 26 шифров располагаются по горизонтали, и каждому из шифров соответствует своя ключевая буква, представленная в крайнем столбце слева. Алфавит, соответствующий буквам открытого текста, находится в первой сверху строке таблицы. Процесс шифрования прост – необходимо по ключевой букве ***x*** и букве открытого текста ***y*** найти букву шифрованного текста, которая находится на пересечении строки ***x*** и столбца ***y***. В данном случае такой буквой является буква *V*.

Чтобы зашифровать сообщение, нужен ключ, имеющий туже длину, что и само сообщение. Обычно ключ представляет собой повторяющееся нужное число раз ключевое слово, чтобы получить строку подходящей длины. Например, если ключевым словом является *deceptive*, сообщение «we are discovered save yourself» шифруется следующим образом:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Открытый текст: | D | E | C | E | P | T | I | V | E | D | E | C | E | P | T | I | V | E | D | E | C | E | P | T | I | V | E |
| Ключ: | W | E | A | R | E | D | I | S | C | O | V | E | R | E | D | S | A | V | E | Y | O | U | R | S | E | L | F |
| Шифрованный текст: | Z | I | C | V | T | W | Q | N | G | R | Z | G | V | T | W | A | V | Z | H | C | Q | Y | G | L | M | G | J |

Расшифровать текст также просто – буква ключа определяет строку, буква шифрованного текста, находящаяся в этой строке, определяет столбец, и в этом столбце в первой строке таблицы будет находиться соответствующая буква открытого текста.

Преимущество этого шифра заключается в том, что для представления одной и той же буквы открытого текста в шифрованном тексте имеется много различных вариантов – по одному на каждую из неповторяющихся букв ключевого слова. Таким образом, скрывается информация, характеризующая частотность употребления букв. Но и с помощью данного метода все же не удается полностью скрыть влияние структуры открытого текста на структуру шифрованного. Повысить надежность шифра поможет использование ключа, длина которого совпадает с длиной сообщения, а текстовые характеристики максимально отклонены от стандартных характеристик языка открытого текста.

Таблица 3. Табло Виженера.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **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** |
| **a** | 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 |
| **b** | 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 | A |
| **c** | C | 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 |
| **d** | 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 |
| **e** | 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 | D |
| **f** | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| **g** | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| **h** | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| **i** | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| **j** | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| **k** | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| **l** | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| **m** | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| **n** | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| **o** | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| **p** | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| **q** | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| **r** | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| **s** | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| **t** | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| **u** | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| **v** | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| **w** | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| **x** | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| **y** | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| **z** | Z | 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 |

**Контрольные вопросы:**

1. Что такое табло Виженера?
2. Как организовать табло Виженера?
3. Алгоритм шифрации.
4. Алгоритм дешифрации.
5. Можно ли организовать дешифрацию с неизвестным ключом?
6. Можно ли программно определить правильный вариант сообщения после дешифрации?
7. Ограничения для ключа.
8. Анализ метода.

**Содержание отчета:**

1. Цель работы.
2. Алгоритм шифрации и дешифрации по заданному методу, который реализует разработанная программа.
3. Описание программы (исходный код с комментариями).
4. Анализ ограничений возможности применения разработанной программы.
5. Анализ ограничений возможности применения данного метода.