Лабораторная работа № 9
«Шифрование информации методом полиалфавитной замены
Построение и использование матрицы Вижинера»

Цель работы:

1. Закрепление теоретического материала по изучению метода полиалфавитной замены.
2. Получение шифротекста по исходным данным.
3. Получение исходного текста по заданному шифротексту и ключу.

Пояснения к работе:

При N-алфавитной замене символ soi из исходного алфавита Ao заменяется символом S11 из алфавита A1, S02 заменяется символом S22 из алфавита A2 и так далее.

После замены s0n символом Snn из An символ so(n+i) замещается символом S1(n+1) из алфавита A1 и так далее.

Наибольшее распространение получил алгоритм полиалфавитной замены с использованием таблицы (матрицы) Вижинера Тв, которая представляет собой квадратную матрицу [RxR], где R - количество символов в используемом алфавите. В первой строке располагаются символы в алфавитном порядке. Начиная со второй строки, символы записываются со сдвигом влево на одну позицию. Выталкиваемые символы заполняют освобождающиеся позиции справа (циклический сдвиг). Если используется русский алфавит, то матрица Вижинера имеет размерность [32x32].

Тв =

АБВГД.....ЪЭЮЯ_
БВГДЕ.....ЭЮЯ_А
ВГДЕЖ.....ЮЯ_АБ
.....
_АБВГ.....ЫЪЭЮЯ

Шифрование осуществляется с помощью ключа, состоящего из М неповторяющихся символов. Из полной матрицы Вижинера выделяется матрица шифрования Тш,, размерностью [(М+1);R]. Она включает первую строку и строки, первые элементы которых совпадают с символами ключа. Если в качестве ключа выбрано слово <ЗОНД>, то матрица шифрования содержит пять строк.

Пример использования матрицы Вижинера для шифрования текста

Алгоритм зашифрования с помощью таблицы Вижинера представляет собой следующую последовательность шагов:

Шаг 1. Выбор ключа К длиной М символов.

Шаг 2. Построение матрицы шифрования ТШ=(Ц) размерностью [(М+1), R] для выбранного ключа К.

Шаг 3. Под каждым символом Sor исходного текста длиной 1 символов размещается символ ключа km (рис. 20). Ключ повторяется необходимое число раз.

Шаг 4. Символы исходного текста последовательно замещаются символами, выбираемыми из Тш по следующему правилу:

- определяется символ к™ ключа К, соответствующий замещаемому символу sor;
- находится строка i в Тш, для которой выполняется условие кт=Ьи;

- определяется столбец j, для которого выполняется условие: sOr=bij;
- символ sot замещается символом by.

Шаг 5. Полученная зашифрованная последовательность разбивается на блоки определенной длины, например, по четыре символа. Последний блок дополняется, при необходимости, служебными символами до полного объема.

Расшифрование осуществляется в следующей последовательности:

Шаг 1. Под шифртекстом записывается последовательность символов ключа по аналогии с шагом 3 алгоритма зашифрования.

Шаг 2. Последовательно выбираются символы sr из шифртекста и соответствующие символы ключа km. В матрице Тш определяется строка i. для которой выполняется условие кщ= Ьп. В строке i определяется элемент by= s)r. В расшифрованный текст на позицию г помещается символ bij.

Шаг 3. Расшифрованный текст записывается без разделения на блоки. Убираются служебные символы.

Пример. Требуется с помощью ключа К = <ЗОНД> зашифровать исходный текст Т = <БЕЗОБЛАЧНОЕ_НЕБО>.

Механизмы зашифрования и расшифрования представлены следующим образом:

Исходный текст	БЕЗОБЛАЧНОЕ_НЕБО
Ключ	ЗОНДЗОНДЗОНДЗОНД
Текст после замены	ИУФТИШНЫФЫТГФУОТ
Шифртекст	ИУФТ ИШНЫ ФЫТГ ФУОТ
Ключ	ЗОНД ЗОНД ЗОНД ЗОНД
Расшифрованный текст	БЕЗО БЛАЧ НОЕ_ НЕБО
Исходный текст	БЕЗОБЛАЧНОЕ_НЕБО

Ход выполнения лабораторной работы:

1. Изучить приведенные в методическом описании к лабораторной работе материал и пример шифрования.
2. Получить у преподавателя исходный текст и ключ для шифрования.
3. Выполнить по шагам процедуру шифровании, полученный шифротекст представить в виде блоков информации.
4. Представить результаты преподавателю.
5. Получить у преподавателя шифротекст и ключ для расшифрования.
6. Выполнить по шагам процедуру расшифрования, полученный исходный текст представить преподавателю для проверки.
7. Оформить отчет в установленной форме.
8. Представить результаты работы преподавателю.

Контрольные вопросы:

1. Понятие криптостойкости. Условия, предъявляемые к криптостойкости.
2. Понятие полиалфавитной замены.
3. Понятие замены с помощью матрицы Вижинера.
4. Перечислите достоинства и недостатки полиалфавитной замены.