Пшенко Артем, ФИТ 3-4

Информационная безопасность

Отчет по лабораторной работе № 4.

Исследование криптографических шифров на основе подстановки

(замены) символов

Вариант 9

В данной лабораторной работе необходимо было реализовать шифр Цезаря. Для математического описания криптографического преобразования предполагаем, что зашифрованная буква ay (ay ∈ Сi), соответствующая символу aх (aх ∈ Мi), находится на позиции

y ≡ x + k mod N, (2.1)

где x, y – индекс (порядковый номер, начиная с 0) символа в используемом алфавите; k – ключ.

Для расшифрования сообщения Сi необходимо произвести расчеты, обратные выражению (2.1), т. е.

х ≡ у – k mod N. (2.2)

Соотношениям (2.1) и (2.2) соответствует классический шифр подстановки – шифр Цезаря. Применяя одновременно операции сложения и умножения по модулю n над элементами множества (индексами букв алфавита), можно получить систему подстановок, которую называют аффинной системой подстановок Цезаря. Определим процедуру зашифрования в такой системе:

y ≡ ax + b mod N, (2.3),

где a и b – целые числа.

При этом взаимно однозначные соответствия между открытым текстом и шифртекстом будут иметь место только при выполнении следующих условий: 0 ≤ a, b < N, наибольший общий делитель (НОД) чисел a, N равен 1, т. е. эти числа являются взаимно простыми. Исходный код данного алгоритма приведен в листинге 1.

Листинг 1. Исходный код алгоритма аффинной системы подстановок Цезаря.

|  |
| --- |
|  |

Следует отметить, что для дешифрования используется та же функция, но вторым параметром передается отрицательное значение смещения reverse\_shift.

Результат шифрования/дешифрования приведен на рисунке 1.

|  |
| --- |
|  |

Рисунок 1. Результат шифрования/дешифрования

Частотная характеристика символов исходного сообщения приведена на рисунке 2.

|  |
| --- |
|  |

Рисунок 2. Частотная характеристика символов исходного сообщения

На рисунке 3 приведена частотная характеристика зашифрованного сообщения.

|  |
| --- |
|  |

Рисунок 3. Частотная характеристика символов зашифрованного сообщения

Следует отметить, что частотные характеристики одинаковы для исходного и зашифрованного сообщения, потому что каждый символ исходного сообщения просто заменяется на новый символ.

Далее было необходимо реализовать алгоритм Трисемуса. При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Исходный код алгоритма приведен в листинге 2.

Листинг 2. Исходный код алгоритма Трисемуса

|  |
| --- |
|  |

Результат работы алгоритма представлен на рисунке 4.

|  |
| --- |
|  |

Рисунок 4. Результат работы алгоритма Трисемуса