Лабораторная работа №5

Конфиденциальность информации. Простейшие методы шифрования данных.

В данной работе предполагается рассмотрение методов обеспечения конфиденциальности информации на примере простейшей криптографической защиты.

Теоретические сведения

В контексте шифрования открытым текстом называется незашифрованное сообщение, а шифртекстом – зашифрованное. Шифр состоит из двух функций: шифрование преобразует открытый текст в шифртест, а дешифрование производит обратное действие.

Шифр Цезаря

Шифр Цезаря назван так, потому что, согласно древнеримскому историку Светонию, им пользовался Юлий Цезарь. Сообщение шифруется путем сдвига каждой буквы на три позиции вправо по алфавиту с оборотом по достижении Z. Например, ZOO шифруется как CRR, результатом дешифрирования FDHVDU является CAESAR. Чтобы дешифрировать заданный шифртекст, нужно сдвинуть каждую букву на три позиции влево. Шифр Цезаря можно сделать более безопасным, определив сдвиг на какое-либо секретное значение.

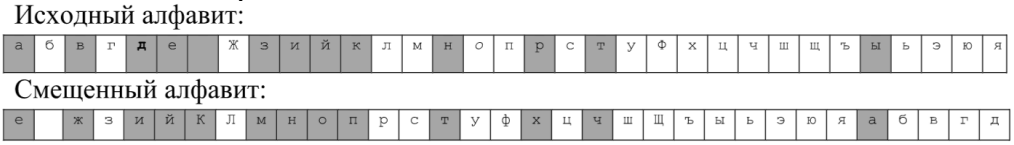

Рис.1. Шифрование сдвигом.

Взлом шифра Цезаря может быть осуществлён простым перебором возможных значений сдвига (для русского алфавита - 33), а также с помощью частотного анализа шифротекста.

Шифр Виженера

Шифр Виженера похож на шифр Цезаря, только величина сдвига составляет не три позиции, а определяется ключом, набором букв, которым соответствуют числа, равные позиции буквы в алфавите. Например, если ключ равен DUH, то буквы открытого текста сдвигаются на 3, 20 и 7 позиций, потому что D отстоит от A на три позиции, U – на 20 позиций, а H – на семь позиций. Последовательность 3, 20, 7 повторяется, пока не будет зашифрован весь открытый текст. Например, слово CRYPTO на ключе DUH было бы зашифровано как FLFSNV: C сдвигается на три позиции и превращается в F, R сдвигается на 20 и превращается в L и т. д. На рис. 2 показано, как этот принцип применяется к шифрованию предложения THEY DRINK THE TEA.

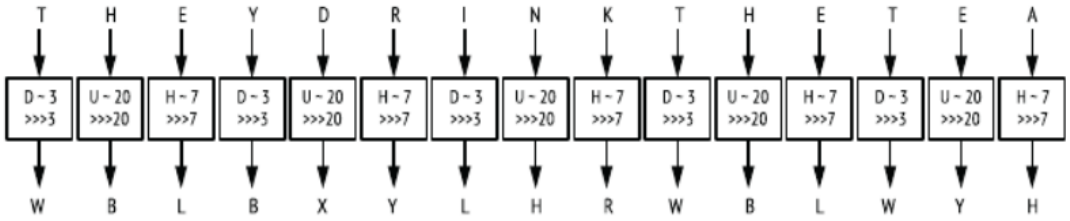

Рис.2. Шифр Виженера

Шифр Виженера безопаснее, чем шифр Цезаря, но все равно его довольно легко взломать. Первый шаг взлома – определить длину ключа. Например, рассмотрим рис. 2, где результатом шифрования фразы THEY DRINK THE TEA с ключом DUH является строка WBLBXYLHRWBLWYH (пробелы обычно удаляются, чтобы не раскрывать границы слов). Можно заметить, что в шифртексте WBLBXYLHRWBLWYH группа из трех букв WBL встречается дважды с интервалом в девять букв. Это позволяет предположить, что было зашифровано одно и то же трехбуквенное слово с одинаковыми величинами сдвига. Поэтому криптоаналитик может сделать вывод, что длина ключа либо равна девяти, либо является делителем девяти (т. е. равна трем). Кроме того, он может догадаться, что повторяющееся трехбуквенное слово – THE, а значит, DUH – возможный ключ шифрования.

Второй шаг взлома шифра Виженера – определение самого ключа методом частотного анализа, в котором используется тот факт, что распределение букв в естественных языках неравномерно. Например, в английском чаще всего встречается буква E, поэтому, обнаружив, что в шифртексте чаще

других встречается X, мы можем заключить, что в соответствующей позиции открытого текста, скорее всего, находится буква E.

Задания:

1. Создать копию «Модели угроз», разработанной в предыдущей лабораторной работе.
2. Согласно Варианту написать программу на любом языке программирования, которая зашифрует текст в вашем файле.
   Вариант вычисляется по формуле: N%2+1= K, где N – номер студента в списке группы, K – номер варианта. Вариант 1 реализует Шифр Цезаря, Вариант 2 – Шифр Виженера.

   Требования
   1. *Программа считывает данные из файла. Допускается предварительный перевод файла в удобный для работы формат.*
   2. *Программа спрашивает «ключ» у пользователя.*
   3. *Программа создаёт новый файл, помещая в него шифротекст, из которого удалены знаки препинания, отступы, пробелы.*
   4. *Программа «умеет» расшифровывать текст по запросу.*
   5. *Программа не использует готовые криптографические библиотеки.*
3. С использованием любого языка программирования написать программу, подбирающую ключ к шифротексту методом подбора или с помощью частотного анализа.

Содержание отчёта:

1. Титульный лист.
2. Блок-схема программы.
3. Листинг кода.
4. Скриншоты работоспособности.
5. Вывод.
6. Ответ на контрольные вопросы:
   a. Какой метод шифрования данных наиболее надёжен на сегодняшний день?
   b. В каких сферах деятельности обычного пользователя встречается потребность в шифровании данных?