Лабораторные работы по курсу
Защита информации (часть 1).

МГТУ им. Баумана
Кафедра ИУ-9
Юдаев П.В., 2014

Лабораторная работа №2.
Взлом шифра 2DES. Использование шифра RC4.

1 Задание

а) Считать из стандартного потока ввода две строки: открытый текст и шифротекст. Открытый текст и шифротекст имеют длину один блок - 64 бита. Методом “встреча посередине” найти ключ шифра 2DES и распечатать его в стандартный поток вывода. Все вводимые и выводимые данные представлены в HEX кодировке.
Ключ у шифра 2DES имеет 2·56 значащих бит. В этой лабораторной работе ключ имеет 2·28 значащих бит. Остальные биты ключа фиксированы.

Пример:
Ввод:
`7177657274797569`
`2FF18DAD7A13EC9F`
Вывод:
`01010101CEB5346B01010101A1134073`

б) Считать из стандартного потока ввода две строки: ключ и сообщение. Создать ключ для шифра RC4 по данному ключу. Зашифровать сообщение шифром RC4. Напечатать шифротекст в стандартный поток вывода. Расшифровать шифротекст и напечатать в стандартный поток вывода полученный текст. Все вводимые и выводимые данные представлены в HEX кодировке.

Пример:
Ввод:
`6B6579`
`6D657373616765`
Вывод:
`7F488FADCEF4F0`
`6D657373616765`

2 Рекомендации по выполнению задания

Язык программирования - по выбору студента. Рекомендуется использовать язык C/C++, ОС Unix и библиотеку libcrypto из пакета OpenSSL. Заголовочные файлы <openssl/des.h>, <openssl/rc4.h>, <openssl/evp.h>. Сборка с библиотекой libcrypto.so.

а) Атака “встреча посередине” рассказана на лекции. Выбрать структуру хранения данных - пар (шифротекст, ключ), - и реализовать эту атаку. Цель - найти ключ шифра 2DES. Каждый байт ключа шифра DES имеет 7 значащих битов и 1 контрольный. В этом задании ключ шифра DES имеет 28 “свободных” значащих бит, по 7 бит в каждом из младших 4 байтов. Во четырех старших байтах ключа значащие биты фиксированы и всегда равны 0. Таким образом, HEX маска ключа шифра 2DES равна 01010101********01010101********.

б) Можно использовать RC4* или EVP* функции. При использовании EVP* функций шифр EVP_rc4() всегда имеет длину ключа 128 бит; обратите внимание на длину и содержимое буфера, в котором хранится ключ.