Лабораторные работы по курсу
Информационные технологии 1. Операционные системы

Лабораторная работа 5
Методы защиты программ и данных

Москва, 2022

Оглавление

Теоретическая часть

Одной из функций операционной системы является задача обеспечения избирательного доступа к программам и данным. Наиболее распространенным методом, обеспечивающим персонифицированный вход в систему и доступ к информации, является система паролей. Она достаточно просто реализуется, однако не обеспечивает полноценной защиты данных. В тех случаях, когда к степени защищенности предъявляются высокие требования (банковское дело, оборона, разведка и т. п.) необходимым становится специальное кодирование (шифрование) данных (или программного кода). При этом пользователь, несанкционированно проникший в систему, не сможет воспользоваться программами и данными, не имея специального средства декодирования (тщательно засекреченного). [1] [2]

Рассмотрим некоторые методы шифрования данных.

1. Шифрование путем замены

В этом методе необходимо иметь **таблицу замены**, где каждому элементу кода данных (например, байту) ставится в соответствие некоторый код. Пример таблицы замены:

Символ	A	B	C	....	m	n	o
Код символа	65	66	67	....	109	110	111
Код замены	110	109	111	....	43	45	47
Символ	M	N	o	....	+	-	/

Шифрование производится путем замены байтов в исходных данных кодом из таблицы замен.

Еще один метод шифрования, основанный на замене, называется **ROT13** (частный случай алгоритма “**шифр Цезаря**”). Он основан на том, что символ в исходном тексте заменяется на символ, расположенный в алфавите на 13 позиций правее.

К недостаткам методов шифрования, использующих простую замену, следует отнести легкость их “взлома” при помощи частотного анализа появления в тексте различных символов и сравнения с частотным словарем.

2. Шифрование путем перестановок

Значительно сложнее расшифровать так называемые перестановочные криптограммы, когда в итоговом сообщении присутствуют те же самые буквы, что и в исходном, но их порядок изменен по некоторому правилу. Рассмотрим примеры.

Исходные данные разбиваются на определенные части (например, по 16 байт). Составляется таблица (закон) перестановок. Возможен такой закон:

8, 16, 1, 4, 3, 6, 10, 9, 11, 2, 5, 7, 12, 14, 13.

Шифрование производится путем перестановки в каждой части исходного текста байтов в соответствии с таблицей перестановок. В нашем случае 8-й байт станет на первое место, 16-й на второе и т. д.

В качестве закона перестановок можно использовать ключевое слово. Пусть это будет слово САПОГ. Составим таблицу:

порядок букв в слове	1	2	3	4	5
	С	А	П	О	Г
порядок букв в алфавите	5	1	4	3	2.

Согласно таблице, символ расположенный в исходном тексте на первом месте перемещается в криптограмме на пятое, стоящий на втором - на первое и т.д.

Более сложная криптограмма получается в случае использования следующего подхода. Пусть исходное сообщение имеет вид - НАДО УЧИТЬ УРОКИ ДОМА. Воспользуемся тем же ключом и запишем сообщение в виде:

5 1 4 3 2

Н А Д О _

У Ч И Т Ь

_ У Р О К

И _ Д О М

А _ _ _ _

Переставим столбцы согласно шифру и прочитаем криптограмму по столбцам. Получается: АЧУ_ _ _ЬКМ_ОТОО_ДИРД_НУ_ИА. Для расшифровки надо проделать обратные операции (в качестве параметра шифра используется также и длина столбца).

3. Шифрование с помощью ключа

3.1.Симметричное шифрование

При использовании этого метода содержимое исходного сообщения преобразуется с помощью содержимого ключа, при этом одному и тому же символу в исходном сообщении может соответствовать несколько различных символов в криптограмме. Это сильно затрудняет проведение частотного анализа. В качестве операции преобразования можно использовать сложение по модулю 2 (**mod 2**).

Пример сложения по mod 2:

шифрование

Исходное слово	01011010
Ключ	00110110
Результат	01101100

дешифрование

Исходное слово	01101100
Ключ	00110110
Результат	01011010

В качестве ключа целесообразно использовать более длинное слово (24 и более байт).

В настоящей работе мы будем использовать для кодирования информации метод сложения по mod 2. При этом в исходный файл должны быть внесены изменения, т.е. изменены его байты, например начиная с 1000 и кончая 2000.

Изменения следует вносить путем сложения по mod 2 байтов исходного файла с “коротким” ключом, значение которого лежит в интервале от 1 до 15.

3.2. Асимметричное шифрование

Асимметричное шифрование — это метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом. Открытый и закрытый ключи — это очень большие числа, связанные друг с другом определенной функцией, но так, что, зная одно, крайне сложно вычислить второе.

Асимметричное шифрование используется для защиты информации при ее передаче, также на его принципах построена работа электронных подписей.

Более подробно об ассиметричном шифровании можно прочитать в источнике [3]

4. Работа с файлами в языке С

В языке СИ для операций с файлами можно использовать следующие функции определенные в <stdio.h>

1. FILE *fopen(const char *fname, const char *mode) - открывает файл;

2. int fclose (FILE *stream) - закрывает файл;

3. int fprintf(FILE * stream, const char * format, ...) - форматированный вывод в поток

4. int fscanf(FILE *stream, const char *format, arg-list) – считывание информации из потока

В приведенном ниже примере происходит чтение аргументов из одного файла, их сложение и запись результата в другой файл.

```
#include <stdio.h>

#define fileW "fileW.txt"
#define fileR "fileR.txt"

int main(int argc, char *argv[])
{
    int a, b, c;
    FILE *fW = fopen(fileW, "w");
    FILE *fR = fopen(fileR, "r");
    fscanf(fR, "%d %d", &a, &b);
    c = a + b;
    fprintf(fW, "%d + %d = %d\n", a, b, c);
    fclose(fR);
    fclose(fW);
    return 0;
}
```

Практическая часть

1. Напишите программу, кодирующую файл одним из приведенных выше методов.

Номер варианта	Название метода
1	Шифрование путем замены
2	Шифрование путем перестановок
3	Шифрование с помощью ключа (симметричное шифрование)

2. *Для любознательных*: вместо п. 1, реализуйте асимметричное шифрование, используя алгоритм RSA.

Контрольные вопросы

1. Какие методы шифрования вам известны?
2. Кратко опишите метод симметричного шифрования
3. Кратко опишите метод асимметричного шифрования

Список рекомендованной литературы

1. Карпов В.Е., Коньков К.А. Основы операционных систем. Москва: Физматкнига, 2019. 326 pp.

2. Таненбаум Э., Бос Х. Современные операционные системы. Санкт-Петербург: Питер, 2021. 1119 pp.

3. Public-key cryptography [Электронный ресурс] // Wikipedia: [сайт]. URL: https://en.wikipedia.org/wiki/Public-key_cryptography