**Реферат по лекции «Шифрование файлов» - Каспер Наталья**

Для шифрования необходимо получить криптопровайдер.

**Криптопровайдер –** объект, который обеспечивает методы шифрования и дешифрования. Получить его можно следующим образом:

*if (!CryptAcquireContext(&hProv, NULL, NULL, PROV\_RSA\_FULL, CRYPT\_VERIFYCONTEXT))*

*&hProv* – получает ссылку на криптопровайдер.

Указывается, что он обеспечивает шифрование по методу RSA. Для шифрования нужно получить ключ, который генерирует система:

*CryptGenKey(hProv, CALG\_RC4, CRYPT\_EXPORTABLE, &hSessionKey);*

Ключ определяется в адресной переменной *hSessionKey*.

Шифрование выполняется по команде:

*if (!CryptEncrypt(hSessionKey, 0, true, 0, (BYTE\*)string, &count, strlen(string)))*

Шифруется строка *string* с помощью подготовленного ключа. Количество шифруемых байтов задается переменной *count*.

Расшифровка выполняется по команде:

*if(CryptDecrypt(hSessionKey, 0, TRUE, 0, pbBuffer, &count))*

Расшифрованная строка помещается в буфер *pbBuffer*.

Важным механизмом шифрования является **хэширование**. Хэширование играет особую роль в системе защиты компьютера. Существуют различные алгоритмы хэширования.

Получаем объект hHash, выполняющий хэширование:

*if (!CryptCreateHash(hProv, CALG\_MD5, 0, 0, &hHash))*

Реализация хэширования:

*if (!CryptHashData(hHash, rgbFile, cbRead, 0))*

Результат хэширования будет хранится в файле *rgbFile*.

**Алгоритм RSA**

Пусть необходимо передать по линии связи числа x. Вместо этого передается число y, которое можно вычислить по формуле:

где *e* и *m* – открытые числа, которые известны всем в сети

! *e* и *m* дб взаимно простыми числами.

Найдем целочисленный остаток *a* от деления *b* на *m*:

Пусть необходимо найти:

Воспользуемся правилом разложения на множители:

Пусть:

=> ;

=> ;

**Пример:**

Пусть x=4, e=11, m=14;

Найдем:

=> y=2 – это значение будет передано вместо х.

Рассмотрим, как восстановить x по y, e, m. Для этой цели нужно найти число d, которые удовлетворяют условию:

*;*

*-* значение функции Эйлера от числа m

;

Если p – простое и r – целое, то

;

=> ;

=> результат функции Эйлера = кол-ву взаимно простых чисел с числом m;

В примере уравнение:

Перепишем его и получим:

*r* и *d –* неизвестные => представим уравнение в виде системы 2 линейных нер-в:

Выделим член с минимальным по модулю коэффициентом (1):

=> получим отсекающее неравенство (2):

где z – новая целочисленная переменная.

Подставим (2) в (1):

Отсюда получим:

Тогда:

Получим значение минимального d:

Пусть =>

Секретный ключ равен 5 => y=2, m=14, e=11 => восстановим x по формуле:

;

=>

Что и требовалось доказать.