

Практическое занятие №4.

Исследование асимметричных алгоритмов шифрования

Создание ключей в системе PGP, передача подписанных и защищенных сообщений.

PGP (Pretty Good Privacy - довольно хорошая секретность) - это криптографическая (шифровальная) программа с высокой степенью надежности, которая позволяет пользователям обмениваться информацией в электронном виде в режиме полной конфиденциальности.

В PGP применяется принцип использования двух взаимосвязанных ключей: открытого (public key) и закрытого (private key). Это очень большие числа, генерируемые случайным образом (1024 бита, 2048 бит и т.д.). К закрытому ключу имеет доступ только отправитель сообщения, а открытый ключ публикуется или распространяется через коммуникационные сети среди своих корреспондентов. При этом открытым ключом информация шифруется, закрытым расшифровывается.

Открытые ключи можно публиковать на сервере открытых ключей или распространять через коммуникационные сети среди корреспондентов. Они хранятся в компьютере в каталоге `pubring.pkr` в виде "сертификатов открытых ключей", которые включают в себя:

- 1) идентификатор пользователя владельца ключа (обычно это имя пользователя);
- 2) временную метку, которая указывает время генерации пары ключей;
- 3) собственно ключи.

Закрытые (секретные) ключи аналогично хранятся в виде «сертификатов секретных ключей» в каталоге `secring.skr`. При этом каждый секретный ключ шифруется отдельным паролем.

Основные функции PGP:

- генерация пары закрытый - открытый ключ;
- шифрование файла с помощью открытого ключа;
- расшифровка файла с помощью закрытого ключа;
- наложение цифровой подписи с помощью закрытого ключа;
- проверка электронной подписи с помощью открытого ключа.

Программа PGP имеет дружественный интерфейс и относительно высокую скорость шифрации-дешифрации сообщений. Ее последняя версия (PGP 8.0) русифицирована, что предопределило широкое распространение PGP среди пользователей.

Процесс шифрования сообщения с помощью PGP состоит из ряда шагов (рис. 1). Сначала программа сжимает текст. Это сокращает время на отправку сообщения через модем и увеличивает надежность шифрования.

Примечание: Большинство приемов криптоанализа (взлома зашифрованных сообщений) основаны на исследовании "рисунков", присущих текстовым файлам, что помогает взломать ключ. Сжатие ликвидирует эти "рисунки".

Для обеспечения установления подлинности сообщения его можно «подписать». Это делается добавлением к сообщению электронной (цифровой) подписи, которую получатель может проверять, используя открытый ключ отправителя для расшифровки.

Цифровая подпись - это блок данных, сгенерированный с использованием секретного ключа. Программа делает это следующим образом:

- 1) Из документа генерируется дайджест сообщения (это 160 или 128 – битная "выжимка" или контрольная сумма файла сообщения), к нему добавляется информация о том, кто подписывает документ и штамп времени.

- 2) Закрытый ключ отправителя используется для зашифровки дайджеста сообщения, таким образом, "подписывая" его.

- 3) Дайджест сообщения передается вместе с самим сообщением в зашифрованном виде. При идентификации подписи создается новый дайджест и сравнивается с переданным дайджестом, если они совпадают, то подпись считается подтвержденной. Если сообщение подвергнется какому-либо изменению, ему будет соответствовать другой дайджест, т.е. будет обнаружено, что сообщение было изменено.

Распознавание электронной подписи показывает, что отправителем был действительно создатель сообщения, и что сообщение впоследствии не изменялось.

Следующим шагом является генерирование так называемого сессионного (временного) ключа, который представляет собой случайное число значительно меньшего размера, чем открытый и закрытый ключ (128 бит, 168 бит), что обеспечивает высокое быстродействие шифрации-дешифрации. Временный ключ генерируется автоматически с использованием строго случайных событий, в качестве источника которых используются параметры нажатий клавиш и движений мыши.

Данным сессионным ключом шифруется сообщение, а сессионный ключ зашифровывается с помощью публичного ключа получателя сообщения и отправляется к получателю вместе с зашифрованным текстом (рис. 1.).



Рис.1. Процесс шифрования сообщения

Расшифровка происходит в обратной последовательности. Программа RGP получателя сообщения использует закрытый ключ получателя для извлечения временного сессионного ключа, с помощью которого программа затем дешифрует зашифрованный текст (рис.2).



Рис.2. Процесс дешифрования сообщения

Задание.

1. Изучите теоретическую часть.
2. Напишите программу на любом языке программирования:
2. Переведите число 3^{43} в двоичную систему счисления.
3. Пусть каждая из 16 первых букв русского алфавита (абвгдежзийклмноп...) имеет четырехразрядный двоичный код, соответствующий ее номеру от 0 до 15, т.е.
а - 0000_2 ,
б - 0001_2 , ...,
п - 1111_2 .
 - а) Составьте из этих букв произвольное сообщение состоящее из 32 символов,
 - б) затем разбейте полученное сообщение на блоки длиной 64 бита.
 - в) Значения полученных блоков запишите в десятичной системе счисления.
4. Найдите состояние 28-разрядного двоичного регистра сдвига после циклического сдвига влево на 5, числа **X**, предварительно записанного в регистр.

вариант	X	вариант	X	вариант	X
1	179317333 ₁₀	2	179316333 ₁₀	3	119317333 ₁₀
4	479317333 ₁₀	5	179327333 ₁₀	6	129317333 ₁₀
7	579317333 ₁₀	8	179337333 ₁₀	9	139317333 ₁₀
10	679317333 ₁₀	11	179357333 ₁₀	12	149317333 ₁₀
13	779317333 ₁₀	14	179117333 ₁₀	15	159317333 ₁₀
16	179317353 ₁₀	17	179217333 ₁₀	18	179317333 ₁₀
19	179317133 ₁₀	20	179517333 ₁₀	21	279317333 ₁₀
22	179317233 ₁₀	23	179717333 ₁₀	24	379317333 ₁₀
25	179317533 ₁₀	26	171317333 ₁₀	27	179317331 ₁₀
28	179311333 ₁₀	29	172317333 ₁₀	30	179317332 ₁₀
31	179312333 ₁₀	32	177317333 ₁₀	33	179317313 ₁₀
34	179317333 ₁₀	35	175317333 ₁₀	36	179317323 ₁₀

5. Найдите сумму по модулю 2 двух чисел 2244899301₁₀ и **X**.