Ассиметричное шифрование

Проблема симметричного шифрования

Проблема распространения ключей (у ассиметричного – если знать ключ шифрования, почти невозможно расшифровать, так как ключи разные).

$M : E(M, K1) => C$

$C : D(C, K2) => M'$

Принципы Диффи–Хеллмана

1. Алгоритм общедоступен.
2. Ключ шифрования общедоступен.
3. Ключ расшифровки секретен.
4. Очень сложная расшифровка / получение ключа расшифровки, даже если есть ключ шифрования.

Алгоритм RSA

RSA – Rivest, Shamir, Aldman (создатели алгоритма). Изначально была опубликована в журнале

Вычисление ключей

Два простых числа – P и Q, вычисляется их произведение, которое называется размером (длиной) зашифрованного алфавита $N = P \cdot Q$. Далее вычисляется функция Эйлера – $F_i(N) = (P - 1)(Q - 1)$.

Используя этим параметры, считают:

- E – открытый ключ: взаимно простое с $F_i(N)$;

- D – секретный ключ: $(E \cdot D) \bmod (F_i(N)) = 1$ => $E \cdot D = 1 + k \cdot (P-1)(Q-1)$

Шифрование

$$C = M^E \bmod N$$

Расшифровка

$$M' = (C^D) \bmod N$$

> $$M = (M^E)^D = M^{E \cdot D} = M \cdot M^{F_i(N)} = M$$

Недостаток

Выполнение алгоритма очень медленное ввиду наличия операции возведения в степень, поэтому используют *гибридную схему*.

Гибридная схема

- генерация симметричного ключа;
- отправка ключа через ассиметричного шифрования;
- расшифровка симметричного ключа;
- симметричное шифрование большого объема данных / потока.

Решето Эратосфена (для получения простых чисел)

1 2 3 ~~**4**~~ **5** ~~**6**~~ 7 ~~**8**~~ ~~**9**~~ ~~**10**~~ **11** ~~**12**~~ **13** ~~**14**~~ ~~**15**~~ ~~**16**~~ **17**

> Более современное решение – теорема Рабина, но трудоемко => используют алгоритм Миллера-Рабина (вероятностный)

Алгоритм быстрого возведения в степень

$R = A^K \bmod N$

R = 1

? K > 0

? K – нечетное (последний бит равен 1): $R = (R \cdot A) \bmod N$

$K = K/2$

$A = (A \cdot A) \bmod N$

Поиск взаимно простых чисел

Алгоритм Евклида – поиск НОД. Нас интересует, чтобы он был равен 1.

Числа A и B.

$B = A \bmod B$

$A = B$

Расширенный алгоритм Евклида

$A \cdot X + B \cdot Y = \text{НОД}(A, B) = 1$

Берем единичную матрицу $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$R = A \bmod B$

? R = 0

$E = E \cdot \begin{pmatrix} 0 & 1 \\ 1 & -q = A/B \end{pmatrix}$

$B = A \bmod B$

$A = B$

Лабораторная работа 5

Реализовать RSA (в ключе хотя бы десятки тысяч).

Хеш-функция

Используется как средство аутентификации.

Требования к хеш-функции

- M произвольной длины;
- H(M) фиксированной длины;
- дешевизна вычислений;
- необратимость (H(M) <= M);
- M1 != M2 => H(M1) != H(M2).

> Гарантировано выявляет изменения сообщения

Message Digest (MD)

Наиболее популярный – MD5. Главная проблема – Birthday-коллизии.

Secure Hash Algorithm (SHA)

SHA1 (данные – 512 бит, хеш 160 бит).

Действующий алгоритм SHA2 (данные – 512 / 1024 бита, хеш – 256 / 224 или **512** / 384), также существует SHA3.

Лавинный эффект (avalanche)

Базируется на двух преобразованиях – конфузия (зависимость ключа и выходных данных делается как можно более сложной, замены) и диффузия (избыточность в статистике входных данных распределяется по всей структуре выходных данных, перемешивание).

> Как правило, в алгоритмы хеширования входят XOR, OR и т.д. (похожи на функции шифрования, но используются не ключи, а константы, которые подергаются преобразованиям).

Электронная подпись

Электронная подпись – некий аналог обычной подписи, служащий для придания электронному документу юридической силы.

Свойства собственноручной подписи

- согласие;
- аутентичность подписанта;
- авторство (неотказуемость);
- непереносимость (жесткая связь с документом);
- целостность.

Договор 1969 года

- открытость;
- подлинность.

DSA

Алгоритм ассиметричного шифрования наоборот (зашифровать может только владелец, а расшифровать – любой), E и D меняются местами.

Подписание

M, E, D

- H(M)
- электронная подпись (ЭП) – шифрование (H(M), E)

Проверка подписи

M, ЭП, D

- H(M)
- H' = расшифровка (ЭП, D)
- ? H = H'

> 63-ФЗ – современное определение электронной подписи

Виды подписей

1. Простая подпись (единоразовый вход).
2. Усиленная подпись (использует специальные алгоритмы):
    - квалифицированная;
    - неквалифицированная.

Модели

1. Децентрализованная модель – каждый отвечает сам за себе (PGP).
2. Централизованная модель – появился арбитр, который сертифицирует ключи (PKI).

Certification Authority (CA) / Удостоверяющий центр (УЦ)

Шаги:

- пользователь создает пару ключей;
- запрос в УЦ на сертификацию открытого ключа;
- выпуск сертификата, который содержит открытый ключ и подпись УЦ.

X.509 – стандарт для выпуска сертификатов

- версия и алгоритм подписания;
- реквизиты УЦ;
- срок действия сертификата;
- данные владельца закрытого ключа (соответствующего открытому);
- открытый ключ.

> Для отзыва сертификата – Certificate Revocation List (CRL)

Лабораторная работа 6

Электронная подпись – подписание и проверка подписи (разрешается использовать стандартные функции, например, в .NET – namespace Cryptography).

Лекция 5 Лекция 7