Ассиметричные шифры

Лекция от 08.11.2022

Определение

- *Асимметричной криптосистемой* или же *криптосистемой с открытым ключом* называется криптографическое преобразование, которое использует два ключа – открытый и закрытый. Пара из закрытого (private key, secret key, SK) и открытого (public key, PK) ключей создаётся пользователем, который свой закрытый ключ держит в секрете, а открытый ключ делает общедоступным для всех пользователей.

Пояснение

- Криптографическое преобразование в одну сторону (шифрование) можно выполнить, зная только открытый ключ, а в другую (расшифрование) – зная только закрытый ключ. Во многих криптосистемах из открытого ключа теоретически можно вычислить закрытый ключ, однако это является сложной вычислительной задачей.

Определения

- Если прямое преобразование выполняется открытым ключом, а обратное -- закрытым, то криптосистема называется *схемой шифрования с открытым ключом*. Все пользователи, зная открытый ключ получателя, могут зашифровать для него сообщение, которое может расшифровать только владелец закрытого ключа.

- Если прямое преобразование выполняется закрытым ключом, а обратное -- открытым, то криптосистема называется *схемой электронной подписи (ЭП)*. Владелец закрытого ключа может подписать сообщение, а все пользователи, зная открытый ключ, могут проверить, что подпись была создана только владельцем закрытого ключа и никем другим.

О применении

- Криптосистемы с открытым ключом снижают требования к каналам связи, необходимые для передачи данных. В симметричных криптосистемах перед началом связи (перед шифрованием сообщения и его передачей) требуется передать или согласовать секретный ключ шифрования по защищённому каналу связи. Злоумышленник не должен иметь возможности ни прослушать данный канал связи, ни подменить передаваемую информацию (ключ).
- Для надёжной работы криптосистем с открытым ключом необходимо, чтобы злоумышленник не имел возможности подменить открытый ключ легального пользователя. Другими словами, криптосистема с открытым ключом, в случае использования открытых и незащищённых каналов связи, устойчива к действиям пассивного криптоаналитика, но всё ещё должна предпринимать меры по защите от активного криптоаналитика.

О применении

- Для предотвращения атак «человек посередине» с активным криптоаналитиком, который бы подменял открытый ключ получателя во время его передачи будущему отправителю сообщений, используют *сертификаты открытых ключей*.
- Сертификат представляет собой информацию о соответствии открытого ключа и его владельца, подписанную электронной подписью третьего лица. В корпоративных информационных системах организация может обойтись одним лицом, подписывающим сертификаты. В этом случае его называют доверенным центром сертификации или удостоверяющим центром. В глобальной сети Интернет для защиты распространения программного обеспечения (например, защиты от подделок в ПО) и проверок сертификатов в протоколах на базе SSL/TLS используется иерархия удостоверяющих центров.

О применении

- При обмене личными сообщениями и при распространении программного обеспечения с открытым кодом вместо жёсткой иерархии может использоваться сеть доверия. В сети доверия каждый участник может подписать сертификат любого другого участника. Предполагается, что подписывающий знает лично владельца сертификата и удостоверился в соответствии сертификата владельцу при личной встрече.

Односторонние функции

- Криптосистемы с открытым ключом построены на основе односторонних (однонаправленных) функций с потайным входом. Под *односторонней* функцией понимают такое отображение, которое подразумевает *вычислительную* невозможность нахождения обратного отображения: вычисление значения функции $y = f(x)$ при заданном аргументе x является лёгкой задачей, вычисление аргумента x при заданном значении функции y -- трудной задачей.

Односторонние функции

- Односторонняя функция $y = f(x, K)$ с *потайным входом* K определяется как функция, которая легко вычисляется при заданном x и аргумент x которой можно легко вычислить из y, если известен «секретный» параметр K, и вычислить невозможно, если параметр K неизвестен.

Односторонние функции

- Примером подобной функции является возведение в степень по модулю составного числа n: $y = f(x) = x^k \bmod n$
- Для того чтобы быстро вычислить обратную функцию, её можно представить в виде $x = y^d \bmod n$, где $d = k^{-1} \, mod \, \varphi(n)$
- В последнем выражении $\varphi(n)$ -- это функция Эйлера. В качестве «потайной дверцы» или секрета можно рассматривать или непосредственно само число d, или значение $\varphi(n)$. Последнее можно быстро найти только в том случае, если известно разложение числа n на простые сомножители. Именно эта функция с потайной дверцей лежит в основе криптосистемы RSA.

Криптосистема RSA

- В 1978 г. Рональд Ривест, Ади Шамир и Леонард Адлеман предложили алгоритм, обладающий рядом интересных для криптографии свойств. На его основе была построена первая система шифрования с открытым ключом, получившая название по первым буквам фамилий авторов -- система RSA.

Криптосистема RSA. Этап 1

- Создание пары из закрытого и открытого ключей

  1) Случайно выбрать большие простые различные числа p и q, для которых $\log_2 p \cong \log_2 q > 1024$ бита. Случайный выбор больших простых чисел не является простой задачей

  2) Вычислить произведение $n = pq$

  3) Вычислить функцию Эйлера $\varphi(n) = (p-1)(q-1)$

  4) Выбрать случайное целое число $e \in [3, \varphi(n) - 1]$, взаимно простое с $\varphi(n)$, то есть $\text{НОД}(e, \varphi(n)) = 1$

Криптосистема RSA. Этап 1

- Создание пары из закрытого и открытого ключей

  5) Вычислить число d такое, что $d \cdot e \equiv 1 \bmod \varphi(n)$.

  6) Закрытым ключом будем называть пару чисел n и d, открытым ключом -- пару чисел n и e.

Криптосистема RSA. Этап 2

- Шифрование с использованием открытого ключа

  1) Сообщение представляют целым числом $m \in [1, n-1]$

  2) Шифртекст вычисляется как $c = m^e \bmod n$ (это тоже целое число из диапазона $[1, n-1]$)

Криптосистема RSA. Пример

1. Генерирование параметров.
   1.1. Выберем числа $p = 13$, $q = 11$, $n = 143$.
   1.2. Вычислим $\varphi(n) = (p-1)(q-1) = 12 \cdot 10 = 120$.
   1.3. Выберем $e = 23$: $\gcd(e, \varphi(n)) = 1$, $e \in [3, 119]$.
   1.4. Найдём $d = e^{-1} \bmod \varphi(n) = 23^{-1} \bmod 120 = 47$.
   1.5. Открытый и закрытый ключи:

$$PK = (e : 23, n : 143),\ SK = (d : 47, n : 143).$$

2. Шифрование.
   2.1. Пусть сообщение $m = 22 \in [1, n-1]$.
   2.2. Вычислим шифртекст:

$$c = m^e \bmod n = 22^{23} \bmod 143 = 55 \bmod 143.$$

3. Расшифрование.
   3.1. Полученный шифртекст $c = 55$.
   3.2. Вычислим открытый текст:

$$m = c^d \bmod n = 55^{47} \bmod 143 = 22 \bmod 143.$$

Электронная подпись

- Предположим, что пользователь не шифрует свои сообщения, но хочет посылать их в виде открытых текстов с подписью. Для этого надо создать электронную подпись (ЭП). Это можно сделать, используя систему RSA. При этом должны быть выполнены следующие требования:
- вычисление подписи от сообщения является вычислительно лёгкой задачей;
- фальсификация подписи при неизвестном закрытом ключе -- вычислительно трудная задача;
- подпись должна быть проверяемой открытым ключом.

Электронная подпись

- Создание параметров ЭП RSA производится так же, как и для схемы шифрования RSA. Пусть у отправителя имеется закрытый ключ $SK = (n, d)$, а у получателя (проверяющий) -- открытый ключ $PK = (e, n)$.

Электронная подпись

- Этапы работы:

  1) отправитель вычисляет подпись сообщения $m \in [1, n-1]$ как $s = m^d \bmod n$ на своём закрытом ключе SK

  2) отправитель посылает сообщение в виде (m, s), где m -- открытый текст, s -- подпись.

  3) получатель принимает сообщение, возводит s в степень e по модулю n (e, n -- часть открытого ключа), в результате вычислений получает открытый текст:
  $s^e \bmod n = \left(m^d \bmod n\right)^e \bmod n = m$

  4) получатель сравнивает полученное значение с первой частью сообщения. При полном совпадении подпись принимается.

Электронная подпись

- Недостаток данной системы создания ЭП состоит в том, что подпись $m^d \bmod n$ имеет большую длину, равную длине открытого сообщения m. Для уменьшения длины подписи применяется другой вариант процедуры: вместо сообщения m отправитель подписывает $h(m)$, где $h(x)$ -- известная криптографическая хэш-функция. Модифицированная процедура состоит в следующем.

Электронная подпись

- Этапы

  1) отправитель посылает сообщение в виде (m, s), где m -- открытый текст, $s = h(m)^d \bmod n$

  2) получатель принимает сообщение (m, s), вычисляет хэш $h(m)$ и возводит подпись в степень: $h_1 = s^e \bmod n$

  3) получатель сравнивает значения $h(m)$ и h_1, при равенстве подпись считается подлинной, при неравенстве -- фальсифицированной.

Электронная подпись: пример

1. Генерирование параметров.
   1.1. Выберем $p = 13, q = 17, n = 221$.
   1.2. Вычислим $\varphi(n) = (p-1)(q-1) = 12 \cdot 16 = 192$.
   1.3. Выберем $e = 25:\ \gcd(e = 25, \varphi(n) = 192) = 1$, $e \in [3, \varphi(n) - 1 = 191]$.
   1.4. Найдём $d = e^{-1} \mod \varphi(n) = 25^{-1} \mod 192 = 169$.
   1.5. Открытый и закрытый ключи:

$$PK = (e : 25, n : 221),\ SK = (d : 169, n : 221).$$

2. Подписание.
   2.1. Пусть хэш сообщения $h(m) = 12 \in [1, n-1]$.
   2.2. Вычислим ЭП:

$$s = h^d = 12^{169} = 90 \mod 221.$$

3. Проверка подписи.
   3.1. Пусть хэш полученного сообщения $h(m) = 12$, полученная подпись $s = 90$.
   3.2. Выполним проверку:

$$h_1 = s^e = 90^{25} = 12 \mod 221,\ h_1 = h.$$

Подпись верна.