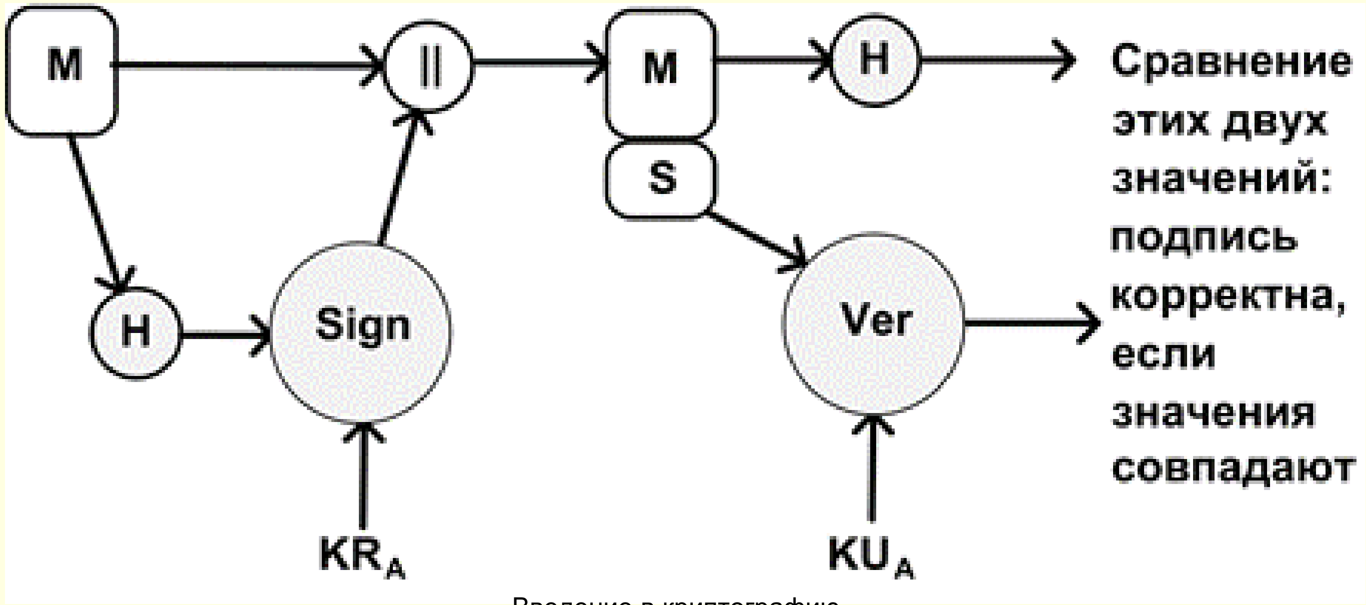
Стандарт цифровой подписи DSS

- Национальный институт стандартов и технологии США (NIST) разработал федеральный стандарт цифровой подписи DSS. Для создания цифровой подписи используется алгоритм DSA (Digital Signature Algorithm). В качестве хеш-алгоритма стандарт предусматривает использование алгоритма SHA-1 (Secure Hash Algorithm). DSS первоначально был предложен в 1991 году и пересмотрен в 1993 году в ответ на публикации, касающиеся безопасности его схемы.

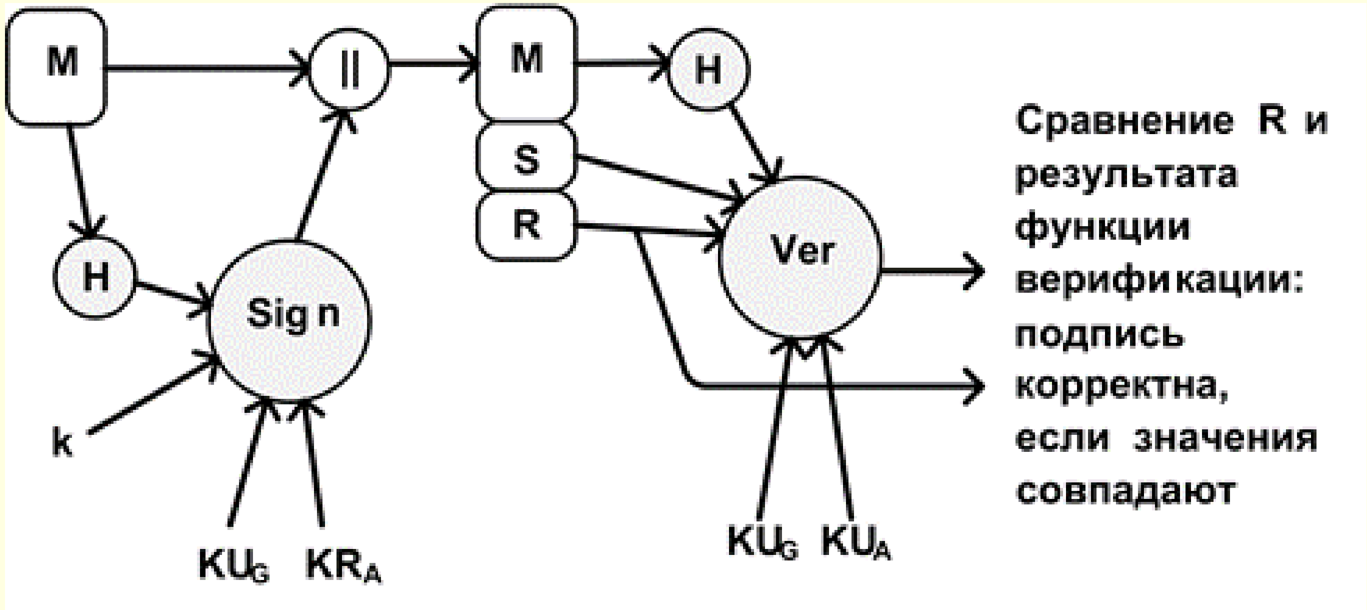
Стандарт цифровой подписи DSS

- Стандарт DSS может использоваться только для создания цифровой подписи. В отличие от RSA, его нельзя использовать для шифрования или обмена ключами. Тем не менее, это технология открытого ключа.
- Рассмотрим отличия цифровых подписей, создаваемых DSS, от цифровых подписей, создаваемых такими алгоритмами как RSA.



Создание и проверка подписи с помощью алгоритма RSA

Стандарт цифровой подписи DSS



Создание и проверка подписи с помощью стандарта DSS

Стандарт цифровой подписи DSS

- В алгоритме RSA подписываемое сообщение подается на вход сильной хеш-функции, которая создает хеш-код фиксированный длины. Для создания подписи этот хеш-код подписывается с использованием закрытого ключа отправителя. Затем сообщение и подпись пересылаются получателю. Получатель вычисляет хеш-код сообщения и проверяет подпись, используя открытый ключ отправителя. Если вычисленный хеш-код равен значению, полученному при проверке подписи, то считается, что подпись корректна.
- В DSS также используется сильная хеш-функция. Хеш-код является входом функции подписи вместе со случайным числом **k**, созданным для этой конкретной подписи. Функция подписи также зависит от закрытого ключа отправителя $\mathbf{KR_A}$ и множества параметров, известных всем участникам. Можно считать, что это множество состоит из глобального открытого ключа $\mathbf{KU_G}$. Результатом является подпись, состоящая из двух компонент, обозначаемых как **S** и **R.**
- Для проверки подписи получатель также создает хеш-код полученного сообщения. Этот хеш-код вместе с подписью является входом в функцию верификации. Функция верификации зависит от глобального открытого ключа $\mathbf{KU_G}$ и от открытого ключа отправителя $\mathbf{KU_A}$. Выходом функции верификации является значение, которое должно равняться компоненте **R** подписи, если подпись корректна. Функция подписи такова, что только отправитель, знающий закрытый ключ, может создать корректную подпись

Стандарт цифровой подписи DSS

- DSS основан на трудности вычисления дискретных логарифмов и базируется на схеме, определенной ElGamal и Schnorr.

Общие компоненты группы пользователей

- Существует три параметра, которые являются открытыми и могут быть общими для большой группы пользователей.
- N-битное простое число **q**, $2^{N-1} < q < 2^N$
- L-битное простое число **p**, $2^{L-1} < p < 2^L$
  - L = 1024, N = 160
  - L = 2048, N = 224
  - L = 2048, N = 256
  - L = 3072, N = 256
- **(p-1)** делится на **q: (p-1)/q** целое.
- $g = h^{(p-1)/q} \pmod p$, где **h** является целым между **1** и **(p-1)**, и **g** должно быть больше единицы.
- Зная эти значения, отправитель выбирает закрытый ключ и создает открытый ключ.

Стандарт цифровой подписи DSS

Закрытый ключ отправителя

- Закрытый ключ x должен быть числом между 1 и $(q-1)$ и должен быть выбран случайно или псевдослучайно.

x - случайное или псевдослучайное целое, $0 < x < q$

Открытый ключ отправителя

- Открытый ключ вычисляется следующим образом:

$y = g^x \pmod p$

- Вычислить y по известному x довольно просто. Однако, имея открытый ключ y, вычислительно невозможно определить x, который является дискретным логарифмом y по основанию g.

Стандарт цифровой подписи DSS

Случайное число, уникальное для каждой подписи.

k - случайное или псевдослучайное целое, $0<k<q$, уникальное для каждого подписывания.

Подписывание

Для создания подписи отправитель вычисляет две величины, **r** и **s**, которые являются функцией от компонент открытого ключа **(p, q, g)**, закрытого ключа пользователя **x**, хеш-кода сообщения **H(M)** и целого **k**, которое должно быть создано случайно или псевдослучайно и должно быть уникальным при каждом подписывании.

$$r = g^k \ ((\mathrm{mod}\ p)\ \mathrm{mod}\ q)$$

$$s = (k^{-1} \cdot (H(M) + x \cdot r))\ (\mathrm{mod}\ q)$$

Подпись равна **(r, s)**.

Стандарт цифровой подписи DSS

Проверка подписи

Получатель выполняет проверку подписи, используя следующие формулы. Он вычисляет значение **v**, которое является функцией от компонент общего открытого ключа, открытого ключа отправителя и хеш-кода полученного сообщения. Если эта величина равна компоненте **r** в подписи, то подпись считается действительной.

$$w = s^{-1} \pmod q$$

$$u1 = (H(M)\cdot w) \pmod q$$

$$u2 = r\cdot w \pmod q$$

$$v = ((g^{u1}\cdot y^{u2}) \pmod p) \pmod q$$

Подпись корректна, если $v = r$

Докажем, что $v = r$ в случае корректной подписи.

Стандарт цифровой подписи DSS

Лемма 1. Для любого целого t, если

$$g = h^{(p-1)/q} (\mathrm{mod}\ p)$$

то $g^t\ (\mathrm{mod}\ p) = g^{t \bmod q} (\mathrm{mod}\ p)$

По теореме Ферма, так как h является взаимнопростым с p, то $h^{p-1} (\mathrm{mod}\ p) = 1$.

Следовательно, для любого неотрицательного целого n

$$g^{nq} (\mathrm{mod}\ p) = (h^{(p-1)/q} (\mathrm{mod}\ p))^{nq} (\mathrm{mod}\ p)$$

$$= h^{((p-1)/q)\ nq} (\mathrm{mod}\ p) = h^{(p-1)n} (\mathrm{mod}\ p)$$

$$= ((h^{(p-1)} (\mathrm{mod}\ p))^n)\ (\mathrm{mod}\ p) = 1^n (\mathrm{mod}\ p) = 1$$

Таким образом, для неотрицательных целых n и z мы имеем

$$g^{nq+z}\ (\mathrm{mod}\ p) = (g^{nq} \cdot g^z) (\mathrm{mod}\ p)$$

$$= (((g^{nq} (\mathrm{mod}\ p)) \cdot (g^z (\mathrm{mod}\ p\ )))\ (\mathrm{mod}\ p) = g^z (\mathrm{mod}\ p)$$

Любое неотрицательное целое t может быть представлено единственным способом как $t = nq + z$, где n и z являются неотрицательными целыми и $0<z<q$. Таким образом $z = t\ (\mathrm{mod}\ q)$.

Стандарт цифровой подписи DSS

Лемма 2. Для неотрицательных чисел $\mathbf{a}$ и $\mathbf{b}$:

$$g^{(a \bmod q\ +\ b \bmod q)} \pmod p = g^{(a+b) \bmod q} \pmod p.$$

По лемме 1 мы имеем

$$g^{(a \bmod q\ +\ b \bmod q)} \pmod p = g^{(a \bmod q\ +\ b \bmod q) \bmod q} \pmod p$$

$$= g^{(a\ +\ b) \bmod q} \pmod p$$

Лемма 3. $y^{(rw) \bmod q} \pmod p = g^{(xrw) \bmod q} \pmod p$

По определению $y = g^x \pmod p$. Тогда:

$$y^{(rw) \bmod q} \pmod p = (g^x \pmod p)^{(rw) \bmod q} \pmod p$$

$= g^{x\ ((rw) \bmod q)} \pmod p$ - по правилам модульной арифметики

$= g^{(x\ ((rw \bmod q))) \bmod q} \pmod p$ - по лемме 1

$$= g^{(xrw) \bmod q} \pmod p$$

Стандарт цифровой подписи DSS

Лемма 4. $((H(M) + x \cdot r) \cdot w) \pmod q = k$

По определению $s = (k^{-1} \cdot (H(M) + x \cdot r)) \pmod q$. Кроме того, так как q является простым, любое неотрицательное целое меньшее q имеет мультипликативную инверсию.
Т.е. $(k \cdot k^{-1}) \pmod{q = 1}$. Тогда:

$$(k \cdot s) \pmod q = (k \cdot (k^{-1} \cdot (H(M) + x \cdot r)) \pmod q) \pmod q =$$

$$= (k \cdot (k^{-1} (H(M) + x \cdot r))) \pmod q =$$

$$= ((k \cdot k^{-1}) \pmod q) \cdot ((H(M) + x \cdot r) \pmod q) \pmod q =$$

$$= (H(M) + x \cdot r) \pmod q$$

По определению $w = s^{-1} \pmod q$, следовательно, $(w \cdot s) \pmod q = 1$. Следовательно:

$$((H(M) + x \cdot r) w) \pmod q = ((H(M) + x \cdot r) \pmod q) \cdot w \pmod q)) \pmod q$$

$$= ((k \cdot s) \pmod q) \cdot w \pmod q)) \pmod q$$

$$= (k \cdot w \cdot s) \pmod q$$

$$= (k \pmod q) \cdot (w \cdot s) \pmod q)) \pmod q$$

$$= k \pmod q$$

Так как $0 < k < q$, то $k \pmod q = k$

Стандарт цифровой подписи DSS

Теорема. Используя введенные выше определения для $\mathbf{v}$ и $\mathbf{r}$, докажем, что $\mathbf{v=r}$.

$$v = ((g^{u1} \cdot y^{u2}) \ (\mathrm{mod}\ p))\ (\mathrm{mod}\ q)$$
$$= (g^{(H(M)\ w)\ (\mathrm{mod}\ q)} \cdot y^{(rw)\ (\mathrm{mod}\ q)})\ (\mathrm{mod}\ p)\ (\mathrm{mod}\ q)$$
$$= (g^{(H(M)\ w)\ (\mathrm{mod}\ q)} \cdot g^{(xrw)(\mathrm{mod}\ q)})\ (\mathrm{mod}\ p)\ (\mathrm{mod}\ q)$$
$$= (g^{(H(M)\ w)\ (\mathrm{mod}\ q) + (xrw)\ (\mathrm{mod}\ q)})\ (\mathrm{mod}\ p)\ (\mathrm{mod}\ q)$$
$$= (g^{(H(M)\ w + xrw)(\mathrm{mod}\ q)})\ (\mathrm{mod}\ p)\ (\mathrm{mod}\ q)$$
$$= (g^{w\ (H(M) + xr)\ \mathrm{mod}\ q})\ (\mathrm{mod}\ p)\ (\mathrm{mod}\ q)$$
$$= (g^{k}(\mathrm{mod}\ p))\ (\mathrm{mod}\ q)$$
$$= r$$

Российский стандарт цифровой подписи ГОСТ 3410

В отечественном стандарте ГОСТ 3410, принятом в 1994 году, используется алгоритм, аналогичный алгоритму, реализованному в стандарте DSS. Оба алгоритма относятся к семейству алгоритмов ElGamal.

В стандарте ГОСТ 3410 используется хеш-функция ГОСТ 3411, которая создает хеш-код длиной 256 бит. Это во многом обуславливает требования к выбираемым простым числам **p** и **q**:

p должно быть простым числом в диапазоне

$2^{509} < p < 2^{512}$ либо

$2^{1020} < p < 2^{1024}$

q должно быть простым числом в диапазоне

$2^{254} < q < 2^{256}$

q также должно быть делителем $(p-1)$.

Аналогично выбирается и параметр **g**. При этом требуется, чтобы

$g^q \pmod{p} = 1$.

В соответствии с теоремой Ферма это эквивалентно условию в DSS, что

$g = h^{(p-1)/q} \pmod{p}$

Российский стандарт цифровой подписи ГОСТ 3410

Закрытым ключом является произвольное число $\mathbf{x}$

$$0 < x < q$$

Открытым ключом является число $\mathbf{y}$

$$y = g^{x} (\mathrm{mod}\ p)$$

Для создания подписи выбирается случайное число $\mathbf{k}$

$$0 < k < q$$

Российский стандарт цифровой подписи ГОСТ 3410

Подпись состоит из двух чисел **(r, s)**, вычисляемых по следующим формулам:

$$r = (g^k \bmod p) \bmod q$$

$$s = (k \cdot H(M) + x \cdot r) \bmod q$$

Еще раз обратим внимание на отличия DSS и ГОСТ 3410.

Используются разные хеш-функции: в ГОСТ 3410 применяется отечественный стандарт на хеш-функции ГОСТ 3411, в DSS используется SHA-1, которые имеют разную длину хеш-кода. Отсюда и разные требования на длину простого числа **q**: в ГОСТ 3410 длина **q** должна быть от 254 бит до 256 бит, а в DSS длина **q** должна быть от 159 бит до 160 бит.

По-разному вычисляется компонента **s** подписи. В ГОСТ 3410 компонента **s** вычисляется по формуле

$$s = (k \cdot H(M) + x \cdot r) \pmod q$$

В DSS компонента s вычисляется по формуле

$$s = (k^{-1} \cdot (H(M) + x \cdot r)) \pmod q$$

Последнее отличие приводит к соответствующим отличиям в формулах для проверки подписи.

Российский стандарт цифровой подписи ГОСТ 3410

Получатель вычисляет

$$w = H(M)^{-1} \pmod q$$

$$u1 = w \cdot s \pmod q$$

$$u2 = (q-r) \cdot w \pmod q$$

$$v = ((g^{u1} \cdot y^{u2}) \bmod p) \pmod q$$

Подпись корректна, если $v = r$.

Российский стандарт цифровой подписи ГОСТ 3410

Структура обоих алгоритмов довольно интересна. Заметим, что значение **r** совсем не зависит от сообщения. Вместо этого **r** есть функция от **k** и трех общих компонент открытого ключа. Мультипликативная инверсия **k(mod p)**(в случае DSS) или само значение **k** (в случае ГОСТ 4310) подается в функцию, которая, кроме того, в качестве входа имеет хеш-код сообщения и закрытый ключ пользователя. Эта функция такова, что получатель может вычислить **r**, используя входное сообщение, подпись, открытый ключ пользователя и общий открытый ключ.

В силу сложности вычисления дискретных логарифмов нарушитель не может восстановить **k** из **r** или **x** из **s**.

Другое важное замечание заключается в том, что экспоненциальные вычисления при создании подписи необходимы только для $g^k(\mathrm{mod}\ p)$. Так как это значение от подписываемого сообщения не зависит, оно может быть вычислено заранее. Пользователь может заранее просчитать некоторое количество значений **r** и использовать их по мере необходимости для подписи документов. Еще одна задача состоит в определении мультипликативной инверсии k^{-1} (в случае DSS). Эти значения также могут быть вычислены заранее.

Российский стандарт цифровой подписи ГОСТ 3410

- Подписи, созданные с использованием стандартов ГОСТ 3410 или DSS, называются **рандомизированными**, так как для одного и того же сообщения с использованием одного и того же закрытого ключа каждый раз будут создаваться разные значения подписи **`(r,s)`**, поскольку каждый раз будет использоваться новое значение **`k`**. Подписи, созданные с применением алгоритма RSA, называются **детерминированными**, так как для одного и того же сообщения с использованием одного и того же закрытого ключа каждый раз будет создаваться одна и та же подпись.