ЭЛЕКТРОННАЯ, ИЛИ ЦИФРОВАЯ ПОДПИСЬ

Прежде чем начать рассмотрение криптографической цифровой подписи, сформулируем три свойства, которым (в идеале) должна удовлетворять любая, в частности, обычная рукописная подпись:

1. Подписать документ может только «законный» владелец подписи (и, следовательно, никто не может подделать подпись).
2. Автор подписи не может от нее отказаться.
3. В случае возникновения спора возможно участие третьих лиц (например, суда) для установления подлинности подписи.

ЭЛЕКТРОННАЯ, ИЛИ ЦИФРОВАЯ ПОДПИСЬ

Электронная подпись RSA

Абонент выбирает случайно два больших простых числа P и Q. Затем он вычисляет число

$$N = PQ. \tag{2.28}$$

(Число N является открытой информацией, доступной другим абонентам.) После этого абонент вычисляет число $\phi = (P-1)(Q-1)$ и выбирает некоторое число $d < \phi$, взаимно простое с ϕ, и по обобщенному алгоритму Евклида находит число c, такое, что

$$cd \bmod \phi = 1. \tag{2.29}$$

Пусть Алиса хочет подписать сообщение $\bar{m} = m_1, \ldots, m_n$. Тогда вначале она вычисляет так называемую хеш-функцию

$$y = h(m_1, \ldots, m_n),$$

которая ставит в соответствие сообщению $\bar{m}$ число y. Предполагается, что алгоритм вычисления хеш-функции всем известен.

Алиса вычисляет число

$$s = y^c \bmod N, \tag{4.1}$$

т.е. она возводит число y в свою секретную степень. Число s это и есть цифровая подпись. Она просто добавляется к сообщению $\bar{m}$, и тем самым Алиса имеет сформированное подписанное сообщение

$$\langle \bar{m},\ s \rangle \,. \tag{4.2}$$

Теперь каждый, кто знает открытые параметры Алисы, ассоциированные с ее именем, т.е. числа N и d, может проверить подлинность ее подписи. Для этого необходимо, взяв подписанное сообщение (4.2), вычислить значение хеш-функции $h(\bar{m})$, число

$$w = s^d \bmod N \tag{4.3}$$

и проверить выполнение равенства $w = h(\bar{m})$.

Утверждение 4.1. *Если подпись подлинная, то* $w = h(\bar{m})$.

Доказательство. Из (4.3), (4.1) и свойств схемы RSA (см. разд. 2.6) следует

$$w = s^d \bmod N = y^{cd} \bmod N = y = h(\bar{m}).$$

Утверждение 4.2. *Описанная электронная подпись удовлетворяет всем требованиям, предъявляемым к подписи.*

Пример 4.1. Пусть $P = 5$, $Q = 11$. Тогда $N = 5 \cdot 11 = 55$, $\phi = 4 \cdot 10 = 40$. Пусть $d = 3$. Такой выбор d возможен, так как $\gcd(40, 3) = 1$. Параметр $c = 3^{-1} \bmod 40$ вычисляем с помощью обобщенного алгоритма Евклида (см. разд. 2.3), $c = 27$.

Пусть, например, Алиса хочет подписать сообщение $\bar{m} = abbbaa$, для которого значение хеш-функции равно, скажем, 13:

$$y = h(abbbaa) = 13.$$

В этом случае Алиса вычисляет по (4.1)

$$s = 13^{27} \bmod 55 = 7$$

и формирует подписанное сообщение

$$\langle abbbaa,\ 7 \rangle\,.$$

Теперь тот, кто знает открытые ключи Алисы $N = 55$ и $d = 3$, может проверить подлинность подписи. Получив подписанное сообщение, он заново вычисляет значение хеш-функции

$$h(abbbaa) = 13$$

(если содержание сообщения не изменено, то значение хеш-функции совпадет с тем, которое вычисляла Алиса) и вычисляет по (4.3)

$$w = 7^3 \bmod 55 = 13.$$

Значения w и хеш-функции совпали, значит, подпись верна. $\square$

Электронная подпись на базе шифра Эль-Гамаля

Алиса собирается подписывать документы. Она выбирает большое простое число $\boldsymbol{p}$ и число $\boldsymbol{g}$, такие, что различные степени $\boldsymbol{g}$ суть различные числа по модулю $\boldsymbol{p}$. Эти числа передаются или хранятся в открытом виде и могут быть общими для целой группы пользователей.

Алиса выбирает случайное число $\boldsymbol{x}$, $\boldsymbol{1 < x < p - 1}$, которое она держит в секрете. Это ее секретный ключ, только она его знает. Затем она вычисляет число

$$y = g^x \bmod p. \tag{4.4}$$

Это число y Алиса публикует в качестве своего открытого ключа. Заметим, что при больших p, зная y, невозможно найти x (это задача дискретного логарифмирования).

Теперь Алиса может подписывать сообщения. Допустим, она хочет подписать сообщение $\bar{m} = m_1, \ldots, m_n$. Опишем последовательность действий для построения подписи.

Вначале Алиса вычисляет значение хеш-функции $h = h(\bar{m})$, которое должно удовлетворять неравенству $1 < h < p$. Затем Алиса выбирает случайно число k ($1 < k < p-1$), взаимно простое с $p-1$, и вычисляет число

$$r = g^k \bmod p. \tag{4.5}$$

Далее Алиса вычисляет числа

$$u = (h - xr) \bmod (p-1), \tag{4.6}$$

$$s = k^{-1} u \bmod (p-1). \tag{4.7}$$

Под k^{-1} в (4.7) подразумевается число, удовлетворяющее уравнению

$$k^{-1}k \bmod (p-1) = 1. \tag{4.8}$$

Такое k^{-1} существует, так как k и $p-1$ взаимно просты, и может быть найдено по обобщенному алгоритму Евклида. Наконец, Алиса формирует подписанное сообщение

$$\langle \bar{m};\ r,\ s \rangle. \tag{4.9}$$

Получатель подписанного сообщения (4.9), прежде всего, заново вычисляет значение хеш-функции $h = h(\bar{m})$. Затем он проверяет подпись, используя равенство

$$y^r r^s = g^h \bmod p. \tag{4.10}$$

Утверждение 4.3. *Если подпись верна, то условие* (4.10) *выполняется.*

Доказательство. Действительно,

$$y^r r^s = (g^x)^r \left(g^k\right)^s = g^{xr} g^{k\left(k^{-1}(h-xr)\right)} = g^{xr} g^h g^{-xr} = g^h \bmod p.$$

(Здесь первое равенство следует из (4.4) и (4.5), второе из (4.7).)

Утверждение 4.4. *Описанная электронная подпись удовлетворяет всем требованиям, предъявляемым к подписи.*

П р и м е р 4.2. Пусть общие параметры для некоторого сообщества пользователей $p = 23$, $g = 5$. Алиса выбирает свой секретный ключ $x = 7$ и вычисляет открытый ключ y по (4.4):

$$y = 5^7 \bmod 23 = 17.$$

Пусть Алиса создала документ $\bar{m} = baaaab$ и хочет его подписать.

Перейдем к вычислению подписи по алгоритму. Прежде всего она вычисляет хеш-функцию, пусть ее значение $h(\bar{m}) = 3$. Затем Алиса генерирует случайное число k, например, $k = 5$. Вычисления по (4.5), (4.6) дают

$$r = 5^5 \bmod 23 = 20,$$

$$u = (3 - 7 \cdot 20) \bmod 22 = 17.$$

Далее Алиса находит $k^{-1} \bmod 22$:

$$k^{-1} \bmod 22 = 5^{-1} \bmod 22 = 9.$$

Вычисления по (4.7) дают

$$s = 9 \cdot 17 \bmod 22 = 21.$$

Наконец, Алиса формирует подписанное сообщение в виде (4.9):

$$\langle baaaab,\ 20,\ 21\rangle.$$

Подписанное сообщение передается, Боб его получает и проверяет подлинность подписи. Вначале он вычисляет значение хеш-функции

$$h(baaaab) = 3,$$

затем вычисляет левую часть (4.10)

$$17^{20} \cdot 20^{21} \bmod 23 = 16 \cdot 15 \bmod 23 = 10$$

и после этого правую часть (4.10)

$$5^3 \bmod 23 = 10.$$

Боб делает вывод, что подпись верна.

Рассмотренный метод электронной подписи сложнее, чем RSA, а его стойкость базируется на другой, нежели в RSA, односторонней функции. Это важно для криптографии, так как в случае дискредитации одного метода можно использовать другой. Кроме того, на основе подписи Эль-Гамаля может быть построен более эффективный алгоритм, в котором время вычислений значительно сокращается за счет использования «коротких» показателей степени. Такой алгоритм представлен в следующем разделе.

Стандарты на электронную (цифровую) подпись.

ГОСТ Р34.10-94. FIPS 186. (DSA)

Вначале для некоторого сообщества пользователей выбираются общие несекретные параметры. Прежде всего необходимо найти два простых числа, q длиной 256 бит и p длиной 1024 бита, между которыми выполняется соотношение

$$p = bq + 1 \tag{4.11}$$

для некоторого целого b. Старшие биты в p и q должны быть равны единице. Затем выбирается число $a > 1$, такое, что

$$a^q \bmod p = 1. \tag{4.12}$$

В результате получаем три общих параметра — p, q и a.

Далее каждый пользователь выбирает случайно число x, удовлетворяющее неравенству $0 < x < q$, и вычисляет

$$y = a^x \bmod p. \tag{4.13}$$

Число x будет секретным ключом пользователя, а число y — открытым ключом.

Пусть имеется сообщение $\bar{m}$, которое необходимо подписать. Генерация подписи выполняется следующим образом:

1. Вычисляем значение хеш-функции $h = h(\bar{m})$ для сообщения m, значение хеш-функции должно лежать в пределах $0 < h < q$ (в российском варианте хеш-функция определяется ГОСТом Р34.11-94).

2. Формируем случайное число k, $0 < k < q$.

3. Вычисляем $r = (a^k \bmod p) \bmod q$. Если оказывается так, что $r = 0$, то возвращаемся к шагу 2.

4. Вычисляем $s = (kh + xr) \bmod q$. Если $s = 0$, то возвращаемся к шагу 2.

5. Получаем подписанное сообщение $\langle \bar{m};\ r,\ s \rangle$.

Для проверки подписи делаем следующее.

1. Вычисляем хеш-функцию для сообщения $h = h(\bar{m})$.

2. Проверяем выполнение неравенств $0 < r < q$, $0 < s < q$.

3. Вычисляем $u_1 = s \cdot h^{-1} \bmod q$, $u_2 = -r \cdot h^{-1} \bmod q$.

4. Вычисляем $v = (a^{u_1} y^{u_2} \bmod p) \bmod q$.

5. Проверяем выполнение равенства $v = r$.

Если хотя бы одна из проверок на шагах 2 и 5 не дает нужного результата, то подпись считается недействительной. Если же все проверки удачны, то подпись считается подлинной.

Утверждение 4.5. *Если подпись к сообщению была сформирована законно, т.е. обладателем секретного ключа* x, *то* $v = r$.

Доказательство. Запишем следующую цепочку равенств, которая следует непосредственно из описания метода (напомним, что показатели степени приводятся по модулю q):

$$\begin{aligned} v &= \left(a^{sh^{-1}} y^{-rh^{-1}} \bmod p\right) \bmod q = \\ &= \left(a^{(kh+xr)h^{-1}} a^{-xrh^{-1}} \bmod p\right) \bmod q = \\ &= \left(a^{k+xrh^{-1}-xrh^{-1}} \bmod p\right) \bmod q = \\ &= (a^k \bmod p) \bmod q = r. \end{aligned}$$

З а м е ч а н и е. Чтобы найти параметр a, удовлетворяющий (4.12), рекомендуется использовать следующий метод. Берем случайное число $g > 1$ и вычисляем

$$a = g^{(p-1)/q} \bmod p. \tag{4.14}$$

Если $a > 1$, то это то, что нам нужно. Действительно, на основании (4.14) и теоремы Ферма имеем

$$a^q \bmod p = g^{((p-1)/q)q} \bmod p = g^{p-1} \bmod p = 1,$$

т.е. выполняется равенство (4.12). Если при вычислении по (4.14) мы получаем $a = 1$ (крайне маловероятный случай), то нужно просто взять другое число g.

П р и м е р 4.3. Выберем общие несекретные параметры

$$q = 11, \quad p = 6q + 1 = 67,$$

возьмем $g = 10$ и вычислим

$$a = 10^6 \bmod 67 = 25.$$

Выберем секретный ключ $x = 6$ и вычислим открытый ключ

$$y = 25^6 \bmod 67 = 62.$$

Сформируем подпись для сообщения $\bar{m} = baaaab$. Пусть для хеш-функции этого сообщения $h(\bar{m}) = 3$. Возьмем случайно число $k = 8$. Вычислим

$$r = \left(25^8 \bmod 67\right) \bmod 11 = 24 \bmod 11 = 2,$$
$$s = (8 \cdot 3 + 6 \cdot 2) \bmod 11 = 36 \bmod 11 = 3.$$

Получаем подписанное сообщение

$$\langle baaaab;\ 2,\ 3\rangle.$$

Теперь выполним проверку подписи. Если сообщение не изменено, то $h = 3$. Вычислим

$$
\begin{aligned}
&h^{-1} = 3^{-1} \bmod 11 = 4,\\
&u_1 = 3 \cdot 4 \bmod 11 = 1,\\
&u_2 = -2 \cdot 4 \bmod 11 = -8 \bmod 11 = 3,\\
&v = \left(25^1 \cdot 62^3 \bmod 67\right) \bmod 11 =\\
&\qquad\qquad\qquad = \left(25 \cdot 9 \bmod 67\right) \bmod 11 = 24 \bmod 11 = 2.
\end{aligned}
$$

Мы видим, что $v = r$, значит подпись верна.

Теперь остановимся на отличиях американского стандарта от российского. Они сводятся к следующему.

1. Длина числа q берется равной 160 бит.
2. В качестве хеш-функции используется алгоритм SHA-1.
3. При генерации подписи на шаге 4 параметр s вычисляется по формуле $s = k^{-1}(h + xr) \bmod q$.
4. При проверке подписи на шаге 3 u_1 и u_2 вычисляются по формулам $u_1 = h \cdot s^{-1} \bmod q$, $u_2 = r \cdot s^{-1} \bmod q$.

С учетом этих отличий нетрудно переписать всю схему подписи в «американском» стиле. Доказательство корректности алгоритма проводится совершенно аналогично.