**ЦИФРОВАЯ ПОДПИСЬ ЭЛЬ ГАМАЛЯ**

# 1 Цифровая подпись Эль Гамаля в группе $F_p*$

Цифровая подпись Эль-Гамаля основана на сложности проблемы дискретного логарифма.

Пусть $p$ — простое число и $\alpha$ — примитивный элемент поля $Z_p$.

$$p = 1277, \alpha = 2$$

Выберем случайное число $a$ в интервале $1 \le a \le p-2$ и вычислим значение
$y = \alpha^a \bmod p$. Например,

$$a = 113, /y = 2^{113} \bmod 1277 = 815$$

Число $a$ является секретным ключом, а набор $(p, \alpha, y)$ – открытым ключом. В нашем примере

$$a = 113,\ (p, \alpha, y) = (1277, 2, 815)$$

Алгоритм вычисления подписи следующий:

1. Выбрать случайное целое число $k,\ 1 \le k \le p-2$, НОД$(k, p-1) = 1$;

$$k = 135;\ (135, 1276) = 1.$$

$$(k = 137;\ (137, 1276) = 1.)$$

Примечание. Здесь и ниже в скобках параллельно рассматривается второй пример при ином выборе $k$.

2. Вычислить $r = \alpha^k \bmod p$;

$$r = 2^{135} \bmod 1277 = 1155$$

$$(r = 2^{137} \bmod 1277 = 789.)$$

3. Вычислить $k^{-1} \bmod (p-1)$.

$$135^{-1} \bmod (1276) = 983$$

$$(137^{-1} \bmod (1276) = 801.)$$

4. Для $x = M$ вычислить $s = (x - ar)k^{-1} \bmod (p-1)$;

$$x = M = 1111,\ s = (1111 - 113 \times 1155)983 \bmod 1276 = 308$$

$$x = M = 1111,\ s = (1111 - 113 \times 789)801 \bmod 1276 = 950$$

5. Объявить пару чисел $(r, s)$ подписью под сообщением $M$.

$$(r, s) = (1155, 308)$$

$$(r, s) = (789, 950)$$

Алгоритм проверки подписи состоит в следующем

1. Получить аутентичный ключ $(p, \alpha, y)$.

$$(1277, 2, 815)$$

2. Поверить, что $1 \leq r \leq p-1$.

$$1155 < 1276$$

$$(789 < 1276)$$

3. Проверить сравнение

$$y^r r^s \equiv \alpha^x (\bmod p).$$

$$y^r r^s \bmod p = 815^{1155} 1155^{308} \bmod 1277 = 387 \times 377 = 321.$$

$$(y^r r^s \bmod p = 815^{789} 789^{950} \bmod 1277 = 7 \times 958 = 321.)$$

$$\alpha^x (\bmod p) = 2^{1111} \bmod 1277 = 321.$$

4. Принять подпись при положительном результате обеих проверок.

В данном случае также возможно получение цифровой подписи для большого числа сообщений с использованием одного секретного ключа.

Доказательство правильности алгоритма проверки подписи. Если подпись вычислена абонентом, владеющим секретным ключом $a$, то

$$s \equiv k^{-1}\{x - ar\} \mathrm{mod}\ (p-1).$$

Умножив обе части сравнения на $k$, получим

$$ks \equiv x - ar (\mathrm{mod}\ (p-1)),$$

что эквивалентно сравнению

$$x \equiv ar + ks\ (\mathrm{mod}\ (p-1)).$$

Отсюда следует

$$\alpha^x \equiv \alpha^{ar+ks} \equiv (\alpha^a)^r (\alpha^k)^s \equiv y^r r^s (\mathrm{mod}\ p).$$

Число $k$ должно уничтожаться сразу после вычисления подписи, так как по этому числу и значению подписи вычисляется секретный ключ:

$$a = (x - ks) r^{-1} \mathrm{mod}\ ((p-1)).$$

(Допустим, что существует $r^{-1} \mathrm{mod}\ ((p-1))$.)

$$a = (1111 - 135 \times 308) 1155^{-1} \mathrm{mod}\ 1276 = ?.$$

в данном случае $r^{-1}$ не существует.

$$(a = (1111 - 137 \times 950) 789^{-1} \mathrm{mod}\ 1276 \times 469 = 113).$$

Это же возможно в случае повторного использования числа $k$, так как в этом случае оно с большой вероятностью вычисляется: пусть с использованием одного и того же числа $k$ получены две подписи $(r, s_1)$ и $(r_2, s_2)$, под сообщениями $x_1$ и $x_2$. При этом

$$s_1 = k^{-1}\{x_1 - ar\} \mathrm{mod} (p-1),$$

$$s_2 = k^{-1}\{x_2 - ar\}\mathrm{mod}\ (p-1).$$

Тогда

$$(s_1 - s_2)k \equiv (x_1 - x_2)(\mathrm{mod}\ (p-1)).$$

При $s_1 \neq s_2$ получаем $k = (s_1 - s_2)^{-1}(x_1 - x_2) \bmod (p-1)$.

Упражнение. Возьмите другое сообщение $M$ и вычислите (при том же $k$) цифровую подпись $r, s$ и затем вычислете открытый ключ, как описано выше.

На шаге 3 алгоритма подписи целесообразно использовать не само сообщение, а значение хэш-функции от него. Иначе возможен подбор сообщения с известным значением подписи. Так можно выбрать случайные числа $i, j,\ 1 < i < p-1,\ 1 < j < p-1,\ (j, p-1) = 1$, например,

$$i = 5,\ j = 127$$

и положить

$$r = \alpha^i y^j \bmod p = \alpha^{i+aj} \bmod p;$$

$$r = 2^{5+113\times 127} \bmod 1277 = 226$$

$$s = -rj^{-1}\mathrm{mod}\ (p-1),$$

$$s = -226 \times 127^{-1}\mathrm{mod}\ (1276) = -226 \times 211\mathrm{mod}\ (1276) = -474\mathrm{mod}\ (1276) = 802,$$

Тогда пара $(r, s)$

$$(226, 802)$$

является подписью под сообщением

$$x = si \bmod (p-1) = -rij^{-1}\mathrm{mod}\ (p-1),$$

$$x = 802 \times 5 \bmod 1276 = 182 = -rij^{-1}\mathrm{mod}\ (p-1),$$

так как

$$(\alpha^x \alpha^{-ar})^{s^{-1}} = \alpha^i y^j = r.$$

Действительно,

$$(\alpha^x \alpha^{-ar})^{s^{-1}} \bmod p = (\alpha^{-rij^{-1}} \alpha^{-ar})^{(-rj^{-1})^{-1}} \bmod p =$$

$$= \alpha^{-rij^{-1}(-r)^{-1}j} \alpha^{-ar(-r)^{-1}j} \bmod p = \alpha^i \alpha^{aj} \bmod p = \alpha^{i+aj} \bmod p = r.$$

Теперь можно получить

$$\alpha^x \alpha^{-ar} \equiv r^s\ (\mathrm{mod}\ )p,$$

откуда следует подтверждение подписи (напоминаем, что $\alpha^a = y$):

$$y^r r^s \equiv \alpha^x\ (\mathrm{mod}\ p):$$

Например, вычисленная выше подпись ((226,474) проверяется на ключе (1277,2,815):

$$815^{226} \bmod 1277 \times 226^{802} \bmod 1277 = 359 \times 730 \bmod 1277 = 285.$$

$$2^{182} \bmod 1277 = 285.$$

На шаге 2 алгоритма проверки подписи предусматривается проверка, что $0 < r < p$. Если эту проверку не делать, то злоумышленник может подписать выбираемое им сообщение $x'$, если располагает подписанным на секретном ключе $a$ сообщением $x$. Пусть $(r, s)$ – подпись под сообщением $x$, например,

$$(r, s) = (789, 848),\ x = 1173.$$

Допустим, что существует $x^{-1} \bmod(p-1)$, например,

$$(1173)^{-1}\mathrm{mod}(1276) = 1053$$

Пусть $x' = 100$.

Тогда можно вычислить

$$u = x' \cdot x^{-1} \bmod (p-1).$$

Затем можно вычислить

$$s' = su \bmod (p-1),$$

и $r'$, такое, что

$$r' \equiv ru \bmod (p-1) \quad r' \equiv r \pmod p.$$

По китайской теореме об остатках это всегда возможно.

В нашем примере

$$u = 100 \cdot 1053\mathrm{mod}(1276) = 668$$

$$s' = 848 \cdot 668\mathrm{mod}(1276) = 1196$$

$$r' \equiv a_1 \ (\mathrm{mod}\ (p-1)), a_1 = ru \bmod (p-1) = 64;$$

$$r' \equiv a_2 \ (\mathrm{mod} p),\ a_2 = r = 789.$$

Китайская теорема об остатках. *Если модули $m_i$ взаимно просты, то система сравнений*

$$x \equiv a_i \ (\mathrm{mod}\ m_i), \quad i = 1,\ \ldots,\ t,$$

*имеет в интервале $[0, m-1]$, $m = m_1 \cdot m_2 \cdot \ldots \cdot m_t$ единственное решение $x$ вида*

$$x = \Sigma_{i=1}^{t} a_i \cdot N_i \cdot\ M_i \bmod m,$$

*где $M_i = \frac{m}{m_i}, N_i = (M_i)^{-1}(\mathrm{mod}\ m_i), i = 1, \ldots, t.$*

В данном примере

$$a_1 = 64;$$

$$a_2 = 789$$

$$m = m_1 m_2 = (p-1)p = 1276 \cdot 1277 = 1629452.$$

$$M_1 = m_2 = p = 1277,$$

$$M_2 = m_1 = (p-1) = 1276.$$

$$N_1 = M_1^{-1} \bmod m_1 = p^{-1}\ \underline{m}od\ (p-1) = 1,$$

$$N_2 = M_2^{-1} \ \bmod p = p - 1 = 1276.$$

$$r' = a_1 M_1 N_1 + a_2 M_2 N_2 \mod m =$$

$$64 \cdot 1277 \cdot 1 + 789 \cdot 1276 \cdot 1276 \mod 1629452 =$$

$$81728 + 622688 = 704416.$$

таким образом,

$$(r', s') = (704416, 1196)$$

есть подпись под сообщением $x' = 100$ на ключе $a = 113$ с ключом проверки $(p, \alpha, y) = 1277, 2, 815$. Она получена без знания ключа $a$.

Проверка подписи:

$$y^r \cdot r^s \mod p = 815^{704416} \cdot 704416^{1196} \mod 1277 =$$

$$1154 \cdot 433 \mod 1255 = 375;$$

$$\alpha^{100} \mathrm{mod}\ 1277 = 375.$$

Другие схемы цифровой подписи, аналогичные рассмотренной, отличаются проверяемым сравнением вида

$$\alpha^A y^B \equiv r^C (\mathrm{mod}\ p),$$

где тройка $(A, B, C)$ совпадает с одной из перестановок чисел $\pm x, \pm s, \pm r$ при некотором выборе знака. Например, описанная схема цифровой подписи Эль-Гамаля получается при $A = x,\ B = -r,\ C = s$.

В американском стандарте DSS используются значения $A = x,\ B = r,\ C = s$.

В российском стандарте $A = -x,\ B = s,\ C = r$.

В схемах данного семейства возможно сокращение длины подписи путём замены пары чисел $(r, s)$ парой $(r \mod qs \mod q)$, где $q$ является некоторым делителем числа $p - 1$. При этом проверяемое сравнение заменяется модифицированным равенством

$$(\alpha^A y^B \mathrm{mod}\ p) \mathrm{mod}\ q = r^C \mathrm{mod}\ q.$$

Это применено в американском стандарте DSS.

# 2 Стандарт DSS, алгоритм DSA

В 1991 году правительственный национальный институт стандартов и технологии США утвердил стандарт цифровой подписи $DSS$ (Digital Signature Stundard), основанный на специальном алгоритме цифровой подписи $DSA$ (Digital Signature Algorithm) для использования в правительственных и коммерческих организациях. Алгоритм основан на трудности проблемы дискретного логарифма мультипликативной группы поля $\mathcal{F}_p$.

Для инициализации, то есть для подготовки к последующему использованию схемы цифровой подписи пользователь $A$ должен проделать следующее:

1) выбрать простое число $q$ из примерно 160 бит, для этого используется генератор случайных чисел и тесты простоты;

2) выбрать второе случайное число $p$, такое, что $q$ является делителем числа $p - 1$, и которое состоит из примерно 500 бит (более точно, рекомендуется выбирать число, кратное 64 между 512 и 1024);

3) выбрать образующий элемент $\alpha$ единственной циклической подгруппы группы $\mathcal{F}_p^*$ порядка $q$ (это делается вычислением $\alpha = g^{(p-1)/q} (\mathrm{mod}\ p)$ для случайно выбираемого целого $g$; если в результате получается число, отличное от единицы, то $\alpha$ является образующим элементом);

4) выбрать случайное целое число $a$ в интервале $0 < a < q$ в качестве секретного ключа и образовать открытый ключ $y = \alpha^a (\text{mod } p)$.

Для подписи сообщения пользователь $A$ применяет к открытому тексту $m$ хеш-функцию, получая целое $h(m)$ в интервале $0 < h(m) < q$. Затем он выбирает случайное целое $k$ в том же интервале, вычисляет $r = \alpha^k (\text{mod } p)$ $(\text{mod } q)$ (то есть $\alpha^k$ вычисляется по модулю $p$ и затем результат приводится по модулю меньшего простого числа $q$). В заключение $A$ находит целое $s$ такое, что $s = k^{-1}\{h(m) + ar\}$ (mod q). Подпись для сообщения $m$ образуется парой чисел $(r, s)$ по модулю $q$.

Чтобы проверить подпись пользователь $B$, получив аутентифицированный открытый ключ $(p, q, \alpha, y)$, отправителя сообщения $A$

а) проверяет, выполняются ли $0 < r < q$ и $0 < s < q$, если нет, то отклоняет подпись,

б) вычисляет $w = s^{-1} \text{mod } q$ и $h(m)$,

в) вычисляет $u_1 = s^{-1} h (\text{mod q})$ и $u_2 = rw (\text{mod } q)$,

г) вычисляет $v = \alpha^{u_1} y^{u_2} (\text{mod } p)$ $(\text{mod } q)$,

д) принимает подпись, если $v = r$, иначе подпись отклоняется.

# 3 Российский стандарт

Российский стандарт цифровой подписи ГОСТ Р 34.10-94 использует следующие параметры: $p$ – простое число в диапазоне 500-512 или 1020-1024 бит, $q$ – простое число, делитель числа $p-1$, длиной от 254 до 256 бит, $a$ – произвольное число, меньшее $p-1$, для которого $a^q \text{ mod } p = 1$. $x$ – число, меньшее $q$, $y = a^x \text{ mod } p$. Используется однонаправленная хэш-функция $h(x)$, определяемая ГОСТ Р 34.11-94 и основанная на алгоритме симметричного шифрования ГОСТ 28147-89.

Параметры $p, q$ и $a$ – открытые и используются всеми абонентами сети. Секретным ключом абонента $A$, подписывающего сообщение является число $x$, его открытым ключом является число $y$.

Чтобы подписать сообщение $m$ абонент $A$ генерирует случайное число $k$, $k < q$.

Затем он вычисляет

$$r = (a^k \text{ mod } p) \text{ mod } q,$$

$$s = (xr + k(h(m))) \text{ mod } q.$$

При этом, если $h(m) \text{ mod } q = 0$, то значение хэш-функции принимается равным 1. Если $r = 0$, то вычисления повторяются при другом $k$.

Подписью является пара чисел $r \text{ mod } 2^{256}$ и $s \text{ mod } 2^{256}$. Подпись посылается (вместе с сообщением) стороне $B$.

Сторона $B$ проверяет подпись, вычисляя

$$v = h(m)^{(q-2)} \text{ mod q},$$

$$z_1 = (sv) \text{ mod } q,$$

$$z_2 = ((q - r) \cdot v) \text{ mod } q,$$

$$u = (a^{z_1} \cdot y^{z_2}) \text{ mod } p) \text{ mod } q.$$

Подпись принимается при $u = r$.

# Список литературы


[1] Саломаа А. Криптография с открытым ключом. М: Мир, 1996.

[2] A.Menezes, P.van Oorschot, S.Vanstone/ Handbooh of Applied Cryptography. CRC Press, Inc. 1997.

[3] Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А..В. Основы криптограии. М.: Гелиос АРВ, 2000.

[4] Чмора А.Л.Современная прикладная криптография. М.: Гелиос–АРВ, 2001 г.

# 4 Обобщенная схема электронной подписи Эль Гамаля

Обобщенная схема электронной подписи Эль Гамаля работает в любой абелевой группе.

Для работы по этой схеме каждый участник

1. Выбирает подходящую циклическую группу $G$, порядка $n$ её образующий элемент $\alpha$ (ниже используется мультипликативное представление группы).

2. Выбирает случайное целое число $a$, $1 \leq a \leq n-1$ и вычисляет элемент $y = \alpha^a$.

3. Открытым ключом абонента А является пара $(\alpha, y)$ и описание операции умножения группы, её секретный ключ есть $a$.

Алгоритм формирования подписи следующий:

а) Выбрать случайное секретное целое $k$, $1 \leq k \leq n-1$, взаимно простое с $n:\ (k,n) = 1$.

б) Вычислить элемент $r = \alpha^k$ группы.

в) Вычислить $k^{-1} (\text{mod } n)$.

г) Вычислить $h(m)$ и $h(r)$, где $h$ – используемая хеш-функция.

д) Вычислить $s = k^{-1}\{h(m) - ah(r)\} (\text{mod } n)$.

е) Цифровой подписью является пара $(r, s)$.

Алгоритм верификации подписи следующий:

а) Получить авторизированную версию открытого ключа $(\alpha, y)$.

б) Вычислить $h(m)$ и $h(r)$.

в) Вычислить $v_1 = y^{h(r)} \cdot r^s$.

г) Вычислить $v_2 = \alpha^{h(m)}$.

д) Принять подпись, если $v_1 = v_2$, и отклонить её в противном случае.

Заметим, что генерация подписи требует вычислений как в группе $G$, так и в группе $Z_n$, в то же время проверка подписи связана с вычислениями только в группе $G$.

# 5 Контрольные вопросы

1. Какой трудной проблеме соответствует безопасность цифровой подписи Эль Гамаля?

2. Каковы последствия повторного использования рандомизатора?

3. Почему следует подписывать хеш-значение от сообщения, а не само сообщение?

4. Почему цифровая подпись Эль Гамаля может быть реализована не только в числовых, но и в полиномиальных алгебраических структурах?

5. В чем отличие американского и российского стандартов цифровой подписи Эль Гамаля?

# Список литературы


[1] Саломаа А. Криптография с открытым ключом. М: Мир, 1996.

[2] A.Menezes, P.van Oorschot, S.Vanstone/ Handbooh of Applied Cryptography. CRC Press, Inc. 1997.

[3] Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А..В. Основы криптограии. М.: Гелиос АРВ, 2000.

[4] Чмора А.Л.Современная прикладная криптография. М.: Гелиос–АРВ, 2001 г.