Электрондық (цифрлық) қолтаңба стандарттары

Көптеген елдерде бүгінде электронды стандарттар бар

(сандық) қолы Бұл бөлімде МЕМСТ R34.10-94 ресейлік мемлекеттік стандартын және АҚШ FIP стандартын сипаттаймыз.Ресей стандарты, оның белгісінен кейін қабылданған

1994, американдық - 1991 жылы. Екі стандарт та негізге алынған

шын мәнінде DSA (Digital Signature Algorithm) деп аталатын және El-Gamal қолтаңбасының вариациясы болып табылады. Алгоритмнің орысша нұсқасын мұқият қарап, содан кейін көрсетеміз американ нұсқасының айырмашылықтары туралы.

Бастапқыда пайдаланушылардың белгілі бір қоғамдастығы үшін жалпы жіктелмеген параметрлер таңдалады. Ең алдымен табу керек q ұзындығы 256 бит және p ұзындығы 1024 бит, арасы осы арақатынас орындалатын

$$p = bq + 1$$

кейбір бүтін бүтін сан үшін, p және q-дағы жоғары ретті биттер тең болуы керек өлшем бірлігіне. Содан кейін сан таңдалады a > 1 осылай

$$a^q mod\ p = 1 \qquad (4.12)$$

Нәтижесінде біз үш ортақ параметрді аламыз – p, q және a.

Ескерту. Теңдік (4.12) А-ны тұрғызған кезде p модулі бойынша дәрежелер көрсеткіштер модуль q бойынша беріледі, сонда $a^b\ modp = \ a^{b\ modp}$ (біз мұндай құбылыстың негіздемесін жасадық 30-беттегі 2.10 мәлімдемесін дәлелдеу кезінде). Мұндай төмендету қолтаңбаны құру және тексеру кезінде үнемі орындалады, нәтижесінде қарастырылып отырған алгоритм шеңберіндегі дәрежелік көрсеткіштердің ұзындығы ешқашан 256 биттен аспайды, бұл есептеуді жеңілдетеді.

Әрі қарай, әрбір пайдаланушы 0 < x < q теңсіздігін қанағаттандыратын x санын кездейсоқ таңдайды және есептейді.

$$y = a^x\ modp$$

X саны пайдаланушының құпия кілті, ал y саны жеке кілт болады. Барлық пайдаланушылардың ашық кілттері кейбір құпия емес, бірақ "сертификатталған ванна" анықтамалығында көрсетілген деп болжануда, ол кез келген адамда болуы керек қолтаңбаларды тексеріңіз. Айта кетейік, қазіргі уақытта p модульдің жоғарыда көрсетілген ұзындығында, x пен y - тан табу мүмкін емес.

Осы кезде параметрлерді таңдау кезеңі аяқталады және Біз қолтаңбаларды қалыптастыруға және тексеруге дайынбыз.

Қол қою керек $\bar{m}$ хабарламасы болсын. Қолтаңбаны құру келесідей

1. m Хабарламасы үшін h = h($\bar{m}$) хэш функциясының мәнін есептейміз, хэш функциясының мәні 0 < h < q шегінде болуы керек (ресейлік нұсқада хэш функциясы ГОСТ арқылы анықталады Р34.11-94).
2. Кездейсоқ k , 0 < k < q санын қалыптастыру.
3. Есептейміз $r = (a^k \ mod p) mod q$. Егер r = 0 болса, онда біз 2-қадамға ораламыз.
4. Есептейміз $s = (kh + xr) mod q$. Егер s = 0 болса, онда біз 2-қадамға ораламыз.
5. Біз қол қойылған хабарламаны аламыз $\langle \bar{m}; r, s \rangle$.
   Қолтаңбаны тексеру үшін келесі әрекеттерді орындаңыз.
   1. Хабарлама үшін хэш функциясын есептеңіз $h = h(\bar{m})$.
   2. 0 < r < q , 0 < S < q теңсіздіктерінің орындалуын тексереміз .
   3. Есептейміз $u_1 = s * h^{-1}, mod q, u_2 = -r * h^{-1} \ mod q$.
   4. Есептейміз $v = (a^{u_1} \ y^{u_2} \ mod p) mod q$.
   5. v = r теңдігінің орындалуын тексеріңіз.

Егер 2 және 5-қадамдардағы тексерулердің кем дегенде біреуі қажет нәтиже бермесе, онда қолтаңба жарамсыз болып саналады. Егер бәрі болса тексерулер сәтті, содан кейін қолтаңба шынайы болып саналады.

Бекіту 4.5. Егер хабарламаға қолтаңба заңды түрде жасалса, яғни x құпия кілтінің иесі болса, онда v = r

Дәлел . Әдістің сипаттамасынан тікелей келетін теңдіктердің келесі тізбегін жазайық (көрсеткіштер q модулі бойынша берілгенін еске түсірейік):

$$v = \left(a^{sh^{-1}} \ y^{-rh^{-1}} \ mod p\right) mod q =$$

$$=(a^{(kh+xr)h^{-1}} \ a^{-xrh^{-1}} \ mod p) \text{ mod q}=$$

$$=(a^{k+xrh^{-1}-xrh^{-1}} mod p) \text{ mod q}=$$

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

Ескерту. (4.12) қанағаттандыратын a параметрін табу үшін келесі әдісті қолданған жөн. Біз кездейсоқ $g > 1$ санын алып, есептейміз.

$$a = \ g^{(p-1)/q} \ mod \ p \qquad (4.14)$$

Егер $a > 1$ болса, бұл бізге қажет нәрсе. Шынында да, (4.14) және Ферма теоремасы негізінде бізде бар.

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

яғни, теңдік орындалады (4.12). Егер (4.14) бойынша есептеу кезінде біз a = 1 (өте екіталай жағдай) сәулесін алсақ, онда сіз жай ғана алуыңыз керек басқа g саны.

Мысал 4.3. Жалпы құпия емес параметрлерді таңдаңыз

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

g = 10 алыңыз және есептеңіз

$$a = 10^6 \; mod \; 67 = 25.$$

X = 6 құпия кілтін таңдап, ашық кілтті есептеңіз

$$y = 25^6 \; mod \; 67 = 62.$$

$\overline{m}$ = baaaab Хабарламасы үшін қолтаңба жасаңыз. Осы хабарламаның хэш функциясы үшін h(m) = 3 болсын. Кездейсоқ K = 8 санын алайық.

Есептейміз

$$r = (25^8 \; mod \; 67) mod \; 11 = 24 \; mod \; 11 = 2,$$

$$s = (8 * 3 + 6 * 2) mod \; 11 = 36 \; mod \; 11 = 3.$$

Біз қол қойылған хабарламаны аламыз

$$\langle baaab; 2, 3 \rangle$$

Енді қолтаңбаны тексерейік. Егер хабарлама сатқындық болмаса, онда h = 3.

Есептейміз

$$h^{-1} = 3^{-1} \; mod \; 11 = 4,$$

$$u_1 = 3 * 4 \; mod \; 11 = 1,$$

$$u_2 = -2 * 4 \; mod 11 = -8 \; mod \; 11 = 3,$$

$$v = (25^1 * \; 62^3 \; mod \; 67 \;) \; mod \; 11 =$$

$$= (25 * 9 \; mod \; 67) mod 11 = 24 mod 11 = 2.$$

Біз v = r қолтаңбаның дұрыс екенін көреміз.

Енді американдық стандарттың ресейлік стандарттан айырмашылығына тоқталайық. Олар келесіге келеді.

1. q санының ұзындығы 160 битке тең.

2. Хэш функциясы ретінде SHA-1 алгоритмі қолданылады.

3. 4- қадамдағы қол таңба жасау кезінде s параметрі

$$s = k^{-1}(h + xr) mod q,$$

формуласымен есептеледі.

4. 3 - қадамдағы жазылымды тексеру кезінде u_1 және u_2,

$$u_1 = h * s^{-1} * mod\ q,$$

$$u_2 = r * s^{-1}\ mod\ q$$

формуласымен есептеледі.

Осы айырмашылықтарды ескере отырып, бүкіл қолтаңба схемасын"американдық" стильде қайта жазу қиын емес. Алгоритмнің дұрыстығын дәлелдеу дәл осындай.