Қолтаңбаны генерациялау:

$$s = (H(m))^d \bmod n .$$

Қабылдаушыға m және s беріледі.

Қолтаңбаны верификациялау:

Хабарлама мен қолтаңба дұрыс деп есептелінеді, егер келесі шарт орындалса:

$$H(m) = s^e \bmod n .$$

Ал егер бұл теңдік орындалмаса, онда хабарлама және қолтаңба дұрыс емес.

4.6.2. Цифрлы қолтаңбаның стандарттары және технологиялар Ұлтық институтының (СТҰИ) DSA алгоритмі

Бұл алгоритм Эль-Гамаль цифрлы қолтаңба әдісінде негізделген және 1991 жылы цифрлы қолтаңба стандарты ретінде СТҰИ арқылы ұсынылды.

Параметрлер:

модуль ретінде қолданылатын жай сан $p(2^{511} < p < 2^{512})$;

q - $(p-1)$ санының жай бөлгіші, $2^{159} < q < 2^{160}$;

$g = h^{(p-1)/q} \bmod p$, мұндағы h - кез келген бүтін сан, $0 < h < p$ және $g > 1$;

m хабарламасы.

H - біржақты хэш-функция;

$k \in Z_q$ кездейсоқ саны;

$x \in Z_q$ құпиялы кілт;

$y = g^x \bmod p$ ашық кілт.

Қолтаңбаны генерациялау:

$$r = (g^k \bmod p) \bmod q,$$
$$s = (k^{-1} H(m) + xr)) \bmod q.$$

Қабылдаушыға m хабарламасы және r, s қолтаңбасы беріледі.

Қолтаңбаны верификациялау:

Бірінші сатыда алынған қолтаңбаның $0 < r < q$ және $0 < s < q$ шарттарына сәйкестігі тексеріледі. Бұдан мыналар есептелінеді:

$$\omega = (s)^{-1} \bmod q,$$
$$u_1 = ((H(m))\omega) \bmod q,$$
$$u_2 = (r\omega) \bmod q,$$
$$v = ((g^{u_1} y^{u_2}) \bmod p) \bmod q.$$

Егер $v = r$, онда хабарлама мен қолтаңба дұрыс деп есептелінеді. Ал егер бұл теңдік орындалмаса, онда хабарлама және қолтаңба дұрыс емес.

4.6.3. Окамото цифрлы қолтаңбасы (ESIGN)

Параметрлер:

құпиялы кілт: p, q $(p > q)$ үлкен жай сандар;

ашық кілт: $n = p^2 q$ оң бүтін сан;

m хабарламасы;

H-біржақты хэш-функциясы, $H(m) \le n - 1$ кез келген m оң саны үшін;

k-бүтін сан, $k \ge 4$.

Бұл қарастырылып отырған жүйеде H функциясы мен k параметрі бекітілген болып келеді.

Қолтаңбаны генерациялау:

x $(0 \le x \le pq - 1)$ кездейсоқ саны таңдалады;

қолтаңба келесідей есептелінеді:

$$\omega = \left[(H(m) - x^k \bmod n) / (pq)\right],$$
$$y = \omega / (kx^{k-1}) \bmod p,$$
$$s = x + ypq.$$

Қабылдаушыға m және s беріледі.

Қолтаңбаны верификациялау:

Қолтаңба қойылған хабарлама (m, s) дұрыс деп есептелінеді, егер келесі шарт орындалса:

$$H(m) \le s^k \bmod n < H(m) + 2^{[2|n|/3]}.$$

Ал егер бұл теңдік орындалмаса, онда хабарлама және қолтаңба дұрыс емес.

4.6.4. Шнорр цифрлы қолтаңбасы

Параметрлер:

p және q жай сандары, $q \ge 2^{140}$, $p \ge 2^{512}$;

$a \in Z_p$, $a^q = 1 (\bmod p)$, $a \ne 1$;

H - біржақты хэш-функция;

$H : Z_p \times Z \to \{0,\ldots,2^t - 1\}$, $t = 72$;

$k \in Z_q$ кездейсоқ саны;

$x \in Z_q$ құпиялы кілт;

$y = (a^x)^{-1} \bmod p$ ашық кілт.

Қолтаңбаны генерациялау:

$$g = a^k \bmod p,$$
$$r = H(g, m),$$
$$s = (k + xr) \bmod p.$$

Қолтаңбаны верификациялау:

Хабарламаны алушы $r' = a^s y^r \bmod p$ есептейді де, келесі шарттың орындалуын тексереді:

$$r = H(r', m).$$

Егер бұл теңдік орындалмаса, онда хабарлама және қолтаңба дұрыс емес.

4.6.5. Микали-Шамир цифрлы қолтаңбасы

Параметрлер:

p және q екі үлкен жай сандары;

$n = pq$ оң бүтін саны;

m хабарламасы;

псевдокездейсоқ функция $f : Z_n \times Z \to \{0,1,\ldots,2^k - 1\}$, $k = 72$;

y_i $(i = 1,\ldots,k)$ ашық кілт; бұл жиын Z_n-нен квадраттық қалдық болатын, бірінші k жай сандардан құралады, яғни $y_i = 2, y_2 = 3, y_3 = 5,\ldots$;

$x_i \in Z_n$ құпиялы кілт, мұндағы $x_i = \frac{1}{\sqrt{y_i}} \bmod n.$

Қолтаңбаны генерациялау:

$r \in Z_n$ кездейсоқ саны алынады;

$e = e_1 \ldots e_k = f(r^2 \bmod n, m)$ және $s = r\prod_{j=1}^{k} x_j^e$ есептелінеді;

алушыға m хабарламасы, s және e қолтаңбасы беріледі.

Қолтаңбаны верификациялау:

Хабарламаны алушы $e = f(s^2 \prod_{j=1}^{k} y_j^e, m)$ шарттың орындалуын тексереді.

Цифрлы қолтаңбаның алгоритмдерін салыстыру үшін келесі параметрлердің мәндері қолданылады:

Модульдердің ұзындығы:

DSA сызбасы үшін p және q модульдерінің ұзындығы сәйкесінше 512 және 160 бит;

RSA сызбасы үшін n модулінің ұзындығы 512 бит;

Шнорр сызбасы үшін p және q модульдерінің ұзындығы сәйкесінше 512 және 160 бит;

Микали-Шамир сызбасы үшін n модулінің ұзындығы 512 бит;

ESIGN сызбасы үшін n модулінің ұзындығы 576 бит;

Құпиялы параметрлер:

Микали-Шамир сызбасы үшін $k = 128, t = 1;$

Шнорр сызбасы үшін $t = 128;$

RSA сызбасы үшін $e = 8;$

ESIGN сызбасы үшін $k = 8.$

Цифрлы қолтаңбаның әртүрлі сызбалары үшін есептеу жұмыстарының көлемінің бағалары 14-кестеде көрсетілген. Барлық бағалаулар белгілі есептеу әдістері үшін ешқандай оптимизациясыз жүргізілді. 14-кестеде (1), (2) цифрларымен ескертулер көрсетілген.

14-кесте.

Есептеу жұмыстарының көлемінің бағалары

Сызба	Кілттерді генерациялау	Қолтаңбаны верификациялау
ESIGN	3M(576)+I(192)<5M(512)[1, 2]	3M(576)<4M(512)[1]
DSA	240M(512)+I(160)<241M(512)[2]	280M(512)+I(160)<281M(512)
RSA	750M(512)	2M(512)
Шнорр	240M(512)[2]	272M(512)
Микали-Шамир	65M(512)	2M(512)

1-ескерту:

$M(b_1) = M(b_2)(b_1/b_2)^2$, $I(b_1) = I(b_2)(b_1/b_2)^2$ және $c = I(512)/M(512)$ болсын делік. Онда ESIGN сызбасы үшін қолтаңбаны генерациялауға $3M(576) + I(192) < (9/8)^2 3M(512) + (3/8)^2 cM(512) = (3{,}8 + 0{,}14c)M(512)$ амал керек.

Берілген деректермен анықталатындай $c < 10$ болғандықтан, ESIGN сызбасы үшін $5M(512)$-ден көп амал керек емес.

2-ескерту:

ESIGN, DSA және Шнорр сызбаларында кілт генерациялау уақытын азайту үшін алдын ала есептеу әдістерін қолдануға болады. Мұндай әдістер Микали-Шамир және RSA сызбалары үшін тиімді емес. Мұндай әдістерді қолдану арқылы, қолтаңба генерациялауға керек есептеулер көлемінің бағалары 15-кестеде келтірілген.

15-кесте.

Қолтаңбаны генерациялау бағалары

Сызба	Алдын ала есептеулер	Қолтаңбаны генерациялау
ESIGN	5M(512)	0 айналасында
DSA	241M(512)	0 айналасында
RSA		750M(512)
Шнорр	240M(512)	0 айналасында
Микали-Шамир		65M(512)

Қарастырылған сызбалар үшін кілттер мен қолтаңба өлшемдері 16-кестеде көрсетілген. Қолтаңбаны генерациялау және верификациялау жылдамдығын өлшеу үшін 8-биттік процессор, 256-байттік жылдам жады блогы, көлемі 10 Кбайт тұрақты сақтау

құрылғысы және көлемі 8 Кбайт болатын бағдарламаланатын тұрақты сақтау құрылғысы қолданылды.

16-кесте.

Кілттер мен қолтаңба өлшемдері

Сызба	Ашық кілт өлшемі (бит)	Құпиялы кілт өлшемі (бит)	Қолтаңба өлшемі (бит)
ESIGN	578	384	576
DSA	1696	160	320
RSA	514	512	512
Шнорр	1696	160	288
Микали-Шамир	2500	65536	640

Өлшеу нәтижелері 17 және 18-кестеде келтірілген. Мұнда M(512) есептеу уақыты 0,07с сәйкес келеді.

17-кесте.

Кілттерді генерациялау және қолтаңбаны верификациялау

Сызба	Кілттерді генерациялау (с)	Қолтаңбаны верификациялау (с)
ESIGN	0,4	0,3
DSA	52	0,1
RSA	17	20
Шнорр	17	19
Микали-Шамир	5	0,1

18-кесте.

Алдын ала есептеулер уақыты

Сызба	Алдын ала ала есептеулер (с)	Қолтаңбаны генерациялау (с)	Қолтаңбаны верификациялау (с)
ESIGN	0,4	0 айналасында	0,3
DSA	17	0 айналасында	20
RSA		52	0,1
Шнорр	17	0 айналасында	19
Микали-Шамир		5	0,1

4.6.6. ГОСТ Р34.10-94 және Р34.11-94 цифрлы қолтаңбасы

1993 жылы Ресейде «Асимметриялық криптографиялық алгоритм негізінде электрондық цифрлы қолтаңбаны шығару және тексеру процедуралары» және «Хэш функциясы» екі мемлекеттік стандарт «Ақпараттық технология. Ақпаратты криптографиялық қорғау» жалпы атаумен шығарылды.

Параметрлер:

p - жай сан, $2^{509} < p < 2^{512}$ немесе $2^{1020} < p < 2^{1024}$;

q - жай сан, $2^{254} < q < 2^{256}$ және q, $(p-1)$ үшін бөлгіш болып келеді;

m хабарламасы;

a - бүтін сан, $1 < a < p-1$, сонымен бірге $a^q \pmod p = 1$;

x - құпиялы кілт, $0 < x < q$;

H - біржақты хэш-функция;

y - ашық кілт, $y = a^x \pmod p$.

Қолтаңбаны генерациялау:

1. $H(m)$ есептелінеді, егер $H(m) = 0$, онда $H(m) = 0^{255} l$ (255 нөл және кіші разрядтың бірлігі).

2. $0 < k < q$, k сеанс кездейсоқ саны алынады.

3. Екі мән есептелінеді:

$$r = a^k \pmod p,$$

$$r^* = r \pmod q.$$

Егер $r^* = 0$ болса, онда 2-қадамға көшеміз де k санының басқа мәнін таңдаймыз.

4. x құпиялы кілтті және k сеанс кілтін қолдану арқылы цифрлік қолтаңбаның s -компоненті есептелінеді:

$$s = (xr^* + kH(m)) \pmod q.$$

Егер $s = 0$ болса, онда 2-қадамға көшеміз, кері жағдайда алгоритм жұмысын аяқтаймыз.

Қабылдаушыға $(m, (r^*, s))$ беріледі.

Қолтаңбаны верификациялау:

1. Келесі шарттар тексеріледі:

$0 < s < q$ және $0 < r^* < q$.

Егер осы шарттардың біреуі ғана орындалмаса, онда қолтаңба дұрыс емес деп есептелінеді.

2. Алынған m^* хабарламасынан $H(m^*)$ хэш-функциясы есептелінеді.

Егер $H(m^*)(\mathrm{mod}\, p) = 0$ болса, онда $H(m^*)$-ға $0^{255}l$ мәнін меншіктейміз.

3. Келесі параметрлер есептеледі:

$$V = (H(m^*))^{q-2}(\mathrm{mod}\, q),$$
$$Z_1 = sV(\mathrm{mod}\, q),$$
$$Z_2 = (q - r^*)V(\mathrm{mod}\, q).$$

4. $U = (a^{Z_1} y^{Z_2}(\mathrm{mod}\, p))(\mathrm{mod} q)$ мәні есептелінеді.

5. $r^* = U$ шарты тексеріледі.

Егер бұл шарт орындалса, онда хабарлама мен қолтаңба дұрыс деп саналады.

19-кестеде RSA және ГОСТ Р34.10-94 алгоритмдері үшін N, P модульдері 512 бит болғандағы, i486 DX2-66-да, цифрлы қолтаңбаны генерациялау және верификациялау орташа уақыттары келтірілген.

19-кесте.

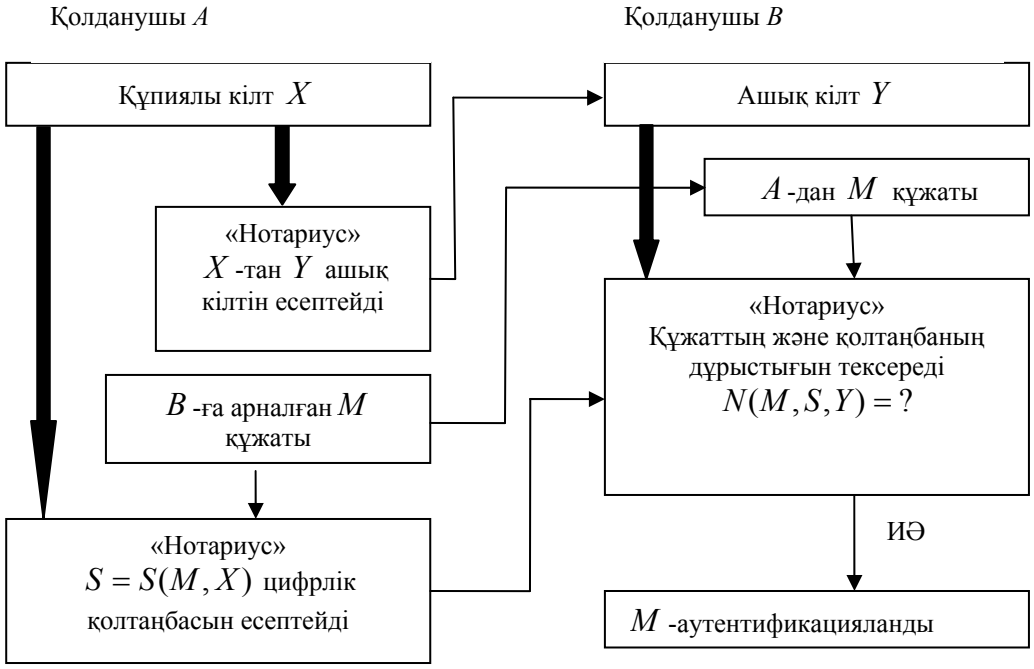
RSA және ГОСТ Р34.10-94 цифрлы қолтаңбаны генерациялау және верификациялау уақыты

Сызба	Қолтаңбаны генерациялау	Қолтаңбаны верификациялау
RSA ГОСТ Р34.10-94	0.48/0.38 0.26/0.18	0.48/0.38 0.66/0.52

Уақыттың алымында Кнут арифметикасын қолданған жағдайдағы нәтижелері келтірілген, көп дәрежелі амалдар кітапханасы Си және Ассемблер тілдерінде жазылған, бөлімінде Кнут оптимизацияланған арифметикасын қолдану арқылы алынған орташа уақыт мәндері. Келтірілген уақыт бағалары хэш-функцияны есептеу уақытын қоспай алынған. Монтгомери арифметикасын және көшу командаларын қолданбай амалдарды орындау уақытын RSA және ГОСТ Р34.10-94 үшін азайтуға мүмкіндік береді.

4.6.7. «Нотариус» цифрлы қолтаңба

«Нотариус» - цифрлы қолтаңба және электронды құжаттар дұрыстығын тексеретін бағдарламалар кітапханасы. «Нотариус» келісімшарттарға қолтаңба қоюды, төлемдер жүргізуді дербес компьютер мен модем қолдану арқылы жүзеге асыруға мүмкіндік береді. «Нотариус» цифрлы қолтаңба сызбасы 8-суретте келтірілген.



8-сурет. «Нотариус» электронды цифрлы қолтаңба сызбасы

«Нотариус» кітапханасының әрбір алгоритмі цифрлы қолтаңбаның беріктігі 10^{20} кем емес болатынына кепіл береді. Құпиялы кілтті білмейтін адамға қолтаңбаны алу үшін, қуаты 100 млрд. операция/с болатын суперкомпьютер көмегімен 250 жыл жұмыс жасау керек болады. Алгоритмдердің жылдамдығы 20-кестеде келтірілген.

20-кесте.

Генерациялау/верификациялау бағдарламасының жұмыс істеу уақыты

Файлдар үшін, кбайт		
1 0.014/0.027	10 0.024/0.038	100 0.124/0.138

Хабарламалардың, деректердің және бағдарламалардың ақиқаттығын және тұтастығын бұзудың барлық қауіптерін RSA және Эль-Гамаль криптожүйелерін, яғни асимметриялық алгоритмдерін цифрлы қолтаңбаларда қолдану арқылы жоюға болады. Оларды қолдану өзара сенімсіздік және қолданушыларды өзара қорғау моделін іске асыруға мүмкіндік береді. Беріктік пен аутентивтілікке өте жоғары талаптар қойылатын жүйелерде, ұзындығы 1024 бит және одан да көп болатын модульдер қолдану керек.

Цифрлы қолтаңбаның асимметриялық криптожүйелерін қолдану кезіндегі негізгі кемшілігі – ол қолтаңбаны генерациялау және верификациялау процедурасын көп уақыт есептеуі осының нәтижесінде цифрлы қолтаңбаның төмен жылдамдықта болуы.

Бақылау сұрақтары

1. Электронды цифрлы қолтаңбаларды атап өтіңіз.
2. Хэш-функцияға анықтама беріңіз.
3. Қолтаңбаны қою және тексеру технологиясы қалай болады?
4. Құжаттарды аутентификациялаудың мақсаты қандай?
5. Электронды цифрлы қолтаңбаға қойылатын талаптар қандай?
6. Елімізде электронды цифрлы қолтаңба қалай қолданылады?

Есептер

1. RSA криптожүйесін қолданып электронды цифрлы қолтаңбаны құру программасын жасаңыз.
2. Эль–Гамаль криптожүйесін қолданып электронды цифрлы қолтаңбаны құру программасын жасаңыз.
3. Хэш-функцияларға программа жасаңыз.
4. Окамото цифрлы қолтаңбасына программа жасаңыз.
5. Микали – Шамир цифрлы қолтаңбасына программа жасаңыз.