Лекция 12 ЭЛЕКТРОНДЫҚ ЦИФРЛЫҚ ҚОЛ

RSA алгоритмға негізделген электрондық қол

RSA алгоритмды пайдалану схемада үлкен N модулі болғанда, қаскүнемде жабық кілтті алу және шифрланған хабарды ашып оқу мүмкіндігі болмайды. Бірақ, бұл схемада қаскүнем абонент *А*-ның абонент *Б*-ға берілетін хабарды ауыстыру мүмкін, өйткені абонент *А* өз хабарын *Б*-дан ашық байланыс арна арқылы алынған ашық кілтпен шифрлайды. Ашық кілт ашық арна арқылы берілгендіктен, кез келген адам оны алып хабарды ауыстыру үшін пайдалану мүмкін. Мұнан құтылуға болады, егер күрделі протоколдарды пайдаланатын болсақ, мысалы, келесі.

Бұрыңғыдай пайдаланушы *А* пайдаланушы *Б*-ға бірнеше m_i блоктан тұратын хабар бергісі келсін. Байланыс сеанстың алдында абоненттер ашық және жабық кілттерді генерациялайды, олар кестеде көрсетілгендей белгіленеді:

	Ашық кілт	**Жабық кілт**
Пайдаланушы *А*	$N_А, d_А$	$e_А$
Пайдаланушы *Б*	$N_Б, d_Б$	$e_Б$

Нәтижесінде әрбір пайдаланушыда өз меншік ашық (екі бөліктен тұратын) және жабық кілттер болады. Сосын пайдаланушылар ашық кілттерімен алмасады. Бұл протоколдың дайындау кезеңі.

Протоколдың негізгі бөлігі келесі қадамнан тұрады:

1. Алдымен пайдаланушы *А* сандарды $c_i = m_i^{eА} \bmod N_А$ есептейді, яғни хабарды өз жабық кілтімен шифрлайды. Осы іс-әрекеттер нәтижесінде пайдаланушы *А* хабарға қол қояды.

2. Сосын пайдаланушы *А* сандарды $g_i = c_i^{dБ} \bmod N_Б$ есептейді, яғни 1-ші қадамда алынғанды пайдаланушы *Б*-ның ашық кілтімен шифрлайды. Бұл кезеңде бөтен адам оқи алмау үшін хабар шифрланады.

3. g_i сандар тізбегі пайдаланушы *Б*-ға беріледі.

4. Пайдаланушы *Б* g_i алады және алдымен өз жабық кілтін пайдаланып рет-ретімен сандарды $c_i = g_i^{eБ} \bmod N_Б$ есептейді. Осы кезде хабар дешифрланады.

5. Сосын пайдаланушы *Б* пайдаланушы *А*-ның ашық кілтін пайдаланып сандарды $m_i = c_i^{dА} \bmod N_А$ анықтайды. Осы кезеңнің орындағанынан пайдаланушы *А*-ның қолы тексеріледі.

Нәтижесінде абонент *Б* бастапқы хабарды алады және оны нақ абонент *А* жібергеніне көз жетеді. Бұл схема бірнеше түрлі бұзулардан қорғауға мүмкіндік береді:

- пайдаланушы *А* өз хабарынан бас тарталмайды, егер ол құпиялы кілт өзіне ғана белгілі болғанын мойындаса;
- бұзушы құпиялы кілтті білмей хабарды не құрастыра, не өзгерте алмайды.

Бұл схема көп қақтығыстан бас тартуға мүмкіндік береді. Кейде берілетін хабарды шифрлауға қажет жоқ, бірақ оны электронды қолмен бекіту керек. Онда, жоғарыда келтірілген протоколдан 2-ші және 4-ші қадамдар жойылады, яғни мәтін жіберушінің жабық кілтімен шифрланады, және алынған тізбек құжатқа қосылады. Алушы жіберушінің ашық кілті көмегімен қосылған қолды ашып оқиды, ол көбінесе негізгі хабардың шифрланған қайталануы. Егер ашып оқылған қол негізгі мәтінмен бірдей болса, онда қол дұрыс.

ЭЦҚ құрастыру үшін RSA алгоритмның басқа да вариантары бар. Мысалы, ашық кілтпен хабардың өзін емес, оның хеш-кодын шифрлауға (яғни қол қоюға) болады.

Электронды қолды алу үшін RSA алгоритмның пайдалану мүмкіндігі осы жүйеде құпиялы мен ашық кілттердің тепе-теңдігінен шығады. Кілттердің әрбіреуі, *d* немесе *e*, шифрлау үшін де дешифрлау үшін де пайдалану мүмкін. Бұл қасиет ашық кілті бар криптожүйелердің бәрінде орындалмайды.

RSA алгоритмды кілттермен алмасу үшін де пайдалануға болады.

12.2 Эль-Гамаль алгоритмға негізделген цифрлық қол

Қолды жасау және тексеру принципі.

Эль-Гамаль алгоритмды да цифрлық қолды құрастыру үшін пайдалануға болады. Пайдаланушылар тобы *P* мен *A* ортақ параметрлерді таңдайды. Сосын топтың әрбір абоненты өз құпиялы санды X_i, $1 < X_i < P$-1, таңдайды, және оған сәйкес ашық санды Y_i есептейді: $Y_i = A^{Xi} \bmod P$. Сонымен, әрбір пайдаланушы жұпты (жабық кілт; ашық кілт) алады (X_i, Y_i). Пайдаланушылардың ашық кілттері кілттерді үлестіру жүйесінің ортақ базасында сақталыну мүмкін және керек кезде жүйенің барлық абоненттеріне беріледі.

Қол қойылатын хабар *P*-ның модулінан кіші сан түрінде көрсетілу керек. Хабар үлкен болса, ол керек мөлшері бар блоктарға бөлінеді. Кейбір жағдайда хабардың өзіне емес, оның хеш-функциясына қол қойылады. Қандай да болса вариантта цифрлық қол кейбір *m* ($m < P$) санға байланысты есептеледі.

Пайдаланушы 1 өз хабарына цифрлық қол қойып оны пайдаланушы 2-ге бергісі келсін. Бұл жағдайда іс-әрекет алгоритмы келесі.

1. Бірінші пайдаланушы *P*-1 мен өзара жай кездейсоқ құпиялы санды *k* таңдайды, және есептейді санды $a = A^k \bmod P$.

2. Сосын кеңейтілген Евклид алгоритмы көмегімен *b* мәнің табу керек келесі теңдеуден:

$$m = (X_1 \cdot a + k\, b) \bmod (P-1).$$

Қос сандар (*a*, *b*) хабардың *m* цифрлық қолы болып табылады.

3. Хабар *m* қолмен (*a*, *b*) бірге пайдаланушы 2-ге жіберіледі.

4. Пайдаланушы 2 хабарды *m* алады және бірінші абоненттің ашық кілтін Y_1 пайдаланып екі санды келесі формулар арқылы есептейді:

$$c_1 = Y_1^a \cdot a^b \bmod P,$$

$$c_2 = A^m \bmod P.$$

Егер $c_1 = c_2$, онда бірінші пайдаланушының цифрлық қолы дұрыс. Әрбір жаңа хабарға қол қою үшін әрбір сайын жаңа *k* мәні таңдалыну керек.

Эль-Гамаль алгоритмды пайдалануымен жасалынған қолдар, *рандомизировалынған* деп аталады, өйткені бірдей хабар үшін бірдей жабық кілтті пайдаланғанда әрбір сайын жаңа қолдар (*a*, *b*) жасалынатын болады, себебі әр сайын *k*-ның жаңа мәні пайдаланады. RSA алгоритмды пайдалануымен жасалынған қолдар, *детерминдалған* деп аталады, өйткені бірдей хабар үшін бірдей жабық кілтті пайдаланғанда әрбір сайын бірдей қол жасыланатын болады.

12.3 Цифрлық қолды есептеу және тексеру мысалы

Интернет арқылы шифрланған хабарлармен алмасатын абоненттерде келесі ортақ параметрлер болсын: $P = 11$, $A = 7$.

Осы байланыс жүйенің пайдаланушылардың біреуі өз хабарына m=5 Эль-Гамаль алгоритмы бойынша құрастырылған қол қойғысы келеді. Алдымен ол өзіне жабық кілт

таңдайды, мысалы, X_1=3 және ашық кілт жасайды $Y_1 = 7^3 \bmod 11 = 2$. Ашық кілт барлық ізденген абоненттерге берілу немесе байланыс жүйенің ашық кілттер деректер базасына салыну мүмкін.

Сосын пайдаланушы P-1 мен өзара жай кездейсоқ құпиялы k санды таңдайды. k=9 болсын (9-да 10-мен ортақ бөлгіштері жоқ). Әрі қарай есептеледі

$$\text{сан } a = A^k \bmod P = 7^9 \bmod 11 = 8.$$

Осыдан кейін кеңейтілген Евклид алгоритмы көмегімен b мәні табылады:

$$m = (X_1 \cdot a + k \cdot b) \bmod (P - 1),$$
$$5 = (3 \cdot 8 + 9 \cdot b) \bmod 10.$$

Соңғы теңдеудің шешімі b=9.

Сонымен, жұп сандар (8, 9) хабардың m=5 цифрлық қолы болады.

Егер желінің қандай да бір пайдаланушысы хабардағы цифрлық қолды тексерем десе, ол деректер базадан бірінші пайдаланушының ашық кілтін алып (ол 2-ге тең), екі санды c_1 мен c_2 есептейді және оларды салыстырады.

$$c_1 = Y_1^a \cdot a^b \bmod P = 2^8 \cdot 8^9 \bmod 11 = 10,$$
$$c_2 = A^m \bmod 11 = 10.$$

$c_1 = c_2$ болғандықтан, m=5 хабардағы бірінші пайдаланушының цифрлық қолы дұрыс.

12.4 Цифрлық қол алгоритмдарының стандарттары

Цифрлық қолдың DSS стандарты.

Бүгін көп елде электронды (цифрлық) қолға стандарттар бар. Цифрлық қолдың DSS (Digital Signature Standard – DSS) стандарты АҚШ-а 1991 жылы қабылданған және 1994 жылы қайта қаралған болатын. Стандарт негізінде DSA (Digital Signature Algorithm) деп аталатын және Эль-Гамаль қолдың вариация болып табылатын алгоритм жатыр. Алгоритмда бірбағытталған хеш-функция $H(m)$ пайдаланылады. Хеш-алгоритм ретінде SHA-1 алгоритмы пайдалынады.

ЭЦҚ генерациялау алгоритмын қарастырайық. Алдымен абоненттер тобы үшін үш ортақ (құпиялы емес) параметр p, q және a таңдалынады:

- параметр p ұзындығы 512 ден 1024 битке дейін жай сан болу керек;
- q – ұзындығы 160 бит жай сан; p мен q арасында кейбір бүтін b үшін $p = bq + 1$ қатынас орындалу керек. p мен q-дағы үлкен биттер бірге тең болу керек (сонымен $2^{159} < q < 2^{160}$);
- теңсіздікке $1 < a < p$-1 сай келетін және $a^q \bmod p = 1$ теңдеудің түбірі болып табылатын сан a.

Осы сандарды біле отырып, жүйенің әрбір абоненты кездейсоқ x санды таңдайды, ол теңсіздікке $0 < x < q$ қанағаттандырылу болу керек, және есептейді

$$y = a^x \bmod p.$$

х саны пайдаланушының құпиялы кілті болып табылады, ал y саны – ашық кілт. Белгілі x бойынша y-ты есептеу қиын емес. Бірақ, ашық кілт y болғанда, x-ты есептеу мүмкін емес, ол g негізі бойынша y-тың дискретті логарифмы болып табылады.

Барлық пайдаланушылардың ашық кілттері кейбір құпиялы емес, бірақ «сертификацияланған» анықтамалықта көрсетіледі деп болжаймыз. Осымен параметрлерді таңдау кезеңі аяқталады, ал абоненттер қолдарды құрастыруға және тексеруге дайын.

Пайдаланушылардың біреуі қол қоятын хабар m бар болсын. Қолды генерациялау үшін пайдаланушы келесі іс-әрекеттер орындау керек:

- 1. Хабар m үшін хеш-функцияның $h = H(m)$ мәнің есептеу. Хеш-функцияның мәні $0 < h < q$ аралығында жату керек.

2. Сосын кездейсоқ k санды генерациялау керек, $0 < k < q$.

3. Есептеу $r = (a^k \bmod p) \bmod q$.

4. Анықтау $s = [k^{-1}(H(m) + x \cdot r)] \bmod q$.

Нәтижесінде пайдаланушы m хабар үшін екі қос саннан (r, s) тұратын қол жасап алады. Хабар қолмен бірге жүйенің қандай да басқа абонентіне жіберілу мүмкін. Қолды мына түрімен тексеруге болады:

1. Хабар m үшін хеш-функцияның $h = H(m)$ мәнің есептеу.

2. $0 < r < q$, $0 < s < q$ теңсіздіктердің орындалуын тексеру.

3. Есептеу $w = s^{-1} \bmod q$.

4. $u_1 = [H(m) \cdot w] \bmod q$.

5. $u_2 = r \cdot w \bmod q$;
$v = [(a^{u1} \cdot y^{u2}) \bmod p] \bmod q$.

6. $v = r$ теңдіктің орындалуын тексеру. Егер $v = r$, онда қол дәл өзі деп саналады, әйтпесе дұрыс емес.

Дискретті логарифмды есептеу күрделі болғандақтан, қаскүнем r-дан k-ны немесе s-тан x-ты қалпына келтіре алмайды, демек жалған қол қоялмайды. Және осы себептен хабар иесі өз қолынан бас тарталмайды, өйткені өзінен басқа жабық x кілтті ешкім білмейді.

12.5 Цифрлық қолдың ГОСТ Р34.10-94 стандарты

Ресейде ГОСТ Р34.10-94 «Ақпараттық технология. Ақпараттың криптографиялық қорғауы. Ассиметриялық криптографиялық алгоритмы негізінде электронды цифрлық қолды жасау және тексеру процедуралары» стандарты қабылданған. Бұл стандартта DSS стандарттағыдай алгоритм пайдаланылады. Алдымен ГОСТ Р34.10-94 бейнеленген алгоритмды толық қарап шығайық, сосын оның DSA алгоритмнан айырмашылықтарын белгілейік.

Басында, DSS стандарты сияқты, абоненттер тобы үшін үш ортақ (құпиялы емес) параметр p, q және a таңдап алынады:

- параметр p ұзындығы 512 ден 1024 битке дейін жай сан болу керек. p-ның үлкен биты бірге тең болу керек;
- q – ұзындығы 254-256 бит жай сан; DSA алгоритмда сияқты, q p-1 санның бөлгіші болу керек; q-ның үлкен биты бірге тең болу керек;
- теңсіздікке $1 < a < p$-1 сай келетін және $a^q \bmod p = 1$ теңдеудің түбірі болып табылатын сан a;
сосын әрбір пайдаланушы жабық және ашық кілт құрастыра алады. Жабық кілті ретінде кез келген сан x, $0 < x < q$ алынады. Ашық кілт $y = a^x \bmod p$ формуладан алынатын y саны болады. Әрбір жаңа қолды жасау үшін әрбір сайын жаңа кездейсоқ сан k, $0 < k < q$ таңдап алынады.

m хабардың қолы екі (r, s) саннан тұрады, олар келесі формула арқылы есептеледі:

$$r = (a^k \bmod p) \bmod q,$$
$$s = k(H(m) + x(r)) \bmod q,$$

мұндағы $H(m)$ – m хабар үшін хеш-функцияны есептеу нәтижесі.

Осымен қолды құрастыру аяқталды, және хабар m ЭЦҚ (r, s) бірге алушыға жіберілу мүмкін. Енді ГОСТ Р34.10-94 бойнша ЭЦҚ құрастыру алгоритмның DSS алгоритмнан айырмашылығын көрсетейік.

1. Қолды есептеудің алдында бастапқы хабар әртүрлі хеширование функцияларымен өңделеді: ГОСТ Р34.10-94 хеш-функцияға ГОСТ Р34.11-94 стандарты қолданылады, DSS-та түрлі ұзындығы хеш-коды бар SHA-1 пайдаланады. Осыдан жай санның q ұзындығына әртүрлі талаптар шығады: ГОСТ Р34.10-94 q-ның ұзындығы 254 тен 256 битке дейін болу керек, ал DSS-та q-ның ұзындығы 159 дан 160 битке дейін болу керек.

2. Колдағы компонент s әртүрлі есептеледі. ГОСТ Р34.10-94 компонент s мына формула бойынша есептеледі

$$s = k(H(m) + x(r)) \bmod q,$$

ал DSS-та компонент s мына формула арқылы есептеледі

$$s = [k^{-1}(H(m) + x(r))] \bmod q.$$

Соңғы айырмашылығы қолды тексеруге арналған формуладағы айырмашылыққа келтіреді.

Нәтижесінде ГОСТ Р34.10-94 бойынша қолды тексеру процедурасы келесі болады. [m, (r, s)]-ты алып алушы есептейді:

$$w = H(m)^{-1} \bmod q,$$
$$u_1 = w \cdot s \bmod q,$$
$$u_2 = (q-r) \cdot w \bmod q,$$
$$v = [(a_{u1} \; y_{u2}) \bmod p] \bmod q.$$

Сосын есептелген v мәннің және ЭЦҚ құрамында алынған r параметрдің теңдігі тексеріледі. Қол дұрыс деп есептеледі, егер $v = r$.

ГОСТ Р34.10-94 бойынша ЭЦҚ жасау алгоритмда, DSS алгоритмдағыдай, есептеуіш ресурстарды қажет ететін күрделі есептер жүргізіледі.

12.6 ГОСТ Р34.10-94 стандарты бойынша қолды жасау және тексеру мысалы

$p = 23$, $q = 11$, $a = 6$ болсын (тексереміз: $6^{11} \bmod 23 = 1$).

Қолды жасау.

Пайдаланушы A жабық кілті ретінде санды x=8 таңдап алсын. Осыдан кейін ол формула $y = a^x \bmod p$ бойынша құпиялы кілтті есептейді. Яғни $y = 6^8 \bmod 23 = 18$.

Қолды жасау үшін пайдаланушы A кездейсоқ санды $k = 5$ таңдайды. Хабар үшін хеш-функцияны есептеу нәтижесі $H(m) = 9$ болсын. Хабардың қолы екі саннан тұрады (r, s):

$$r = (a^k \bmod p) \bmod q = (6^5 \bmod 23) \bmod 11 = 2,$$
$$s = (k\,H(m) + x \cdot r) \bmod q = (5 \cdot 9 + 8\;2) \bmod 11 = 6.$$

Сонымен, хабардың қолы қос саннан (2, 6) тұрады.

Қолды тексеру.

Хабарды қолмен (2, 6) бірге алып, пайдаланушы есептейді w

$$= H(m)^{-1} \bmod q = 9^{-1} \bmod 11 = 5,$$

$$u_1 = w\; s \bmod q = 5\;6 \bmod 11 = 8,$$
$$u_2 = (q-r)\; w \bmod q = (11-2)\;5 \bmod 11 = 1,$$
$$v = [(a^{u1}\; y^{u2}) \bmod p] \bmod q = [(6^8\; 18^1) \bmod 23] \bmod 11 = 2.$$

$v = r$ болғандықтан, қол дұрыс деп саналады.

ГОСТ Р34.10 немесе DSS стандарттарды пайдалануымен жасалынған қолдар, Эль-Гамаль алгоритмы арқылы алынған қолдар сияқты, рандомизироваланған болып табылады, себебі бірдей хабарлар үшін бірдей жабық кілтті x пайдаланғанда, әрбір сайын түрлі қолдар (r, s) жасалынатын болады (түрлі кездейсоқ k мәні пайдалануына себепті).

12.7 ЭЦҚ жаңа стандарты

Ресейде 2001 жылы ЭЦҚ құрастыруға және тексеруге жаңа стандарт қабылданды. Оның толық аты: «ГОСТ Р34.10-2001. Ақпараттық технология. Ақпараттың криптографиялық қорғауы. Электронды цифрлық қолды құрастыру және тексеру процестері».

ГОСТ Р34.10-2001 негізінде эллипстік қисықтар үстінде операцияларды пайдаланатын алгоритмдар жатыр. ГОСТ Р34.10-2001 беріктігі эллипстік қисықтын нүктелер тобында дискретты логарифм алудың күрделілігіне негізделген, және де ГОСТ Р34.11-94 бойынша хеш-функцияның беріктігіне. Құрастырылатын цифрлық қолдың мөлшері - 512 бит.

Толық айтқанда, ГОСТ Р34.10-2001 алгоритмы бойынша есептеу алгоритмы ГОСТ Р34.10-94 стандартқа ұқсайды. Алдымен кездейсоқ сан k генерацияланады, оның көмегімен қол компонентасы r есептеледі. Сосын компонента r, k саны, құпиялы кілт мәні және қол қойылатын деректердің хэш-мәні негізінде ЭЦҚ-ң s-компонентасы құрастырылады. Қолды тексергенде сол сияқты белгілі r, s қатынастарға ашық кілттің және ақпараттың хэш-мәннің сәйкестігі тексеріледі. Қатынастар дұрыс болмағанда, қол дұрыс емес деп саналады.

Ескі стандарт ГОСТ Р34.10-94 жойылмаған, сондықтан қазіргі уақытта ЭЦҚ екі стандарты бірге істейді. Бірақ, бұрыңғы ГОСТ үшін шектеу қойылған: p параметрдің тек 1024-битты мәнің пайдалануға болады.

Жаңа ГОСТ Р34.10-2001 стандартта эллипстік қисықтағы нүктелер тобының математикалық аппаратын пайдалануы p модульдің ретін қысқартуға мүмкіндік береді, критпоберіктігін жоғалтпай. Стандартта жазылған, p санның ұзындығы 256 немесе одан артық бит болу мүмкін.

12.8 Симметриялық немесе асимметриялық криптография ма?

Қандай алгоритмдар жақсы - симметриялық немесе асимметриялық па – бұл сұраққа бірмәнді жауап әрине жоқ. Симметриялық криптографияның негізгі артықшылығы – деректерді өңдеудің үлкен жылдамдығы. Жабық кілті бар жүйелердің проблемалары бұрын қарастырылған болатын. Енді ашық кілті бар шифрлау алгоритмдардың ерекшеліктерін бағалап көрейік.

Ассимметриялық криптографияның басты құны - хабарлармен құпиялы алмасуда алдын ала сенімді кілттермен алмасудың қажеттілігінің болмауы. Ассимметриялық криптожүйелердің негізгі кемшіліктері келесі:

1. Ашық кілті бар алгоритмдар жабық кілті бар классикалық алгоритмдардан жүздеген есе баяу жұмыс істейді. Бұл олардың ең басты кемшілігі. Өйткені ашық кілті бар жүйелерде негізгі операция үлкен модулі бойынша 500-1000 битты сандарды дәрежелеу.

2. Ашық кілті бар алгоритмдар ашық кілттердің анықтығын қажет етеді, кейде бұл әжептәуір күрделі есеп. Осы да цифрлық қол протоколдарына да қатысты. Ашық кілттерді басқару үшін арнайы инфрақұрылымды пайдаланады.

3. Ашық кілті бар алгоритмдар таңдалған ашық мәтін бойынша шабуылдарға сезгіш болады.

Сонымен, тәжірибелік жағынан ашық кілті бар және ассиметриялық шифрлау жүйелерді тек құпиялы кілттерді үлестіруге және цифрлық қолдарды ұйымдастыруға пайдалану жөн, себебі осы есептерді шешу үшін үлкен деректер блоктарын шифрлаудың қажеті жоқ.

Ассиметриялық алгоритмдың пайдалануы шифрлаудың сеанстық кілттерін жасауға мүмкіндік береді, олар байланыс сеансы аяқталғаннан кейін жойылады. Бұл шифрланған хабардың ашу тәуекелдігін тым төмендетеді. Мұнда симметриялық шифрлаудың алдында кілттермен алмасу протоколын орындамаса да болады. Шифрланған деректерді кілтпен бірге беру протоколының мүмкін вариантын көрсетейік.

1. Пайдаланушы *А* кездейсоқ сеанстық кілтті *К* генерациялайды және онымен симметриялық алгоритмы $F_{\text{сим}}$ көмегімен өз хабарын *М* шифрлайды:

$$Cт = F_{\text{сим}}(M, K)$$

2. Пайдаланушы *А* деректер қорынан *Б* пайдаланушының ашық кілтін *U* алады және онымен сеанстық кілтті *К* шифрлайды:

$$Cк = F_{\text{асим}}(K, U)$$

3. Пайдаланушы *А* өзінің абонентіне шифрланған хабарды *С*т және шифрланған сеанстық кілтті *С*k жібереді. «Адам ортада» ашудан қорғау үшін берілетін деректерге цифрлық қол қосылу мүмкін.

4. Пайдаланушы *Б* алынған сеанстық кілтті *С*k өз жабық кілті *R* көмегімен дешифрлайды:

$$K = F_{\text{асим}}^{-1}(Cк, R)$$

5. Пайдаланушы *Б* сеанстық кілт *К* көмегімен хабарды ашып оқиды:

$$M = F_{\text{сим}}^{-1}(Cт, K)$$

Осындай криптографиялық жүйе *аралас* деп аталады, себебі онда асимметриялық та, симметриялық та шифрлау пайдаланылады. Аралас криптожүйелер тәжірибеде кең қолданылады: деректерді берудің банктік және төлем желілерде, мобильді байланыста, электронды пошта жүйелерде және т.б. Қауіпсіздікті күшейту үшін олар пайдаланушылардың және растау орталықтын цифрлық қолдарымен, уақыт белгілермен толтырылу мүмкін.

12.9 Ашық кілттерді басқару

Асимметриялық криптографияның арқасында құпиялы кілттерді үлестіру проблемасы шешілген болатын, бірақ жаңа проблема туды – ашық кілттердің нағыздығын дәлелдеу проблемасы. Бұл проблеманың мағынасы – кейбір *А* абоненттың ашық кілтін алғанда, пайдаланушы осы кілт дәл *А* абоненттікі деп сенімді болу керек.

Ашық кілттерді сертификациялау проблеманы шешуде үлкен роль цифрлық қолды жасау атқарды. Көп абоненттері бар асимметриялық криптографияны қолданылатын байланыс жүйелерде арнайы ұйымдастыру құрылымды пайдалана бастады. Бұл ұйымдастыру құрылымдар сенімді үшінші жағының ролін атқарады және абоненттердің ашық кілтерін өз цифрлық қолдарымен куәландырады. Сонымен, ашық кілті бар криптожүйелерді пайдаланатын таратылған байланыс жүйелерде, **ашық кілттер инфрақұрылымы** (Public Key Infrastructure - PKI) деген ұғым енгізіледі. Оған кіреді бағдарлама-аппараттық құралдар кешені, және де ашық кілттерді басқару үшін қажетті сервисты қамтамасыз ететін ұйымдастыру-техникалық және әкімшілік іс-шаралар.

Ашық кілттер инфрақұрылымның негізгі элементі **сертификациялау орталығы** (куәландыру орталығы) (Certification authority, CA). Ол барлық процедураларды бақылайды: кілттерді жасау, тіркеу, сақтау және жаңарту, **ашық кілттердің сертификаттарын** және кері шақырып алынған сертификаттар тізімін. Сертификат дегеніміз - бұл орталықтын цифрлық қолымен куәландырылған ақпарат, оған кіреді ашық

кілт және абонент туралы басқа мәліметтер. Осындай мәліметтер, мысалы, электронды қол алгоритмның идентификаторы, куәландыру орталықтын аты, сертификаттің жарамдылық мерзімі, сертификат иесінің аты. Халықаралық стандарт ISO X.509 ашық кілттер сертификатының құрылымын және аутентификациялау үшін олардың пайдалану ережесін анықтайды.

Сертификаттың келесі қасиеті бар:

- сертификациялау орталығының әрбір пайдаланушысы сертификатқа кіретін ашық кілтті алу мүмкін;
- сертификациялау орталығынан басқа ешкім сертификатты жасырып өзгерте алмайды (сертификатты жалған жасау мүмкін емес).

Сертификатты жалған жасап мүмкін емес болғандықтан, оларды ашық анықтамалыққа салып жариялауға болады.

Байланыс жүйенің әрбір пайдаланушысы бір немесе бірнеше сертификатқа ие болу мүмкін. Абоненттің ашық кілтін, куәландыру орталығының әкімшінің ашық кілтін білетін, қандай да пайдаланушы сертификаттан алу мүмкін. Сертификациялау орталығының әкімшісі әдетте адам емес - жоғары өнімді автоматтандырылған жүйе болады.

Көп абоненттері бар таратылған байланыс жүйелерде бірнеше сертификациялау орталығы жасалу мүмкін. Сертификациялау орталықтары ағаш тәріздес құрылымға бірлеседі, оның түбірінде басты куәландыру орталығы орналасады. Басты орталығы оған тәуелді орталықтарға сертификаттар береді, сонымен осы орталықтардың ашық кілтерін куәландырады.

Пайдаланушының ашық кілті жабық кілттің негізінде құрастырылады. Әрбір пайдаланушы өзінің жабық кілтін берік сақтау керек. Егер жабық кілтті тағы да біреу білетің болса, онда кілт иесі байланыс жүйенің басқа абонеттерін осы туралы хабарландыру керек.

Ашық кілттер сертификаттарының іс-әрекет мерзімі бар, бірақ қандай да болса сертификат одан бұрын да шақырылып алыну мүмкін, егер кілттің абыройы түсіп қалса. Куәландыру орталығы өз абоненттерін шақырылып алынған сертификаттар туралы хабарландыру керек. Осы мақсатпен шақырып алынған сертификаттар тізімі немесе жойылу тізімі жасалынады.

Осындай ұйымдастыруда куәландыру орталығының әкімшісі пайдаланушылардың құпиялы кілттеріне рұқсат алалмайды. Әкімші тек сертификат анықтамалығындағы ашық кілтті ауыстыру мүмкін немесе жалған абонентті енгізіп, оның атынан байланысқа кіріп хабарды алу мүмкін. Осындай қақтығыстан құтылу үшін кілттерді дайындау және таратудың келесі схемасы қолданылу мүмкін.

1. Куәландыру орталығының әкімшісі қос кілттерді (жабық кілт, ашық кілт) генерациялайды және өзінің ашық кілтін абоненттердің бәріне хабарлайды.
2. Пайдаланушы *A* шифрлауды орындауға және ЭЦҚ құрастыру үшін жабық кілттерді таңдайды, және де сәйкес ашық кілттерді есептейді.
3. Шифрлаудын және қолдын ашық кілттері әкімшінің ашық кілтімен шифрланады және куәландыру орталыққа тіркеуге ұсынылады.
4. Куәландыру орталығының әкімшісі *A* пайдаланушының ашық кілттерін тексереді (өзінің жабық кілтімен дешифрлайды); пайдаланушы *A*-ның ашық кілттер сертификаттарын жасап оларға қол қояды және шифрлаудың ашық кілттері мен қолдар ашық кілттерінің анықтамалығына орналастырады.
5. Жүйенің әрбір пайдаланушысы анықтамалықтан қажетті абоненттің сертификатын алады, әкімшінің қолын тексеріп (оны әкімшінің ашық кілтімен дешифрлайды) ашық кілтті шығарып алады.

Тәжірибеде қарастырылған схема уақыт белгілермен, сертификаттағы қосымша өрістерді (мысалы, іс-әрекет мерзімі) тексерумен және жүйенің қауіпсіздігін күшейтетін басқа тексерістермен толықтырылады.

Негізгі терминдер

DSS (Digital Signature Standard) – цифрлық қолға АҚШ-ң стандарты. Стандарт негізінде DSA (Digital Signature Algorithm) деп аталатын және Эль-Гамаль қолдың вариациясы болып табылатын алгоритм жатыр.

ГОСТ Р34.10-2001 – ЭЦҚ құрастыру және тексеру алгоритмға ресейлік жаңа стандарты. Эллипстік қисықтын нүктелер тобында дискретты логарифм алудың күрделілігіне негізделген, және де ГОСТ Р34.11-94 бойынша хеш-функцияның беріктігіне. Құрастырылатын цифрлық қолдың мөлшері - 512 бит.

ГОСТ Р34.10-94 – 1995 жылдан істейтін ЭЦҚ құрастыру және тексеру алгоритмның ресейлік стандарты. Стандартта пайдаланылады ашық кілті бар Эль-Гамаль шифрлау схемасының түрлендіруі және ГОСТ Р34.11-94 бойынша хеш-функцияны жасау алгоритмы.

Ашық кілттер инфрақұрылымы - бағдарлама-аппараттық құралдар кешені, ашық кілттерді басқару үшін қажетті сервисты қамтамасыз ететін ұйымдастыру-техникалық және әкімшілік іс-шаралар.

Ашық кілттің сертификаты - орталықтын цифрлық қолымен куәландырылған ақпарат, оған кіреді ашық кілт және абонент туралы басқа мәліметтер (электронды қол алгоритмның идентификаторы, куәландыру орталықтын аты, сертификаттің жарамдылық мерзімі, сертификат иесінің аты және т.б.).

Сертификациялау орталығы – электронды цифрлық қолдың кілттер сертификатын шығаратын ұйым, ол пайдаланушылардың кілттерін басқаруға жауап береді. Ашық кілттер және пайдаланушылар туралы басқа ақпарат куәландыру орталықтарында цифрлық сертификаттар түрінде сақталынады.

Сұрақтар

1. Қандай ассиметриялық алгоритмдар электронды цифрлық қолды құрастыруға және тексеруге қолданылу мүмкін?
2. Түрлі ассиметриялық алгоритмдарды пайдаланып цифрлық қолды жасау және тексеру процесін сипаттап беріңіз.
3. Электронды цифрлық қолды құрастыру және тексеру алгоритмдарға қандай стандарттар іс істейді?
4. Қандай цифрлық қолдар рандомизированған деп аталады?
5. Ашық кілттердің сертификациялау проблемасы неде?
6. Ашық кілттердің инфрақұрылымы деген не?
7. Ашық кілттерді сертификациялау орталығының функциясы қандай?
8. Ашық кілттің сертификаты деген не?
9. Ашық кілттерді сертификациялау орталығы бар байланыс жүйеде абоненттердің ашық кілттерін үлестірудің қандай схемасы пайдалану мүмкін?