4.1. RSA электрондық қолтаңбасы

Ашық кілт криптографиясы пайда болғаннан кейін заманауи компьютерлік және желілік технологияларда нақты революция болды. Бұрын шешілмейтін деп саналған және қазір кеңінен қолданылатын мәселелерді шешуге мүмкіндік туды тәжірибе. Қазіргі уақытта осы технологиялардың көмегімен күн сайын есептеулер жүргізіліп көптеген миллиардтаған мәмілелер жасалуда доллар, рубль, еуро және т.б. бұл технологиялардың маңызды элементтерінің бірі-электрондық немесе цифрлық қолтаңба. Көптеген елдер, атап айтқанда Ресейде электронды стандарттар енгізілді (сандық) қолтаңба және бұл тұжырымдаманың өзі азаматтық заңнамаға енгізілген. "Электрондық қолтаңба" термині таныс Ресей, дегенмен соңғы уақытта қабылданған жиі қолданылады басқа елдерде (ең алдымен АҚШ-та) "цифрлық қолтаңба"термині,бұл жаңа ресейлік стандарттарда да көрінеді.

Екі термин де бір мағынаны білдіреді.Криптографиялық сандық қарастыруды бастамас бұрын қолтаңбалар, біз үш қасиетті тұжырымдаймыз (ең дұрысы) қанағаттандыру кез келген, атап айтқанда, тұрақты қолмен жазылған қолтаңба:

1. Құжатқа тек "заңды" қол қоюшы қол қоя алады (сондықтан ешкім қолтаңбаны қолдан жасай алмайды).

2. Қолтаңба авторы одан бас тарта алмайды.

3. Дау туындаған жағдайда үшінші тұлғалардың қатысуы мүмкін (мысалы, соттар) қолдың түпнұсқалығын анықтау үшін

Әрине, цифрлық (электрондық) қолтаңбада да осы қасиеттердің барлығы болуы керек, бірақ құжаттарға қол қоятын және олардың түпнұсқалығын тексеретін адамдар бір-бірінен мыңдаған шақырым қашықтықта бола алады және тек компьютерлік желі арқылы өзара әрекеттесе алады.

Кәдімгі қолтаңбадан басқа, нақты өмірде арнайы бөлінген адам болған кезде нотариаттық қолтаңба қолданылады (нотариус) құжаттарды қолымен және мөрімен куәландырады, сондықтан кез келген басқа адам олардың түпнұсқалығына көз жеткізе алады. Аналогы бұл қолтаңба киберкеңістікте де сұранысқа ие. Электрондық нотариаттық қол қою кез келген басқа адамның қолы сияқты жүзеге асырылады.

Бұл бөлімде біз RSA схемасына негізделген электрондық қолтаңбаны қарастырамыз.

Егер Алиса құжаттарға қол қоюды жоспарласа, онда ол керек алдымен RSA параметрлерін сипатталғандай таңдаңыз бөлім. 2.6. Ол үшін Алиса екі үлкен жай санды таңдайды P және Q, N = P Q және ϕ = (P − 1)(Q − 1) есептейді. Содан кейін ол таңдайды d Саны, өзара қарапайым ϕ, және есептейді c = d^{-1} mod ϕ. Соңында, ол n және d сандарын жариялайды, мысалы, оларды өздеріне орналастырады сайт өзінің атымен байланыстырады және C санын құпия сақтайды (қалған P , Q және ϕ сандарын ұмытуға болады, олар енді қажет болмайды).Енді Алиса құжаттарға қол қоюға дайын немесе хабарламалар.

Алиса m = m_1. . . , m_n хабарламасына қол қойғысы келсін. Содан кейінбастапқыда ол хэш функциясы деп аталатын нәрсені есептейді.

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

бұл хабарламаға сәйкес келеді m саны y. Хэш функциясын есептеу алгоритмі бәріне белгілі деп болжанады. Бірақ біз

әзірге есептеу қасиеттері мен әдістеріне тоқталмайық хэш функциялары, өйткені бұл мәселе 8-тарауда толығырақ қарастырылады. Біз үшін ең маңызды қасиетті ғана атап өтеміз: негізгі мәтінді өзгерту мүмкін емес m1,. . . , mn, емес y өзгерту арқылы . Сондықтан келесі қадамда Алиса

жеткілікті қолтаңба тек y саны болып табылады және бұл қолтаңба бәріне қатысты болады хабарлама m .

Алиса санды есептейді

$$s = y^{c} \bmod N, \qquad (4.1)$$

яғни, ол y санын өзінің құпия дәрежесіне көтереді. S саны және сандық қолтаңба бар. Ол жай ғана m хабарламасына қосылады және осылайша Алисада қалыптасқан қол қойылған хабарлама алу

$$(m,s) \qquad (4.2)$$

w = h(m) теңдігінің орындалуын тексеріңіз.

Бекіту 4.1. Егер қолтаңба шынайы болса, онда w = h(m).

Дәлел . (4.3), (4.1) және RSA схемасының қасиеттері (бөлім. 2.6) керек.

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

Бекіту 4.2. Сипатталған электрондық қолтаңба қол қоюға қойылатын барлық талаптарды қанағаттандырады.

Дәлел . Қолтаңбаның бірінші сипатын тексеріңіз. Ешкім N санын жай көбейткіштерге бөле алмайды (2005 жылғы жағдай бойынша 1024 биттік тәртіптегі үлкен N-де бұл тапсырма іс жүзінде шешілмейді). Сондықтан N және d білу мүмкін емес . $c = d^{-1} \bmod \phi$ есептеу үшін шынымен, ф білу керек = (P-1) (Q-1) және ол үшін жай факторларды білу қажетP және Q. осылайша, бірінші қасиет орындалды-Алисадан басқа ешкім с санын біле алмайды, сондықтан қол қоя алмайды.

Екінші қасиет біріншісіне байланысты орындалды. Қолтаңба авторы ол одан бас тарта алмайды, өйткені оның атынан басқа ешкім қолтаңбаны "ойдан шығара" алмайды.

Үшінші мүлік те айқын-дау туындаған жағдайда мүдделі тарап судьяға оларды тексеру және шындықты анықтау үшін барлық есептеулерді ұсына алады. ол үшін хэш мәні, айталық, 13:

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

Бұл жағдайда Алиса есептейді (4.1)

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

және қол қойылған хабарламаны қалыптастырады

$$\{abbbaa, 7\}.$$

Енді Элис N = 55 және d = 3 ашық кілттерін білетін адам, қолтаңбаның түпнұсқалығын тексере алады. Қол қойылған хабарламаны алғаннан кейін ол хэш функциясының мәнін қайта есептейді

$$h(abbbaa) = 13$$

(егер хабарламаның мазмұны өзгертілмесе, онда хэш функциясының мәні Алиса есептегенмен сәйкес келеді) және есептейді (4.3)

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

w мәндері мен хэш функциялары сәйкес келді, сондықтан қолтаңба дұрыс.

Назар аударыңыз е. біз бірдей RSA схемасына назар аударамыз, Алиса жасаған, екі мәселені шешу үшін пайдалануға болады. Біріншіден, Алиса хабарламаларға көрсетілгендей қол қоя алады бұл бөлімде өзінің құпия кілтін қолдана отырып с. екіншіден, кез келген адам Алисаға шифрланған

хабарлама (Сан) жібере алады, шифрын шеше алады бұл көрсетілгендей бөлім. 2.6, тек ол пайдалана алады шифрлау үшін оның ашық кілті d.