4.1. РСА-ның РСА-ға қолы етілмеді..

Қоғамдық кілтті криптография пайда болғаннан кейін қазіргі компьютерлік және желілік технологияларда нағыз төңкеріс болды. Бұрын шешілмейтін деп саналған проблемаларды шешуге мүмкіндік туып, енді практикада кең қолданыс табуға мүмкіндік туды. Қазіргі уақытта осы технологиялардың көмегімен күн сайын есеп айырысулар жүргізіледі және көптеген миллиардтаған долларға, рубльге, еуроға және т.б. транзакциялар жасалады. Көптеген елдерде, атап айтқанда, Ресейде электрондық (цифрлық) қол қою стандарттары енгізілді, бұл тұжырымдаманың өзі азаматтық заңнамаға енгізілді. «Электрондық қолтаңба» термині Ресейге көбірек таныс, дегенмен соңғы кездері басқа елдерде (ең алдымен АҚШ-та) қабылданған «цифрлық қолтаңба» термині жиі қолданыла бастады, бұл ресейлік жаңа стандарттарда көрініс табады. Екі термин де бірдей дегенді білдіреді

Криптографиялық сандық қолтаңбаны қарастыра бастамас бұрын кез келген, атап айтқанда, қарапайым қолжазба қолтаңбаны қанағаттандыруы тиіс (идеалды) үш қасиетті тұжырымдайық:

1, Құжатқа тек "заңды" қол иесі ғана қол қоюы мүмкін (сондықтан қолды ешкім жырлай алмайды).

2, Қолдың авторы одан бас тарта алмайды.

3, Дау туындаған жағдайда үшінші тұлғалардың (мысалы, соттың) қолының түпнұсқалығын анықтауға қатысуы мүмкін.

Әрине, сандық (электрондық) қолтаңба да осы қасиеттердің барлығына ие болуы тиіс, бірақ құжаттарға қол қоятын және олардың түпнұсқалығын тексеретін адамдар бір-бірінен мыңдаған шақырым қашықтықта болуы және тек компьютерлік желі арқылы өзара әрекеттесуі мүмкін.

Бұл бөлімде RSA сұлбасы негізіндегі электрондық қолтаңбаны қарап шығамыз.

Егер Алиса құжаттарға қол қоюды жоспарласа, ол алдымен RSA параметрлерін секта сипатталғандай таңдауы керек. 2.6. Ол үшін Алиса екі үлкен P және Q сандарын таңдайды, $N = P\,Q$ және $\varphi = (P-1)(Q-1)$ деп есептейді. Содан кейін φ өзара премьераланған d санын таңдап алып, $c = d^{-1}$ мод φ есептейді. Сайып келгенде, ол N және d нөмірлерін жариялайды, мысалы, оларды өз атымен байланыстыра отырып, өз веб-сайтына қояды және c нөмірін құпия сақтайды (қалған P, Q және φ сандарын ұмытуға болады, олар енді қажет болмайды). Енді Алиса құжаттарға немесе хабарламаларға өз қолтаңбаларын қоюға дайын. Алиса $m^{-} = m\ 1$ хабарына қол қойғысы келсін, . . $м_н$. Содан кейін алдымен хэш функциясы деп аталатын функцияны есептейді

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