Электрондық сандық қолтаңба

**Электрондық сандық қолтаңба (ЭСҚ)** – бұл [электрондық құжаттың](https://kk.wikipedia.org/w/index.php?title=%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D2%B1%D0%B6%D0%B0%D1%82&action=edit&redlink=1) деректемесі, жасанды көшірмеден осы электрондық құжатты қорғау үшін арналған. Электрондық сандық қолтаңба ақпаратты [криптографиялық](https://kk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F) қорғау құралдарын (АҚҚҚ) пайдалануымен [ақпаратты](https://kk.wikipedia.org/wiki/%D0%90%D2%9B%D0%BF%D0%B0%D1%80%D0%B0%D1%82) қайта жасау нәтижесінде қалыптасады және [кілттің](https://kk.wikipedia.org/wiki/%D0%9A%D1%96%D0%BB%D1%82) қол қою [сертификатының](https://kk.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%82) иесін сәйкестендіруге, сондай-ақ электрондық құжатта ақпараттың бұрмалануының жоқ болуын белгілеуге рұқсат етеді.[[1]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-1)

**Негізгі терминдер**

**Электрондық сандық қолтаңбаның жабық кілті** – тіркеу куәлігінің иесіне белгілі электрондық сандық [рәміздерінің](https://kk.wikipedia.org/wiki/%D0%A0%D3%99%D0%BC%D1%96%D0%B7) дәйектілігі және электрондық сандық қолтаңбаның құралдарын пайдалануымен электрондық сандық қолтаңбаны құру үшін арналған.[[2]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-2)

*Электрондық сандық қолтаңбаның ашық кілті* – электрондық сандық рәміздерінің дәйектілігі, кез келген тұлғаға қол жеткізілімді және электрондық құжатта электрондық сандық қолтаңбаны растау үшін арналған; ашық кілт тек қана жабық кілтпен жұптасып жұмыс жасайды.[[3]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-3) Ашық кілтке тіркеу куәлігі беріледі, ол автоматты түрде электрондық сандық қолтаңба қол қойылған сіздің хатыңызбен бірге беріледі. Сіз кіммен қол қойылған құжаттарды алмасқыңыз келетініңіздің барлығында өз кілтіңіздің бар болуын қаматамасыз етуіңіз тиіс. Сіз сонымен қатар оның тіркеу куәлігін көріп, сіз алған құжаттың электрондық қолтаңбасымен қол қойған тұлға туралы көз жеткізесіз. Ашық кілттің телнұсқасы куәландырушы орталығына жолданады, онда электрондық сандық қолтаңба ашық кілтінің кітапханасы құрылған. Куәландырушы орталығының кітапханасында жасанды көшірмені жасаудан немесе бұрмалауды енгізуден қашуға ашық кілттердің тіркеуі мен сенімді сақталуы қамтамасыз етіледі.[[4]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-4)

**Пайдалану**

Қолтаңбаны пайдалану өте қарапайым. Ешқандай арнайы білім, дағдылар және икемділік бұл үшін талап етілмейді. Электрондық [құжаттарды](https://kk.wikipedia.org/wiki/%D2%9A%D2%B1%D0%B6%D0%B0%D1%82) алмасуға қатысушысы, электрондық сандық қолтаңба әрбір пайдаланушысына бірегей ашық және жабық (құпия) криптографикалық кілттер туындатады.[[5]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-5)

Негізгі элемент құпия кілт болып табылады, оның көмегімен электрондық құжаттардың шифрлеуі жасалады және электрондық сандық қолтаңба қалыптасады. Сонымен қатар құпия кілт пайдаланушыда қалады, оған бөлек тасығышта беріледі, бұл дискета, смарт-карта или touch memory болуы мүмкін. Оны басқадай пайдаланушылардың желісінен құпияда сақтау қажет.

*Электрондық сандық қолтаңба* түпнұсқасын тексеру үшін ашық кілт пайдаланылады. Куәландырушы орталығында ашық кілттің телнұсқасы тұр, ашық кілттердің тіркеу куәліктерінің кітапханасы құрылған. Куәландырушы орталық ашық кілттердің тіркеуін және бұрмалауды енгізуден немесе жасанды көшірмені жасаудан қашуға сенімді сақтауды қамтамасыз етеді.[[6]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-JPH2001-6)

Сіз электрондық құжатқа тиістіге өзіңіздің электрондық сандық қолтаңбаңызды орнатасыз. Бұл ретте электрондық сандық қолтаңба құпия кілтінің және ұсталатын құжаттың негізінде криптографиялық қайта жасау жолымен кейбір үлкен сан қалыптасады, ол осы нақты құжатқа тиісті осы пайдаланушының электрондық сандық қолтаңбасы болып табылады. Электрондық құжаттың аяғына осы сан қосылады немесе бөлек файлда сақталады.[[7]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-7)

[*Қолтаңбаға*](https://kk.wikipedia.org/wiki/%D2%9A%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0)*мынадай ақпарат жазылады:*

* Қолтаңба ашық кілті файлының аты.
* Қолтаңбаны қалыптастырған тұлға туралы ақпарат.
* Қолтаңбаның қалыптасқан күні.

Жөнелтуші құжатының мәтіні және ашық кілтінің негізінде жөнелтушінің электрондық сандық қолтаңба ашық кілтіне ие және қол қойылған құжатты алушы, жөнелтушінің электрондық сандық қолтаңбасының тексеруін қамтамасыз етуші, кері криптографиялық қайта жасауды орындайды. Егер электрондық сандық қолтаңба құжатқа тиістісі дұрыс болса, онда яғни бұл құжат шынында жөнелтушімен қол қойылған және құжаттың мәтініне ешқандай өзгертулер енгізілмеген. Әйтпесе жөнелтушінің сертификаты шынайы болып табылмайды деп хабарлама берілетін болады.[[8]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-lysythesis-8)

**Үнемдеу**

[[өңдеу](https://kk.wikipedia.org/w/index.php?title=%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0&veaction=edit&section=3) | [қайнарын өңдеу](https://kk.wikipedia.org/w/index.php?title=%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0&action=edit&section=3)]

*Электрондық*[*цифрлық*](https://kk.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80)*қолтаңба пайдалану рұқсат етеді:*

* [Құжаттарға](https://kk.wikipedia.org/wiki/%D2%9A%D2%B1%D0%B6%D0%B0%D1%82) заңды маңыздылықты берумен құжаттардың ақпарат алмасу құпиялығын арттыру есебінен қаржылық шығындардың тәуекелін азайту;
* Құжаттамалардың есебін беру және алмасу үрдісінде құжаттар қозғалысы уақытын айтарлықтай қысқарту;
* Электрондық саудада бір электрондық сандық қолтаңба пайдалану, мемлекеттік органдарға есептілікті тапсыру, қаржы құжаттарымен жұмыс жасау және бұрыштамалау мүмкіншілігі;
* Құжаттарды жеткізудің, есебін жүргізудің және сақтаудың даярлық рәсімдеуін жетілдіру және арзандату; құжаттаманың сенімділігіне кепіл болу;
* Кросс-сертификация туралы негізгі шетелдік куәлік жүйелерімен келісім. Халықаралық құжат айналымы үшін ресейлік электрондық сандық қолтаңба пайдалану мүмкіншілігін қамтамасыз ету;
* Электрондық сандық қолтаңба қағазсыз құжат айналымда дәстүрлі мөрді және қол қоюды ауыстыруға рұқсат етеді. Мөр немесе жазбаша қол қоюдың және қағаз парақтың арасында әдеттегі байланыспен бірге сандық қолтаңбаны құрған кезде электрондық құжат, құпия және ашық кілттердің арасында күрделі математикалық тәуелділік пайда болады.
* Құжат алмасудың корпоративтік жүйесін құру.[[9]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-rsa-9)

*Электрондық сандық қолтаңба* – уақыттың жаңа талаптарымен бірге кім қадам басуды қалағандардың барлығы үшін тиімді шешім. Егер алынған ақпараттың келісім қортындысын немесе түпнұсқалығын растауды тексеру үшін жүздеген шақырымнан фельдъегерлік немесе [шабармандық](https://kk.wikipedia.org/wiki/%D0%A8%D0%B0%D0%B1%D0%B0%D1%80%D0%BC%D0%B0%D0%BD) [поштаның](https://kk.wikipedia.org/wiki/%D0%9F%D0%BE%D1%88%D1%82%D0%B0) келуін күтуге [уақытыңыз](https://kk.wikipedia.org/wiki/%D0%A3%D0%B0%D2%9B%D1%8B%D1%82) болмаса. Электрондық сандық қолтаңба артықшылығы анық - электрондық сандық қолтаңбамен қол қойылған құжат, бірнеше секундта белгіленген жеріне берілуі мүмкін. Құжатты электрондық алмасудың барлық қатысушылары олардың бір бірінен қашықтығына байланысты емес тең мүмкіншілікті алады. Шек жаңа технологиялардың арқасында [21 ғасырда](https://kk.wikipedia.org/wiki/21_%D2%93%D0%B0%D1%81%D1%8B%D1%80) жойылады.[[10]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-10)

*Электрондық сандық қолтаңба жасанды көшіру мүмкін емес* – ол үшін есептеп шығарудың орасан санын талап етеді, ол қолайлы уақытта заманауи деңгейдегі есептеу техникасы мен математиканы іске асыру мүмкін емес, яғни қол қойылған құжатта ұсталатын әзірге ақпарат, өзектілікті сақтайды.

Жасанды көшірмеден қосымша қорғау қолтаңбаның ашық кілті куәландырушы орталығының сертификатымен қамтамасыз етіледі. Одан басқа клиенттің қалауы бойынша куәландырушы орталық клиенттің электрондық сандық қолтаңба сақтандыра алады.

Электрондық сандық қолтаңба пайдаланумен ойлау ауысады, "электрондық түрде жобаны әзірлеудің – қол қою үшін қағаз көшірмесін жасау – қол қойылуымен қағаз көшірмелерді жіберу - қағаз көшірмелерді қарау – оны электрондық түрде [компьютерге](https://kk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) көшіру" келмеске кетеді.[[11]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-11)

**Қолтаңба алу**

[[өңдеу](https://kk.wikipedia.org/w/index.php?title=%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0&veaction=edit&section=4) | [қайнарын өңдеу](https://kk.wikipedia.org/w/index.php?title=%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0&action=edit&section=4)]

Электрондық сандық қолтаңба алу үшін, ([Қазақстан Республикасы](https://kk.wikipedia.org/wiki/%D2%9A%D0%B0%D0%B7%D0%B0%D2%9B%D1%81%D1%82%D0%B0%D0%BD_%D0%A0%D0%B5%D1%81%D0%BF%D1%83%D0%B1%D0%BB%D0%B8%D0%BA%D0%B0%D1%81%D1%8B) бойынша) сіз жақын жердегі ҚР ҰҚО тіркеу орталығына өтініш білдіруге тиіссіз.

Заңды және жеке тұлғаларға тіркеу куәлігін алу үшін <http://www.knca.kz/> [Мұрағатталған](https://web.archive.org/web/20101226110947/http%3A/www.knca.kz/) 26 желтоқсанның 2010 жылы. : адрес бойынша қол жеткізілімді тұлғалардың түрлеріне сай үшін тіркеу куәлігін қолдану саясатында аталған құжаттарды беру, сондай-ақ электрондық сандық қолтаңба төлемі туралы (төлем үшін деректемелер) куәландыратын төлем тапсырмасын беру немесе электрондық сандық қолтаңба қолда бар қаражатпен төлеу қажет;

Электрондық сандық қолтаңба алу үшін, сіз барлық жоғарыда аталған құжаттарды ҚР ҰҚО тіркеу орталығына беруіңіз қажет.[[12]](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_note-12)

**Дереккөздер**

[[өңдеу](https://kk.wikipedia.org/w/index.php?title=%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0&veaction=edit&section=5) | [қайнарын өңдеу](https://kk.wikipedia.org/w/index.php?title=%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0&action=edit&section=5)]

1. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-1) [US ESIGN Act of 2000](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf)
2. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-2) [The University of Virginia](http://www.itc.virginia.edu/virginia.edu/fall00/digsigs/home.html) [Мұрағатталған](https://web.archive.org/web/20090302095310/http%3A/www.itc.virginia.edu/virginia.edu/fall00/digsigs/home.html) 2 наурыздың 2009 жылы.
3. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-3) [National Archives of Australia](http://www.naa.gov.au/recordkeeping/er/Security/6-glossary.html) [Мұрағатталған](https://web.archive.org/web/20060712004640/http%3A/www.naa.gov.au/recordkeeping/er/Security/6-glossary.html) 12 шілденің 2006 жылы.
4. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-4) [State of WI](http://enterprise.state.wi.us/home/strategic/esig.htm) [Мұрағатталған](https://web.archive.org/web/20060925104000/http%3A/enterprise.state.wi.us/home/strategic/esig.htm) 25 қыркүйектің 2006 жылы.
5. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-5) *Government of India* [The Information Technology Act, 2000](http://www.dot.gov.in/Acts/itbill2000.pdf).
6. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-JPH2001_6-0) A. Jøsang, D. Povey and A. Ho. "What You See is Not Always What You Sign". Proceedings of the Australian Unix User Group Symposium (AUUG2002), Melbourne, September 2002. [PDF](http://www.unik.no/people/josang/papers/JPH2002-AUUG.pdf)(қолжетпейтін сілтеме)
7. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-7) "New Directions in Cryptography", IEEE Transactions on Information Theory, IT-22(6):644–654, Nov. 1976.
8. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-lysythesis_8-0) "[Signature Schemes and Applications to Cryptographic Protocol Design](http://theory.lcs.mit.edu/~cis/theses/anna-phd.pdf) [Мұрағатталған](https://web.archive.org/web/20070629113255/http%3A/theory.lcs.mit.edu/~cis/theses/anna-phd.pdf) 29 маусымның 2007 жылы.", Anna Lysyanskaya, PhD thesis, [MIT](https://kk.wikipedia.org/w/index.php?title=Massachusetts_Institute_of_Technology&action=edit&redlink=1), 2002.
9. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-rsa_9-0) Rivest, R.; A. Shamir; L. Adleman (1978). ["A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"](http://theory.lcs.mit.edu/~rivest/rsapaper.pdf). *Communications of the ACM* **21** (2): 120–126. [doi](https://kk.wikipedia.org/w/index.php?title=Digital_object_identifier&action=edit&redlink=1):[10.1145/359340.359342](https://doi.org/10.1145/359340.359342). [ISSN](https://kk.wikipedia.org/w/index.php?title=International_Standard_Serial_Number&action=edit&redlink=1) [0001-0782](http://www.worldcat.org/issn/0001-0782).
10. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-10) "A certified digital signature", Ralph Merkle, In Gilles Brassard, ed., Advances in Cryptology – [CRYPTO](https://kk.wikipedia.org/w/index.php?title=CRYPTO&action=edit&redlink=1) '89, vol. 435 of Lecture Notes in Computer Science, pp. 218–238, Spring Verlag, 1990.
11. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-11) "Modern Cryptography: Theory & Practice", Wenbo Mao, Prentice Hall Professional Technical Reference, New Jersey, 2004, pg. 308. [ISBN 0-13-066943-1](https://kk.wikipedia.org/wiki/%D0%90%D1%80%D0%BD%D0%B0%D0%B9%D1%8B%3A%D0%9A%D1%96%D1%82%D0%B0%D0%BF_%D2%9B%D0%B0%D0%B9%D0%BD%D0%B0%D1%80%D0%BB%D0%B0%D1%80%D1%8B/0130669431)
12. [↑](https://kk.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%B4%D1%8B%D2%9B_%D1%81%D0%B0%D0%BD%D0%B4%D1%8B%D2%9B_%D2%9B%D0%BE%D0%BB%D1%82%D0%B0%D2%A3%D0%B1%D0%B0#cite_ref-12) Ұлттық куәладырушы орталығы, <http://www.pki.gov.kz/cms?host=kz-ekey&path=/ekey/about> [Мұрағатталған](https://web.archive.org/web/20111023020725/http%3A/www.pki.gov.kz/cms?host=kz-ekey&path=%2Fekey%2Fabout) 23 қазанның 2011 жылы.